

業務用電子計算機システム用機器借上げ

及び運用支援業務

民間競争入札実施要項（案）

令和 7 年

目次

1. 趣旨	1
2. 本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質に関する事項	1
3. 実施期間に関する事項	4
4. 入札参加資格に関する事項	4
5. 入札に参加する者の募集に関する事項	5
6. 本業務を実施する者を決定するための評価の基準その他本業務を実施する者の決定に関する事項	7
7. 本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	9
8. 本業務の請負者に使用させることができる財産に関する事項	10
9. 本業務請負者が、当センター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本業務の適正かつ確実な実施の確保のために本業務請負者が講じるべき措置に関する事項	10
10. 本業務請負者が本業務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本業務請負者が負うべき責任に関する事項	15
11. 本業務に係る法第7条第8項に規定する評価に関する事項	15
12. その他業務の実施に関し必要な事項	16
13. その他業務の実施に関し必要な事項	17

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斷の見直しを行い、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、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、独立行政法人大学入試センター（以下「当センター」という。）は「公共サービス改革基本方針」（平成 25 年 6 月 14 日閣議決定）別表において民間競争入札の対象として選定された「業務用電子計算機システム用機器借上げ及び運用支援業務」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とする。

2. 本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質に関する事項

（1）業務の概要

ア 業務の経緯等

当センターは、大学に入学を志願する者に対し大学が共同して実施する試験に関する業務等を行うことにより、大学の入学者の選抜の改善を図り、もって大学及び高等学校（中等教育学校の後期課程及び特別支援学校の高等部を含む。）における教育の振興に資することを目的として業務を行っている。

現在の業務用計算機システムは、2021 年（令和 3 年）8 月に導入されたものであり、当センターの教職員が業務を遂行するための端末利用システム、グループウェア・ファイル等各種サーバ群とこれらのシステムを統合するネットワークシステムから構成されている。

現在の業務用電算機システムが、令和 8 年 7 月末に契約を終了することに伴い、令和 8 年 8 月に更新する必要がある。

なお、業務用電算機システムの更新に当たっては、当センターの業務運営がより一層効率化されるように、可用性、利便性、信頼性に優れたシステムであること、かつ、経費削減の観点からコストパフォーマンスの高いシステムであることに配慮する必要がある。

イ システムの概要

システムの概要是別添 1「業務用電子計算機システム用機器借上げ及び運用支援業務要求仕様書」のとおり。

ウ 業務内容

別添 1「業務用電子計算機システム用機器借上げ及び運用支援業務要求仕様書」に基づき、以下の業務を行う。

（a） サーバ等機器の賃貸借及びソフトウェアの調達（ライセンス契約）を、リ

ース契約を代行して行うこと。なお、提案する機器及びソフトウェアは、入札時点で原則として製品化されていること。入札時点で製品化されていない機器またはソフトウェアにより応札する場合には、要件を満たすこと及び納入期限までに製品化され納入できることを証明できる書類を添付すること。

- (b) サーバ等機器の設置を行うこと。なお、搬入、据付、配線、調整、既設設備との接続に要するすべての費用は本調達に含まれる。
- (c) O S やソフトウェアのインストール、設定、動作確認を行うこと。
- (d) 導入した業務システムの運用上必要な運用手引書（マニュアル）を作成すること。
- (e) サーバ等機器及びソフトウェアの保守を行うこと。
- (f) 現行のシステムからデータ等を移行すること。
- (g) 設定情報、マニュアル等の成果物を納品すること。
- (h) 契約終了後に機器を撤去すること。

なお、本調達は、日常のバックアップ運用やヘルプデスク対応は行わず、運用管理業者（ヘルプデスク）を支援するものである。

エ 請負業務の引継ぎ

- (a) 現行請負者又は当センターからの引継ぎ

当センターは、当該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措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務を新たに実施することとなった請負者は、本業務の開始日までに、業務内容を明らかにした書類等により、現行請負者（又は当センター）から業務の引継ぎを受けるものとする。なお、その際の事務引継ぎに必要となる経費は、当センターの負担とする。

- (b) 請負期間満了の際、業者変更が生じた場合の引継ぎ

当センターは、当該引継ぎが円滑に実施されるよう、請負者及び次回請負者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

本業務の終了に伴い請負者が変更となる場合には、請負者は、当該業務の開始日までに、業務内容を明らかにした書類等により、次回請負者に対し、引継ぎを行うものとする。なお、その際の事務引継ぎに必要となる経費は、請負者の負担となる。

(2) 確保されるべき対象業務の質

ア 業務内容

2(1)ウ「業務内容」に示す業務を適切に実施すること。

イ システム障害への対応。

- (a) 本システムにおいて障害が発生した場合は、原因の特定、解決策の検討、復旧作業の実施等の措置を迅速かつ的確に行うこと。
- (b) サーバ及びネットワーク機器等システムの基幹部分に障害が発生したときは、当センター又は運用管理事業者からの連絡を受けてから4時間以内に状況の確認、原因の調査を開始すること。
- (c) 障害状況の確認後4時間以内に解決できるように努めること。
- (d) 障害発生の原因を解明し、当センターと協議の上、再発防止策を講じること。

ウ セキュリティ上の重大障害件数

個人情報、組織・施設等に関する情報その他の契約履行に際し、知り得た情報の漏洩件数は0件であること。

エ システム運用上の重大障害件数

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。

(3) 創意工夫の発揮可能性

本業務を実施するに当たっては、請負者の創意工夫を反映し、サービスの質の向上（包括的な質の向上、効率化の向上、経費の削減等）に努めるものとする。

この場合請負者は、事業内容に対し、改善すべき提案（コスト削減に係る提案を含む）がある場合は、別途定める様式に従い、具体的な方法等を示すとともに、従来の実施状況と同等以上の質が確保できる根拠等を提案すること。

(4) 契約の形態及び支払

ア 契約の形態は、業務請負契約とする。

イ 当センターは、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、契約の履行に関し、別添1「業務用電子計算機システム用機器借上げ及び運用支援業務の要求仕様書」に定めた内容に基づく監督・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、適正な支払請求書を受領した日から40日以内に、毎月、契約金額を支払うものとする。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、又は達成

できないおそれがある場合、当センターは、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、業務改善報告書を速やかに当センターに提出するものとする。

業務改善報告の提出から 1 か月の範囲で、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、当センターは、請負費の支払を行わないことができる。なお、請負費は、本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。

ウ 法令変更による増加費用及び損害の負担

法令の変更により事業者に生じた合理的な増加費用及び損害は、(a)から(c)に該当する場合には当センターが負担し、それ以外の法令変更については請負者が負担する。

- (a) 本業務に類型的又は特別に影響を及ぼす法令変更及び税制度の新設
- (b) 消費税その他類似の税制度の新設・変更（税率の変更含む）
- (c) 上記(a)及び(b)のほか、法人税その他類似の税制度の新設・変更以外の税制度の新設・変更（税率の変更含む）

3. 実施期間に関する事項

(1) 設計・開発業務

契約締結日から 2026 年（令和 8 年）7 月 31 日まで。

(2) 保守・運用業務

2026 年（令和 8 年）8 月 1 日から 2031 年（令和 13 年）7 月 31 日まで。

	令和 7 年度			令和 8 年度			令和 9 年度	令和 10 年度	令和 11 年度	令和 12 年度	令和 13 年度		
	4-6	7-9	10-12	1-3	4	5	6	7	8	9	10	11	12
業務用電子計算機システム用機器借上げ及び運用支援業務	調達	構築・移行											

構築・移行に関する各工程のスケジュールは協議の上決定する。必要に応じて他業者と連携（※）して実施すること。なお、他業者との連絡調整は当センターが行う。（※現行システムに関する情報提供、別調達機器との接続試験等）

4. 入札参加資格に関する事項

- (1) 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。

- (2) 大学入試センター契約事務取扱規則第6条第1項に基づき、令和7年度文部科学省競争参加資格（全省庁統一資格）「役務の提供等」A、B又はC等級に格付された関東・甲信越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」に登録している者であること。）。又は、独立行政法人大学入試センター契約事務取扱規則第6条第2項の規定に基づき、契約担当役により資格を有する者として認められた者であること。
- (3) 適切な品質管理体制を保証するものとして ISO9001 の認証を取得していること。環境負荷軽減への取り組みを組織的に行っていることの証明として ISO14001 を取得していること。また、情報セキュリティについて、ISO27001 の認証あるいは、プライバシーマークを取得していること。
- (4) 法人税並びに消費税及び地方消費税の滞納がないこと。
- (5) 労働保険、厚生年金保険等の適用を受けている場合、保険料等の滞納がないこと。
- (6) 文部科学省及び他府省等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。
- (7) 要求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。
- (8) 大学入試センター情報化統括責任者（CIO）補佐官及びその支援スタッフ業務について、CIO補佐官等が現に所属する又は過去2年間に属していた事業者及びその関連事業者ではないこと。
- (9) 単独で対象業務を行えない場合、又は、単独で実施するより業務上の優位性があると判断する場合は、適正に業務を実施できる入札参加グループを結成し、入札に参加することができる。その場合、入札書類提出時までに入札参加グループを結成し、入札参加資格の全てを満たす者の中から代表者を定め、他の者は構成員として参加するものとする。また、入札参加グループの構成員は、上記(1)から(7)までの資格を満たす必要があり、他の入札参加グループの構成員となり、又は、単独で参加することはできない。なお、入札参加グループの代表者及び構成員は、入札参加グループ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。
- 注) 「入札参加グループ」とは、本業務の実施を目的に複数の事業者が組織体を構成し、本業務の入札に参加する者のことを指す。

5. 入札に参加する者の募集に関する事項

- (1) スケジュール（予定であり変更する場合がある）
- | | |
|--------------|------------|
| 入札公告：官報公告 | 令和7年7月中旬 |
| 入札説明会 | 8月上旬 |
| 質問受付期限 | 8月下旬 |
| 入札書及び提案書提出期限 | 9月下旬 |
| 提案書の審査 | 9月下旬～10月上旬 |
| 開札及び落札予定者の決定 | 10月上旬 |
| 契約締結 | 11月中旬 |

(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 入札説明会後の質問書

入札公告以降、当センターにおいて入札説明書の交付を受けた者は、本実施要項の内容や入札に係る事項について、入札説明会後に、当センターに対して質問を行うことができる。質問は原則として電子メールにより行い質問内容及び当センターからの回答は原則として入札説明書の交付を受けたすべての者に公開することとする。ただし、民間事業者の権利や競争上の地位等を害するおそれがあると判断される場合には、質問者の意向を聴取した上で公開しないよう配慮する。

イ 提案書等

別添1「業務用電子計算機システム用機器借上げ及び運用支援業務要求仕様書」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。

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110分の100に相当する金額）を記載した書類。

※消費税率については、入札時の税率に応じて適宜修正する。また、入札参加者ごとに税率の想定が異なることを避けるため、具体的に明示すること。

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

令和7年度文部科学省競争参加資格（全省庁統一資格）「役務の提供等」A、B又はC等級に格付けされた関東・甲信越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」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。

- カ 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（落札予定者となった者のみ提出。）
- キ 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）
- ク 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7月5日政令第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
- ケ 入札参加グループによる参加の場合は、入札参加グループ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
- コ 取引停止等に関する申出書
各府省庁から取引停止を受けていないことを確認する書類。
- サ 誓約書
本請負を完了できることを証明する書類。

6. 本業務を実施する者を決定するための評価の基準その他本業務を実施する者の決定に関する事項

以下に本業務を実施する者の決定に関する事項を示す

(1) 評価方法

本業務を実施する者の決定は、総合評価落札方式によるものとする。なお、技術の評価に当たっては、当センターが任命する技術審査職員が行う。

また、総合評価は、価格点（入札価格の得点）に技術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。

価格点と技術点の配分は1：1とする。

(2) 決定方法

当センターが別途示す評価項目において必須と定められた要求要件を全て満たしている場合に「合格」とし、1つでも欠ける場合は「不合格」とする。

(3) 総合評価点

ア 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。

イ 技術点の評価は以下のとおりとする。

(a) 全ての仕様を満たし、「合格」したものに所定の「基礎点」を与える。

(b) 「合格」した提案書について、技術審査職員ごとに加点の評価を行う。

なお、加点の評価は、以下の評価基準に基づき点数化する。確定した各

技術審査職員の採点結果について、その平均値を算出し「加点」とする。

① 評価基準

評価	評価基準
○	提案内容が優れている。
△	提案内容が標準的である。
×	要件は満たしているが、加点すべき要素がない。

② 配点表

評価	最大加点				
	10 点	20 点	30 点	40 点	50 点
○	10	20	30	40	50
△	5	10	15	20	25
×	0	0	0	0	0

(c) 「基礎点」と「加点」の合計点を「技術点」とする。

(4) 落札者の決定

ア 別添1「業務用電子計算機システム用機器借上げ及び運用支援業務要求仕様書」に示す全ての要求要件を満たし、かつ、入札者の入札価格が予定価格の制限の範囲内であり、かつ、「総合評価落札方法」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、落札者となるべき者の入札価格によっては、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は、予定価格の範囲内で申込みをした他の者のうち、次順位の者を落札者とすることがある。

イ 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。

ウ 契約担当役は、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。

(5) 落札決定の取り消し

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、契約担当役が、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、契約担当役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。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ため、内訳金額の補正を求められた入札者は、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。

(6) 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は、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監理委員会（以下、「監理委員会」という。）に報告するとともに公表するものとする。

7. 本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

以下に本業務を実施する者の決定に関する事項を示す

(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

(2) 資料の閲覧

前項オ「従来の実施方法等」の詳細な情報は、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、所定の手続を踏ました上で閲覧可能とする。

また、民間競争入札に参加する予定の者から追加の資料（本業務の引継ぎや他業者との連携に必要な、現行システムの設定等及び現行請負者が保有する情報等を含む。）の開示について要望があった場合は、当センターは当センター規程等、法令及び機密性等に問題のない範囲で適切に対応するよう努めるものとする。

8. 本業務の請負者に使用させることができる財産に関する事項

(1) 当センター財産の使用

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、当センター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、本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、あらかじめ当センターと協議した上で、当センター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. 本業務請負者が、当センター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本業務の適正かつ確実な実施の確保のために本業務請負者が講じるべき措置に関する事項

(1) 本業務請負者が当センターに報告すべき事項、当センターの指示により講じるべき措置

ア 報告等

(a) 請負者は、別添1「業務用電子計算機システム用機器借上げ及び運用支援業務要求仕様書」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センターに提出しなければならない。

(b) 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、直ちに当センターに報告するものとし、当センターと請負者が協議するものとする。

(c) 請負者は、契約期間中において、(b)以外であっても、必要に応じて当センター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

(a) 当センターは、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 項に基づき、請負者に対し必要な報告を求め、又は当センター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。

- (b) 立入検査をする当センターの職員は、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

当センターは、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に必要な措置

ア 請負者は、本業務の実施に際して知り得た当センターの情報等（公知の事実等を除く）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センター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、当センター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）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、当センターの保有個人情報の適切な管理のための措置に関する規則（平成 17 年規則第 2 号）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に関して遵守しなければならない。

オ アからエまでのほか、当センターは、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じるべき措置

ア 請負業務開始

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、書面による当センターの事前の承認を得たときはこの限りではない。

ウ 権利義務の帰属等

- (a) 本業務の実施が第三者の特許権、著作権その他の権利と抵触するときは、請負者は、その責任において、必要な措置を講じなくてはならない。
- (b) 請負者は、本業務の実施状況を公表しようとするときは、あらかじめ、当センターの承認を受けなければならない。

エ 契約不適合責任

- (a) 当センターは、成果物が契約の内容に適合しないもの（以下「契約不適合」という。）であるときは、請負者に対し、履行の追完を請求することができるものとし、履行の追完に必要な費用は、全て請負者の負担とする。
- (b) 前項の契約不適合の場合において、当センターがその不適合を知った日から1年以内にその旨を請負者に通知しないときは、当センターは、その不適合を理由として、履行の追完の請求、請負代金の減額の請求、損害賠償の請求及び契約の解除をすることができないものとする。
- (c) 契約不適合が請負者の責に帰すべき事由によるものである場合は、当センターは、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。

オ 再委託

- (a) 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。
- (b) 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、あらかじめ書面において、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。
- (c) 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、当センターの承認を受けなければならない。
- (d) 請負者は、(b)又は(c)により再委託を行う場合には、請負者が当センター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。

(e) (b)から(d)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。

カ 契約内容の変更

当センター及び請負者は、本業務の質の確保の推進、またはその他やむをえない事由により本契約の内容を変更しようとする場合は、あらかじめ変更の理由を提出し、それぞれの相手方の承認を受けるとともに法第 21 条の規定に基づく手続を適切に行わなければならない。

キ 機器更新等の際における民間事業者への措置

当センターは、次のいずれかに該当するときは、請負者にその旨を通知するとともに、請負者と協議の上、契約を変更することができる。

- (a) ハードウェアの更新、撤去又は新設、サポート期限が切れるソフトウェアの更新等に伴い運用管理対象機器の一部に変更が生じるとき
- (b) セキュリティ対策の強化等により業務内容に変更が生じるとき
- (c) 当センターの組織変更や人員増減に伴うシステム利用者数の変動等により業務量に変動が生じるとき

ク 契約の解除

当センターは、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、請負者は当センターに対して、契約金額から消費税及び地方消費税を差し引いた金額の 100 分の 10 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、当センター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、当センターとの協議に基づき、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。

- (a) 法第 22 条第 1 項イからチまで又は同項第 2 号に該当するとき。
- (b) 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。
- (c) 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。
- (d) 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。
- (e) 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。

ケ 談合等不正行為

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

コ 損害賠償

請負者は、請負者の故意又は過失により当センターに損害を与えたときは、当センターに対し、その損害について賠償する責任を負う。また、当センターは、契約の解除及び違約金の徴収をしてもなお損害賠償の請求をすることができる。なお、当センターから請負者に損害賠償を請求する場合において、原因を同じくする支払済の違約金がある場合には、当該違約金は原因を同じくする損害賠償について、支払済額とみなす。

サ 不可抗力免責・危険負担

当センター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、当センター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。

シ 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。

ス 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は、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。

セ 法令の遵守

請負者は、本業務を実施するに当たり適用を受ける関係法令等を遵守しなくてはならない。

ソ 安全衛生

請負者は、本業務に従事する者の労働安全衛生に関する労務管理については、責任者を定め、関係法令に従って行わなければならない。

タ 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、本業務を終了した日又は中止した日の属する年度の翌年度から起算して5年間、保管しなければならない。

チ 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、当センターと請負者との間で協議して解決する。

10. 本業務請負者が本業務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本業務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) 当センターが当該第三者に対する賠償を行ったときは、当センターは請負者に対し、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センターの責めに帰すべき理由が存する場合は、当センターが自ら賠償の責めに任す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センターの責めに帰すべき理由が存するときは、請負者は当センターに対し、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すべき金額を超える部分を求償することができる。

11. 本業務に係る法第 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

当センターは、本業務の実施状況について、総務大臣が行う評価の時期（令和 11 年 7 月を予定）を踏まえ、本業務開始後、毎年 11 月に状況を調査する。

- (2) 調査項目及び実施方法

ア 業務の質

納品物（報告書等）により調査

イ システムの障害発生件数及び時間

保守作業報告書等により調査

ウ セキュリティ上の重大障害の件数

保守作業報告書等により調査

エ システム運用上の重大障害件数

保守作業報告書等により調査

- (3) 意見聴取等

当センターは、必要に応じ、本業務請負者から意見の聴取を行うことができるものとする。

- (4) 実施状況等の提出時期

当センターは、令和 11 年 7 月を目指として、本業務の実施状況等を総務大臣及び監理委員会へ提出する。

なお、調査報告を総務大臣及び監理委員会に提出するに当たり、監事の意見を

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監理委員会への報告

当センターは、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) 監督体制

ア 運用管理業務全体に係る監督は、当センターの事業部事業第三課が行い、事業部事業第三課長を責任者とする。

イ 実施要項に基づく民間競争入札に係る監督は、当センターの総務部財務課が行い、総務部財務課長を責任者とする。

(3) 本業務請負者の責務

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 54 条の規定に該当する場合は、1 年以下の懲役又は 50 万円以下の罰金に処される。

ウ 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 条により、法人の代表者又は法人もしくは人の代理人、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。

エ 請負者は、会計検査院法（昭和 22 年法律第 73 号）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センターを通じて、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センター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、当センターが承認した場合は、この限りではない。

ウ ア及びイに関わらず、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。

(5) 本業務の要求仕様書

本業務を実施する際に必要な仕様は、別添 1「業務用電子計算機システム用機器借上げ及び運用支援業務要求仕様書」に示すとおりである。

13. その他業務の実施に関し必要な事項

民間競争入札実施要項（本紙）

別紙 1 従来の実施状況に関する情報の開示

別紙 2 保守・運用支援概念図

別紙 3 組織図

別添 1 業務用電子計算機システム用機器借上げ及び運用支援業務要求仕様書

別添 2 業務用電子計算機システム用機器借上げ及び運用支援業務要件定義書

別添 3 業務用電子計算機システム用機器借上げ及び運用支援業務総合評価基準書

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)

		令和3年	令和4年	令和5年	令和6年
人件費	常勤職員	—	—	—	—
	非常勤職員	—	—	—	—
物件費		—	—	—	—
請負費等	役務	1,920	2,880	2,880	2,880
	機器・回線等料	116,880	116,880	116,880	116,880
	その他				
計(a)		118,800	119,760	119,760	119,760
参考値	減価償却費	—	—	—	—
	退職給付費用	—	—	—	—
	(b) 間接部門費	—	—	—	—
(a)+(b)		118,800	119,760	119,760	119,760

(注記事項)

大学入試センターでは、民間競争入札の対象である業務用電子計算機システム用機器借上げ及び運用支援業務業務の全部を請負契約により実施している。

なお、支払い金額は、一般競争入札の落札額である。

2 従来の実施に要した人員

(単位:人)

	令和3年	令和4年	令和5年	令和6年
(受託者におけるシステム運用業務従事者)				
管理者(非常駐)	0	0	0	0
担当者(常駐)	0	0	0	0

(業務従事者に求められる知識・経験等)

管理者

知識・経験等は問わない。(本調達には含まない)

担当者

知識・経験等は問わない。(本調達には含まない)

(注意事項)

保守・運用業務従事者は非常駐であるが、年一回、大学入試センターにおける全館停電日に併せてサーバ等のメンテナンス作業を行っている。

また、大学入学共通テスト実施日及びその後2週間程度については、特に繁忙となる機関であるので、障害発生時に直ちに対応できる体制を整えている。

(令和3年度)

(件)

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
問い合わせ 受付件数					6	1	2	7	10	3	4	3	36
障害/不都合の 受付件数					2	2	5	3	3	1	2	6	24

(令和4年度)

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
問い合わせ 受付件数	6	4	3	4	1	4	8	8	6	2	5	8	59
障害/不都合の 受付件数	0	1	1	2	0	0	0	1	3	1	0	1	10

(令和5年度)

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
問い合わせ 受付件数	5	17	22	14	3	4	3	2	4	13	3	2	92
障害/不都合の 受付件数	1	3	5	1	1	3	2	1	1	4	2	1	25

(令和6年度)

	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
問い合わせ 受付件数	3	8	6	4	2	3	9	6	5	6			52
障害/不都合の 受付件数	1	2	2	1	2	4	1	1	1	4			19

3 従来の実施に要した施設及び設備

【施設】

施設名称:独立行政法人 大学入試センター 2階サーバー室

【設備】

本業務に必要な什器備品(事務用机・椅子、棚、PC、電話)を設置

外部拠点
なし

4 従来の実施における目的の達成の程度

本業務は、大学入試センター試験関連業務を確実に実施するため、安全かつ円滑に適用し、安定的かつ効果的で確実な動作を行うことを目的としている。

- ①システムの停止回数及び時間
事例は発生していない。
- ②セキュリティ上の重大障害件数
事例は発生していない。
- ③システム運用上の重大障害件数
事例は発生していない。

5 従来の実施方法等

従来の実施方法(業務フロー図等)

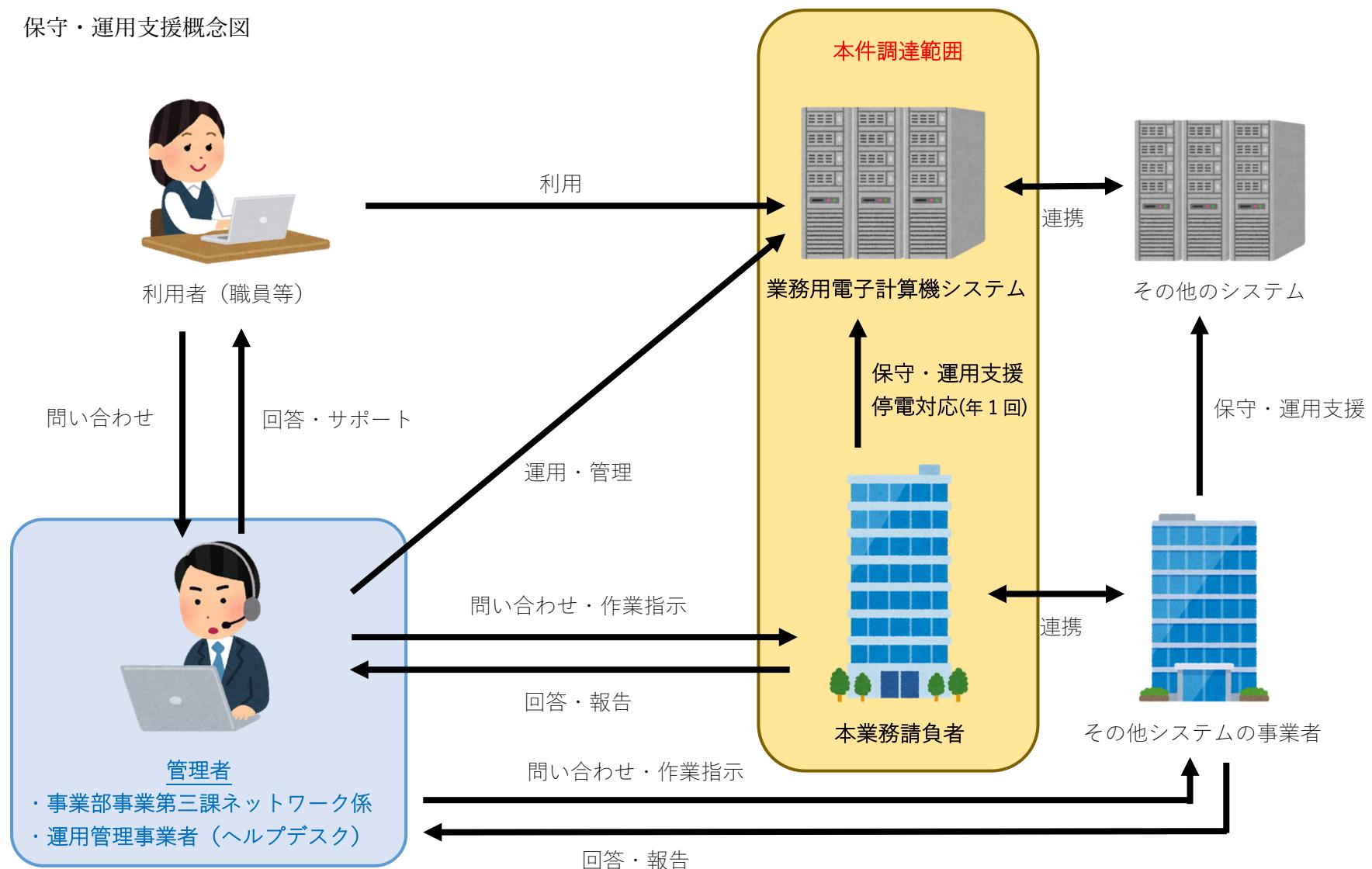
別紙2 保守・運用支援概念図のとおり。

別紙3 センター組織図のとおり。

(注記事項)

大学入試センター試験の受験特別措置の申請作業を開始する8月から翌年3月までの対応は、本センターと協議の上、その指示に従うこと。この期間においては土日祝日の対応が必要となる場合が多くある。(例年10日程度)

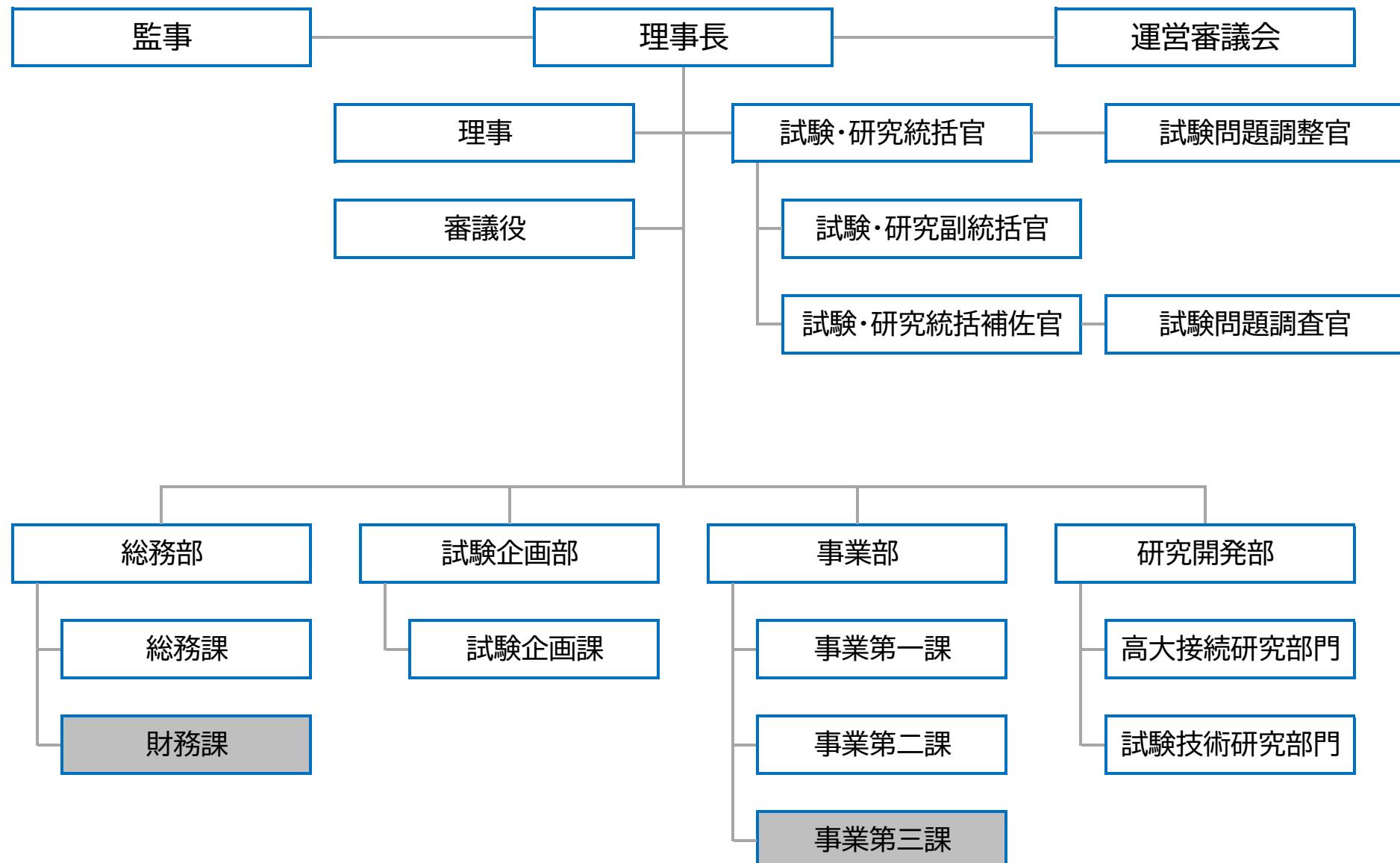
保守・運用支援概念図



組織図

別紙 3

(網掛けは本業務の実施に関連する部署)



業務用電子計算機システム用機器借上げ
及び運用支援業務
要求仕様書(案)

令和7年
独立行政法人 大学入試センター

目次

第 1 章 概要	1
1.1. 調達案件名	1
1.2. 調達の背景及び目的	1
1.3. システムの内容	1
1.3.1. 概要	1
1.3.2. システム要件	3
1.3.3. 構築作業日程	3
第 2 章 調達に関する事項	3
2.1. 本調達の内容、範囲及び成果物	3
2.1.1. 調達内容	3
2.1.2. 調達範囲	3
2.1.3. 納入、履行期間	4
2.1.4. 成果物	5
2.2. 搬入・設置及び履行期間終了後の引き上げ	6
2.2.1. 搬入・設置	6
2.2.2. 履行期間終了後の引き上げ	6
2.3. その他留意事項	6
第 3 章 役務作業要件	7
3.1. 作業前提	7
3.2. 作業体制	8
3.3. 機器の搬入・設置等	8
3.4. 設計・構築	9
3.5. 運用・保守	10
3.5.1. SLA に関する提供事項	10
3.5.2. 実施に関する提供事項	11
第 4 章 契約条件等	11
4.1. 秘密保持	11
4.2. 情報セキュリティの確保	12
4.3. 契約不適合責任	14
4.4. 賠償・復旧	14
4.5. 個人情報保護法に関する事項	15
4.6. 第三者への請負、著作権等	15
第 5 章 提案書記載要項	17
5.1. 概要	17
5.2. 記載に際しての基本要件	17
5.3. 提案必須項目	18
5.4. 提案書作成要領	18
5.5. 留意事項	19
第 6 章 提出物	19

第7章 その他特記事項.....	19
7.1. 応札者としての条件	19
7.2. 受注者間の協議.....	20
7.3. 政府・省庁規定及び各種ガイドラインへの準拠	20
7.4. 政府・省庁規定及び各種ガイドラインの動向への留意.....	21
7.5. 法律・規格への準拠	21
7.6. 閲覧・提供資料	21
7.7. 技術仕様等に関する留意事項.....	22
7.8. 提案に関する留意事項.....	22
7.9. その他の留意事項	23

第1章 概要

1.1. 調達案件名

業務用電子計算機システム用機器借上げ及び運用支援業務

1.2. 調達の背景及び目的

大学入試センターでの業務用電子計算機システム(以下「本システム」という)は、大学入試センターの主な業務連絡手段となっている電子メールや、事務文書などのファイル共有の機能を有した事務処理系のネットワークシステムであるとともに、各種業務システムの安定稼働を支える業務基盤となるネットワークシステムとしての役割を担っている。

大学入試センターでは、志願者情報や試験実施に関する機密性の高い情報を多数保有しているため、昨今の公的機関などに対する「標的型攻撃」などに備えた対策として、本システムをインターネットなどの外部通信が可能なアクセス環境(OPEN 環境)と外部通信が不可能でセキュアなアクセス環境(CLOSED 環境)の 2 つの環境を用意し、業務で取り扱う情報の機密性に応じて、各々のネットワークを使い分けるなどして、情報セキュリティを更に強化している。

現有の本システムは、令和3年8月に更新したものであり、令和8年7月末に契約が終了することに伴い、令和8年8月に更新する必要がある。

なお、本システムの更新に当たっては、大学入試センターの業務運用がより一層効率化されるように、可用性、利便性、信頼性に優れたシステムであり、経費削減の観点からコストパフォーマンスの高いシステムとともに、情報セキュリティを強化した柔軟かつ堅牢な基盤システムの構築を目的に行うものである。

1.3. システムの内容

1.3.1. 概要

本システムは、主として大学入試センター内の利用者に向けてサービスを提供するものであり、メール・グループウェア機能及びファイル共有システム等のサービスを提供している。およそ 220 台のクライアント端末が稼働しており、職員数(ユーザ数)は 180 名程度である。

ネットワークとしては、不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを分離し、さらに業務目的、所属部局等に応じて内部のネットワークを分離している。

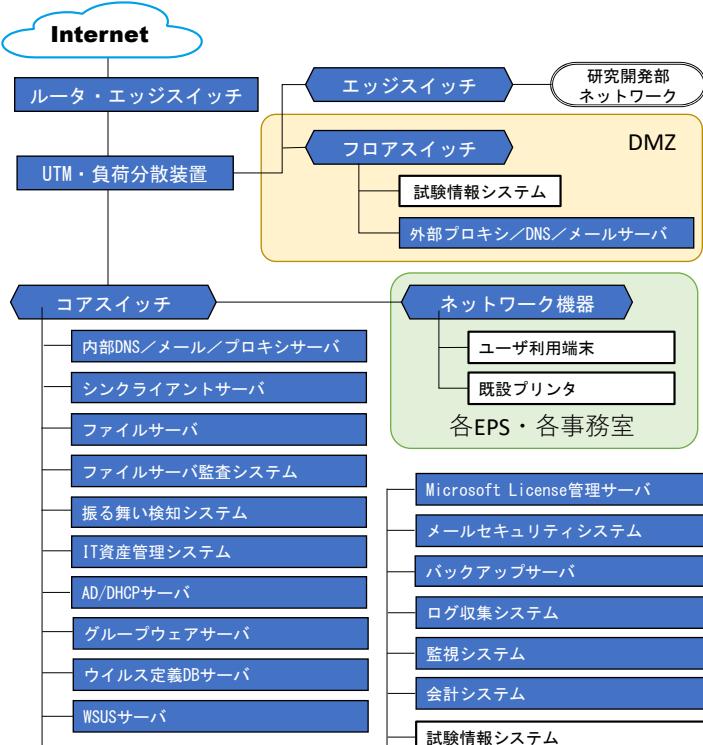
(1) システムの基本構成

(ア) 次期システムの基本構成はオンプレミスで構築しつつ、OPEN 環境とそこで使用するサービスについては受注者の判断により、大学入試センターと協

議の上、で、クラウドサービスを利用して構築することも可能とする。

- (イ) サーバ、ストレージ及びネットワーク等のハードウェア機器は、仮想化が適さないものを除き、仮想化技術を用いて集約すること。
- (ウ) ハードウェアリソース(CPU、メモリ、ディスク容量、ネットワーク回線等)及びシステムリソース等を可視化し容易に再分配することに加えて、一元的に管理することでリソース配分の最適化、システム運用業務の負荷軽減、増築等に伴う設定変更の簡素化を図る。
- (エ) 障害時における業務継続性を向上させるため、物理障害のポイントを削減し、各サービスの特性を踏まえた冗長化構成、バックアップ体制を講じる。
- (オ) ハードウェアリソース逼迫時、障害時、災害時における各サービスの業務継続性の向上のため、論理構成及び物理構成を実装する。
- (カ) 昨今及び将来のサイバー攻撃に対応すべく、より強固なセキュリティ対策として、ゼロデイ脆弱性(せいじやくせい)や既知及び未知の脅威に対しても常に最速、かつ、確実な検知・遮断、対応等を実現するために、最新の技術を適用した振る舞い検知、ログ分析、監視等を導入し、侵入防止及び侵入後における適切な対策によるセキュアな環境を構築する。
- (キ) 職員は、次期システムを利用するに当たり、利便性とセキュリティ性に優れたシンクライアント端末を利用する。
- (ケ) 無線 LAN 環境においては IEEE802.1x 認証を導入し、セキュリティを確保する。

(2) システムの概要図



※ 青地白抜き文字の部分が調達範囲。

※ この他、今回の調達に含まれないシステムもネットワーク上に存在する。

1.3.2. システム要件

各サービスの機能及びシステム要件については別添2「業務用電子計算機システム用機器借上げ及び運用支援業務要件定義書」を参照

1.3.3. 構築作業日程

受注者は、契約締結後速やかに大学入試センターと打ち合わせの上、計画する。計画後、速やかに以下の書類を提出すること。

- (1) プロジェクト計画書
- (2) システム構築作業スケジュール表(WBS)
- (3) システム構築作業体制表(国籍、資格、役割分担)
- (4) 連絡先一覧
- (5) その他大学入試センターから依頼のあった書類

次期システムの稼働は計画した作業スケジュールに沿って遅延なくサービスを提供すること。

第2章 調達に関する事項

2.1. 本調達の内容、範囲及び成果物

2.1.1. 調達内容

本調達においては、以下のサービスを提供する。

- (1) システム及びネットワークに関する提供サービス

別添2「業務用電子計算機システム用機器借上げ及び運用支援業務要件定義書」に記載するシステム及びネットワーク

- (2) 作業に関する提供サービス

次期システムのライフサイクルに係る作業等提供一式(次期システムの設計、構築、導入、運用支援、保守、物品の納入、現行システムからの移行に関する作業等)

2.1.2. 調達範囲

本システム用機器の賃貸借(クラウドサービスを利用する場合にはその利用料も含む)、設計、構築、現行システムから次期システムへの移行、動作検証、教育、研修、各種調整及び保守等、受注者が実施する全ての事項に適用する。

これには、既設のネットワーク環境下にあるサーバ等と論理的に接続し、それらに対応する動作検証、教育、研修、各種調整及び大学入試センター電算機室内に設置してある分電盤から各機器へ接続するための電源変圧器、電源ケーブル及びコンセント形状等を含める。

既設 LAN の敷設ケーブル等で流用可能な場合は流用しても差し支えない。新たに必要なケーブル敷設は、上述の全ての事項に適用する。

また、契約満了時には、原状に復すこと(一部除く)。

(1) 現行事業者との責任分界点

次期システムへの移行は受注者が責任を持って管理すること。移行計画においては、大学入試センター及び現行システム側で行うべき作業も含めて検討した上で計画書を作成し、現行事業者と協力して対応すること。移行計画作成に必要な現行システムの情報は大学入試センターから提供する。

また、移行作業は現行システムの運用中の作業となるため、受注者は現行システムの停止や性能劣化等を発生させないための対策を講ずること。

(2) 各種個別システムとの責任分界点

インターネット方向においては対外接続用 L3 スイッチを責任分界点とし、それらの機器へ接続するケーブルを含めた下流以降を受注者の責任範囲とする。ただし、クラウドサービスを利用する場合、今回の調達において構築した部分までを責任範囲とする。

現時点での接続予定機器は別添2「業務用電子計算機システム用機器借上げ及び運用支援業務要件定義書」にて示すが、移行時点で新規に追加されている機器の情報提供を大学入試センターから受けた上で全機器を次期システムへ接続すること。

接続に当たり受注者は事前に接続する情報及びスケジュールの提示を受けること。

なお、運用期間中において、ファイアウォールの更改等により再接続が発生した場合、次期システム側で必要となる作業を行うこと。

2.1.3. 納入、履行期間

(1) 納入期限

令和8年7月 31 日(金)

受注者は本調達機器等の搬入・設置、本システムの設計・構築・インストール及び環境設定・動作検証・教育・研修、データ移行等を納入期限までに完了すること。

なお、他システム(特に試験情報用電子計算機システム)との連携を考慮し、少なくとも 6 月末までにシステムの環境構築及び動作確認を済ませ、総合的な接続確認ができるようにすること。

(2) 履行期間

令和8年8月1日(土)から令和 13 年 7 月 31 日(木)まで

(3) 納入場所

本調達機器等については、主に以下の設置場所に納入するものとし、詳細については、大学入試センターと協議の上、作業を実施すること。
ただし、情報セキュリティの観点から応札者のみ、現地調査を許可する。

〒153-8501

住所：東京都目黒区駒場 2-19-2 大学入試センター電算機室内

(端末類は各執務室及び指定する場所に設置、スイッチ等は LAN 網敷設場所等に設置)

(4) 納入検査

本システムの構築が完了(動作検証済み)する前日までに正常に稼働していること。なお、本システムに大学入試センターによる納入検査を行う。

また、納入検査には、受注者が立ち会うこと。納入検査の結果、本システムの調達機器等の全部または一部に不合格品が発見された場合には、受注者は直ちに当該機器等を引き取り、正常な機器または代替機器等を大学入試センターの指定した日時までに納入り交換すること。

2.1.4. 成果物

提出する成果物は別添2「業務用電子計算機システム用機器借上げ及び運用支援業務要件定義書」を参照すること。

(1) 提出期限

令和8年7月 27 日(月)までに仮提出し、大学入試センターの担当が確認を行う。

修正指示や追記事項等を依頼された場合はそれに従うこと。

(2) 提出方法

受注者は成果物を電子媒体で正・副 2 部提出すること。

(3) 納入成果物の書式について

(ア) 電子ファイル(Microsoft Office 2024 (Word, Excel, PowerPoint の下位互換保存)), PDF ファイル)で保存した DVD-R/W 等で納品すること。ただし、LAN 配線図においては、PDF ファイルに加え大学入試センターが指示する CAD ファイル (DXF ファイル等) でも納品すること。

(イ) 容易に加除できる仕組みとし、変更履歴をつけて変更管理が行えるようにすること。

(ウ) 使用言語は日本語で記述し、英文等を引用する場合は、日本語訳を併記または脚注を必ず付すこと。

(エ)ドキュメントは、原則MS P明朝で、フォントサイズは11pt以上とし、A4縦の様式にて作成すること。

ただし、A4縦の様式で作成困難な場合(見づらい場合等)は、A3横又はA4横の様式を採用して作成してもよい。

2.2. 搬入・設置及び履行期間終了後の引き上げ

本調達機器等の搬入・設置及び履行期間終了後の引き上げは、受注者の責任と負担において行うものとする。

搬入出のルート等は、大学入試センターの指示に従い、決定すること。また、必要な手続きについては、遅滞なく行うこと。

2.2.1. 搬入・設置

- (1) 大学入試センターの指示する場所に搬入・設置を行い、梱包箱・残ケーブル等当該機器の利用に不要なものは、撤去する(持ち帰る)こと。
なお、運用開始日以前に当該機器の設置場所の変更が生じた場合は、大学入試センターの担当と日程等の調整を協議し、決定すること。また、実施に当たっては大学入試センターの指示に従って移設等を行うこと。
- (2) 本調達機器等に付随するDVD-ROMなどの電子媒体については、当該機器の運用及び保守に必要なもののみ大学入試センターにおいて保管し、それ以外は受注者において保管すること。
- (3) 運用管理事業者に対して教育・研修等を行い、運用引継ぎを円滑に行うこと。

2.2.2. 履行期間終了後の引き上げ

- (1) 廃棄に係る撤去・搬出するために必要な全ての経費(養生品(ようじようひん)、機材、車両等を含む)は、全て受注者の負担とすること。
- (2) 新システムが完全に稼働することを確認した後、受注者は既存機器等のうち使用しないこととなる機器等を大学入試センターの敷地内より撤去・搬出すること。その際、各機器を接続している配線についても撤去し、原状に復すこと。
- (3) 電源及びケーブルの引き上げについては、大学入試センターが指定するものの以外の全てを残置し、指定したものについては撤去し原状に復すこと。
- (4) 大学入試センターの敷地内から搬出する際には、データ復元ソフトウェア等を用いても再度データ入手できないよう完全にデータを消去し、破碎証明書を提出してから搬出すること。
- (5) 新たに敷設した電源やLAN配線等々は原状に復すること。なお、原状に復せない場合は、その理由を書面にて提出すること。また、大学入試センターで原状に復した発生費用と要した人件費相当を受注者は負担すること。

2.3. その他留意事項

- (1) 本調達は、総合評価落札方式とする。

- (2) 技術的要件は、全て必須の要求要件である。
- (3) 必須の要求要件は、大学入試センターが必要とする最低限の要求要件を示しており、入札機器の性能等がこれを満たしていないとの判定がされた場合には不合格となり、落札決定の対象から除外する。
- (4) 入札機器の性能等が技術的要件を満たしているか否かの判断は、本調達にかかる総合評価委員が、入札機器に係る技術仕様書を含む提出資料を審査して行う。
- (5) 保守料は、賃借料に含めること。
- (6) 本システムの導入と並行して別途、調達する試験情報用電子計算機システムの導入(更新)を予定していることから、同システムの受注者とスケジュールや設定等、万事協議し連携して構築すること。また、システム間の連携テスト期間(一ヶ月程度)は十分に確保すること。ただし、協議を要する場合は、大学入試センター立会いの下とする。
- (7) 本調達物品に係る性能、機能及び技術等の要求要件は、別添2「業務用電子計算機システム用機器借上げ及び運用支援業務要件定義書」に示す。ただし、指定した要件・機能を満たすことができる機能・技術・構成が別にある場合は、そのことを証明する資料を添付したうえで提案してもよい。

第3章 役務作業要件

プロジェクト開始時における前提条件やプロジェクト全体に関わる内容、システム設計・構築・試験、システム運用・保守等における提供内容を示す。

なお、個々の要件に関する内容は別添2「業務用電子計算機システム用機器借上げ及び運用支援業務要件定義書」を参照すること。

3.1. 作業前提

- (1) 本システムの運用開始日は、令和 8年 8月 1日とする。
本仕様書で要求する全機能について、大学入試センターが指定する設定を完了させ、運用開始日から利用できること。運用開始日になつても利用できないう場合は、代替機能を受注者の負担で提供すること。
- (2) 受注者は、契約後、直ちに作業実施計画書(全体工程表、作業体制表等を含む。)を提出すること。なお、作成に当たっては大学入試センターと十分に協議の上、承諾を得ること。
- (3) 本仕様書に明記されていない事項について、本システムが正常稼働するために必要な物品の納入、調整作業等については、大学入試センターと受注者とで協議の上、進めること。また、運用管理事業者との必要な調整等も、本調達範囲とする。
- (4) 受注者は施行に当たり、法令に定められた手続きが必要な場合、関係各所に対し必要な手続きを行うこと。また、手続き完了後は大学入試センターに報告すること。

- (5) 業者間の各種調整等については、受注者の責任と負担のもとに実施することとし、本システム導入に当たり、その調整等による不都合、負荷等が発生しないようにすること。
- (6) 本調達におけるシステム構築作業により、本システム及び本調達外の稼動中の機器及びシステムに影響を与えた場合は受注者の責任と負担において対処すること。特に、運用管理事業者に対して本作業に起因して発生した作業を依頼する場合は、大学入試センターと協議し、受注者が費用を負担すること。

3.2. 作業体制

- (1) 本調達の確実な実施を担保するためのプロジェクト体制を整えること。
- (2) プロジェクト体制表の作成に当たっては、作業責任者(国籍、居住都道府県、資格)、役割、連絡先を明確にすること。
- (3) プロジェクトマネージャについて、以下の各条件を満たすこと。
 - (ア) 過去 3 年以内に実施された、本件と同等又は同等以上の規模(利用者数: 200 人以上)の案件において、プロジェクトマネージャを務めた経験を有していること。なお、業務の受注実績を示す文書を提出すること。
 - (イ) システム設計・構築・運用等の業務経験を 10 年以上有していること。
- (4) 大学入試センターから受注者に対する指示、協議申し出等は、全てプロジェクトマネージャを介して行うものとする。
- (5) プロジェクトマネージャは、業務の進捗状況全体を把握し、大学入試センターに対して内容及び結果を大学入試センターの指定する頻度で定期的に報告すること。また、大学入試センターからの業務等に対する問い合わせに対し、プロジェクトマネージャは速やかに対応するとともに、各工程の終了時においては、作業結果について大学入試センターの承諾を得ること。
- (6) 原則としてプロジェクト体制の変更は認めないこととする。ただし、進捗に著しい遅れが発生した等で要員の追加及び作業担当者の変更がやむを得ない場合は、速やかに改善策を提示し大学入試センターの承諾を得ること。
- (7) 受注者は、マルチベンダ構成により調達を行う場合、納入及び運用を確実に実現するため、関係する業者間で十分な合意を得るとともに、その実施のための体制を整備し、大学入試センターに報告すること。

3.3. 機器の搬入・設置等

- (1) 本システムの導入は、「行政機関の休日に関する法律」に定める休日を利用する等、極力大学入試センター職員の業務が停止しないよう、実施すること。
- (2) 大学入試センターのネットワーク停止が伴う等、大学入試センターの業務に影響を与える場合には、原則として、平日 9:00 から 18:00 以外の間で実施すること。また、事前にその工程及び方法について大学入試センターの承諾を得ること。なお、平日 9:00 から 18:00 以外であっても大学入試センターのネットワーク等の停止が許容されない場合があるため、担当者と協議の上、日時

を決定すること。

- (3) 受注者は、本調達機器等の事前稼働検証、搬入・設置、各種ソフトウェアのインストール及び環境設定、動作確認、教育、研修、機器等の撤去・搬出等を行うに当たり、当該各作業の実施前に大学入試センターとの調整の十分な時間的余裕をもって、各作業の実施等に関する工程表を作成し、大学入試センターと打ち合わせを行うこと。本作業の実施に当たって、既存本番システム・業務に影響を与えないこと。
- (4) 切替えに当たって、大学入試センター職員の負担を軽減する方策を検討すること。
- (5) 工事が発生する又は導入機器及び必要な資材の搬入を行う場合は、その一週間前までに詳細な施行及び作業内容、範囲、作業者名、スケジュール及び使用車両を大学入試センターに報告し、承諾を得ること。また、大学入試センターが行うべき作業がある場合には、これを明示すること。
- (6) 大学入試センターの指示する場所に搬入・設置を行い、持ち込んだ梱包箱・残ケーブル等当該機器の利用に不要なものは撤去すること。
- (7) 搬入・設置・導入のために必要となる工事用機材や機器等については、受注者の負担において準備し、作業終了後に撤去すること。
- (8) 運用開始日以前に当該機器の設置場所の変更が生じた場合は、大学入試センターの指示に従って移設等を行うこと。
- (9) 本調達機器等については、各々の納入場所における調整を行い、正常に動作することを確認すること。また、導入した本システムが大学入試センターのネットワークや WAN 回線と連携して動作し、大学入試センター職員が使用している既存システムやアプリケーションが問題なく動作することを確認すること。なお、大学入試センターのネットワークや WAN 回線等、本業務を遂行するに当たり必要な詳細設定情報については、本業務の契約締結後に大学入試センターより提示する(ただし、詳細設定を含まない資料の閲覧を希望する場合、「8.5. 留意事項」のとおりとする。)。

3.4. 設計・構築

本調達において、以下の作業を含むシステム設計・構築を受注者の責任と負担において実施すること。

- (1) 本システムが、円滑かつ迅速に導入され、かつ運用されるよう設計を行うこと。
- (2) 大学入試センターのネットワークの安定した稼働及び業務の継続に影響を与えることがないよう、安全で確実な導入計画を策定すること。
- (3) 大学入試センターと協議の上、導入計画書を作成し、承諾を得ること。
- (4) 導入準備、導入作業及び検証の手順等を示した導入手順書を作成すること。
導入作業の手順には、各作業が正しく行われていることの確認を含めること。
- (5) 導入の際に、大学入試センターネットワークに連携する各システム等に影響を及ぼす場合は、事前に大学入試センターに連絡すること。
- (6) 既存環境や既存機器に設定変更、ツール等のインストールが必要となる際に

- は、大学入試センター及び運用管理事業者に設計等の情報を開示するとともに、各種調整や協議の上、大学入試センターの指示に従うこと。
- (7) 成果物一覧に記している可用性設計等システム設計・ストレージ設計・バックアップ設計・リストア設計・電源管理／UPS 導入設計等を実施すること。また、各設計にて作成したドキュメントは、大学入試センターの承認を得て納品すること。
 - (8) 大学入試センターへ搬入する前に行う設定等の作業(キッティング作業)のための構築環境(作業場所、電源設備等)は、受注者の負担、責任において用意すること。
 - (9) 調達した機器の組立・調整及び据付調整を実施すること。
 - (10) 構築及び納品する大学入試センターネットワークのネットワーク機器、サーバ及びアプライアンス等の物品は全て適正な設定・構築を行うこと。
 - (11) 本調達機器等については、仕様を満たす増設機器(メモリ及びハードディスク等)を全て本調達機器等に取り付けた形で正常動作の確認を行った後に納入すること。
 - (12) 大学入試センターネットワークを構築するため LAN ケーブル等を敷設し、調達した機器を接続すること。調達した機器は、本調達で構築(更新)するネットワーク又は大学入試センターと合意したネットワーク以外に接続しないこと。
 - (13) 必要な UTP/STP ケーブルや光ファイバは、受注者が準備すること。
UTP/STP ケーブルはカテゴリ 6 以上のケーブルとすること。

3.5. 運用・保守

3.5.1. SLA に関する提供事項

- (1) SLA を評価する上で前提条件
 - (ア) サービス提供開始時点から 2 か月間は調整期間とし、3 か月目から SLA の遵守の対象とする。また、達成及び未達成の評価は、月単位で行う。
 - (イ) 受注者は、各サービスの監視、測定等を行い、後述する「3.5.1.(2)SLA 項目」に記載されているサービスレベルの達成状況を逐次確認、把握すること。なお、監視、測定方法については、担当職員と協議の上、決定すること。
 - (ウ) 受注者は、月単位でサービスレベル目標値を設定した項目に対して実績を報告し、SLA 達成度合いを評価する。
 - (エ) SLA を満たせない可能性がある場合、速やかに担当職員に報告すること。また、サービスレベルを保つための対策について検討し準備すること。
 - (オ) 受注者は、SLA を遵守できなかった場合には、対応策について検討し、担当職員の了承を得た上で実施すること。
 - (カ) 対応の実施に当たっては、サービスレベル目標値に達成できる対応がなされるまで月次レベルで報告すること。
 - (キ) 対応に必要な人的リソースの追加、体制の変更、対応のために必要なシステムの導入等に費用がかかる場合、受注者の負担により、実施すること。
 - (ク) サービスレベルの評価に当たって、以下の事項に該当する場合は、SLA 規

程の範囲外とする。

- ① 大学入試センターの都合によって障害復旧できなかった場合
- ② 大学入試センターの事由によって障害連絡を受けることができなかつた場合
- ③ 予見できない不測の事態(社会通念上、受注者に責任がないことが認められる事態)が生じた場合

(2) SLA 項目

- (ア) SLA 項目については、大学入試センターと受注者で協議の上、決定する。
- (イ) 設計・開発業務の過程にて、受注者が提供するシステムに起因しない事由によって要求水準を達成できないと判断された場合、設定 SLA 値については担当職員と別途協議の上、決定する。
- (ウ) SLA 項目は、大学入試センター及び受注者双方の合意事項に明確な変更が生じた場合、大学入試センター及び受注者双方が必要と認めた場合等、必要に応じて見直しを実施し改訂するものとする。

3.5.2. 実施に関する提供事項

- (1) 保守・運用支援の実施体制を示すこと。
- (2) 統括責任者を配置し、全体の管理を担うこと。
- (3) 独立行政法人 情報処理推進機構が定める「IT スキル標準(ITSS)レベル 4」相当以上の能力を有する担当技術者を配置すること。
- (4) 実施体制、統括責任者及び担当技術者に変更がある場合は、事前に大学入試センターに連絡すること。

第4章 契約条件等

4.1. 秘密保持

- (1) 受注者は、履行期間中はもとより履行期間終了後にあっても、本業務を履行するうえで知り得た大学入試センターに係る情報を第三者に開示又は漏洩(ろうえい)しないこととし、そのために必要な措置を講ずること。
(ア) 受注者において秘密情報に関する目的外の利用、不正アクセス又は秘密情報の紛失、破壊、改ざん、漏洩等の事故が発生したとき、又はその恐れがあると認められるとき(第三者から通報があった場合を含む。)は、当該事故の発生の有無、その範囲及び発生原因の如何に関わらず、受注者は直ちにその旨を大学入試センターに報告し、大学入試センターの指示に従って直ちに応急措置を講じるものとする。
また、当該措置を講じた後直ちに当該事故の経緯及び応急措置の結果並びに事故再発防止策を書面により大学入試センターに報告しなければならない。
(イ) 前号の事故が受注者による本覚書の違反に起因する場合において、大学

入試センターが当該事故により費用を支出し又は損害を被ったときは、大学入試センターは受注者に対し、賠償を請求することができる。

- (ウ) (ア)の事故が受注者の本調達の違反に起因する場合は、受注者は(イ)ほか、当該事故の拡大防止や収拾のために必要な措置について、大学入試センターの指示に従うものとする。
- (2) 大学入試センターが提供する資料は原則貸し出しとし、大学入試センターの指定する日までに返却すること。当該資料は複製してはならず、原則として第三者に提供し、又は閲覧させてはならない。
- (3) 上記(1)の情報及び(2)の資料を第三者に開示することが必要となる場合は、事前に大学入試センターと協議の上、大学入試センターの承諾を得ること。
- (4) 大学入試センター内で本調達でのシステム構築・作業に従事する受注者は、以下の内容を履行すること。
- (ア) やむを得ず受注者内のパソコン等の電子機器類(付属品含む)を持込む場合には、目的などやその機器にインストールされている全てのソフトウェア名称等を記載した確認書(持込み／持出し)を大学入試センターにあらかじめ提出し、承認を得ること。
- (イ) 導入・設置(データ移行等)に伴い、個人情報等を漏らさないこと。また、大学入試センターの建屋内や執務室、電算機室内の撮影は原則許可しない。なお、執務室での覗き見などの行為が見られた場合には、当該担当の交代などの措置を受注者は講じ、再発防止策を書面により大学入試センターに報告すること。

4.2. 情報セキュリティの確保

本調達機器等について、セキュリティを確保するために受注者は以下の作業を実施することとし、発生する費用は本調達に含まれるものとする。また、実施した作業内容については履歴(作業日、作業をおこなった機器、作業内容、作業者を含む)を残すこと。

- (1) 本調達に係る業務を行う事業者は、事業者組織全体のセキュリティを確保するとともに、大学入試センターから求められた当該業務の実施において意図しない変更や機密情報の搾取等が発生しないよう、情報セキュリティを確保するための体制を整備すること。
- (2) 本体制における実務担当者には、「情報処理の促進に関する法律」(昭和 45 年法律 90 号)に基づき行われる情報処理技術者試験のうち、情報セキュリティに関する資格を有する者若しくは同等の知識及び技能を有することを自ら証明できる者を含むこととし、当該者については、継続して新たな知識の補充を行うことに配慮すること。本調達に係る業務の実施のために大学入試センターから提供する国の安全に関する重要な情報その他当該業務の実施において知り得た国の安全に関する重要な情報については、情報のライフサイクルの観点から管理方法を定め、その秘密を保持し、また、当該業務に目的以外に利用しないこと。

- (3) 本調達に係る本システムにおいて以下のセキュリティ機能を具体化し、実装すること。
- (ア) 本調達に係る情報システムにて使用するウィルスチェック対策機能。
- (イ) 本調達に係る情報システムへのアクセスを業務上、必要な者に限るための機能。
- (ウ) 本調達に係る情報システムに対する不正アクセス、ウィルス・不正プログラム感染等インターネットを経由する攻撃、不正等への対策機能。
- (エ) 本調達に係る情報システムにおけるセキュリティ事故及び不正の原因を事後に追跡するための機能。
- (4) 本調達に係る情報システムの構成における以下の脆弱性対策を実施すること。
- (ア) 構築する情報システムを構成する機器及びソフトウェアの中で、脆弱性対策を実施するものを適切に決定すること。
- (イ) 脆弱性対策を行うとした機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。
- (ウ) 把握した脆弱性情報について、対処の要否、可否を判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を納品時に大学入試センターに報告すること。
- (5) 本調達に係る業務の遂行において、定期的に情報セキュリティ対策の履行状況を報告するとともに情報セキュリティが侵害され又はその恐れがある場合には、直ちに大学入試センターに報告すること。これに該当する場合には、以下の事象を含む。
- (ア) 受注者に提供し、又は受注者によるアクセスを認める大学入試センターの情報の外部への漏洩及び目的外利用。
- (イ) 受注者による大学入試センターのその他の情報へのアクセス。また、被害の程度を把握するため、受注者は必要な記録類を契約終了時まで保存し、大学入試センターの求めに応じて成果物とともに大学入試センターに引き渡すこと。
- (6) 受注者の講ずる情報セキュリティ対策が大学入試センターの所有するポリシー等の基準を満たしていない場合には、受注者は、大学入試センターと協議の上で追加的なセキュリティ対策を講ずること。
- (7) 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状況を確認するために、大学入試センターが情報セキュリティ監査の実施を必要と判断した場合は、大学入試センターがその実施内容(監査内容、対象範囲、実施等)を定めて、情報セキュリティ監査を行う(大学入試センターが選定した事業者による監査を含む。)。
- 受注者は自ら実施した外部監査についても大学入試センターへ報告すること。
- (8) 情報セキュリティ監査の実施については、これらに記載した内容を上回る措置を講ずることを妨げるものではない。

4.3. 契約不適合責任

- (1) 納入日から起算して1年以内に本調達機器・装置等の設計・設定及びこれらに搭載されるソフトウェアに瑕疵のあることが発見された場合には、受注者は大学入試センターの請求により他の正常な機器・装置等と引き換え又は修理し、又はその瑕疵によって生じた損害を賠償すること。
- (2) 履行期間終了までに以下に示す契約不適合について、大学入試センターは知り得たときから1年以内に受注者へ「通知」するものとし、受注者は、調査の上、修正又は措置を講じること。ただし、検収後1年を経過したものに関しては、本適用の対象外とする。
 - (ア) 成果物に不備(記載とおりに動作しない場合など)や汚損等があるとき
 - (イ) 大学入試センターの帰責事由(故意又は過失に加えて、信義則上それと同視することができる事情を含む事由)によらずに、大学入試センターと受注者が合意したプロジェクト計画書で予定された工程の全てが納入期限までに完了しないとき、もしくは完了しないことが明らかになったとき
 - (ウ) 大学入試センターの帰責事由によらずに、大学入試センターと受注者が合意した要件の全てが満たされないとき、又は業務に支障が出ることが想定される不具合が残存していたとき
 - (エ) 受入試験中及び納品後に発見された不具合について、その改修計画又は調査計画立案及び不具合残存中の対応策検討のための協議に受注者が応じないとき、又は受注者が合意した期限までに示されないとき
 - (オ) 大学入試センターの帰責事由によらずに、大学入試センターと受注者が合意した期限までに不具合の改修が完了しないとき、もしくは完了しないことが明らかになったとき

4.4. 賠償・復旧

本業務に起因して、正常な使用状態で大学入試センターの他の機器及び本システムに不具合が発見された場合は、受注者の責任と負担で復旧のための措置を迅速に実施すること。

- (1) 検収後、賃貸借期間中は、サーバ及びネットワーク関係機器・装置等が正常な使用状態で不具合が発見された場合には、受注者において無償にて迅速にシステム(ソフトウェア、ハードウェアを問わず)の修正及び調整を行い正常に使用できる状態に復旧すること。なお、修正したプログラムや設定情報に関するドキュメントを修正して提出すること。
 - (2) 調達物品の導入に際しては、大学入試センターの施設設備に損傷を与えることがないよう充分注意するとともに、搬入時には受注者が必ず立ち会うこと。損傷を与えた場合には、原状に復すること。
 - (3) 大学入試センターに不相当な負担を課するものでないときは、受注者は、大学入試センターが請求した方法に従い、追完請求(修補、代替物の引渡し、不足分の引渡しなど)に応じること。
- なお、契約不適合が大学入試センターの帰責事由による場合を除き、追完

請求できるものとする。

4.5. 個人情報保護法に関する事項

受注者は、「個人情報の保護に関する法律(平成 15 年法律第 57 号)」又は、当該法律を遵守するために受注者が定めた個人情報保護に関するガイドライン等を遵守し、個人情報を取り扱うこと。

4.6. 第三者への請負、著作権等

- (1) 受注者は、本業務の全部を一括して又は主たる部分を請負等により第三者に実施させてはならない。ただし、次の場合においてはこの限りではない。
 - (ア) 受注者が、書面により請負等を受ける者の名称・住所・請負等の業務の範囲・請負等の必要性・請負等の金額等を事前に大学入試センターに申請し、その承諾を受けた場合。なお、請負等の内容を変更しようとする場合も同様とする。
 - (イ) 受注者がコピー・ワープロ・印刷・製本・トレース・資料整理・計算処理・翻訳・参考書籍等の購入・消耗品購入・会場借上等の軽微な業務を請負等しようとする場合。
- (2) 上記に基づき、第三者に業務を請負等する場合は、「4.1.秘密保持」に従いその者に対し、秘密の保持を同様に請負契約等において課すこと。
- (3) 受注者及び請負等を受けた第三者は、大学入試センターが保有する情報セキュリティポリシー等(以下「ポリシー等」という。)を遵守しなければならない。また、大学入試センターの保有するポリシー等については、「4.1.秘密保持」に基づき、その内容を秘密にする措置をとらなければならない。
- (4) 受注者が上記(1)に基づき第三者に請負等する場合において、請負等を受けた第三者が更にその業務の一部を請負等する等複数の段階で請負等が行われるときは、あらかじめ当該複数段階の請負等を受ける業者の名称・住所・請負等の業務の範囲を記載した書面(履行体制に関する書面)を大学入試センターに提出しなければならない。当該書面の内容を変更しようとする場合も同様とする。
- (5) 受注者が上記(1)に基づき第三者に業務を請負等する場合において、これに伴う第三者の行為については、その責任を受注者が負うものとする。なお、再々請負等の場合も同様とする。
- (6) 本業務の実施に当たっては、必要に応じて納入場所の環境について事前に確認を行うこととし、大学入試センターの業務に極力支障が生じないよう計画し実施すること。また、運用管理事業者、大学入試センターの他の現行システム請負業者等関係者との連携・協力を図りつつ大学入試センターネットワーク及び関連する各種システムの円滑かつ安定的な稼働に支障を来すことのないよう業務を実施すること。
- (7) 試験計画書に基づき、総合試験を実施する際に使用する試験用データは、受注者において準備すること。なお、運用管理事業者の協力が必要な場合

は大学入試センターと協議し、原則として受注者の責任と負担において行うこと。

- (8) 本業務の実施に必要となる工業所有権及び著作権等については、全て受注者の責任において当該産業財産権及び著作権等の使用に必要な費用を負担し、使用承諾等に係る一切の手続きを行うこと。
- (9) 本仕様書に基づく作業に関し、第三者との間に著作権に係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大学入試センターの責めに帰す場合を除き、受注者の責任と負担において一切の処理をすること。
- (10) 本業務の実施に伴い、本調達機器等の搬入・設置・修理・交換等物理的作業の実施に当たって大学入試センターの敷地内の作業場所を使用する場合は、事前に大学入試センターに申請しその承諾を得なければならない(ただし緊急に措置しなければならない場合を除く)。その場合、受注者は作業場所を整理・整頓し、安全に留意して事故の防止に努めるとともに、労働基準法・労働安全衛生法を遵守して安全の徹底を図り作業すること。当該作業に伴い必要となった養生品・梱包箱等で当該作業の後不要となるものは、受注者の負担で速やかに撤去すること。
- (11) 既設建物(特に室内装飾)を汚損又は破損しないように細心の注意をもって行うこと。また、受注者の責めに帰す事由による構造物及び道路の損傷、土地の踏み荒らし等、第三者に与えた損害に対する費用等は全て受注者の負担とする。
- (12) 受注者は、本仕様書に疑義が生じた場合、本仕様書により難い事由が生じた場合及び本仕様書に記載のない事項については、直ちに大学入試センターと協議の上、解決に向け両者とも最善の努力を行うものとし、独自の解釈によって行うことがないように十分注意すること。
- (13) 本仕様書に記載なき事項でも、本システムの構築・稼働・運用に必要と認められる事項は、大学入試センターと協議の上、実施すること。
- (14) 受注者は、大学入試センターとの協議の結果(いわゆる議事録を意味)を協議の都度作成し、文書あるいは電子メール等にて4日以内に提出し、大学入試センターの承認を得ること。

第5章 提案書記載要項

5.1. 概要

応札者は、本提案書記載要項に基づき、本調達を履行する能力があることを、提案書における具体的な記載によって証明すること。提案内容が要求要件を満たしているか否かの判定は、大学入試センターにおいて、提出資料の書面により行う。

5.2. 記載に際しての基本要件

- (1) 提案書は、単なる意思表示ではなく、提案するシステムが本仕様書の要求要件をどのように満たすか、あるいはどのように実現するかを要求要件ごとに詳細かつ具体的に分かりやすく専門用語を用いず、図解や資料を添付する等して説明すること。
また、以下についても明記すること。
 - (ア) 運用に関する運用管理事業者への教育、障害発生時の一次対応方法等についての教育、研修計画
 - (イ) 一般利用者に対する端末側における基本的な使用方法(OS、オフィス、グループウェア等)についての教育、研修計画
- (2) ハードウェア及びソフトウェア構成一覧には、機器毎の名称、バージョン名、ライセンス数、機能及び概要を明記すること。
- (3) ネットワーク、ハードウェア(サーバ等)、OS、ミドルウェアの選定・構築方法を標準化した、システム・インフラの選定・構築方法論(IT インフラ構築における方法論)を応札者自身が有し、システム・インフラの設計において属人性を排除したインフラ構築が可能であることを具体的(特殊な技法やフレームワークを利用せず、最終的には完成図書を見れば誰もが分かるような内容であること。)に記載すること。
- (4) 提案する調達物品には、納入期限までに製品化又はバージョンアップを予定している製品を含めてもよい。
ただし、納入期限までに製品化又はバージョンアップされ、仕様書に記載する技術的要件を全て満たすことが可能である旨を示す書類を提出すること。
- (5) 提案する調達物品に他社製品を含めてもよい。
ただし、他社製品を含める場合は代理店証明又はそれに相当する書類を提出すること。(他社製品の保守管理についても自社製品と同様に品質責任及び保守責任を持つこと。)
- (6) 本仕様書は、本調達の履行に最低限必要とされる要件を示したものである。
従って、仕様書の要件を全て満たしたうえで、仕様書に記載されていない事項であっても、本調達の履行に当たり、必要と思われる事項については提案書に記載すること。
- (7) 保守体制・サービスを具体的に提案すること。
- (8) 提案書において記載された内容は、本調達範囲に含むものとする。

5.3. 提案必須項目

(1) 本調達の基本方針

本件の業務目的、業務内容を踏まえ、応札者が本調達に対応するに当たつての応札者の基本方針を具体的に記載すること。

(2) 基本情報

応札者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性(情報セキュリティに係る資格・研修実績等)・実績及び国籍に関する情報を記載すること。

(3) 機能要件に関する提案

別添2「業務用電子計算機システム用機器借上げ及び運用支援業務要件定義書」における下記の要件について、項目毎に提案内容を具体的に記載すること。

- (ア) 提案する機器構成について、構成品一覧を提示すること。(メーカー型番が分かる品目表を提出すること。)
- (イ) 可用性を確保するために、直接的にユーザサービスに関わる機器は二重化構成とし、単一障害点(SPoF)が無い設計とすること。
- (ウ) 電源容量計算を提案書に記載すること。

(4) 役務作業要件に関する提案

「第3章 役務作業要件」における下記の要件について、業務の実施方法等を創意工夫し、各項目に提案内容を具体的に記載すること。

- (ア) 大学入試センターネットワークの安定した稼働及び業務の継続に影響を与えることがないよう、安全で確実な導入計画を策定すること。
- (イ) 運用管理事業者に対する教育・研修等には、本調達システムの利用において、大学入試センターの業務が滞りなく継続できるような運用を可能とする内容を含んだトレーニングを提案し、実施すること。

(5) 作業体制、応札者条件に関する提案

- (ア) 「3.2. 作業体制」に示す各要件について、必要な資格・実績等を具体的に記載し、証明書の写し等を添付すること。
- (イ) 「7.1. 応札者としての条件」に示す各要件について、必要な資格・実績等を具体的に記載し、証明書の写し等を添付すること。

5.4. 提案書作成要領

- (1) 提案書の印刷書式は、原則としてA4判縦長・横書きとし、11pt以上のフォントサイズで作成すること。
ただし、図表等についてはA3判も可とする。添付する説明資料やパンフレット等がある場合には、この限りではない。
- (2) 提案書本文は日本語で記載し、分かりやすい構成を心がけ、目次及び通しのページ番号を付与すること。なお、必要に応じて用語解説等を添付すること。
- (3) 応札者の名称、所在地、代表者氏名等を記載すること。

- (4) 提案した製品や提案書内容等に対する照会先(連絡担当者名, 所属, 電話番号, ファクシミリ番号, E-mail アドレス)を記載すること。また, 問い合わせやヒアリングを行うことがあるので, 問い合わせに対する体制を整えておくこと。

5.5. 留意事項

- (1) 提案に係る経費は, 応札者の負担とする。
- (2) 提出された提案書について, 照会や資料要求を行うことがある。
- (3) 仕様要件を満たしていないと大学入試センターが判断した場合には, 応札できないものとする。また, 一旦提出された提案書の差し替えや再提出は, 一切認めない。
- (4) 本調達に係る資料(既存環境における「機器一覧」, 「全体概要図(詳細設定情報を含まないシステム構成図, ネットワーク構成図等)」)の閲覧については落札者に対し, 閲覧を許可する。ただし, 応札者の現地視察については, 本調達の入札公告期間中に限り, 大学入試センターが指示する日時及び場所において視察を認める。
- (5) 提案された内容等について, 大学入試センターの総合評価委員に対する説明会を実施する場合があるので対応すること。
なお, 説明会の日時及び場所については, 大学入試センターの所管部門から連絡する。
- (6) 提案した機器リストの中に, 大学入試センターにおいてサプライチェーン・リスクがあると判断した機器等がある場合には, 応札者は, 別の機器等(同等品)と交換した機器リストを大学入試センターが指定する日までに再提出すること(政府調達におけるサプライチェーン・リスク対策のため)。なお, 指定する日までに再提出がない場合には, 辞退したものとみなす。

第 6 章 提出物

応札者は以下の書類を紙媒体で5部, 電子媒体(CD-R 又は DVD-R)で2部提出すること。

- (1) 機能証明書
実現可否を追記の上, , 適合表として提出すること。
- (2) 提案書
「第 5 章 提案書記載要項」の記載内容に従い, 実現する提案を具体的に記載すること。

第 7 章 その他特記事項

7.1. 応札者としての条件

応札者は, 次に掲げる条件を全て満たすこと。

- (1) 大学入試センター情報化統括責任者(CIO)補佐官及びその支援スタッフ業

- 務について、CIO 補佐官等が現に所属する又は過去 2 年間に属していた事業者及びその関連事業者ではないこと。
- (2) 保守業務に携わる主たる担当者の体制図を明記した担当者一覧表(国籍、資格、居住都道府県)を提出すること。
 - (3) 本業務の実施予定部門が組織的に品質管理を行っていることの証明として、品質マネジメントシステム ISO9001:2015 版以上を取得していること。実績の継続性確保のため更新した実績を有すること。
 - (4) 本業務の実施予定部門が環境負荷軽減への取り組みを組織的に行っていることの証明として、環境マネジメントシステムの国際規格である ISO14001:2015 版を取得していること。実績の継続性確保のため更新した実績を有すること。
 - (5) 本業務の実施予定部門が組織的に情報セキュリティマネジメントシステム ISO27001:2014 (ISO/IEC27001, ISO/IEC27002) 版以上を取得していること、若しくは同等以上の情報セキュリティマネジメントシステムの仕組みを有していること。あるいは、本業務の実施予定部門が組織的に個人情報保護を行っていることの証明として、セキュリティマネジメントにかかる公的資格であるプライバシーマークを取得していること。実績の継続性確保のため更新した実績を有すること。

7.2. 受注者間の協議

本システムの導入と並行して、大学入試センターにおいて別途調達する試験情報用電子計算機システムの導入(更新)を予定していることから、同システムの受注者とスケジュールや設定等、万事協議し連携して構築すること。ただし、協議をする際は、大学入試センター立会いの下とする。

7.3. 政府・省庁規定及び各種ガイドラインへの準拠

以下に示す各種ガイドライン(最新版)を遵守すること。今後契約期間中に当該文書が改定された場合には、それに従うこととするが、より良い作業の進め方又は手法について提案がある場合には、担当職員に提案、協議の上、当該提案に基づき実施してもよい。

- (1) 内閣官房内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省所管「政府情報システムのためのセキュリティ評価制度 (ISMAP)」
- (2) 経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」
- (3) 経済産業省「IT 製品の調達におけるセキュリティ要件リスト」
- (4) 独立行政法人大学入試センター「独立行政法人大学入試センターサイバーセキュリティ対策基準」
- (5) 独立行政法人情報処理推進機構「『高度標的型攻撃』対策に向けたシステム設計ガイド」
- (6) 独立行政法人情報処理推進機構「『新しいタイプの攻撃』の対策に向けた設

計・運用ガイド」

- (7) サイバーセキュリティ対策推進会議「高度サイバー攻撃対処のためのリスク評価等のガイドライン」
- (8) 内閣官房内閣サイバーセキュリティセンター「高度サイバー攻撃対処のためのリスク評価等のガイドライン付属書」
- (9) サイバーセキュリティ戦略本部決定「政府機関等のサイバーセキュリティ対策のための統一規範」、「政府機関等のサイバーセキュリティ対策の運用等に関する指針」及び「政府機関等のサイバーセキュリティ対策のための統一基準」
- (10) 内閣官房内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン」
- (11) 総務省「電子政府システムの IPv6 対応に向けたガイドライン」
- (12) ISO/IEC15408
- (13) ISO27017(クラウドサービスセキュリティ管理策)
- (14) ISO27001(情報セキュリティマネジメントシステム)
- (15) デジタル社会推進会議幹事会決定「デジタル・ガバメント推進標準ガイドライン」

7.4. 政府・省庁規定及び各種ガイドラインの動向への留意

以下に示す各種ガイドライン(最新版)及び関連する施策の動向に留意し提案すること。

- (1) 令和 5 年 4 月 1 日関係省庁申合せ「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」
- (2) 令和 3 年 9 月 28 日閣議決定「サイバーセキュリティ戦略」

7.5. 法律・規格への準拠

- (1) 導入するハードウェア及びソフトウェア等の構成要素は、オープンシステム環境の整備を可能とするため、ITU-T(国際電気通信連合 電気通信標準化部門)、ISO(国際標準化機構)等が規定、又は、推奨する各種国際標準及び装置の製造・データ処理に関して、IEEE(米国電気電子学会)等が規定、又は、推奨する各種デファクトスタンダードに準拠していること。また、これらと必要な十分なインターフェースを有すること。
- (2) 「民法(明治 29 年 4 月 27 日法律第 89 号)」、「刑法(明治 40 年 4 月 24 日法律第 45 号)」、「著作権法(昭和 45 年 5 月 6 日法律第 48 号)」、「不正アクセス行為の禁止等に関する法律(平成 11 年 8 月 13 日法律第 128 号)」、「個人情報の保護に関する法律(平成 15 年 5 月 30 日法律第 57 号)」の関連法規を遵守すること。

7.6. 閲覧・提供資料

- (1) 応札予定者は、(ア)の資料を閲覧することができる。また資料の閲覧を希望する場合は、必要な手続きを行った上、大学入試センターが定める期間、場

所、方法において閲覧を許可する。また、以下の資料の他に閲覧を希望する資料がある場合には、大学入試センターと相談すること。

- (2) (イ)参考資料は必要な手続きを行った上で、本仕様書の添付資料として応札予定者に提示する。
- (ア) 現行システムに係る資料
- ・完成図書
 - ・基本設計書
 - ・詳細設計書(パラメータ設計書)
 - ・運用マニュアル
- (イ) 参考資料
- ・【参考 1】現行業務用電子計算機システム全体構成図
 - ・【参考 2】現行スイッチ配置一覧
 - ・【参考 3】現行無線 AP 設置一覧
 - ・【参考 4】端末配置一覧
 - ・【参考 5】複合機配置一覧
 - ・【参考 6】平面図
 - ・【参考 7】端末別利用ソフトウェア等対応表

7.7. 技術仕様等に関する留意事項

- (1) 提案システムのうち、納入期限までにバージョンアップが予想されるハードウェア又はソフトウェアについては、その予定時期等が記載された資料を提出すること。
- (2) 納入時における全てのソフトウェアは、契約時の最新バージョンで提供すること。なお、日本語版があるものは日本語版で提供すること。
- (3) 性能、機能に関する要件の各項目で述べる性能、機能を満たすならば、複数個の装置で実現するように指定している場合でも、設置場所ごとの単一の装置で実現してもよい。

7.8. 提案に関する留意事項

- (1) 提案に際しては、提案システムが仕様書の要求要件をどのように満たすのか、あるいはどのように実現するのかを要求要件ごとに具体的かつ分かりやすく、記載すること。したがって、技術的要件に対して、単に「できます。」「提案します。」といった回答の場合、提案書とみなさないので十分に留意して作成すること。
- (2) 提出資料等に関する照会先を、明記すること。
- (3) 提案書提出時に既に存在するハードウェア及びソフトウェアについて納入稼働実績がある場合には、そのリストを提出すること。
- (4) 調達内容が不明確である場合は、有効な提案書とみなさないので留意されたい。
- (5) 提案書の内容に関してヒアリングを行う場合がある。

7.9. その他の留意事項

- (1) 技術的要件に“大学入試センターで別途調達した”と記載のあるソフトウェア以外は全て現行システムの契約満了に伴い、リースアップするため、ハードウェア及びソフトウェアのライセンス等は受注者が新規で用意し、その費用は本調達に含めること。
- (2) 納品・提出する資料等は、原則として全て日本語で記述されていること。やむを得ず外国語による資料を提出する場合は、日本語に翻訳した文書を添付すること。
- (3) 原則として、グリーン購入法に適合した機器を提供すること。
- (4) 本調達に係る経費は見込まれる全ての事項を見込むこと。
- (5) 受注者は、本仕様書に記載なき事項であっても、本業務遂行に必要と認められる事項・作業については、大学入試センターと協議の上、誠意を持って対応すること。

業務用電子計算機システム用機器借上げ
及び運用支援業務
要件定義書案

令和7年
独立行政法人 大学入試センター

目次

第1章 概要	1
1.1. 名称	1
1.2. 目的	1
1.3. 構成	1
第2章 情報システムの要件(調達物品に備えるべき技術的要件)	2
2.1. 基本要件	2
2.2. ネットワーク接続機器に関する要件	4
2.2.1. 基本要件	4
2.2.2. セキュリティ要件	4
2.2.3. 対外接続用 L3 スイッチ(2 台)及び装置間接続用 L2 スイッチ(7台)	4
2.2.4. リンク負荷分散装置(ロードバランサー)(2台)	5
2.2.5. UTM 装置(統合管理装置を含む)(2台)	7
2.2.6. コアスイッチ(1式)	8
2.2.7. パッチパネル(2式)	9
2.2.8. フロアスイッチ及びエッジスイッチ	9
2.2.9. メディアコンバータ(6 台)	11
2.2.10. 無線LANアクセスポイント (20台)	11
2.3. サーバ等に関する要件	12
2.3.1. サーバの基本要件	12
2.3.1.1. 時刻同期	12
2.3.1.2. ログレポート機能	12
2.3.1.3. ハードウェアの特質、要件	12
2.3.1.4. ソフトウェア要件	14
2.3.2. 外部向け(DMZ)及び内部向けを一組とするサーバの共通事項	15
2.3.2.1 プロキシサーバ	15
2.3.2.2. DNS サーバ	16
2.3.2.3. メールサーバ	16
2.3.3. シンクライアントシステム(一式)	16
2.3.3.1. シンクライアントサーバ(一式)	17
2.3.3.2. シンクライアントシステムストレージ(一式)	19
2.3.3.3. 仮想デスクトップ環境	20
2.3.3.4. シンクライアント端末の設定(180 式)	20
2.3.3.5. リモートアクセス	21
2.3.4. ファイルサーバ(一式)	21
2.3.5. ファイルサーバ監視システム(一式)	23
2.3.6. 振る舞い検知管理サーバ	23
2.3.7. IT 資産管理システム	24

2.3.8. AD/DHCP サーバ(一式)	24
2.3.9. グループウェアサーバ.....	25
2.3.10. ウィルス定義 DB サーバ	26
2.3.11. パッチ管理サーバ.....	26
2.3.12. Microsoft License 管理サーバ	27
2.3.13. メールセキュリティシステム.....	27
2.4. バックアップサーバ(1 台)	28
2.5. ログ収集システム(1台)	28
2.6. 監視システム(1台)	29
2.7. 無停電電源装置(UPS)(一式)	29
2.8. KVM スイッチ(一式)	30
2.9. 財務会計システム(一式)	30
2.9.1. 会計システム管理サーバ(1 式)	30
2.9.2. 会計システム管理用パソコン(1 台)	32
2.9.3.無停電電源装置(UPS)(一式)	33
2.10. フットクライアント端末の設定(40 台)	33
2.11. データ移行.....	34
第3章 保守要件	36
3.1. 基本要件	36
3.2. 問い合わせ受付窓口対応	37
3.3. システム保守対応	37
3.4. ハードウェア保守対応.....	38
3.5. ソフトウェア保守対応	39

第1章 概要

1.1. 名称

業務用電子計算機システム用機器借上げ及び運用支援業務

1.2. 目的

- (1) 本システムは、主として大学入試センター内の利用者に向けてサービスを提供するものであり、メール・グループウェア機能及びファイル共有システム等のサービスを提供している。およそ 220 台のクライアント端末が稼働しており、職員数(ユーザ数)は 180 名程度である。
- (2) ネットワークとしては、不正の防止及び発生時の影響範囲を限定するため、外部との通信を行うサーバ装置及び通信回線装置のネットワークと、内部のサーバ装置、端末等のネットワークを分離し、さらに業務目的、所属部局等に応じて内部のネットワークを分離している。

1.3. 構成

- (1) 基本構成はオンプレミスで構築しつつ、OPEN 環境とそこで使用するサービスについては受注者の判断により、大学入試センターと協議のうえで、クラウドサービスを利用して構築することも可能とする。
- (2) サーバ、ストレージ及びネットワーク等のハードウェア機器は、仮想化が適さないものを除き、仮想化技術を用いて集約すること。
- (3) ハードウェアリソース(CPU、メモリ、ディスク容量、ネットワーク回線等)及びシステムリソース等を可視化し容易に再分配することに加えて、一元的に管理することでリソース配分の最適化、システム運用業務の負荷軽減、増築等に伴う設定変更の簡素化を図る。
- (4) 障害時における業務継続性を向上させるため、物理障害のポイントを削減し、各サービスの特性を踏まえた冗長化構成、バックアップ体制を講じる。
- (5) ハードウェアリソース逼迫時、障害時、災害時における各サービスの業務継続性の向上のため、論理構成及び物理構成を実装する。
- (6) 昨今及び将来のサイバー攻撃に対応すべく、より強固なセキュリティ対策として、ゼロデイ脆弱性や既知及び未知の脅威に対しても常に最速、かつ、確実な検知・遮断、対応等を実現するために、最新の技術を適用したふるまい検知、ログ分析、監視等を導入し、侵入防止及び侵入後における適切な対策によるセキュアな環境を構築する。
- (7) 職員は、次期システムを利用するにあたり、利便性とセキュリティ性に優れたシンクライアント端末を利用する。
- (8) 無線 LAN 環境においては IEEE802.1x 認証を導入し、セキュリティを確保する。

第2章 情報システムの要件(調達物品に備えるべき技術的要件)

2.1. 基本要件

■ 全般要件

- (1) 提案する本システムの構成について、構成品一覧を提示すること(メーカー型番が分かる品目表を必ず提出すること)。
- (2) 本調達機器等及びその構成・配置については、運用環境を考慮して、可能な限り実績のある最新の技術を採用すること。
- (3) 本調達機器等について、特に定めないものは、JIS 等の国内規格、ISO 等の国際規格又はそれと同等の規格に適合する品質優良なものを使用すること。
- (4) ハードウェア及びソフトウェアは、製品の動作が保証又は確認されたものであること。
- (5) 納入期限までに発見された本調達機器等の不具合については、受注者の責任と負担で迅速に対応すること。

■ 導入要件

- (1) センターネットワークに組み込むために必要となる設計・設定・テスト作業等を必ず実施し、センターネットワーク及び大学入試センター業務に何ら支障をきたさないようにすること。
- (2) 本システム以外で利用しているネットワーク機器やサーバが問題なく動作するための結合／総合設計・設定・テスト作業等を実施すること。
- (3) 現行システムと新システムとで併設する期間、業務に影響のない形で併設することとし、現行システムの設定変更が必要な場合には、現行事業者と調整の上、受注者の責任と負担において作業すること。

■ ハードウェア要件

- (1) 同一の種類の機器に関しては、用途に応じて型番・スペックを最適化し、用途に応じて機器を統一すること。
- (2) 本調達機器等に係る製品候補においては、契約期間中の保守が可能なものを選定すること。
- (3) 原則として、特定調達品目として指定されている製品については、国等による環境物品等の調達の推進等に関する法律(平成12年法律第100号)(グリーン購入法)に基づく環境物品等の調達の推進に関する基本方針に規定された基準及び配慮事項を満たす製品であること。
(ア) 環境(3R:リデュース／リユース／リサイクルの3つを含む)に配慮した設計・製造がなされている
(イ) 使用済後も、引取り・リユース／リサイクル・適正処理がなされている
(ウ) 環境に関する適切な情報開示がなされている
- (4) 機器等の製造工程において、意図しない変更が加えられないよう適切な措置がとられていること。また、大学入試センターが求めた際、当該措置を証明する資

料を提出すること。

- (5) 受注者が提示した機器リストの中に、大学入試センターにおいてサプライチェーン・リスクがあると判断した機器等がある場合には、受注者は、別の機器等(同等品)と交換すること。(政府調達におけるサプライチェーン・リスク対策のため)
- (6) 本調達機器等は、機械的及び電気的に人体に危険がないものであること。
- (7) 電源容量計算等の諸元(電源のコンセント形状、定格電圧、定格電流)を提案書に記載すること。
- (8) ネットワーク機器については、IPv6 に対応済み、若しくは、将来的にソフトウェアのバージョンアップ等により IPv6 に対応できる機器であること。
- (9) ネットワーク監視ソフトウェアによる死活監視に対応するために、サーバ及びネットワーク機器については、ping に対する応答が可能なこと。

■ ソフトウェア要件

- (1) ソフトウェアは、バージョンを統一すること。また、原則日本語版であること。
- (2) ソフトウェアのバージョン確定に当たっては、大学入試センターと協議すること。また、バージョン確定後から納入期限までにバージョンアップのあることが確認された場合には、動作確認が済んでいるものに限り、大学入試センターの承諾を得た後に最新バージョンを導入するものとする。
- (3) ソフトウェアのライセンスを本調達に含めること。また、納入期限までに指摘されている脆弱性(ぜいじやくせい)の有無を確認し、これを大学入試センターに書面にて報告し、大学入試センターと協議の上で納入期限までに修正モジュールの導入等適切な対策を施すこと。
- (4) クラウドサービスを使用する場合、原則として ISMAP に登録されているサービスを利用すること。また、保管するデータセンターは国内に限ること。また、想定される利用料についても本調達に含めること。

■ セキュリティ要件

- (1) システム構築に当たっては不正操作から保護するための対策を講ずること。
- (2) 各種管理画面等へのアクセスに当たってはセキュリティ強化のため、多要素認証を実装すること。なお、知識要素(ID・パスワード等)及びネットワークによる制限で実装してもよい。
- (3) DNS/Proxy/メール等の内部通信は、暗号化通信とすること。また、大学入試センターから指示した外部／内部通信に係るサーバに対し、SSL 証明書の適用を行うこと。
ただし、障害通知の SMTP/SMTPs 通信も発生するため、設定は、暗号／平文の両方が通信可能な設定とすること。
- (4) システム環境構築完了後に、情報セキュリティを担保するため、セキュリティ診断とペネトレーションテストを実施すること。不備が発見された際は、修正し、再度ペネトレーションテストを実施し、安全性を確保すること。実施後には報告書

(実施方法や確認方法など、実施した内容が分かる資料含む。)を提出し、成果物として納めること。

■ 信頼性要件

- (1) 各種災害(地震等)対策等を十分に考慮し、安全かつ信頼性のあるシステムを構築すること。無停電電源装置(UPS)を使用した安定的な電源の供給やデータ保護、外部媒体又はクラウド環境へのデータバックアップ等の措置を講ずること。
- (2) 将来におけるハードウェア・ソフトウェアの増強・ネットワークの拡大・接続機器の増設及び拡張のため、互換性・移植性・接続性を確保でき柔軟に対応できるよう標準化が考慮されていること。
- (3) 直接的にユーザサービスに関わる機器は、二重化構成とし、単一障害点(SPoF)がない設計とすること。

2.2. ネットワーク接続機器に関する要件

2.2.1. 基本要件

別紙「主なネットワーク配線及びスイッチ配置の概略図」を参照し適切なネットワーク機器を配置し、ネットワークを構築すること。

- (1) 各EPSに設置するスイッチは、ケーブルの破損を防ぐため収納可能なEIA規格準拠した19インチラックの情報コンセントボックス等に収納すること。
- (2) コアスイッチから各フロアスイッチ・サーバ室内に設置のサーバまでは10Gbps以上の回線を接続すること。
- (3) EPS内に設置する各フロアスイッチからエッジスイッチ及び端末までは1Gbps以上で接続すること。

2.2.2. セキュリティ要件

ネットワークの構築に当たっては以下のセキュリティ要件を満たすこと。インシデント等の発生時には管理者への通知と関連するログを保存すること。

- (1) 構内ネットワークにおいて許可のない端末の接続及び許可されないプロトコルの通信(不正アクセスや異常な通信)をブロックする機能を有すること。
- (2) ウィルス、スパイウェア、マルウェア等の不正プログラムの侵入を防ぐとともに、内部で感染を広げないために不正な通信を防ぐ機能を有すること。
- (3) DoS/DDoS攻撃を防御する機能を有すること。

2.2.3. 対外接続用L3スイッチ(2台)及び装置間接続用L2スイッチ(7台)

以下の仕様を満たす対外接続用L3スイッチ及び装置間接続用L2スイッチを用意すること。

■ 一般機能

- (1) ループ防止機能により、ネットワークでのケーブル誤接続によるループ構成を自動的に検出し、該当ポートを切り離すことが可能のこと。
- (2) VLAN(Port VLAN, Tag VLAN)機能を有しており、マルチサポートしているこ

と。

- (3) トラフィック解析のためポートミラーリング機能を有すること。

■ ハードウェア要件

- (1) EIA 規格準拠 19 インチラックに搭載可能なこと。
- (2) 対外接続用 L3スイッチ(2 台)は、以下の要件を満たすこと。
 - (ア) 1GbE インタフェースを 4 ポート以上備えていること。
 - (イ) 10GbE に対応したインターフェースを 4 ポート以上、SFP/SFP+インターフェースを 4 ポート以上有し、いずれかで排他制御できること。
- (3) 装置間接続用 L2 スイッチ(7台)は、以下の要件を満たすこと。
 - (ア) 1GbE インタフェースを 4 ポート以上備えていること。
 - (イ) 10GbE に対応したインターフェースを 4 ポート以上、SFP/SFP+インターフェースを 4 ポート以上有し、いずれかで排他制御できること。
- (4) SFP インタフェースは、IEEE802.3 規格に準拠した 1000BASE-SX/LX に対応していること。
- (5) SFP/SFP+の 10Gbps ポートを 4 ポート以上有すること。なお、接続先インターフェースに合わせて 10GBASE-SR もしくは 10GBASE-LR から選択可能なこと。

■ セキュリティ要件

- (1) 不正な DHCP サーバの接続を防止できること。
- (2) システムの機能設定情報をパスワード等で保護する機能を有すること。

■ 管理要件

- (1) シリアル接続等のコンソールポートを有すること。
- (2) セキュアなリモート・コンソール機能を有すること。
- (3) NTP または SNTP クライアント機能を有し、一貫したタイムスタンプを刻むことが可能なこと。
- (4) Syslog サーバにメッセージを送信可能のこと。
- (5) SNMPv1/v2c/v3 による管理機能を有すること。
- (6) コマンドや再起動により作成した設定を反映できること。

■ 信頼性要件

- (1) 対外接続用 L3スイッチ(2 台)は、SINET データセンター文京ノード及び武蔵野ノードに接続し、冗長化すること。

2.2.4. リンク負荷分散装置(ロードバランサー)(2台)

負荷分散装置は 2 台用意し、リンク負荷分散及びサーバ負荷分散が可能な冗長化構成とすること。また、大学入試センターの指示に基づき、SSL 証明書の適用を行うこと。

■ 一般機能

- (1) 大学入試センターで稼働しているシステム(試験情報システム, Web 会議(外部サービス), メール等)のサーバ負荷分散ができること(1 つのサーバや通信機器にかかる負荷を軽減し, 停止状態を防ぐ機能を有すること)。なお, これらシステムの負荷分散に当たっては, 試験情報用電子計算機システムの受注者及び大学入試センターと協議の上, その設定をすること。
- (2) 業務に最適なサーバ振り分け(IP アドレス/ポート番号, HTTP ヘッダ, URL 等)を選択できること。
- (3) 様々なアプリケーションやサービスの負荷分散(ロードバランサ)に対応できること。
- (4) IPv6 に対応し, IPv6 環境でのサーバ負荷分散を実現できること。
- (5) サーバの負荷状況を監視し, 負荷分散(ロードバランサ)を制御(負荷計測エンジメント)可能なこと。
- (6) 一連のトランザクションを同一サーバに転送(セッション維持)できること。
- (7) セッションリカバリ機能があり, サーバ故障時でも別サーバとの通信が継続できること。
- (8) SSL アクセラレーター機能を有し, 処理能力は 2,000tps 以上であること。
- (9) IPv4, IPv6 ルーティング機能を有すること。
- (10) IP アドレスとポート番号を対象とした負荷分散処理(レイヤー4ロードバランシング)が可能なこと。
- (11) URI に応じてリクエストを特定のサーバ群に割り振る処理(レイヤー7トラフィック処理)が可能なこと。
- (12) 100,000 セッション/秒以上の負荷分散処理性能を有すること。
- (13) IP アドレスやポート番号, プロトコル, MAC アドレスによるフィルタリングが行えること。

■ ハードウェア要件

- (1) 100BASE-TX/1000BASE-T のインターフェースを 4 ポート以上有すること。
- (2) 10Gbps ポートを 4 ポート以上有し, 接続先インターフェースに合わせて 10GBASE-SR または 10GBASE-LR から選択可能なこと。
- (3) 19 インチラック搭載型とし, 1U 以内に収納可能であること。

■ 管理要件

- (1) セキュアなリモート・コンソール機能を有すること。
- (2) Syslog サーバにメッセージを送信可能なこと。
- (3) NTP または SNTP クライアント機能を有し, 一貫したタイムスタンプを刻むことが可能なこと。

■ 信頼性要件

- (1) 2 台以上による冗長化構成を実現し, 片方に障害が発生しても, 自動的に切

替わり、もう一方により正常な運用が可能であること。

- (2) 障害時の保守サービスを迅速に行うため、監視サーバから監視しその結果により運用保守対応が可能であること。

2.2.5. UTM 装置(統合管理装置を含む)(2台)

通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。

将来、ネットワークが仮想化される可能性を見据え、対応可能な製品を 2 式用意し、冗長化すること。

■ 一般機能

- (1) IPアドレスの変換機能を有し、ルーティング機能を有していること。また、プライベートアドレス(ローカルアドレス)を変換するための NAT 及び NAPT に対応していること。
- (2) DoS/DDoS 攻撃防御機能を有すること。
- (3) IEEE802.3ad リンクアグリゲーション機能を有すること。
- (4) ファイアウォールのポリシー毎にウィルス・スパイウェア、URL フィルタリング等のコンテンツ検査機能を有効/無効の設定が可能であること。
- (5) 脆弱性防御、アンチウィルス、アンチスパイウェア機能を有すること。
- (6) 既知及び未知のあらゆる脅威に対する保護について。
- (ア) 一般的な脅威回避技法が実装されているかに関わらず、エクスプロイト、マルウェア、スパイウェアを含む様々な既知の脅威をブロックできること。
- (イ) ファイルや機密データの無許可の転送を制限し、大学入試センターのシステム及び業務とは関係ない Web の利用を制御できること。また、制御には、カテゴリごとの分類と、最新の URL 情報に基づくフィルタリング機能を有すること。
- (ウ) 未知のマルウェアを識別して悪意ある動作について分析を行い、自動的にシグネチャを作成し更新時に配信できること。
- (エ) クラウドシステムと連携するなど、早期に未知のマルウェアの発見と対策が可能な機能を有すること。
- (7) ボットネット感染が疑われる端末をリストアップするボットネットレポート等の機能を有すること。
- (8) Web UI 上で動的に表示を切り替えることができるリアルタイムレポート機能を搭載し、利用頻度の多いアプリケーション、URL カテゴリ、脅威をランキング形式で表示できること。
- (9) IEEE802.1Q VLAN トランク機能を有すること。

■ ハードウェア要件

- (1) 1000BASE-T インタフェースを 4 ポート以上、SFP+を 4 ポート以上有すること。
- (2) 19 インチラック搭載型とし、2U 以内に収納可能であること。

■ 管理要件

- (1) http 及び https 対応の Web インタフェースを有すること。
- (2) ssh によるコマンドラインインタフェースを有すること。
- (3) 複数台を一元管理が可能であること。
- (4) ログの閲覧が可能であり、他のサーバに Syslog のログ出力が可能なこと。
- (5) ログを保存するためのストレージとして、最適な RAID 構成で 10TB 以上の容量を有すること。なお、「2.5. ログ収集システム」に集約してもよい。

■ 信頼性要件

- (1) ファイアウォール機能を有する装置で、冗長化構成が可能な製品であること。
- (2) Active/Passive, Active/Active いずれかの冗長構成に対応していること。
- (3) ファイアウォールスループットとして IPv4 ファイアウォールスループット 10Gbps 以上、アプリケーション制御スループット 10Gbps 以上以上処理能力を有すること。また、SSL インスペクション実行時にも安定的な運用が可能な処理能力を有すること。
- (4) IPS, アンチウィルス, アンチスパイウェア機能を同時に使用した場合でも 3.0bps 以上の処理能力を有すること。

2.2.6. コアスイッチ(1式)

導入するコアスイッチは、制御ユニット・電源ユニット・ネットワークポート等の構成要素、またはコアスイッチ本体を冗長化可能な構成とし、いずれか一方に障害が発生した場合でも、ネットワーク機能を中断することなく継続運用できること。

■ 一般機能

- (1) 全ての通信モードにおいて全二重通信の機能を有し、インターフェースが独立し、オートネゴシエーションにより全二重／半二重を自動的設定する機能を有すること。
- (2) IPv4／IPv6 に対応できること。
- (3) GEC (Gigabit Ether Channel:リンクアグリゲーション) 機能を有すること。
- (4) QoS (Quality of Service) 機能を有すること。
- (5) ネットワークを介して、ファームウェアのバージョンアップ及びルーティング機能設定情報ソフトウェアをロードあるいはセーブ可能のこと。
- (6) IPv4 パケット処理性能として 900MPPS(Packet per Second)以上を有すること。
- (7) IPv4/IPv6 に対応し、1K 以上のルーティングエントリ数(スタティック)を有すること。
- (8) 64,000 以上の MAC アドレス学習テーブル数を有すること。

■ ハードウェア要件

- (1) 片系あたり、10Gbps 以上に対応した光インターフェースを 12 ポート以上有すること。また、1000BASE-T/10GBASE-T インタフェースを 24 ポート以上有する

こと。

- (2) コアスイッチからサーバ室内の各機器までの帯域は、10Gbps の帯域で接続すること。

■ セキュリティ要件

- (1) システムの設定情報をパスワード等で保護する機能を有すること。
- (2) パケットフィルタリング機能を有すること。
- (3) IEEE802.1x 相当以上の認証機能を有すること。

■ 管理要件

- (1) VLAN (Port VLAN, Tag VLAN) 機能を有していること。
- (2) SNMP, SSH をサポートしていること。

■ 信頼性要件

- (1) 電源ユニットを筐体内で冗長化すること。
- (2) VRRP 等の冗長化機能を有すること。
- (3) 起動時、稼動中、トラブルシューティング時など、機器動作の信頼性を維持するための総合的な自己診断機能を有すること。自己診断機能は稼働中にも任意のタイミングで実行可能であること。

2.2.7. パッチパネル(2式)

ラックマウントタイプのパッチパネルを用意し、コアスイッチから各 EPS 等までの間の光回線を集約する。

■ ハードウェア要件

- (1) ラックマウントタイプで1U であること。
- (2) 適用コネクタは 24 心以上であること。

2.2.8. フロアスイッチ及びエッジスイッチ

L2 スイッチ単位で VLAN を構成し、IP アドレスが付番可能で、以下の仕様を満たす機器とすること。

なお、可能な限り機器を統一するものとし、設置場所のスペース等を踏まえ適切なものを用意すること。

■ 一般機能

- (1) ポート数×1Gbps 以上のスイッチファブリックを実装する固定型の L2 スイッチ製品であること。
- (2) ループ防止機能を有すること。
- (3) IEEE802.1x に準拠した認証機能を有すること。
- (4) IEEE 802.3ad リンクアグリゲーション機能を有すること。
- (5) IEEE802.1p に準拠したパケット優先順位制御が可能なこと。
- (6) 8 千以上の MAC アドレス学習テーブルを有すること。

■ ハードウェア要件

- (1) フロアスイッチは、IEEE802.3 規格に準拠した 1000BASE-T インタフェースを有する機器を用意すること。
- (2) コアスイッチと10Gbps で接続すること。
- (3) 物理コンソールポートを有すること。
- (4) EIA 規格準拠 19 インチラックに搭載可能なこと。

■ セキュリティ要件

- (1) ポートごとに通信可能な MAC アドレス、又は MAC アドレス数を制限できること。
- (2) 不正な DHCP サーバの接続や DHCP メッセージを使った DOS 攻撃を防止できること。
- (3) システムの機能設定情報をパスワード等で保護する機能を有すること。
- (4) QoS (Quality of Service) 機能を有すること。
- (5) パケットフィルタリング機能を有すること。

■ 管理要件

- (1) Web ブラウザを使用して設定を行える機能を有すること。
- (2) SSH によるリモート・コンソール機能を有すること。
- (3) Web 設定画面や CLI 上のコマンド説明が表示できること。
また、コマンドや再起動により作成した設定を反映する機能を有すること。
- (4) トライック解析のためポートのミラーリング機能を有すること。
- (5) ソフトウェア及び設定情報を FTP 又は TFTP にてアップロード及びダウンロードが可能であること。
- (6) NTP 又は SNTP クライアント機能を有し、一貫したタイムスタンプを刻むことが可能のこと。
- (7) DNS を参照し IP アドレスの代わりにホスト名を使用できる機能を有すること。
- (8) Syslog サーバにメッセージを送信可能のこと。
- (9) SNMPv1/v2/v3 による管理機能を有すること。
- (10) VLAN (Port VLAN, Tag VLAN) 機能を有しており、マルチサポートしていること。

■ 信頼性要件

- (1) サーバ室に設置されない機器であるため、動作温度は、0°C～45°Cに対応可能であること。
- (2) 保管温度が 10°C～50°Cに対応可能であること。
- (3) VCCI クラス A に準拠していること。
- (4) サーバ室でなく EPS 又は事務室に設置される機器であり、様々なノイズ源からの影響を受ける可能性が高いため、ノイズ規制 EN61000-3-2,

EN61000-3-3, EN300386 等に準拠していることが望ましい。

- (5) パケット処理性能として 1,330MPPS(packet per second)以上を有すること。

2.2.9. メディアコンバータ(6 台)

スイッチのみで構成可能な場合は、不要。なお、SFP に適用可能な場合は、SFP を用いても良いものとする。

■一般要件

- (1) オートネゴシエーションと 100Mbps Full-Duplex をモード切替する機能有すること。
- (2) 回線は殆どがマルチモードで敷設しているが、マルチモードファイバー(MMF)／シングルモードファイバー(SMF)の両方に対応していることが望ましい。なお、SFP/SFP+ を適用する場合は、1000BASE-SX 又は 1000BASE-LX のいずれかを選択できること。

■ハードウェア要件

- (1) IEEE802.3 規格に準拠した 100/1000BASE-TX インタフェースを1ポート以上有すること。

■信頼性要件

- (1) AC100V で動作し、動作環境は 0~50°C 以上であること。

2.2.10. 無線LANアクセスポイント (20台)

大学入試センターが指定した場所に適切な台数を配置する。

■一般要件

- (1) AutoMDI／MDI-X 機能を有すること。
- (2) NTP 又は SNTP サーバ、クライアント機能を有すること。(コントローラにおける機能で実現可能でも構わない。)
- (3) DHCP クライアント機能を有すること。
- (4) Wi-Fi6 をサポートしていること。また、同時に二つ以上の周波数帯で利用可能のこと。
- (5) 1 台あたり複数の SSID が設定可能なマルチ SSID 機能を有すること。

■セキュリティ要件

- (1) 無線 LAN 端末の通信用インターフェースとアクセスポイント管理用インターフェースを物理ポートで分離することにより、高セキュリティな物理構成が取れること。
- (2) パケットフィルタリング機能(アクセスコントロールリスト機能)を有すること。
- (3) ハードウェアによる AES 暗号化機能を有すること。
- (4) 脆弱性対策をした WPA2 認証、又は WPA3 認証に対応していること。

■管理要件

- (1) Web ブラウザにより設定が可能なこと。
- (2) コマンドの説明を CLI, Web ブラウザ上で表示できること。また、日本語のマニュアルが提供されていること。
- (3) アクセスポイントのコントローラにより、コントローラから一元管理できる機能を有すること。

■信頼性要件

- (1) ポートのペアを現用、待機として経路を冗長化する機能を有すること。
- (2) 有線 LAN 障害時に無線 LAN 接続を自動的に切換する機能を有すること。
- (3) 設定時の誤操作を防止するための機能を有すること。
- (4) 給電インジェクタを有し、無線 LAN アクセスポイントに電源を供給できること。

2.3. サーバ等に関する要件

2.3.1. サーバの基本要件

大学入試センターサーバ室内にサーバを設置する場合、仮想化基盤、クラウドサービスの活用によりサーバ集約を図ること。また、以下の 2.3.1.1 から 2.3.1.4 に記述した内容を物理サーバ及び仮想サーバそれぞれの基本要件とする。

2.3.1.1. 時刻同期

NTP による時刻同期に対応しており、NICT にある NTP サーバと同期させること。

ただし、公開 NTP サーバは、これ以外にも提供されているので、同期させる公開サーバは、大学入試センターと協議し、決定すること。

2.3.1.2. ログレポート機能

ログレポート機能として、HTTP, Syslog, SNMP, SMTP メールに対応していること。

2.3.1.3. ハードウェアの特質、要件

各サーバにおいて個別の指定がある場合、そちらを優先とする。

- (1) EIA 規格準拠 19 インチラックに搭載可能であること。
- (2) CPU については、クロック周波数 2.5GHz 以上で 6 コア以上を有し、8 コア以上拡張可能であること。なお、キャッシュメモリを 20MB 以上有すること。
- (3) メインメモリについては、32GB 以上のメモリを有し、認識すること。また、拡張時には、512GB 以上まで拡張可能であること。
- (4) 補助記憶装置は、次の仕様を満たすこと。なお、SSD 以外のストレージ(アプライアンス装置や Flash モジュール等)を適用する際には製品特性やメリット・デメリットについての資料を提示すること。
 - (ア) OS 格納用として記憶容量が 100GB 以上の SSD をミラーリングとして有すること。

- (イ) ホットスワップをサポートしていること。
- (ウ) データ格納用として、最適なストレージを使用し、最適な RAID で構成すること。
- (エ) ホットスタンバイディスクを 1 個以上有すること。
- (オ) ファイルサーバを除き DVD 光学ドライブを1台、内蔵していること。ただし、メディアのイメージを仮想ドライブとしてサーバ上にマウントできるのであれば、外付け DVD-ROM ドライブ3台の用意で構わない。
- (5) IEEE802.3 規格に準拠した 1000BASE-T 以上に対応したネットワークインターフェースを 2 ポート以上有していること。
- (6) キーボード、ディスプレイは、次の仕様を満たすこと。
 - (ア) ラックマウントタイプとし、ラック内に格納すること。
 - (イ) 日本語対応キーボードであること。
 - (ウ) 17 インチ(ワイド画面も含む)以上の TFT カラー液晶で 1280×1024 ピクセル以上の解像度の入力に対応していること。
 - (エ) 切替えスイッチ等を使用して、他サーバと共有も可とする。
- (7) リモート管理機能として、次の仕様を満たすこと。
 - (ア) サーバ運用を補助するため、2.6. 監視システムと連携すること。
 - (イ) サーバの状態に関係なく、動作可能であること。
 - (ウ) サーバの状態に関係なく、遠隔からサーバ電源/リセット制御を行えること。
 - (エ) サーバの状態に関係なく、リモート管理機能又は監視システムにより、サーバ死活・温度・電源状態を監視する機能を有すること。
 - (オ) 異常の発生を管理者へ通知する機能を有すること。
 - (カ) 管理インターフェースとして、Web インタフェースを有すること。
- (8) その他、次の仕様を満たすこと。
 - (ア) 24 時間×7 日間／週稼動可能な構成とすること。
 - (イ) 無停電電源装置(UPS)と接続し、停電時に安全に停止できること。
 - (ウ) OS 格納用のストレージをバックアップ/リストア可能な、バックアップ装置またはシステムを有すること。
 - (エ) データ格納用のストレージのデータ部分を複数世代、スケジューラで外部保管用メディア又はクラウド上にバックアップ可能であること。
 - (オ) 電源ユニットを二重化しており、ホットスワップに対応していること。
 - (カ) 情報漏出を防止するため、HDD 及び SSD の障害発生等で交換が必要になった場合、故障した HDD/SSD はデータ消去又は破碎すること。なお、交換した HDD/SSD は管理の上、データ消去又は破碎証明書を発行し、提出すること。
 - (キ) なお、サーバをクラウド上に構築するに当たっては、ISMAP に登録されているクラウドサービスを使用すること、及び使用するデータセンターは国内に限ること。

2.3.1.4. ソフトウェア要件

- (1) OS は、マルチユーザ、マルチタスク、TCP/IP ベースのネットワーク機能及びグラフィカルユーザインターフェースを持つサーバ用オペレーティングシステムであること。なお、Windows OS の場合は、クライアントに必要なユーザ CAL(Client Access License)及びリモートアクセス CAL も調達すること。
- (2) 「Microsoft Enterprise Agreement for Government Partners」等のソフトウェアの提供ベンダが用意する大学、独立行政法人を対象としたプログラムを適用し、ソフトウェアライセンス管理の負荷の軽減及び投資対効果の向上を図ること。
- (3) UPS の管理機能により、停電を検出した場合には、システムを自動的にシャットダウンすること。
- (4) バックアップ／リストア可能なソフトウェアを有すること。
- (5) ウィルス対策ソフトウェアは、ウィルス対策ソフトウェア本来の機能に加え、マルウェア（ウィルス、ワーム、ボット等）による脅威に備えるため、マルウェア感染を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。以下の機能・要素を用いたものを適用すること。
 - (ア) ウィルス対策
 - (イ) ファイアウォール機能
 - (ウ) 不正ソフト・マルウェア対策
 - (エ) フィッシング詐欺対策／Web 脅威のブロック
 - (オ) 脆弱性対策
 - (カ) 不正侵入防止機能
 - (6) ウィルス対策ソフトウェアは、履行期間中、最新のパターンファイルを適用すること。
 - (7) 不要な匿名接続を許可しないこと。
 - (8) 各サーバは、以下に記載するマルウェア対策、アクセス制御、証跡管理ができることが望ましい。且つ、統合管理（単一製品等）で実現できることが望ましい。
 - (ア) サーバに対する未知のウィルス・不正プログラム感染等への対策機能として、実行を許可するプログラムをホワイトリスト化し、ホワイトリストに存在しないプログラムの実行を防止できる機能を有すること。
 - (イ) 特権ユーザ(root)を含むシステム管理者であっても、特定のプログラムの実行を防止できる機能を有すること。
 - (ウ) 実行を許可したいプログラムを指定し、ホワイトリストに追加できる機能を有すること。
 - (エ) ホワイトリスト作成時にプログラムのハッシュ値を取得するなど、システムに負荷を掛ける手段は避けること。
 - (オ) サーバへのアクセスを業務上必要な者に限るために、全てのユーザ、プロセスに対して強制的にアクセス制御を実行できる機能を有すること。

- (カ) サーバに対する不正アクセスを防止するために、システム管理者であっても、保護された領域へのアクセスを不可とすることがされること。
 - (キ) ファイルの改ざんなどの不正操作をリアルタイムに検知できること。
 - (ク) セキュリティ事故による被害を最小化するため、サーバ管理者の権限を最少化させることができること。
 - (ケ) セキュリティ事故による被害を最小化するため、サーバ管理者であっても、サーバの重要なサービスや保護されたプロセスは、停止不可とすることがされること。
 - (コ) セキュリティ事故による被害を追跡調査できるよう、ログの改ざん禁止を目的とし、ログに対して特権ユーザー(root)を含め、書き込みや削除の禁止設定をすることがことができる。
 - (サ) セキュリティ事故及び不正の原因を事後に追跡するための機能として、OS 機能では、残らない詳細ログ(OS コマンドレベル)を収集することができること。
- (9) 攻撃に利用されたユーザやプロセス、マルウェアファイルなどを事後に調査するための詳細ログを収集することができること

2.3.2. 外部向け(DMZ)及び内部向けを一組とするサーバの共通事項

以下のサーバ(2.3.2.1～2.3.2.3)は、仮想化基盤により、外部向け、内部向けをそれぞれ構築し、冗長化構成とし、以下の要件を満たすこと。また、それぞれの機能に必要なCPU、メモリ、ストレージを以って構築すること。

なお、詳細なセキュリティ設定条件等は、大学入試センターと打ち合わせの上、決定するものとする。

2.3.2.1 プロキシサーバ

外部向け(OPEN 環境用)の Proxy サーバを用意すること。なお、セキュアな環境を維持するため内向け(CLOSED 環境用)にも Proxy サーバを用意すること。

- (1) WEB/FTP Proxy システムを構築し、PROXY 機能を提供すること。
- (2) OS は、Red Hat Enterprise Linux 9 と同等以上であること。
- (3) http, https の通信に関して、Web プロキシ、キャッシング及び URL フィルタリングを行うこと。
- (4) アクセス制御、認証、ロギング、不正アップロードとウィルス付きコンテンツのダウンロード、HTTP トライフィック管理などとともに、不正確なサーバ証明書が実装されたサーバに対処できること。
- (5) 管理者がカテゴリごとにフィルタリングの有効／無効を切り替えられること。
- (6) フィルタリングは、ユーザのアクセスに対して、警告表示のみと遮断の 2 種類以上が利用する機能を有すること。
- (7) 本機能、性能を満たす場合は、アプライアンス製品での提案も可とする。
- (8) 外部向け Proxy サーバは冗長構成とするが、内部向け Proxy サーバはシン

グル構成とする。

- (9) 外部向け Proxy サーバについてはクラウド上に構築してもよい。

2.3.2.2. DNS サーバ

外部向け、内部向けの DNS サーバを用意すること。

- (1) OS は、Red Hat Enterprise Linux 9 と同等以上であること。
- (2) DNS サーバの構築は、として BIND あるいはこれと同等以上の性能を有するソフトウェアを搭載し、DNS サーバとして機能すること。
- (3) DNS サーバのアドレスを自動的に取得する設定とし、IP アドレス情報を取得し、ドメイン名とリンクさせること。
- (4) ズーンの動的更新を許可し、DNS のクライアント・コンピュータの名前と IP アドレスを、DNS サーバに動的に登録できること。
- (5) 本機能、性能を満たす場合は、アプライアンス製品での提案も可とする。
- (6) 外部向け、内部向けともに DNS サーバについてはクラウド上に構築してもよい。

2.3.2.3. メールサーバ

外部向け、内部向けのメールサーバを用意すること。

- (1) OS は、Red Hat Enterprise Linux 9 と同等以上であること。
- (2) ラックマウントタイプであること。ただし集約化が図られていればこの限りでない。
- (3) Postfix あるいはこれと同等以上の性能を有する MTA(Message Transfer Agent)を搭載し、Mail サーバとして機能すること。
- (4) スパムフィルター機能を有すること。
- (5) メール詐欺を防ぐため DMARC/DKIM/SPF 機能を有すること。
- (6) 外部向け、内部向けともにメールサーバについてはクラウド上に構築してもよい。

2.3.3. シンクライアントシステム(一式)

シンクライアントシステムの共通事項として次の条件を満たすとともに、2.3.3.1～2.3.3.4.に記載する要件を満たすこと。

■一般要件

- (1) シンクライアント端末 180 台以上を管理する機能を有すること。
- (2) シンクライアントシステムの方式としては、OPEN 環境及び CLOSED 環境においてユーザごとに独立した環境を設定できる仮想デスクトップ(VDI)方式とする。
- (3) OPEN 環境 180 台及び CLOSED 環境 30 台が同時に運用可能のこと。CLOSED 環境は約 120 名の利用者が利用可能のこと。OPEN 環境及び CLOSED 環境は利用者ごとの環境を用意すること。
- (4) 管理者がリモート操作からユーザ画面を表示することができ、操作が可能で

あること。

- (5) ネットワークプリンタに対して印刷指示が可能であること。また、印刷環境を各利用者が個別に設定できる機能を有すること。
- (6) 音声ファイルの再生やWEB配信動画の視聴の際、音声の聴取が可能であること。また、音声環境は、各利用者が個別に設定可能であること。
- (7) シンクライアント端末全台から同時利用が可能であること。
- (8) ウィルス対策ソフトウェアを搭載し、動作させること。ソフトウェアのライセンスは、受注者が用意すること。
- (9) ウィルス対策ソフトウェアは、履行期間中、最新のパターンファイルを適用すること。
- (10) 2.3.3.1.のサーバは、Windows Server 2025 同等以上の機能、性能を持つOSを動作させること。
- (11) OPEN 環境の 2.3.3.1./2.3.3.2./2.3.3.3.については、クラウド上に構築してもよいものとする。
- (12) シンクライアントシステムの管理用画面は日本語のUIが提供されること。
- (13) 日本語のマニュアルが提供されるだけでなく、管理画面上にもヒントボタンが提供され、設定方法や注意事項をUI上でも確認できること。
- (14) 仮想環境を構成する各サーバは、環境構築状況や問題の発生状況を正しく確認できるよう、UI上に構成図として視覚的に表示されること。
- (15) サーバの負荷が高い場合、仮想端末の同時起動数を制限することで、サーバ負荷集中による仮想端末不具合を防止できること。
- (16) 仮想端末起動の集中によるサーバの負荷を軽減させるため、あらかじめ仮想端末を起動するスケジュールを設定できること。(曜日 / 時刻)
- (17) 運用管理において、各仮想端末の利用状況を把握するため、仮想端末の操作画面を管理用画面で一覧表示する機能を有すること。また、ログオン/ログオン中(切断)/利用不可/ログオフ中/デスクトップ画面を表示する機能を有すること。

2.3.3.1. シンクライアントサーバ(一式)

■一般要件

- (1) アプリケーションソフトウェアが遅滞なく動作すること。
- (2) OS 及び各種アプリケーションの配信及びパッチの適用が速やかに実施可能であること。
- (3) 一人のユーザに対して複数の環境を割り当てる機能を有すること。
- (4) 座席移動等により、ユーザがある端末から別の端末へ引き継いだ場合でも、同一仮想デスクトップを移動前の状態から持続利用する機能を有すること。
- (5) シンクライアント端末に接続された USB デバイスを仮想デスクトップ上で利用する機能を有すること。また、利用制限もできること。
- (6) USB デバイス使用の許可/不許可を管理側で設定する機能を有すること。
- (7) シンクライアント端末に接続されたイヤホン、マイク、カメラを仮想デスクツ

プ上で利用する機能を有すること。また、利用制限もできること。

- (8) 許可したデバイス以外をシンクライアント端末のパソコンに接続しても、ユーザが利用できない状態とすること。
- (9) USB 接続するマウス及びキーボード等は、ヒューマンインターフェースデバイスとしてUSBのポリシー設定に影響されず利用可能とすること。
- (10)ストレージのディスク消費を抑えるため、マスターイメージを共有利用する機能を有すること。
- (11)パッチ適用やアプリケーションの配布といった、仮想デスクトップ環境展開後の変更においてもマスターイメージを更新することで適用させることができること。
- (12)マスターイメージ以外に仮想デスクトップ上で生じたデータについては、マスターイメージと分離されること。

■ サーバ構築要件

- (1) 複数の同構成のサーバが容易に運用できるよう、サーバイメージ原本取得/配付の仕組みを提供すること。
- (2) CPU、メモリ使用率をホスト間で負荷分散が可能なこと。
- (3) 物理サーバのメンテナンス時に当該サーバで稼働中の仮想デスクトップを停止する必要がないこと。

■ セキュリティ要件

- (1) OS のセキュリティパッチの適用及び OS のアップデートを管理者が自動的に行える機能を有すること。
- (2) 画面転送の通信が暗号化可能であること。
- (3) パソコンから情報漏洩を防ぐため、パソコンに標準装備されたデバイスの遮断・許可、及び、不正なネットワークの利用を制限する機能を有すること。
次のデバイスのポリシーを設定・変更する機能を有すること。
 - (ア) CD/DVD ドライブ
 - (イ) その他の記録メディア
 - (ウ) USB ポート
- (4) 各ポリシー情報など、システムの設定情報は、暗号化されていること。
- (5) 仮想デスクトップ環境の管理権限を分割できる機能を有すること。
- (6) 仮想デスクトップ環境をユーザの部門、業務に応じてグループ単位で管理、展開が可能であること。
- (7) パソコンをログオフした状態でも、パソコンに設定したポリシーが有効であること。
- (8) ポリシーの設定・変更を行なうには、専用パスワードによる認証を必要とすること。
- (9) ポリシーの変更等の操作は、OS ログイン時の利用者権限に依存せず、専用パスワードの保有者だけが行えること。

■管理要件

- (1) 各ユーザの仮想デスクトップにインストールされているアプリケーションの一覧を取得する機能を有すること。
- (2) 仮想デスクトップの展開, 変更, 追加/削除, ユーザーアサインなどの機能を GUI で提供していること。
- (3) 仮想デスクトップ環境の状態を目視可能とする機能を有すること。
- (4) 仮想デスクトップ環境は, コンピュータ名で画面に表示されること。
- (5) 集中管理機能を利用した場合, 各パソコンのポリシー登録・変更作業は, 集中管理機能で定義されるネットワークパスワードによる認証でのみ利用する機能を有すること。

2.3.3.2. シンクライアントシステムストレージ(一式)

■一般要件

- (1) HDD と SSD を併用する場合, I/O 処理の大部分を SSD で処理することで Read と Write の両面で高い I/O 性能を実現していること。
- (2) 重複排除及び圧縮処理を実行し, SSD の容量空間を効率的に使用する機能を有すること。
- (3) 2.3.3.1 シンクライアントサーバ及び 2.3.4 ファイルサーバと集約化してもよい。

■ハードウェア要件

- (1) ハイブリッド HDD 又はオールフラッシュストレージのいずれかで構築すること。
- (2) 実効容量 25TB 以上を有すること。また, 圧縮機能の利用により 50TB 以上の実効容量を有すること。

■管理要件

- (1) 仮想マシン単位で性能を可視化した管理用 GUI を採用していること。なお, Web ベース (HTML5) GUI を備えたストレージ管理ソフトウェアが利用できること。
- (2) 各仮想マシン／仮想デスクトップの稼働状況をグラフィカルに表示できること。
- (3) 装置で発生したイベント通知として Email, SNMP Trap, Syslog Server 等のいずれかで通知する機能を有すること。

■信頼性要件

- (1) SSD 又は, HDD が独立した RAID6 相当以上で冗長化されていること。ただし, キャッシュとして利用される SSD はディスク障害によってデータロストが発生しない場合に限り, RAID 構成を不要とする。

- (2) 仮想マシン単位でのスナップショット機能を有し、4 世代までをサポートすること。
- (3) 日次・週次・月次のスケジュール、及び採取したスナップショット毎に保持期間を設定できること。
- (4) 仮想マシン単位でのクローン機能を有すること。

2.3.3.3. 仮想デスクトップ環境

シンクライアントシステムを利用するユーザ(職員)の仮想デスクトップについて、以下の環境及び機能を有すること。

■一般要件

- (1) 2vCPU、16GB 以上のメモリを搭載していること。
- (2) C ドライブに 150GB 以上を割り当てること。また、ユーザプロファイルとして 50GB 以上を割り当てること。
- (3) センターが指定する既存の各プリンタをシンクライアント環境にて利用できること。また、必要に応じて異なる機種の追加設定が行えること。
- (4) 次のソフトウェアをあらかじめインストールし、ユーザが利用できること。
 - (ア) Microsoft Windows 11 Professional と同等以上のOS
 - (イ) Microsoft Office2024 と同等以上のオフィスソフトウェア
 - (ウ) セキュリティ対策ソフトウェア
 - (エ) 一太郎ビューア
 - (オ) 7Zips 等の圧縮・解凍ツールの最新版
 - (カ) IT 資産管理ソフトウェア
 - (キ) レーザプリンタ等の通常使用するプリンタドライバ(職員が使用できる状態に設定していること。)
- (ク) 各ユーザが個別にインストールしているソフトウェアについては、大学入試センターとの協議の上、対応すること。

2.3.3.4. シンクライアント端末の設定(180 式)

シンクライアントシステムに接続するための端末に必要となる設定を行うこと。シンクライアント端末及び接続するディスプレイ、キーボード、マウス等については、大学入試センターが別途用意するので、受注者はそれに対して必要となるソフトウェアのインストール及び各種設定等を行うこと。

なお、用意するPCはWindows11ProがインストールされたノートPCを想定している。

■一般要件

- (1) シンクライアントシステムで実行された画面情報を表示すること。
- (2) USB メモリ等の外部媒体の利用について管理者が有効／無効を設定する機能を有すること。
- (3) 管理者が遠隔によりパソコンごとに電源のオン／オフの切替え、ストレージに対する環境復元の操作(環境復元モードの ON/OFF)ができること。

また、再起動、スタンバイへの移行、ログオン／ログオフ、メッセージ表示およびコマンド実行による任意のプログラム起動などをスケジュール実行できること。

- (4) PC のストレージへの書込みを行っても元の状態に復元する機能(環境復元)を有すること。ただし、パッチの適用やウィルス対策ソフトウェアのパターンファイルは、最新を維持できること。
- (5) 端末のみで(仮想デスクトップ環境に接続せずに)Webex・Zoom が接続可能のこと。
- (6) 2.3.3.5. のとおり機能により大学入試センター外から仮想デスクトップに接続可能のこと。
- (7) 端末本体は、再起動により設定した初期状態に復帰すること。また、本体端末に設定することなく、設定情報の集中管理が可能であること。
- (8) 端末本体起動時には、端末本体の OS へのログイン操作を必要とせずに仮想デスクトップへのログオン画面を表示させること。
- (9) 2.3.9 ウィルス対策 DB サーバ、2.3.10WSUS サーバからの配信を受けられること。また、自宅へ持ち出した場合には、各サービス事業者からインターネットを介して直接配信を受けられること。

2.3.3.5. リモートアクセス

■一般要件

- (1) 大学入試センター敷地外からも OPEN 環境の仮想デスクトップに接続可能のこと。
- (2) 最大同時に 180 台が接続可能であること。
- (3) 2.3.3.4. で設定したシンクライアント端末からのみリモートアクセスを可能とすること。
- (4) リモートアクセスの際には多要素認証を行うこと。ID・パスワードの他に端末固有情報およびデジタル証明書での認証を行うこと。

2.3.4. ファイルサーバ(一式)

■一般要件

- (1) 各端末に対して、ファイルサーバとして動作すること。OPEN 環境用と CLOSED 環境用の2つの環境分を用意すること。
- (2) 共有領域として、Active Directory に登録されたグループ及びユーザ毎にフォルダ単位で書き込み、参照のアクセス権を個別に設定すること。格納するデータは、各部署等において共有する文書、表計算、画像、音声及び各種アプリケーションで作成したファイルである。
- (3) ユーザが一斉に移動プロファイルをクライアントにダウンロードすることを想定した構成であること。
- (4) 職員全員が同時に接続できるサーバライセンスを有しており、かつデータの読み込み、書き込みが遅滞なく行えることを想定した構成であること。また、日

本語のフォルダ名及びファイル名が不具合なく使用する機能を有すること。

- (5) 個別に利用できる領域として個人領域ファイルサービスを行うこと。格納するデータは、各個人のメール、文書、表計算、データベース、画像、音声、及び各種アプリケーションで作成したファイルである。また、ユーザごとに使用量の制限を行うこと。
- (6) 構成される機器は、電源ユニットを二重化しており、ホットスワップに対応していること。
- (7) 格納するデータは利用者が意識することなく自動的に暗号化して記録する機能を有すること。
- (8) システムを正常にかつ自動的にシャットダウンする機能を有すること。
- (9) ウィルス検索及び駆除等が可能であること。
- (10) 共有領域に対してアクセスログを採取すること。

■ハードウェア要件

- (1) 実効容量として OPEN 環境用を 20TB 以上、CLOSED 環境用を4TB 以上利用可能のこと。
 - (ア) OPEN 環境用 20TB のうち4TB を、各職員の個人領域及び移動プロファイル用の領域、残りの 16TB は共有フォルダ及びスナップショット用の領域とすること。
 - (イ) CLOSED 環境用4TB のうち1TB を、各職員の個人領域及び移動プロファイル用の領域、残りの3TB は共有フォルダ及びスナップショット用の領域とすること。
 - (ウ) ストレージは、ホットスペアストレージを1本以上含めること。
 - (エ) 容量の拡張が可能で、RAID6相当以上で構成すること。

■信頼性要件

- (1) ファイルサービスを行うサーバあるいはノードが、複数台で構成され、障害対策として両現用クラスタ構成(Active/Active)であること。ただし、十分なパフォーマンスが提供できる機器ならば、Active/Standby も可とする。
- (2) 動的に容量増減を可能とするファイルシステムであること。
- (3) 故障したストレージ装置の交換を行う際には、ファイルサーバの運用を停止することなく、交換が可能であり、短時間で利用可能な領域に組み込めるこ。
- (4) 停電発生時に備え、ディスク装置上のキャッシュデータを保護する機構を備えること。
- (5) スケジュールバックアップが実行でき、実行時点におけるボリューム内データブロックのマッピングテーブルが作成できるスナップショット機能を有していること。
- (6) 常にサーバ及びストレージ等の状況を監視し、ハードウェアの障害が発生した場合は、メールによる通報を行えること。
- (7) サーバ等構成機器の動作状況及び管理、保守は、全てネットワーク経由で行

えること。

2.3.5. ファイルサーバ監視システム(一式)

■セキュリティ要件

- (1) ファイルサーバへのアクセスログを収集する機能を有すること。
- (2) ログは、以下の種類を取得可能のこと。
 - (ア) 選択、読み込み、書き込み、コピー、作成、削除、名前変更、印刷
 - (イ) フォルダ作成、フォルダ削除
 - (ウ) ログオン、ログオフ、ログオン失敗
 - (エ) ドメインログオン、ドメインログオン失敗、アクセス拒否
- (3) ファイルの持出し有無を検知するため、ファイルの読み込みとファイルのコピーを分類する機能を有すること。
- (4) あらかじめ指定した条件に一致するアクセスがあった場合、管理者へのアラート通知機能を有すること。

2.3.6. 振る舞い検知管理サーバ

外部攻撃者から大学入試センターネットワークへの標的型サイバー攻撃を検知した場合、直ちにシステム管理者に通知可能なシステムであること。

■一般要件

- (1) DHCP 及び固定 IP について、設定を変更せずに導入できること。
- (2) マルウェア検知対象端末にエージェント(ソフトウェア)をインストールすることなく、導入・運用できること。

■セキュリティ要件

- (1) マルウェアを検知した場合、直ちに感染端末の全ての通信を自動的に遮断できること。
- (2) マルウェアの検知を実施するネットワークセグメントごとに監視できること。(セグメントは 20 以上を想定)
- (3) マルウェア検知の事象は、メールや SNMP トランプによる通知が行えること。通知先のメールアドレスは複数指定できること。
- (4) システム管理者に加え、マルウェア感染端末の利用者にもマルウェア検知について通知できること。
- (5) マルウェア検知時には、感染端末、攻撃対象端末、及び C&C サーバの情報が採取できること。また、攻撃のパターンや攻撃に使用されたツールの情報も採取できること。
- (6) 監視するセグメントのスイッチに接続し、監視できる VLAN 構成数は、20 セグメント以上有していること。
- (7) 禁止アプリケーションの利用端末の検知と自動遮断する機能を有すること。
- (8) 不正な通信を発信している端末をネットワークから切り離し不正な接続を遮断できる機能を有していること。

- (9) 持ち込み PC など、登録されていない機器を検知・遮断する不正接続防止機能を備えていること。
- (10) ファイアウォール等と連携が可能な場合は、連携しマルウェア感染疑義端末を自動検知できること。

2.3.7. IT 資産管理システム

■一般要件

- (1) コンピュータ名や OS バージョンなどの情報を自動取得・管理可能であること。
- (2) 利用されているソフトウェアの情報を自動取得し台帳化する機能を有すること。
- (3) ソフトウェア辞書を活用しライセンス違反を把握する機能を有すること。
- (4) Windows アップデートの適用状況を把握し、デバイスを適切な状態であるかを確認する機能を有すること。

2.3.8. AD/DHCP サーバ(一式)

ドメインコントローラ機能を有し、ディレクトリ DB、主体認証と承認、グループポリシーによる利用者、端末を制御する役割設定すること。OPEN 環境用と CLOSED 環境用の2環境分を用意し、障害発生時の対応のため冗長構成とし、障害発生時には自動的に切り替わること。

■ 一般要件

- (1) OS は Windows Server 2025 相当以上であること。
- (2) MS Windows Server 2025 に搭載される Active Directory と同等以上のドメイン管理が可能であること。
- (3) ユーザの利用者情報、ドメイン管理、アクセス管理等が可能であること。
- (4) ユーザが利用するパソコンの IP アドレスは、執務室に定めた VLAN 構成単位下のアドレスを動的に付与する DHCP 機能を持つこと。また、管理者によって事前定義されたマッピングに基づいて、端末の識別子に応じて IP アドレスの発行ができること。
 - (ア) DHCP サーバで管理している IP アドレス情報は、リリース時間(解放時間(28H 想定):協議の上設定する)を設定すること。
 - (イ) サーバレベル及びスコープレベルのポリシーベースのアドレスの割り当て機能を可能にすること。
- ただし、重複する DHCP オプション設定の場合は、スコープレベルを優先する設定とする。
- (ウ) DHCP サービスの継続的な可用性を実現する機能として、DHCP フェールオーバー環境を構築すること。
- (エ) パケットフィルタリングにより正規の DHCP サーバ以外からの offer、 acknowledgement メッセージを遮断(Untrusted に設定されたポートから offer、 acknowledgement メッセージを遮断)することで、不正な DHCP サーバを防止すること。
- (5) 正規のクライアントになりすまし、MAC アドレスを適当なものに変更しつつ

DHCP サーバに対して IP アドレスを要求することで IP アドレスが枯渇する事態を防ぐため、アドレスプールの枯渋を防止する機能を有すること。

(6) ユーザの端末に DHCP サービスを提供し、Mac アドレス固定で IP アドレスを付与できる機能を有していること。

(7) 機能管理者があらかじめ設定した範囲の IP アドレスや DNS サーバのアドレスなどの情報を端末に自動的に割り当てできる機能を有すること。

なお、サーバやプリンタ及びプロジェクター等の周辺機器及び指定する機器・装置等は、固定 IP アドレスを割り振ること。

■ セキュリティ要件

(1) ワンタイムパスワード機能を有していることが望ましい。

(2) トラップアカウントを設け、当該アカウントを用いた攻撃のためのログイン行為を検知すること。

(3) セキュリティに関する設定については、大学入試センターと協議の上決定すること。

2.3.9. グループウェアサーバ

グループウェアサーバは冗長化構成とし、以下の要件を満たすこと。

■ 一般要件

(1) 納入されるグループウェアソフトウェアが推奨する動作条件以上の処理能力を有すること。

(2) グループウェアソフトウェアは、現在使用しているソフトウェア（サイボウズガルーン 6.0 の最新版）同等以上であり、以下の機能を有すること。

(ア) ポータル

(イ) リンク集

(ウ) スケジュール

(エ) 社内メール

(オ) 掲示板

(カ) ファイル管理

(キ) メモ

(ク) To Do リスト

(ケ) メール

(コ) 通知一覧

(サ) ワークフロー

(シ) グループメール・メーリングリスト

(3) 現行のグループウェアソフトのデータ移行については、業務に支障を来たすことなく移行し、引き渡し後直ちに運用できること。

(4) 各端末やサーバにソフトウェアのインストールを必要としないこと。

■ セキュリティ要件

- (1) ユーザ名別にファイルの書き込み、作成、コピー、名前変更、削除、フォルダの作成及び削除のログを採取すること。
- (2) 収集したログは、データベース形式で保存し、日時、曜日、時間帯等の複数の条件を指定して、アクセスログの検索が可能であること。
- (3) 収集したログは、CSV 形式で自動的にエクスポートが可能であること。

■ハードウェア要件

- (1) OS 領域を除き、提供できる実効容量として 800GB 以上を有すること。
- (2) ログの保存が1年間可能なハードディスク容量を有すること。

■信頼性要件

- (1) グループウェアサーバは冗長構成とすること。ただし、クラウドサービスを使用する場合は除く。

2.3.10. ウィルス定義 DB サーバ

OPEN 環境用と CLOSED 環境用の2つの環境分を用意し、以下の要件を備えたウィルス対策定義サーバを用意すること。

■ 一般要件

- (1) 必要となるウィルス対策ソフトウェアのライセンスを用意すること。
- (2) 430 台以上(OPEN 環境用／CLOSED 環境用仮想デスクトップ及びクライアント端末)に対応してウィルス定義ファイルを提供する機能を有すること。
- (3) ウィルス対策ソフトウェアの動作状況及び更新状況を一括管理するための統合管理機能を有すること。
- (4) ウィルス対策ソフトウェアのウィルスパターン定義情報をインターネット経由で取得し、所内 LAN に接続された端末が起動された際には、自動的に最新のウィルスパターン定義情報を反映させること。
- (5) 大学入試センターが管理するファイルサーバ等についてスケジュールされたウィルススキャンを定期的に実行可能なこととし、短時間で処理できるよう設計すること。なお、ウィルススキャンの実行時間の短縮のため仮想スキャンサーバを複数構築しても構わない。

2.3.11. パッチ管理サーバ

OPEN 環境用と CLOSED 環境用の2つの環境分を用意し、以下の要件を備えたパッチ管理サーバを各 1 台用意すること。なお、2.3.10.のウィルス対策定義 DB サーバと兼用しても構わない。

■ 一般要件

- (1) 430 台以上(OPEN 環境用／CLOSED 環境用仮想デスクトップ及びクライアント端末)に対応して Windows 更新プログラムや脆弱性のある修正パッチ等を提供する機能を有すること。
- (2) 更新プログラムやパッチ等をインターネット経由で取得できること。

- (3) 本サーバから所内 LAN に接続されたパーソナルコンピュータへの配信は、スケジュール機能により、設定した日時に配信可能であること。
- (4) 任意のグループごとに複数に分けて、設定した日時に配信できること。
- (5) 本システムで管理する端末の Windows 系 OS の脆弱性パッチ(修正プログラム)を受信／配信できること。

2.3.12. Microsoft License 管理サーバ

WindowsOS, MS Office 等の Microsoft 製品における総合的なライセンス管理を行うため、以下の要件を備えた KMS サーバを1台用意すること。

■ 一般要件

- (1) 総合的なライセンス管理・ライセンス認証ができること。
- (2) ライセンス認証の状態を保つため、クライアントは定期的にアクティベーションを更新できること。

2.3.13. メールセキュリティシステム

以下の要件を備えたメールセキュリティシステムサーバを 1 台用意すること。

■ 一般要件

- (1) MTA 及び外部データベースとの同居が不要であること。
- (2) 管理 GUI は Web ブラウザ上で日本語にて操作可能であること。
- (3) レポート機能を有し、当日分ランキング/送受信結果や、月/日/時間別メール流通量の確認、レポート結果 CSV 出力が可能なこと。
- (4) 送信メールを即時送信せず、一時保留可能なこと。一時保留の時間を指定できること。保留時間設定箇所は、宛先が組織内か組織外かで分かれており、組織内外時間差配送が可能なこと。
- (5) 大容量の添付ファイル付メールを添付しても、自動的にメール本文と添付ファイルとに分割し、添付ファイルのみをセキュアなファイル転送サービスで転送可能であること。
- (6) 複数のルールを組み合わせ一つのセットとして管理し、有効/無効の切替えが可能であること。また、利用者全体やグループごとなど、任意の利用者単位でルールのセットが適用可能であること。
- (7) 添付ファイルのパスワード通知先を任意に指定可能のこと。

■ セキュリティ要件

- (1) メーラーで送信した添付ファイル付きのメールは自動的に「メール本文」と「添付ファイル」を分離し、メール本文はそのまま送信できること。一方、添付ファイルは自動的にファイルが取得できる URL を受信者に通知すること。
- (2) SMTP／SMTPs, POP3／POP3s, IMAP4／IMAP4s の全てに対応しており、平文と暗号化通信の両方に対応していること。
- (3) ユーザが意識することなく、宛先ドメインごとに送信メールの添付ファイル自動暗号化ルール適用を実現できること。

- (4) SMTP 認証(SMTP-Auth)に対応していること。
- (5) 暗号化は ZIP 形式や AES(Advanced Encryption Standard) 256bit 形式で行えること。あわせて、添付ファイル暗号化時の拡張子やファイル名を指定可能のこと。

■ ハードウェア要件

- (1) OS 領域を除き、提供できる実行容量として2TB 以上を有すること。

2.4. バックアップサーバ(1 台)

■ 一般要件

- (1) 本調達におけるグループウェアサーバ、プロキシサーバ、DNS サーバ、メールサーバ、ウィルス対策定義 DB サーバ等に対するバックアップ機能を有すること。
- (2) Windows/Linux 等の OS 混在環境であってもバックアップ可能であること。

2.5. ログ収集システム(1台)

■ 一般要件

- (1) 本調達に係る全てのネットワーク機器、サーバ、ストレージのログを一元管理できること。
- (2) ログ収集システムから出力されたファイルが暗号化されていること。また、出力され暗号化されているファイルを再度読み出しが可能なこと。
- (3) 不正な改ざんを防止するため、ログに対するアクセス制御及び改ざんを検出する機能並びにログを保護する機能を備えていること。
- (4) 収集したログを自動的に圧縮する機能を有すること。
- (5) 表示したレポートを csv 形式、pdf 形式で保存可能のこと。
- (6) 次のとおり分析を実施する。
 - (ア)ウイルス・セキュリティリスク検知件数
 - (イ)プロキシブロック検知件数なお、詳細については、別途、協議の上で決定することとする。
- (7) WEB ブラウザ経由で、ログの検索、分析、レポート表示、レポート出力ができること。
- (8) 検索結果に基づいたアラートの通知、アクション実行が可能のこと。
- (9) ログレポート機能として、HTTP/HTTPPs、Syslog、SNMP、SMTP/SMTPs 等に対応していること。
- (10) 別のシステムでもログ収集システムを利用するため、ログ収集システムにおいてクライアントライセンスが必要な場合には、18 ライセンス分を上乗せして調達すること。
- (11) ログ収集システムについてはクラウド上に構築してもよい。

■ ハードウェア要件

- (1) OS 領域を除き、提供できる実行容量として 20TB 以上を有すること。

2.6. 監視システム(1台)

物理サーバのリモート管理機能、無停電電源装置(UPS)等を監視対象とする監視システムを構築すること。

■ 一般要件

- (1) ネットワーク上の SNMP 情報を元に監視対象のデバイスを検出する機能を有すること。
- (2) IP アドレスの範囲をスキャンして監視対象のデバイスを検出する機能を有すること。
- (3) 監視対象のデバイス同士の接続をグラフィカルに表示する機能を有すること。
- (4) 監視対象の障害の有無が視覚的に確認する機能を有すること。
- (5) SNMP にて取得した情報をグラフィカルにモニタリングする機能を有すること。
- (6) デバイスのネットワーク I/F 毎に通信状況を監視可能なこと。
- (7) 監視対象にて障害が発生した際に、Email, Web アラーム, Windows ポップアップ、外部プログラム、SMNP トрап等でのいずれかで通知する機能を有すること。
- (8) 障害発生時/復旧時に Email にて通知する機能を有すること。
- (9) デバイスの稼働状況のレポートを出力する機能を有すること。
- (10) リモート端末のドライブをサーバのデバイスとして利用する機能を有すること。
- (11) リモートからの電源制御(電源投入/強制再起動)によりサーバを操作する機能を有すること。
- (12) 電源 ON/OFF を伴うサーバのスケジュール運転の設定できる機能を有すること。ただし、UPS の機能で実現できるのであればこの限りではない。
- (13) 故障・異常箇所を確認する機能を有すること
- (14) サーバ監視で取得した情報を定期的に保存可能で、過去のサーバ情報を参考し現在の状態と比較できること
- (15) Web インタフェースは、日本語の表示ができること。
- (16) 振る舞い検知システムとの連携を想定し、機種選定・設計・設定を行うこと。また、既存システムを組み込むうえで、必要となる作業、ネットワーク機器やサーバにおける設計・設定・検証作業を行うこと。

2.7. 無停電電源装置(UPS)(一式)

導入するサーバ等の諸元に基づき、容量を算出し、必要な無停電電源装置(UPS)として、以下の仕様を満たす装置を用意すること。

■ 一般要件

- (1) 本システムでデータ消失等の可能性のあるサーバや重要なネットワーク機器等は、安全性を考慮し、UPS に全て接続すること。
- (2) 導入するサーバ等から算出し、必要な容量の UPS を設置すること。なお、諸元情報は提出すること。ただし、5,000KV 以上の UPS は設置しないこと。

- (3) 管理 OS からゲスト OS をシャットダウンさせるために、仮想マシンの自動停止機能を設定できること。
- (4) 故障予防策として、電源の状態をモニタリングし、電源障害を検知できること。また、信頼性の向上策として、停電を検知した際にネットワーク接続している端末等に同報メッセージの通知が可能なこと。
- (5) バッテリー寿命を監視し、交換時期をLED点灯で判断できること。点灯時、バッテリーを交換すること
- (6) 計画による停止することが可能なこと。

■ ハードウェア要件

- (1) 1台当たり 6U 以下のラックマウント型であること。
- (2) センターの供給定格電圧及び定格容量を考慮し、10,000VA / 8,000W 以下に抑えた構成とすること。また、ステップダウントランスマスフォーマ等を活用し、100V 入力の装置に電力を供給することも可能な構築も可とする。
- (3) 常時商用方式又はラインインタラクティブ方式であり、AC100V 又は AC200V 入出力であること。
- (4) 入力端子形状は、並行 2 極アース付き(NEMA 5-15P/MEMA 5-30P/MEMA L6-30P) 固定とすること。
- (5) IEEE802.3 規格に準拠した 100BASE-TX/1000BASE-T の管理用ポートを 1 つ以上持つこと。

2.8. KVM スイッチ(一式)

2.3. ~ 2.7.の各装置のうちラックマウントタイプについて格納できること。

■ 一般要件

- (1) 導入するサーバの台数に応じた複数台のサーバを接続可能な KVM スイッチ(Keyboard/Video/Mouse switch)を搭載し、未使用時 3U 以下の高さで収納できること。
- (2) ラック搭載型のフラットディスプレイ(キーボード付き)を搭載し、対角 17 インチ以上で解像度 1280×1024において 1677 万色以上表示可能な TFT 液晶ディスプレイを有していること。
- (3) 日本語キーボード機能を有していること。
- (4) ポインティングデバイスを有していること。
- (5) 設置及びサーバの収納については、大学入試センターの指示に従うこと。

2.9. 財務会計システム(一式)

2.9.1. 会計システム管理サーバ(1 式)

■ 一般要件

- (1) OS は VMware vSphere 7 と同等以上であること。ただし、使用するソフトウェアやミドルウェア等が対応していない場合には、大学入試センターからの指示によりライセンスのダウングレードをすること。

- (2) 財務会計向けとして
- (ア) AP/DB サーバ用として、仮想 OS は Red Hat Enterprise Linux 9 相当を用意し、大学入試センターからの指示によりダウングレードが可能であること。
なお、RHEL8系が使用可能なライセンスであること。
- (イ) CPU:コア数 6 以上、メモリ:28GB、ストレージ:2.4TB 以上を割り当てること。
- (ウ) SVF for PDF を用意すること。ただし、インストール作業は財務会計システム担当事業者が行う。
- (3) 旅費精算向けとして
- (ア) C/S サーバ用として、仮想 OS は Windows Server2022 相当であること。
- (イ) CPU:コア数 4 以上、メモリ:12GB 以上、ストレージ(OS 含む):1TB 以上を割り当てること。
- (ウ) 必要なソフトウェアやデータベース(Oracle)のインストール作業は財務会計システム担当事業者が行う。
- (エ) RMS-CAL 及びデバイス CAL は最低数(5 個)のライセンスを用意すること。

■ セキュリティ要件

- (1) ウイルス対策ソフトウェアを有すること。
- (2) ウイルス対策ソフトウェアは、履行期間中、最新のパターンファイルを適用すること。
- (3) 各サーバは、マルウェア対策、アクセス制御、証跡管理を行うこと。

■ ハードウェア要件

- (1) 内蔵は SSD で 600GB 以上のストレージ 4 本以上でホットスペアディスク1本以上を含む RAID1+0 若しくは RAID5 で構成し、提供できる実効容量として 4.2TB 以上を有すること。
- (2) メモリは、42GB 以上有すること。
- (3) DVD-ROM 機能を有するドライブを有すること。
- (4) 1000BASE-T に対応したネットワークインターフェースを 2 ポート以上有していること
- (5) ラックマウントタイプであること。ただし集約化が図られていればこの限りでない。

■ 管理要件

- (1) サーバの状態に関係なく動作可能なりモート管理機能を有すること。
- (2) リモート管理機能は、サーバの状態に関係なく、遠隔からサーバ電源/リセット制御を行えること。
- (3) リモート管理機能又は監視システムにより、サーバの状態に関係なく、以下の項目が監視する機能を有すること。
- (ア) サーバ死活
- (イ) 温度

(ウ) 電源

- (4) リモート管理機能は、異常の発生をリモートへ通知する機能を有し、管理インターフェースとして、Web インタフェースを有すること。
- (5) 収集したログはデータベース形式で保存し、日時、曜日、時間帯等の複数の条件を指定して、アクセスログの検索が可能であること。

■ 信頼性要件

- (1) UPS を有し、UPS からの停電信号を受けシステムを正常にかつ自動的にシャットダウンする機能を有すること。ただし、集約化されていれば個々に設置なくともよい。
- (2) 構成される機器は電源ユニットを二重化しており、ホットプラグに対応していること。
- (3) 各サーバ内でデータをバックアップすること。
- (4) ディスクドライブの診断を行うことにより、故障の予兆監視が可能であること。予防交換が必要と判断したディスクドライブについて、冗長性を維持した状態でホットスペアディスクドライブへデータを自動コピーし、コピー完了後に自動切替えを行う機能を有すること。

2.9.2. 会計システム管理用パソコン(1台)

■ 一般/ハードウェア要件

- (1) デスクトップ省スペース型パソコンであること。
- (2) OS は、Microsoft Windows 11 Professional 相当以上を用意すること。
- (3) CPU は、3.2GHz 以上であること。
- (4) システムメモリについては、32GB 以上のメモリを有すること。
- (5) ストレージは 200GB 以上の容量 SSD 装置を内蔵すること。
- (6) DVD ドライブを有すること。
- (7) 15 インチ以上で解像度 1280×1024において、1677 万色以上表示可能なディスプレイを有すること。
- (8) JIS 配列若しくは OADG 配列準拠の 109 又は 109A 日本語キーボードを有すること。
- (9) ポイントティングデバイスとしてホイール付き 2 ボタンマウスを有すること。
- (10) RS-232C D-SUB9 ピン(オス)のシリアルポートを 1 個以上有すること。
- (11) インタフェースは、1000BASE-T 対応のポートを有すること。
- (12) USB 3.0 準拠以上の USB ポートを 3 個以上有すること。
- (13) マルウェア(ウィルス、ワーム、ボット等)による脅威に備えるため、マルウェアの感染を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。
- (14) アンチウィルスソフトウェアは、履行期間中、最新のパターンファイルを適用すること。
- (15) Microsoft Office 2024 Professional と同等以上の日本語ワープロ、表計算ソフ

トウェア、データベースシステム、プレゼンテーションソフトウェアを含む統合オフィスソフトウェアの入手及びインストールを代行すること。

(16) 筐体は、横置きが可能であること。

(17) その他、次の仕様を満たすこと。

(ア) 製造事業者において、法人向け製品として製造・販売されていること。

(イ) 情報漏出を防止するため、HDD/SSD 障害発生時に当該 HDD/SSD を取り外し交換した場合、故障した HDD/SSD は破碎すること。なお、HDD/SSD の破碎証明書(破碎前後の写真含む)を発行し、提出すること。

(18) 環境配慮に関して、次の仕様を満たすこと。

(ア) 省エネ法に基づくエネルギー消費効率について、省エネ基準達成率が AA 以上であること。

2.9.3. 無停電電源装置(UPS)(一式)

財務会計システム向けの無停電電源装置(UPS)として、以下の仕様を満たすハードウェアを納入すること。

■ ハードウェア要件

- (1) 本システムでデータ消失等の可能性のあるサーバや重要なネットワーク機器等は、安全性を考慮し、UPS に全て接続すること。
- (2) 3U 以下のラックマウント型であること。
- (3) 常時商用方式であり、AC100V もしくは AC200V の入出力であること。
- (4) 入力端子形状は、並行 2 極アース付き(NEMA 5-15P)固定とすること。
- (5) IEEE802.3 規格に準拠した 100BASE-TX/1000BASE-T の管理用ポートを 1 つ以上持つこと。
- (6) 導入機器の消費電力、接続形態、無停電電源装置のバッテリ容量を考慮すること。

2.10. フットクライアント端末の設定(40 台)

各職員が執務室や会議室で利用するための端末。シンクライアントシステムへの接続は行わない。それ以外の OPEN 環境(ネットワーク含む)への接続・利用を可能とすること。フットクライアント端末については、大学入試センターが別途用意するので、受注者はそれに対して必要となるソフトウェアのインストール及び各種設定等を行うこと。

なお、用意する PC は Windows11Pro がインストールされたノート PC を想定している。

■ 一般要件

- (1) USB メモリ等の外部媒体の利用について管理者が有効／無効を設定する機能を有すること。
- (2) 管理者が遠隔によりパソコンごとに電源のオン／オフの切替え、ストレージに対する環境復元の操作(環境復元モードの ON/OFF)ができること。また、再起動、スタンバイへの移行、ログオン／ログオフ、メッセージ表示およびコマン

- ド実行による任意のプログラム起動などをスケジュール実行できること。
- (3) PC のストレージへの書き込みを制限する機能(環境復元)を有すること。ただし、パッチの適用やウィルス対策ソフトウェアのパターンファイルは、最新を維持できること。
 - (4) 端末本体は、再起動により設定した初期状態に復帰すること。また、本体端末に設定をすることなく、設定情報の集中管理が可能であること。
 - (5) 2.3.9 ウィルス対策 DB サーバ、2.3.10 WSUS サーバからの配信を受けられること。また、自宅へ持ち出した場合には、各サービス事業者からインターネットを介して直接配信を受けられること。
 - (6) 次のソフトウェアをあらかじめインストールし、ユーザが利用できること。
 - (ア) Microsoft Office2024 と同等以上のオフィスソフトウェア
 - (イ) セキュリティ対策ソフトウェア
 - (ウ) 一太郎ビューア
 - (エ) 7Zips 等の圧縮・解凍ツールの最新版
 - (オ) IT 資産管理ソフトウェア
 - (カ) レーザプリンタ等の通常使用するプリンタドライバ

2.11. データ移行

移行作業においては、業務系電子計算機システムの利用方法及び運用管理办法を考慮した上で、提案・入札及びシステム構築作業を行うこと。また、既存システムを継続利用しているので、これらの業務に影響しない形での構築作業及び移行作業を行うこと。

現行稼働中のシステムから下記のデータとサービスを引き継ぎ稼働させること。なお、移行の詳細範囲については、移行計画書を作成し、大学入試センターと協議し、指示に従うこと。

- (1) ネットワーク機器の設定については、現行システムの設定を踏襲するものとするが、変更が必要な場合、事前に大学入学センターと協議すること。
- (2) 現行利用者管理サーバにて保持しているユーザアカウント情報(200 名)
- (3) 現行ファイルサーバにて保持している各部署の全てのデータ(約 8TB)
- (4) 現行ファイルサーバ監視システムのデータを移行すること。ただし、現行の CLOSED 環境のファイルサーバにあるデータの移行に当たっては、大学入試センターの担当者と協議のうえ、移行先を決定すること。
- (5) 現行のガルーンの掲示板文書データと全メールデータ、予定データをユーザアカウント毎に移行する。
ただし、掲示板文書データは、一旦全てバックアップし、直近の過去2年分を有効データとして移行する。(約1TB)
- (6) ウィルス対策用パラメータやパターンファイルデータは、同一製品のソフトウェアの場合に限り、セキュリティ対策管理サーバよりウィルス対策サービスを移行する。(1GB)
- (7) 現行のシンクライアント環境(デスクトップ等)からの移行(80GB×160 台)

- (8) ユーザ毎のブラウザのお気に入り情報
- (9) 財務会計システムについては、当該システム担当者の指示に従い移行すること。
なお、移行作業は、あらかじめ協議のうえ、現行システムのインストール作業、データ移行等の作業内容を確認し、決定すること。また、移行後はシステムの動作検証をすること。
- (10)シンクライアントシステムの移行に当たっては、以下の点を留意すること。
 - (ア) 各端末にアプリケーションソフトウェアの導入作業を実施すること。
 - (イ) アプリケーションの動作確認は、受注者側で実施すること。
 - (ウ) シンクライアント環境での動作をサポートしないソフトウェアについては、大学入試センターと協議の上、導入作業の対象から除外すること。
 - (エ) Active Directory で登録されたユーザ名とパスワードでシンクライアントにログインさせること。
- (11)各職員は、管理者が特別に認めた場合を除き、アプリケーションのセットアップ制限やアクセス制限を受けた一般ユーザの権限で利用できること。

第3章 保守要件

3.1. 基本要件

本件は日常のヘルプデスク対応は行わず、運用管理事業者(ヘルプデスク)を支援するものである。運用管理事業者が一次切り分けや一次回答ができるようドキュメント等を整備すること。

以下の保守やサポートの実績については、翌月(営業日の3日まで)に報告書を提出すること。

なお、保守作業の内容(日時、担当、原因、調査、対策)や交換部品等が明記された作業完了報告書を都度提出すること。

と。また、サポートについては、日時別にまとめ、完了・未完了・完了予定等が判別できること。様式については、A4縦書式とし、Microsoft Office 2024(Word, Excel)以降で作成したものとする。

- (1) 受注者は、次の(2)～(7)に示す条件を満たす保守体制を用意すること。なお、保守対応とは、問い合わせ受付窓口対応、システム保守対応、ハードウェア保守対応、ソフトウェア保守対応の総称を示すものとする。
- (2) 保守期間は、履行期間が終了するまでとする。なお、保守期間中にハードウェア及びソフトウェアのサポート期間が終了しないこと。
- (3) 受注者は、保守対応における責任体制を明確にするため、担当者名を明記した保守体制図を提出すること。なお、体制を変更する必要が生じた場合には、変更内容を記載した書面をもって報告し、大学入試センターの承諾を得ること。
- (4) 障害発生時には、大学入試センター及び運用管理事業者と綿密な調整・連携を行い、受注者の責任と負担で保守作業を行うこと。
- (5) 調達機器について、技術的サポートを行うこと。また、今後の運用中に調達機器と他の機器との接続及び別途調達したソフトウェアを大学入試センター又は運用管理事業者がインストールするような場合、大学入試センターと密接に連絡が取れる体制にあり、連絡があった場合は支援すること。
- (6) サーバ及びネットワーク機器に障害が発生したときは、受注者は、大学入試センター又は運用管理事業者からの連絡を受けてから4時間以内に状況の確認、原因の調査を開始すること。なお、障害状況の確認後4時間以内にシステムを復旧させること。

ただし、復旧が困難な障害については、3営業日以内に解決を目指すこととし、それ以上時間を要する場合には、大学入試センターと協議の上、善後策を講じること。発生した障害が、大学入試センターの業務に支障を来す重大なもの場合には、暫定的な処置を施し、業務への影響を取り除いた上で、3営業日以内の解決を目指すこと。

- (7) 保守対応は、日本語で実施すること。

3.2. 問い合わせ受付窓口対応

- (1) 受注者は、大学入試センター及び運用管理事業者からの本システムに関する問い合わせや、各種保守対応依頼を一元的に受け付ける問い合わせ受付窓口を設け、大学入試センターに対して適切な回答ができるように、提案するシステム、稼動させるハードウェア、ネットワーク、セキュリティの環境、特性を熟知し、十分な技術支援、運用支援体制を有すること。
- (ア) 電話、電子メール、FAX等による保守・運用に関する技術的問い合わせに対応する体制を有すること。
- (イ) 受注者は、提案するシステムの機能修正、不具合対応等、運用に必要な情報を提供すること。
- (ウ) 受注者は、連絡体制、担当保守員を含む保守体制を記載した資料を提出すること。
- (エ) 大学入試センターにおけるサーバ及びネットワーク機器に障害が発生した際には、受注者の受付後 4 時間以内に保守員が到着し、状況の確認、原因の調査を開始すること。なお、システムの復旧は、障害状況の確認後 4 時間以内に実施し、報告書を提出すること。
- ただし、復旧が困難な障害については、3 営業日以内に解決を目指すこととし、それ以上時間を要する場合には、大学入試センターと協議の上、善後策を講じること。発生した障害が、大学入試センターの業務に支障を来す重大なもの場合には、暫定的な処置を施し、業務への影響を取り除いた上で、3 営業日以内の解決を目指すこと。
- (オ) 本システムのプログラムの不具合、システムの不具合によるシステム修正については、迅速に改修作業を行うこと。
- (カ) 障害対応や不具合対応等に対応するため、導入するサーバ等機器、ミドルウェア及びソフトウェア等のサポート契約について本調達に含めること。
- (キ) 提案するシステムの運用に、影響を及ぼす恐れのあるセキュリティ情報を速やかに提供すること。
- (ク) 大学入試センターからの照会は、2時間以内に回答するよう努め、照会内容は全て記録(照会者、照会日時、電話・メール等の照会方法、完了の有無を含む)し、以下を網羅した内容の報告書を月初めに提出すること。
- (2) システム保守の受付時間(24H／365 日)は、電話によるサポートを隨時行うこと。
- (3) 大学入試センターからの問い合わせをインシデントとして管理し、インシデントのクローズまで、対応を継続すること。
- (4) 障害について対応したときは、障害報告書を作成し、大学入試センターに報告すること。

3.3. システム保守対応

- (1) 本調達システムにおいて、運用開始後、障害発生時の一時切り分け及び運用管理支援については、運用管理事業者が行うこととする。なお、重大障害発生時や切り分け困難時等、本調達で納品されたハードウェア及びソフトウェアの各

製造元(メーカー)が単独では解決できない事象発生を想定し、受注者において、ハードウェア・ソフトウェアで構成されるシステム全体の保守を実施すること。

- (2) 受注者は、対応依頼を受け付けた障害を解消するため、適切かつ迅速な対応を行うこと。必要に応じて、各メーカーと協力し、ハードウェア保守対応、ソフトウェア保守対応を行うこと。
- (3) システム保守対応の対応時間は、問い合わせ受付窓口対応の受付時間に準ずる。ただし、対象製品の故障の重要度、緊急度が大きいと判断した場合、大学入試センターから要請した場合は、この限りでない。なお、対応時間外のシステム保守対応については、本調達に含まないものとする。
- (4) 発生した障害に対して解析を行い、原因を究明し、再発防止策を検討し、対策を施すこと。

サーバ及びネットワーク機器等のシステムに障害が発生したときは、受注者の受付後2時間以内に状況の確認、原因の調査を開始すること。なお、障害状況の確認後、原則4時間以内にシステムを復旧させること。

ただし、復旧が困難な障害については、3営業日以内に解決を目指すこととし、それ以上時間を要する場合には、大学入試センターと協議の上、善後策を講じること。発生した障害が、大学入試センターの業務に支障を来す重大なもの場合には、暫定的な処置を施し、業務への影響を取り除いた上で、3営業日以内の解決を目指すこと。

- (5) 年に1～2回程度、休日における停電作業を予定しているため、作業に伴い障害が発生した際には、保守対応を行うこと。特に、大学入試センターの業務に支障を来す重要な障害が発生した場合には、当日中に復旧させること。

ただし、当日中の復旧は暫定対応とし、3営業日以内の解決を目指すことも構わない。なお、障害復旧に係るOSやバックアップデータのリストア作業は、運用管理業者が実施するため、本調達の範囲外とする。

- (6) 大学入学共通テスト実施時期における障害発生等、不測の事態に備え、事前に協議の上、センター内で保守対応のため、12日間程度の待機を要請する。

【内訳】本試験・追試験の実施日(4日間)、採点期間(8日間)、成績提供(4日間)

- (7) 本調達内容に関する大学入試センター及び運用管理事業者からの問い合わせ、相談に応じること。なお、「実施要項(案)別紙2」の他業者と連携対応を含む。

3.4. ハードウェア保守対応

- (1) 各ハードウェア障害時には、当該機器又はそれを構成する部品等の調達・交換・修理等を迅速に行う等、受注者の負担により常時正常な稼動を保証すること
- (2) 本調達機器の保守に関して、メーカー等が提供するハードウェア保守サービスに準ずる安定したサポート及び保守サービス品質の維持を図ること。なお、サーバ及びネットワーク機器の保守サービスレベルについては、24時間×7日間／

週のオンサイト保守対応とすること。

少額部材等の場合には、提供しているメーカー等が提供している一般的な内容の保守を提供すること。

- (3) 調達機器に障害が発生した場合、(2)の保守サービスレベルの範囲で、ハードウェア障害と判断された時点から、原則4時間以内に保守員を派遣し、障害装置の修復、故障部品の修理にあたるものとする。なお、賃貸借及び保守期間中は、必要な交換部品を必ず提供することが可能のこと。
- (4) 受注者は、問い合わせ受付窓口対応の受付時間外における障害に備えるため、各ハードウェア及びソフトウェアのメーカー等へ、大学入試センター及び運用管理事業者から直接問い合わせが可能な窓口を用意すること。
- (5) ハードウェアの修理又は交換を行う際に、ラックからの取り外しや、据え付け・調整作業が必要な場合は、実施すること。また、必要に応じて、大学入試センターと協議のうえ、設定内容の再投入等、設定作業を行うこと。
- (6) 修理対応後、障害個所の修理又は交換後、機器が適正に機能するか動作確認すること。大学入試センター及び運用管理事業者と連携が必要な場合には、連携すること。
- (7) 保守期間中、ハードウェアに対する修正ファームウェアの適用要否に関する情報を大学入試センターに対し提供すること。また、大学入試センターがファームウェアの修正が必要と判断した場合、受注者が適用作業を行うこと。大学入試センター及び運用管理事業者と連携が必要な場合には、連携すること。
- (8) 本調達ハードウェアに搭載されたHDD／SSDに障害が発生した際に、当該HDD／SSDを取り外し交換した場合、故障したHDD/SSDは破碎すること。なお、HDD/SSDの破碎証明書(破碎前後の写真含む)を発行し、提出すること。

3.5. ソフトウェア保守対応

- (1) 受注者は、ソフトウェア(OS含む)に関する問い合わせ、セキュリティ情報等の提供、障害発生時における解決支援に対応すること。
- (2) 納入したソフトウェアに対する修正パッチ及び修正モジュールがメーカーより提供された場合、大学入試センター又は運用管理業者によるこれらの適用要否の問い合わせに対しては、対応を行うこと。

修正パッチ及び修正モジュールの適用については、運用管理事業者にて実施するものとする。なお、適用中に不測の事態が発生した場合には、大学入試センター又は運用管理事業者からの問い合わせに対しては遅滞なく対応すること。

【別表】評価項目一覧

評価項目	評価基準	評価種別	配点	提案書記載箇所	評価	得点
1. 本業務の実施姿勢に関する基本的な評価						
提案内容の妥当性	提案内容は仕様書等に記載されている要求要件が網羅されており、かつ、本業務の実施に当たっての準備・調整に配慮されていること。	必須	50			
	本業務の内容・目的を理解し、目的に沿った妥当な提案であること。	加点	50			
	提案内容は、論理的に整理されており、わかりやすく、具体的に記載されていること。	加点	30			
2. 本業務の提案内容への評価						
全般に係る業務	本業務遂行に足る体制の提案であること。仕様書に記載の経験・能力・実績・資格を有すること。適正な人数で体制を構築していること。	必須	10			
	役務作業について、仕様書等に記載している要求要件を満たす提案となっていること。	必須	10			
	役務作業について、妥当性のあるスケジュール・業務手順がわかりやすく、具体的に記載されていること。	加点	20			
	導入するシステムの保守について、仕様書等に記載している要求要件を満たす提案となっていること。	必須	10			
	導入するシステムの保守について、合理性・妥当性を考慮した上で、要求要件を超える提案であること。	加点	30			
	契約条件等について、仕様書等に記載している要求要件を満たす提案となっていること。	必須	10			
	本業務に係る情報の取り扱い、法令等の順守等について、十分に理解しているか。	加点	30			
	システム利用者（大学入試センター教職員）及び管理者のユーザビリティに配慮した提案であること。	加点	50			
	大学入試センターのBCP（事業継続計画）対策に寄与する提案であること。	加点	50			
導入機器等	導入する機器は、仕様書等に記載している要求要件を満たす提案となっていること。	必須	10			
	ネットワーク接続機器について、安定性の向上についての提案はあるか。	加点	40			
	ネットワーク接続機器について、セキュリティの向上についての提案はあるか。	加点	30			
	ネットワーク接続機器について、通信速度の向上についての提案はあるか。	加点	20			
	ネットワーク接続機器について、管理・運用の利便性向上の向上についての提案はあるか。	加点	10			
	特にUTM装置について、セキュリティの向上についての提案はあるか。	加点	50			
	サーバ等について、安定性の向上についての提案はあるか。	加点	50			
	サーバ等について、セキュリティの向上についての提案はあるか。	加点	30			
	サーバ等について、性能の向上についての提案はあるか。	加点	40			
	サーバ等について、管理・運用の利便性向上の向上についての提案はあるか。	加点	10			
	特に外部向け及び内部向けを一組とするサーバについて、安定性の向上についての提案はあるか。	加点	10			
	特に外部向け及び内部向けを一組とするサーバについて、セキュリティの向上についての提案はあるか。	加点	20			
	特にシンクライアントシステムについて、安定性の向上についての提案はあるか。	加点	30			
	特にシンクライアントシステムについて、セキュリティの向上についての提案はあるか。	加点	30			
	特にシンクライアントシステムについて、性能の向上についての提案はあるか。	加点	30			

評価項目	評価基準	評価種別	配点	提案書記載箇所	評価	得点
	特にシンクライアント端末の設定について、端末に要求されるスペックや設定作業のスケジュール等が明確にされていること。	加点	10			
	特にファイルサーバについて、安定性の向上についての提案はあるか。	加点	50			
	特にファイルサーバについて、セキュリティの向上についての提案はあるか。	加点	30			
	特にファイルサーバについて、性能・容量の向上についての提案はあるか。	加点	30			
	特にメールセキュリティシステムについて、セキュリティの向上についての提案はあるか。	加点	20			
	特にログ収集システムについて、対象となるログと必要となるストレージ容量が明確にされていること。	加点	10			
	特にファットクライアント端末の設定について、端末に要求されるスペックや設定作業のスケジュール等が明確にされていること。	加点	10			
	データ移行について、妥当性のあるスケジュール・業務手順がわかりやすく、具体的に記載されていること。	加点	40			

ワーク・ライフ・バランス等の推進に関する指標

ワーク・ライフ・バランス等の推進に関する指標	<p>女性の職業生活における活躍の推進に関する法律（女性活躍推進法）に基づく認定（えるぼし認定企業・プラチナえるぼし認定企業）等</p> <ul style="list-style-type: none"> ・ プラチナえるぼし (※①) 40 点 ・ えるぼし 3段階目 (※②) 32 点 ・ えるぼし 2段階目 (※②) 28 点 ・ えるぼし 1段階目 (※②) 16 点 ・ 行動計画 (※③) 8 点 <p>※① 女性活躍推進法第12条の規定に基づく認定 ※② 女性活躍推進法第9条の規定に基づく認定 なお、労働時間等の働き方に係る基準は満たすことが必要。 ※③ 常時雇用する労働者の数が100人以下の事業主に限る（計画期間が満了していない行動計画を策定している場合のみ）。</p> <p>次世代育成支援対策推進法（次世代法）に基づく認定（くるみん認定企業・トライくるみん認定企業・プラチナくるみん認定企業）等</p> <ul style="list-style-type: none"> ・ プラチナくるみん (※④) 40 点 ・ くるみん（令和7年4月1日以後の基準） (※⑤) 32 点 ・ くるみん（令和4年4月1日～令和7年3月31日までの基準） (※⑥) 28 点 ・ トライくるみん（令和7年4月1日以後の基準） (※⑦) 28 点 ・ くるみん（平成29年4月1日～令和4年3月31日までの基準） (※⑧) 24 点 ・ トライくるみん（令和4年4月1日～令和7年3月31日までの基準） (※⑨) 20 点 ・ くるみん（平成29年3月31日までの基準） (※⑩) 16 点 ・ 行動計画（令和7年4月1日以後の基準） (※⑪) 8 点 <p>※④ 次世代法第15条の2の規定に基づく認定 ※⑤ 次世代法第13条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則の一部を改正する省令（令和6年厚生労働省令第146号。以下「令和6年改正省令」という。）による改正後の次世代育成支援対策推進法施行規則（以下「新施行規則」という。）第4条第1項第1号及び第2号に掲げる基準による認定 ※⑥ 次世代法第13条の規定に基づく認定のうち、令和6年改正省令による改正前の次世代育成支援対策推進法施行規則第4条第1項第1号及び第2号又は令和6年改正省令附則第2条第2項の規定によりなお従前の例によることとされた令和6年改正省令による改正前の次世代育成支援対策推進法施行規則第4条第1項第1号及び第2号に掲げる基準による認定（ただし、※10及び※12の認定を除く。）</p>	加点	40			
------------------------	---	----	----	--	--	--

評価項目	評価基準	評価種別	配点	提案書記載箇所	評価	得点
	<p>※⑦ 次世代法第13条の規定に基づく認定のうち、新施行規則第4条第1項第3号及び第4号に掲げる基準による認定</p> <p>※⑧ 次世代法第13条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則の一部を改正する省令（令和3年厚生労働省令第185号。以下「令和3年改正省令」という。）による改正前の次世代育成支援対策推進法施行規則第4条又は令和3年改正省令附則第2条第2項の規定によりなお従前の例によることとされた令和3年改正省令による改正前の次世代育成支援対策推進法施行規則第4条に掲げる基準による認定（ただし、※12の認定を除く。）</p> <p>※⑨ 次世代法第13条の規定に基づく認定のうち、令和6年改正省令による改正前の次世代育成支援対策推進法施行規則第4条第1項第3号及び第4号又は令和6年改正省令附則第2条第2項の規定によりなお従前の例によることとされた令和6年改正省令による改正前の次世代育成支援対策推進法施行規則第4条第1項第3号及び第4号に掲げる基準による認定</p> <p>※⑩ 次世代法第13条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則等の一部を改正する省令（平成29年厚生労働省令第31号。以下「平成29年改正省令」という。）による改正前の次世代育成支援対策推進法施行規則第4条又は平成29年改正省令附則第2条第3項に掲げる基準による認定</p> <p>※⑪ 次世代法第12条の規定に基づく一般事業主行動計画のうち、育児休業、介護休業等育児又は家族介護を行う労働者の福祉に関する法律及び次世代育成支援対策推進法の一部を改正する法律（令和6年法律第42号）による改正後の次世代法第12条第5項の規定に基づき令和7年4月1日以後に策定又は変更を行ったもの</p> <p>青少年の雇用の促進等に関する法律（若者雇用促進法）に基づく認定 ・ユースエール認定 32点（複数の認定等に該当する場合は、最も配点が高い区分により加点を行う）</p> <p>※ 内閣府男女共同参画局長の認定等相当確認を受けている外国法人については、相当する各認定等に準じて加点する。</p>					
	合 計 (得 点)	-	1000			-