業務系情報基盤システム一式

仕様書案

（意見招請）

IT Infrastructures for Office Work 1 Set

国立大学法人一橋大学

2024 年 4 月

内容

I.　仕様書概要説明

1.　調達の背景及び目的

一橋大学では、業務系情報システムの情報セキュリティの向上、コンプライアンスの向上、業務の効率化等を実現するために、サーバ機器及びネットワーク機器等の構成を見直した上でオンプレミス型プライベートクラウドを刷新すると共に、情報システム資源の有効活用や運用の合理化を実現してきた。

本調達については、これまでの要件に加え、コスト削減や実態に沿った費用負担を図るためにパブリッククラウド（以下、「クラウド」という。）での構築を目的とし、実施するものである。

2.　調達内容

一橋大学業務系情報基盤システム　一式

（構成内訳）

(1)　クラウド環境

（ⅰ）各仮想サーバ部分

① 仮想サーバ

② ストレージ

③ ネットワーク

（ⅱ)各サービス・機能部分

④ セキュリティサービス（負荷分散、ファイアウォール、WAF、ウィルス対策、パッチ適用 等）

⑤ 運用系サービス（認証、DNS、DHCP、時刻同期、ログ収集、監視、資産管理、メール転送 等）

⑥ リモート接続サービス

⑦ バックアップサービス

⑧ ファイル共有サービス（NAS に相当するもの）

(2)　物理環境（本学サーバ室に残置するもの）

① ファイアウォール装置

② 事務用基幹スイッチ

③ 無停電電源装置

④ 管理操作用端末

なお、これらのシステム等に付帯する設置・導入、5 年間の保守・運用の役務も本調達に含む。

3.　調達の種類

クラウドサービス利用する。また、物理機器については購入とする。

II. 全体要件

1. 納入場所及び納入期限

1.1. 納入場所について、以下のとおりとする。

① クラウドサービスについては、国内のリージョンから選択し構築する。

② 物理機器は本学国立キャンパスとする。

1.2. 納入期限は 2025 年 9 月 30 日（火）とし、本稼働日は 2025 年 10 月 1 日（水）とする。ただし、クラウド基盤については、少なくとも 2025 年 6 月 2 日（月）から各業務システムの構築が開始できるようクラウド基盤を設定し、各サーバを遠隔から操作できるようネットワーク設定作業を終えること。

また、別途調達する事務用端末については、2025 年 7 月から同年 9 月を入れ替え時期と想定している。こちらについても事務用端末構築業者と協力して、進めること。

搬入計画について本学の承認を得ること。

1.3. 指定する期日までに、本システム構築にかかわるすべての作業を終え、本学の希望する状態にすること。すべての機器及び機能についての稼働を確認し受入検査が完了していることを想定する。

2. 納入（搬入、据付、配線、調整等）に関すること

2.1. 本案件に関する作業において、打ち合わせ、現地調査、資料搬入、撤去搬出等で作業員が本学に出入りする場合は、必ず事前に作業員の所属する組織名、組織の住所及び組織の代表電話番号に加えて、各作業員の所属部署、役職、氏名、連絡先（直通電話番号、電子メールアドレス等）を本学に対して通知又は申請し、本学の承認を得ること。本学立入り後は本学の指示に従うこと。

2.2. 納入品の搬入及び設置に関しては、本学施設に損害を与えないように、また、本学業務の妨げにならないように配慮し計画的に行うこと。搬入の日程、機器の据付、配線箇所等については別途本学と協議しその指示に従うこと。

2.3. 本案件に係る作業用資源（機器類等）、作業場所、その他必要となる環境や費用については、受注者の負担で用意すること。

2.4. 機器搬入時に生じる梱包材等は持ち帰ること。

2.5. 受注者が故意又は過失により、本学の建物、機器類等の一部又は全部を、滅失又は毀損した場合は、受注者が直ちに原状に復すること。

2.6. クラウド基盤接続までのネットワークの設計、構築、初期設定及び動作テスト、すべての納入品の搬入、据付及び配線、並びにこれに付帯する工事はすべて受注者が責任をもって実施し、システムの稼働確認を行って報告すること。なお、これらに要する費用はすべて本調達に含まれる。

2.7. すべての物理的な調達機器に対して、本学の指定する様式でラベルを作成・貼付すること。

2.8. ネットワークケーブルには、接続元と接続先が判別できるようなケーブルラベルを作成し

貼付すること。

2.9. 機能、性能に関する要件の各項目で、機器の接続に際し特に記載がない場合でも、要件を満たすのに必要なインタフェース、アダプタ、ケーブル及びドライバーソフトウェア等を実装すること。なお、これらに要する費用はすべて本調達に含まれる。

2.10. 本学ネットワークとの接続及びこれに付帯する設定、調整及び工事はすべて受注者が責任をもって実施すること。ただし、接続に関する実作業については、受注者は現行の保守・運用業者及び本学と協議・調整の上、本学の指示により行うこと。なお、これらに要する費用はすべて本調達に含まれる。また、本学ネットワークとの接続に際しては、本学ネットワークの運用に支障のないよう配慮すること。

2.11. 本調達範囲の各システムの OS、ミドルウェア（クラウド基盤に関連するもの。導入作業期間のみ必要となるものを含む）のインストール、設定及び調整はすべて受注者が責任をもって実施し、利用可能な形で提供すること。ライセンスやインストールメディア等、これらに要する物品及びその費用はすべて本調達に含まれる。ただし、本学が所有するマイクロソフト社の Microsoft 365 Education A3 プログラム（M365 EDU A3 SHRDSVR ALNG SUBSVL PERUSR（ORIGINAL）CAMPUS 3 A）に標準的に含まれるライセンスについては、受注者がこれを利用してシステム構築をしてもよいものとする。

2.12. 受注者はシステム設置調整後、仕様に定められた機能、性能であることを本学担当者の立ち会いのもとで確認すること。

2.13. 本学の都合によりサーバ群、ネットワーク機器等のキャンパス内における移転の必要が生じた際には、対応すること。ただし、移転に係る費用は別途請求とする。

3. 情報セキュリティ要件

3.1. 受注者が実施する作業、構築するシステム、構築するネットワーク、提示する納入物等、受注者の責任範囲にある役務、物品及びシステムに対して、受注者は本仕様書の要件及び本学の指示に基づいて責任をもってセキュリティ対策を実施すること。諸経費は受注者で負担すること。

3.2. 受注者はシステム構築後にセキュリティ専門サービスを提供する第三者によるプラットフォーム診断（ポートスキャン、サービスの情報取得・挙動確認、アプリケーションの脆弱性、脆弱点やアクセス可能ポートに対する侵入等）を実施し、本学に報告書を提出すること。また、運用に支障のない軽微な脆弱性及び本学が許容すると認めたもの以外の脆弱性については対応を行うこと。診断対象は、クラウド基盤に構築する運用系サーバ（別紙 1 での No47～64）、ロードバランサーや WAF 等のセキュリティサービス及びⅢ.2.2.に示す本学に設置する物理ファイアウォール装置（2 台）を想定すること。

3.3. 導入時に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出る事態が発生した場合は、受注者の責任を問い、本学から受注者に対して損害賠償を求め

るものとする。

3.4. 受注者が実施する作業、構築するシステム、構築するネットワークが影響を及ぼす可能性がある他の役務、物品及びシステムに対して、受注者が事前に予測できる範囲内で、本学に対して本仕様書の要件に基づくセキュリティ対策の提案を行うこと。

3.5. 受注者は、システムが構築中であるか完成であるかといった状態にかかわらず、システム及び各ファイルの信頼性とセキュリティを十分に考慮して、以下のセキュリティ対策を施し、システムへの不正侵入や攻撃、ウィルス感染等への防止に万全を期すること。また、システムに関する開発、導入等の一連作業においても、受注者は以下のセキュリティ対策を行うこと。詳細については、受注者と本学で協議して決定すること。

(1) 受注者は、原則として ISO/IEC 15408（JIS X 5070）「情報技術セキュリティ評価基準」によるセキュリティに係る基本設計を行うこと。また、本学からセキュリティポリシー等の提示があった場合は、本学からの提示要件を優先して設計を行うこと。

(2) 不正アクセス及び悪意のあるソフトウェアによる情報の誤用、破壊、破損、改ざんからシステム及びデータを保護するとともに、他のシステム及びネットワークに影響を及ぼすことのない仕組みを持つこと。

(3) システムの動作に必要のないIPアドレスや通信ポートからのリクエストを遮断すること。

(4) 許可しないユーザに不正に侵入されない仕組みを持つこと。

(5) コンテンツ、ログ、設定、環境等を改ざんされないよう対策を講ずること。

(6) セキュリティホールが発見された場合は、パッチ、サービスパック、レベルアップ等の適用といった必要な対策情報を提供し、本学が実施する作業の支援を行うこと。

3.6. セキュリティ事件、事故及びセキュリティの違反については、本学に速やかに報告し、本学の指示に従って対応を行うこと。

3.7. 受注者は、契約不適合責任期間中、上記の対策を講じているにもかかわらず、セキュリティ侵害、各種攻撃、ウィルス感染又はそれらが推測される兆候があった場合は、本学と協議の上、速やかに必要な作業、対策を講じ、サービスを維持すること。

3.8. システムへのアクセス記録が採取可能であり、必要に応じて参照及び電子データ出力が行えること。

3.9. 本学の情報処理設備及び施設の利用は、本学が承認したアクセス方法及びアクセス制御によること。

3.10. 受注者は、個人情報の取扱いについて適切な保護措置を講ずる体制を整備しており、ISO/IEC 27001（JIS Q 27001）「情報セキュリティマネジメントシステム（ISMS）」認証を取得済であること。

3.11. 個人情報の管理の状況について、本学の調査に協力すること。

3.12. 暗号化の際に使用する暗号アルゴリズムについては、「電子政府における調達のために参

照すべき暗号のリスト(CRYPTREC 暗号リスト)」を参照し決定することが望ましい。

3.13. 受注者が本調達・役務内容の一部を外部に再委託する場合は、本学の了解を得なければならない。また、再委託されることにより生ずる脅威に対して、情報セキュリティが十分に確保されるよう本仕様書と同水準の措置の実施を再委託先にも担保すること。

4. 守秘義務及び厳守事項

4.1. 受注者は、案件及び案件に関連する役務過程において知り得た案件に関する一切の情報（以下、「案件に関する情報」という。）について、次の義務を遵守すること。

4.2. 故意又は過失にかかわらず、案件に直接従事する担当者であることを本学が書面にて認めた者以外の者（以下、「他者」という。）に案件に関する情報を漏らさないこと。

4.3. 案件の履行に関連して知り得た本学の秘密情報の加工、改ざん、複写、複製等をしてはならない。ただし、委託契約の範囲内のものや安全管理上必要なバックアップを目的とするものはこの限りではない。

4.4. 契約中は、案件に関する情報の取扱いに十分留意し、他者に情報を開示しないこと。

4.5. 契約終了後は、案件に関する情報を返却し、又は確実に破棄するとともに、本学の書面による許可なく案件に関する情報を他者に開示しないこと。

4.6. 案件に関する情報を知り得た者が、異動、転職、退職等の事由によって案件と無関係になった場合でも、本学の書面による許可なく案件に関する情報を他者に開示させないこと。

4.7. 万が一受注者先において秘密情報の漏えい等の事故が発生した場合は、直ちに本学へ報告し、また、受注者先が責任をもって対応すること。

4.8. 本学秘密情報の取扱いにおいて、再委託をする場合は、本学の了解を得なければならない。本システムの開発及びカスタマイズに関して、業務の再委託を行う場合は、委託先企業についても本義務を遵守させること。

4.9. その他、本学の指示に基づいて守秘義務を全うすること。

5. その他

5.1. 技術仕様等に関する留意事項

5.1.1. 提案書は日本語で具体的に記述すること。

5.1.2. 本調達物品に係る機能、性能、技術等の要求要件（以下、「技術的要件」という。）は、「III 調達物品に備えるべき技術的要件」に示すとおりとする。

5.1.3. 技術的要件は、すべて必須の要求要件とする。技術的要件を満たしていないと判断される提案は、不合格とし落札決定の対象から除外する。

5.1.4. 本調達物品については、原則として全て新品、又は新品と同等の品質を持つもので調達し納品すること。

5.2. 提案に関する留意事項

5.2.1. 提案書には、本仕様書の要件（Ⅱ.全体要件、Ⅲ.調達物品に備えるべき技術的要件、Ⅳ.設置・導入、Ⅴ.保守・運用　に記載の全ての要件）の各項目とそれに対する提案内容を明確かつ簡潔に示した対照表を添付すること。

5.2.2. 提案書には以下の項目を明瞭に記載すること。

5.2.2.1. システムの全体構成

5.2.2.2. 物理・論理ネットワークの構成・機能・性能等にかかわる資料
特に論理ネットワーク構成については、グローバル・プライベート・DMZ 等の別を明示的に示すこと（ネットワークアドレスは仮のもので示せばよい）。

5.2.2.3. ハードウェアの構成・機能・規格・性能等に係る資料

5.2.2.4. システムの設置に必要な電源、面積、重量、環境温度等に係る資料

5.2.2.5. クラウドサービスの構成・機能・性能等に係る資料

5.2.2.6. クラウドサービスの SLA （Service Level Agreement）に係る資料

5.2.2.7. ソフトウェアの構成、規格、性能等に係る資料

5.2.2.8. ソフトウェアの仕様と機能要件を満たしていることを示す具体的資料

5.2.2.9. ソフトウェアの稼働実績を求める項目については、実績を示す資料

5.2.2.10. 導入の作業日程と体制（再委託する場合は委託先の体制も含む）、Ⅱ.3.10.記載の認証取得証明書の写し、受注者側と本学側の作業の区分

5.2.2.11. 保守計画に係る資料

5.2.2.12. イニシャルコスト及びランニングコストの見積りに係る資料

5.2.2.13. その他、提案内容を説明するために必要な資料

5.2.3. 提案書に疑義が生じた場合、詳細な資料の提出を求めることがある。また、必要に応じ、提案物品についてサンプルの提供やデモンストレーションの実施を求めることがある。

5.2.4. 提出要領

5.2.4.1. 提出先及び提出期限は入札説明書を参照すること。

5.2.4.2. 紙媒体で 3 部、電子媒体で 1 部提出すること。

(1) 電子データを格納する媒体の種別は CD-R 又は DVD-R とする。また、データの形式はマイクロソフト社の Office 製品で可読なこと。

(2) 納入媒体及びデータについては、ウィルス等を混入させないように、納入前に受注者側で責任をもってチェックを行うこと。

(3) 紙媒体でしか納入できないもの（手書き図面等）又は電子データのみで納入する方が効率的であるもの（膨大なログデータ等）の納入方法については、受注者と本学が協議して決定すること。

5.2.4.3. 問い合わせの受付については、入札説明書を参照すること。

5.3.　その他の留意事項

5.3.1.　システムの本稼働後、契約期間中にソフトウェア、システム構成、作業等に契約不適合があった場合、本学はこれらの修復、代替物への交換、再作業に加えて、本学が被った損害の賠償を求めることができるものとする。

5.3.2.　本システムの稼働期間は 5 年間を予定している。期間中の保守のほか、クラウド基盤の各種設定変更及び運用条件の変更に伴うシステムの改修等に対応できること。なお、導入開始から本稼働後 5 年間の保守の費用を本調達に含めること。

5.3.3.　導入時、各仮想サーバのリソース等については、3 年間の稼働を見込んだ設定値とし、稼働から 3 年後に再度リソース等のサイジングを行い、それまでの稼働状況等を踏まえ必要に応じてリソース等の追加変更設定を行う想定である。

5.3.4.　本調達により納入された機器の台数追加やクラウド基盤への各種設定変更等が必要になった際には、その費用分について必要に応じて別途契約を行うとともに、増設・追加分の保守については本調達分と一本化すること。なお、本学にて追加作業を行う際には保守の範囲内において支援を行うこと。

5.3.5.　各種設定及び登録は本学担当者と打ち合わせの上実施すること。

5.3.6.　受注者が自社製以外の製品を納入する場合、受注者は一元的な窓口となり、自社製以外の製品についても自社製品と同様の保証をすること。

5.4.　仕様変更及び未定義事項

5.4.1.　案件を遂行する上で役務内容、仕様若しくは条件に疑問点や変更が生じた場合又は本仕様書に記載のない内容の案件が生じた場合、受注者は直ちに本学と協議し、解決に向けて最善の努力を行うこと。

III. 調達物品に備えるべき技術的要件

1. 要件概要

1.1. 本調達はクラウドサービスを主体とした構築を行うこと。その際、本学とクラウド間はSINET 経由で接続を行うこと。

1.2. 本学拠点に設置されている端末からクラウド環境へ接続し、各システムが利用可能なこと。

1.3. クラウドサービス以外で別途用意するハードウェア、ソフトウェア類は、2025 年 10 月から 5 年間保守可能なこと。

1.4. 構築期間中におけるクラウド利用料金については、見積りに含むこと。また、別紙 1 に示すクラウド構成に必要なリソース量を基に構築後のクラウド利用料金を見積もること。

1.5. 別紙 1 にある運用系サーバについて、設計・構築を行うこと。

1.6. 別紙 1 にある業務系サーバについては、必要な仮想サーバ（OS、ミドルウェアを含む）や PaaS、SaaS サービスのデプロイを行い、各システム担当課へ引き渡すこと。その際、初期パラメータが必要な際は、あらかじめ打合せなどを行いデプロイに必要な情報をとりまとめること。引き渡し後の各種チューニングについては、各システム担当課にて行うこととする。

1.7. 各システムの通信要件は、事前に協議しネットワークを設計すること。なお、必要となる通信量は、月間でインバウンド・データ転送量が 7.5TB、アウトバウンド・データ転送量が 27.6TB を想定している。

1.8. 各システムの監視・ログ管理の要件は、事前に協議し設計すること。

1.9. オンプレミス構成での運用をそのまま踏襲するのではなく、クラウド構成における妥当な運用を検討し、設計・構築、運用設計を行うこと。

2. 物理環境における要件

2.1. 共通要件

2.1.1. クラウドサービスで提供可能なサービスや機能については、極力クラウドサービスで実現すること。

2.1.2. サービスを十分提供可能なリソース量（CPU、メモリ、ストレージなど）、ポート数、帯域などを有する製品を選定すること。

2.1.3. 電源、冷却装置などの部品機器は活線挿抜に対応した冗長構成とすること。

2.1.4. GUI でのリモート操作、管理が可能なこと。

2.1.5. 電源は AC 単相 100V とすること。

2.1.6. 国立キャンパスには、EIA 規格準拠の 42 ラックユニットサイズの 19 インチラック（「高さ 2,000mm、横幅：700mm、奥行：1,100mm」を目安とする。）が既設されており、今回導入する機器はラック内に収容可能なサイズであること。

2.2. ネットワーク機器（ファイアウォール）

2.2.1. 19 インチラック搭載可能なタイプであること。

2.2.2. AC100V 電源供給で動作可能であること。

2.2.3. GbE SFP+インタフェースを 8 ポート以上有すること。

2.2.4. 10GbE SFP+インタフェースを 4 ポート以上有すること。

2.2.5. 10GbE SFP+ / 25GbE SFP+インタフェースを 4 ポート以上有すること。

2.2.6. 高さは 1U 以下であること。

2.2.7. 最大同時セッション数は 8,000,000 以上であること。

2.2.8. 最大新規セッション数/秒は 550,000 以上であること。

2.2.9. ファイアウォールスループットは 70Gbps(1518 / 512 / 64 バイト UDP パケット） 以上であること。

2.2.10. ポリシー数は 10,000 以上対応可能なこと。

2.2.11. 専用アプライアンスであること。

2.2.12. 独自ファームウェア(OS)を使用していること。

2.2.13. ファームウェア(OS)は、フラッシュメモリに格納されていること。

2.2.14. Active-Active, Active-Standby の冗長構成が可能なこと。

2.2.15. ASIC を実装することにより高速処理を実現し、且つ、CPU の負荷を軽減する構造となっていること。

2.2.16. ファイアウォール機能として NAT および PAT が可能なこと。

2.2.17. ブリッジ接続による、透過型ファイアウォールとしての機能を有すること。

2.2.18. 仮想ドメインを複数設定可能なことドメイン数は 10 個以上作成できること。

2.2.19. ファイアウォールポリシ毎に UTM 機能の有効・無効の設定が可能なこと。

2.2.20. 仮想ドメインを利用することにより NAT 型ファイアウォールと透過型ファイアウォールが 1 台で混在可能なこと。

2.2.21. ユーザ数によるライセンスは必要ないこと。

2.2.22. 設定は WebUI, CLI いずれにも対応し、且つ、WebUI は日本語対応していること。

2.2.23. WebUI アクセスは http, https ともに可能なこと。

2.2.24. 管理用のアクセスプロトコル(telnet, ssh, http, https, ping, snmp 等)をそれぞれ停止/開始ができること。

2.2.25. OSPF, RIPv2 のルーティングプロトコルに対応すること。また、本学拠点とクラウド間を SINET 経由で接続するために、BGP 機能を持つこと。

2.2.26. SNMPv1, v2c をサポートすること。

2.2.27. NTP クライアント機能をサポートすること。

2.2.28. DHCP サーバ/クライアント/リレー機能をサポートすること。

2.2.29. 設定による物理ポートの停止(ソフトウェアベース)が可能であること。

2.2.30. radius, RSA, LDAP によるユーザ認証をサポートすること。

2.2.31. IPsecVPN 機能を有すること。
2.2.32. PPTP サーバ機能を有すること。
2.2.33. PPPoE クライアント機能を有すること。
2.2.34. IEEE802.1Q VLAN タグを認識すること。
2.2.35. セキュリティポリシー設定の変更時にシステムの再起動を必要としないこと。
2.2.36. 任意の管理アカウントを作成できること。
2.2.37. アラートの種類・深刻度に応じたアラートメールの送信が可能なこと。
2.2.38. ログ(本体メモリや、SYSLOG, 専用ログ管理装置)に出力可能なこと。
2.2.39. アンチウィルス機能のシグネチャは時間、日、週ごとに自動更新可能なこと。
2.2.40. アンチウィルス機能は、HTTP, FTP, SMTP, POP3, IMAP に対応可能なこと。
2.2.41. アンチウィルス機能をファイアウォールのファイアウォールポリシと連係して行うこと。
2.2.42. ウィルス定義ファイルを自社で開発していること。
2.2.43. 不正侵入検知および防御性能は 14Gbps 以上であること。
2.2.44. 不正侵入検知および防御機能のシグネチャは時間、日、週ごとに自動更新可能なこと。
2.2.45. SYN Flood や ICMP Flood に対して閾値を設定することにより、検知・防御可能なこと。
2.2.46. Winny 等の P2P ソフトや AOL, Yahoo, MSN 等のインスタントメッセンジャ(IM)の遮断が可能なこと。
2.2.47. 不正侵入検知および防御機能をファイアウォールのファイアウォールポリシと連係して行うこと。
2.2.48. IPS シグネチャを自社で開発していること。
2.2.49. アンチスパム機能は、SMTP, POP3, IMAP に対応可能なこと。
2.2.50. アンチスパム機能は、外部データベース参照型機能を有し、(1)メール送信元 IP (2)本文内に含まれる URL (3)本文のチェックサムによるスパム判定を行えること。
2.2.51. アンチスパム機能は、DNSBL を利用できること。
2.2.52. アンチスパム機能は、特定の E-mail アドレスや送信元 IP、文字列でブロック可能なこと。
2.2.53. アンチスパム機能でスパム判定時、SMTP の場合：タグ付け及びメール破棄、POP3, IMAP の場合：タグ付けを行えること。
2.2.54. アンチスパム機能をファイアウォールのファイアウォールポリシと連係して行うこと。
2.2.55. WEB フィルタリング機能はファイアウォールポリシ・カテゴリ毎に設定可能なこと。
2.2.56. WEB フィルタリング機能をファイアウォールのファイアウォールポリシと連係して行うこと。
2.2.57. SSL-VPN 機能を有し、ブラウザだけで完結するブラウザオンリーモードと、仮想 NIC を利用するトンネルモード機能を有すること。以下の要件を満たすこと。

2.2.57.1. 遠隔操作のための通信は、暗号化（公開鍵を使用する場合は 2048bit 以上の鍵長を活用する等、十分に安全な暗号を使用すること）を行うこと。

2.2.57.2. ID、パスワード、IP アドレスによる単純認証のみによらない仕組みを用意すること。

2.2.57.3. 通信路は必要な場合以外は常に閉じた状態にしておき、通信路が開かれた場合及び開こうとして失敗した際のログを保存して異常なアクセスがあった場合には、速やかに本学に通知すること。

2.2.57.4. 作成された通信路から保守対象となるシステム以外のシステムにアクセスできない仕組みを構築すること。

2.2.58. アプリケーション識別によるブロック動作や、ログの出力機能を有すること。

2.2.59. リンクアグリゲーション(IEEE P802.3ad)機能を有すること。

2.2.60. ネットワーク機器（ファイアウォール）は、「Ⅲ.2.5.無停電電源装置」と接続すること。

2.3. 事務用基幹スイッチ（ファイアウォール接続用）

2.3.1. 事務用基幹スイッチは 2 台のスイッチによる構成とすること。

2.3.2. 事務用基幹スイッチはスタック機能を用いて、2 台のスイッチを論理的に 1 台のスイッチとして構成すること。

2.3.3. 事務用基幹スイッチを構成する各スイッチはスタック専用のポートを有し、スタック帯域幅は 80Gbps 以上有すること。

2.3.4. 事務用基幹スイッチを構成する各スイッチは 19 インチラックマウント可能であり、1 ラックユニット以内におさまること。

2.3.5. 事務用基幹スイッチを構成する各スイッチは 10GbE ポートを 4 ポート以上有すること。

2.3.6. タグ VLAN（IEEE802.1Q）機能を有すること。

2.3.7. IEEE 802.3ad リンクアグリケーション機能を有すること。

2.3.8. シリアル接続のためのポートとして、USB ポート又は RJ45 ポートが利用可能なこと。

2.3.9. 起動時、稼動中、トラブルシューティングなど、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できること。

2.3.10. ポートにループ等の障害を検知した際、ポートを一時的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。

2.3.11. ルーティングプロトコルとして、Static, RIPv1/v2, RIPng, EIGRP stub に対応していること。

2.3.12. VLAN 情報を他のスイッチに伝播できる機能を有すること。

2.3.13. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。

2.3.14. TELNET、SSH によるリモートアクセスが可能なこと。

2.3.15. 事務用基幹スイッチを構成する各スイッチは 10GbE インタフェース（10GBase-LR）を

１つ用いて、本学既設のネットワーク機器と接続し、IEEE 802.3ad リンクアグリケーションを構成すること。

2.3.16. 事務用基幹スイッチを構成する各スイッチは 1GbE インタフェース（1000Base-T）を１つ用いて、本学のネットワーク機器と接続し、IEEE 802.3ad リンクアグリケーションを構成すること。

2.3.17. 事務用基幹スイッチを構成する各スイッチは 10GbE インタフェース（10GBase-SR）を１つ用いて、「2.2.ネットワーク機器（ファイアウォール)」と接続すること。

2.3.18. 事務用基幹スイッチ（ファイアウォール接続用）は、「Ⅲ.2.5.無停電電源装置」と接続すること。

2.4. 運用管理用スイッチ

2.4.1. 運用管理用スイッチは 1 台で構成すること。

2.4.2. 運用管理用スイッチは 19 インチラックマウント可能であり、1 台あたり 1 ラックユニットにおさまること。

2.4.3. 運用管理用スイッチは、10/100/1000Base-T のインタフェースを 24 ポート以上有すること。

2.4.4. スイッチ帯域幅が 56Gbps 以上であること。

2.4.5. 256MB 以上の Flash メモリを有すること。

2.4.6. 512MB 以上の DRAM を有すること。

2.4.7. VLAN（IEEE802.1Q）機能を有すること。

2.4.8. IEEE 802.3ad リンクアグリケーション機能を有すること。

2.4.9. ポート単位のブロードキャスト、マルチキャスト、及びユニキャストのストーム制御機能を有すること。

2.4.10. シリアル接続のためのポートとして、USB ポート又は RJ45 ポートが利用可能なこと。

2.4.11. TELNET、SSH によるリモートアクセスが可能なこと。

2.4.12. 隣接するデバイス間で、トポロジの管理を行う機能を有すること。

2.4.13. VLAN 情報を他のスイッチに伝播可能なこと。

2.4.14. 運用管理用スイッチはスイッチ 1 台あたり 1GbE インタフェースを 2 つ用いて、「Ⅲ.2.3.事務用基幹スイッチ（ファイアウォール接続用)」と接続すること。

2.4.15. 運用管理用スイッチは、「Ⅲ.2.5.無停電電源装置」と接続すること。

2.5. 無停電電源装置

2.5.1. 商用同期常時インバータ給電方式であること。

2.5.2. バッテリー期待寿命　25℃　5 年／バッテリー交換周期 3～5 年の長寿命バッテリーを搭載すること。

2.5.3. 抜け止めタイプのコンセントを搭載すること。

2.5.4. 契約停電時、接続機器を順次、安全にシャットダウンできる機器を選定すること。

2.6. 管理操作用端末

2.6.1. 管理操作用端末として、KVM コンソールを準備すること。

2.6.2. 管理操作用端末は、既設の 19 インチラックに設置すること。

3. クラウド環境における要件

3.1. 共通要件

3.1.1. 「政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: 通称、ISMAP（イスマップ））」に登録されているクラウドサービスを選定すること。

3.1.2. 保存された情報等に対して日本法に準拠し、国内法令のみが適用されること。

3.1.3. 本調達及び契約に関する紛争は、東京地方裁判所を管轄裁判所とすること。

3.1.4. 基本方針として、IaaS での提案を行うこと。

3.1.5. PaaS、SaaS を利用の際は、技術要素、現行環境で提供している機能に漏れがないことを確認し、設計、構築を行うこと。

3.1.6. 現行のサーバ情報から、適切なクラウドサービス、リソースを選定し、現行環境同等のサービスを提供可能なこと。

3.1.7. 提案する構成については、各サービス、機能が現行システム同様の非機能レベル以上を提供すること。特に冗長構成となっている現行システムのサーバが提供するサービス、機能については、高可用性での提案を行うこと。

3.1.8. 「各サービス・機能要件」を参考にし、適切なクラウドサービスサービスを選定すること。

3.1.9. 本項より下記に記載する要件については一般的に IaaS で構成する際に必要な要件を記載する。機能面、非機能面や価格など、本学において適当なサービスについては PaaS、SaaS での提案をいただきたい。

3.2. クラウドサービス契約

3.2.1. クラウドの支払いについて、毎月本学へ日本円による請求書払いとすること。

3.2.2. 従量課金による後払いに対応できること。

3.2.3. リセールサービス（請求代行）を使用する際、クラウド料金にサービス料金を上乗せする場合は、その旨を伝えること。

3.2.4. 使用しているクラウドサービス、利用料金について、Web 上で確認可能なこと。

3.2.5. 使用しているクラウドサービスについてサポート可能なこと。

3.2.6. 本調達に含まれる OS やミドルウェア等の各種ソフトウェアについて、サポート可能なこと。

3.2.7. サポートは 24 時間 365 日受付可能とすること。

3.3. リージョン

3.3.1. 日本国内から選択できること。

3.3.2. 地理的要因によりデータ転送時間、データ連携時間などが著しく低下し、サービスに影響がないこと。

3.3.3. 本学の機密情報について、国外リージョンで保管及び管理しないこと。

3.4. アカウント

3.4.1. 受託者は本学と協議を行い、クラウドにおけるセキュアなアカウント管理方法を設計すること。

3.4.2. 各クラウドサービスのベストプラクティス、本学の運用状況を考慮した設計、運用とすること。

3.4.3. アカウントの管理方法について、本学へ説明を行い、受託者と本学で運用方法を合意すること。

3.4.4. GUI 操作でのアカウント運用方法だけでなく、CUI 操作で使用するアカウントについても運用方法やソースコード中の扱いについても合意すること。

3.4.5. クラウド環境へログインを行う際、多段階認証を行うこと。

3.4.6. 設計時に組織やアカウント単位で適切な権限設定を行い、必要以上に権限を付与しないこと。

3.4.7. 特権ユーザ、一般ユーザなど、組織やユーザごとに本学運用を踏まえた管理を行うこと。

3.5. コスト管理

3.5.1. クラウド利用に伴うサービス利用料は、常に確認可能なこと。

3.5.2. 各クラウドサービスに、サービス利用料が確認可能なこと。

3.5.3. クラウド利用料に閾値を設け、アラートメールを発報可能なこと。

3.6. ネットワーク

3.6.1. クラウド上に仮想ネットワークを構築し、必要なサービス、機能を提供可能なこと。

3.6.2. ネットワーク構成やセグメント、IP アドレス体系などネットワーク全般に係る内容については、本学と協議し設計、構築を行うこと。

3.6.3. 学内ネットワークとクラウド間を SINET 経由で BGP 接続すること。双方向から通信が可能なこと。

3.6.4. 学内ネットワークとクラウド間の回線は冗長化すること。その際の接続帯域は 1Gbps 以上であること。接続帯域の変更が可能であること。

3.6.5. 学内ネットワークとクラウドの接続、各セグメント間など、ファイアウォール機能やセ

キュリティサービスを使用して、通信の制御が可能なこと。

3.7. クラウド-オンプレミス間接続サービス

3.7.1. 本学拠点とクラウド間を SINET 経由で閉域接続可能なこと。

3.7.2. ネットワーク間の通信制御可能なこと。

3.7.3. クラウド・オンプレミス間において、名前解決が可能なこと。

3.7.4. 閉域接続とは別に VPN など暗号化して接続可能なこと。

3.8. 仮想サーバ

3.8.1. OS について、Windows Server、Red Hat Enterprise Linux での構築が可能なこと。

3.8.2. 各クラウドサービス特有の OS など、上記以外の OS を利用する際は、現行同様のサービス、機能を提供可能なこと。

3.8.3. CPU、メモリは別紙 1 の性能を基本採用し、適切なリソース容量を選定すること。別紙 1 の性能にならない場合は、説明を行うこと。

3.8.4. 仮想サーバが利用する OS 領域やデータ領域を格納するストレージは、拡張性が考慮されているストレージサービスを利用すること。

3.8.5. 仮想サーバ単位で通信制御可能なこと。

3.8.6. 仮想サーバのバックアップやイメージが取得でき、リストアやサーバの増減が可能なこと。

3.9. ストレージ

3.9.1. 仮想サーバの用途、特徴を考慮し、ストレージの種類については適切なサービスを選択すること。

3.9.2. ストレージの容量について、ストレージ容量の拡張が可能なこと。

3.9.3. バックアップが可能なこと。バックアップは手動、自動でどちらも可能なこと。

3.9.4. ストレージ領域について暗号化されていること。

3.10. データベース

3.10.1. ライセンス料金込みの構成で PaaS サービスに対応できること。

3.10.2. PaaS サービスの場合、OS 領域へ管理者権限でアクセスが可能なこと。

3.10.3. 定期パッチについて、ユーザ側で適用タイミングを選択可能なこと。

3.10.4. CPU、メモリは、別紙 1 の性能を基本採用し、適切なリソース容量を選定すること。別紙 1 の性能にならない場合は、説明を行うこと。

3.11. セキュリティ要件

3.11.1. クラウド環境へのログインは、学内のファイアウォール機器を経由しシステムへ接続すること。

3.11.2. インターネットからアクセスが必要の際は、ファイアウォール機能や VPN 機能を使用し、安全に接続できる設計とすること。

3.11.3. サブネットや仮想 NIC 単位で通信制御可能なこと。

3.11.4. PaaS、SaaS において、技術上仮想 NIC や IP アドレスを使用するサービスは、サブネットや仮想 NIC 単位で通信制御可能なこと。

3.11.5. 外向けに提供する Web サービスについて、WAF などのサービスの導入を積極的に検討し、DDOS 攻撃やクロスサイトスクリプティングなどの脅威から保護すること。

3.11.6. 内部セグメントからインターネット接続が必要な際は、NAT サービスなどを使用し、セキュアな接続を行うこと。

4. 各サービス・機能要件

4.1. 認証サービス

4.1.1. マイクロソフト社の WindowsServer シリーズが提供する「Active Directory」同等のサービス、機能を提供が可能なこと。

4.1.2. 証明機関 CA を構成し、証明書の発行及び失効状態の管理が可能なこと。

4.1.3. ユーザ 、グループ や コンピュータ等の情報を一元管理、認証する機能を提供すること。

4.1.4. 現行サーバ OS である「Windows Server 2016」と同等の機能レベル（ドメイン、フォレスト）を有すること。

4.1.5. 本学の他システムへ認証連携が可能なこと。

4.1.6. グループポリシー、ドメインや OU については、新システムの特徴を考慮し、本学と協議し設計を行うこと。

4.1.7. クラウドサービス特有な技術要件から、現行設定から修正が必要な場合は、適当な対応を行うこと。

4.1.8. 本サービスにおいては、サーバの冗長化を行い、高可用性を実現すること。

4.1.9. 学内にある事務用端末が本サービスを利用できること。

4.2. DNS サービス

4.2.1. 基本的に現行ドメイン、現行ゾーン情報を移行し運用が可能なこと。ただし IP アドレス体系に沿って必要な設定変更を行うこと。

4.2.2. フォワーディング機能を有すること。

4.2.3. クラウド環境と本学内ネットワーク環境間で双方向の名前解決が可能なこと。

4.2.4. クラウドサービス特有な技術要件から、現行設定から修正が必要な場合は、適当な対応を行うこと。

4.2.5. 本サービスにおいては、サーバの冗長化、クラウドのマネージドサービスを使用し、高可用性を実現すること。

4.3. DHCP サービス

4.3.1. 学内にある事務用端末などに対して本サービスを提供可能なこと。

4.3.2. MAC アドレスフィルタリング機能を有するなど、IP アドレス割当先へ制限、フィルタリングなどの制御が可能なこと。

4.3.3. クラウドサービス特有な技術要件から、現行設定から修正が必要な場合は、適当な対応を行うこと。

4.3.4. 本サービスにおいては、サーバの冗長化、クラウドのマネージドサービスを使用し、高可用性を実現すること。

4.4. 時刻同期サービス

4.4.1. 基本的にクラウド事業者が提供する時刻同期サービスを使用すること。

4.4.2. 本学サイトのネットワーク環境と時刻同期を行うこと。

4.4.3. クラウドサービス特有な技術要件から、現行設定から修正が必要な場合は、適当な対応を行うこと。

4.4.4. 本サービスにおいては、サーバの冗長化、クラウドのマネージドサービスを使用し、高可用性を実現すること。

4.5. メールサービス

4.5.1. 許可元以外からのメール送信を制限可能なこと。

4.5.2. SMTP-AUTH など、SMTP 利用者であるクライアントに対して認証可能なこと。

4.5.3. DKIM、SPF、DMARC など、なりすまし対策が可能なこと。

4.5.4. 各サーバ、各クラウドサービスから障害通知が可能なこと。

4.5.5. 職員、学生向けに学内外へメール送信が可能なこと。

4.6. パッチ適用サービス

4.6.1. Windows 端末、Windows サーバ及び Linux サーバ等の各 OS、各クラウドサービスへ定期的にパッチの適用を行うことができること。

4.6.2. パッチ適用の際は、ネットワーク全体の通信に負担をかけないこと。

4.6.3. PaaS、SaaS へのパッチ適用が必要の際、パッチの適当タイミングについて調整が可能なこと。

4.7. KMS サービス

4.7.1. WindowsOS や製品に対して、ライセンスキーの管理、配布が可能なこと。

4.8. ウィルス対策サービス

4.8.1. 各サーバ、各クライアント端末へ配布が可能なこと。なお、現行は ESET を使用している。

4.8.2. マネージャーとクライアントは随時同期を行い、パターンファイル、セキュリティ対策リストや検索エンジンなど、最新の状態を保持可能なこと。

4.8.3. 管理コンソールからポリシー設定、デバイス管理などが可能なこと。

4.8.4. クライアントから現在の状態を定期的にマネージャー側へ送信可能なこと。また、管理コンソール上で状況をモニタリング可能なこと。

4.8.5. クライアントがウィルスに感染するなど、セキュリティ上問題が検出された際は、メールの通知が可能なこと。

4.8.6. その他業務システム側の振舞い検知機能、アンチウィルス機能など、必要なウィルス対策機能を盛り込むこと。

4.8.7. クライアントへパッチ適用の際は、ネットワーク全体の通信に負担をかけないこと。

4.9. バックアップサービス

4.9.1. バックアップ対象は、各サーバ、ファイル共有サービス中のデータとする。

4.9.2. ただし、PaaS や SaaS の利用の際、バックアップが必要なサービスについては、バックアップの取得を行うこと。

4.9.3. バックアップタイミングや世代数については、クラウド環境を意識した設計を行うこと。

4.9.4. クラウド上のコンポーネントについては、クラウドサービス上で提供しているバックアップサービスを使用する想定だが、バックアップソフトでのバックアップが必要の際は、提案すること。

4.9.5. バックアップの成功や失敗などのステータスについて、メール通知可能なこと。

4.10. リモート接続サービス

4.10.1. クラウド上のコンポーネントに対して、SSH や RDP、接続サービスを使用して接続可能なこと。

4.10.2. 接続における通信は、通信制御可能なこと。

4.10.3. 各システムの特性や運用状況を理解し、必要な環境を提供すること。

4.10.4. 各システムの同時利用者数は以下となる。必要となるライセンスを調達に含めること。

- 人事給与システム用ターミナルサーバ：50
- 学務情報システム用ターミナルサーバ：70
- 管理用ターミナルサーバ ：20

4.11. ファイル共有サービス

4.11.1. 各クライアント端末、サーバなどからファイル共有、データのやり取りが可能なこと。

4.11.2. 利用者や利用範囲、権限について、本学と協議を行うこと。

4.11.3. データのバックアップを行うこと。

4.12. ログ収集サービス

4.12.1. クラウド利用に伴う、各ユーザの操作ログ（GUI、CUI）の取得が可能なこと。

4.12.2. 特権アカウントの操作ログの取得が可能なこと。

4.12.3. 各クラウドサービスのコンポーネントから出力されるログについて収集が可能なこと。

4.12.4. ログの文言について条件設定をし、アラート検知が可能なこと。

4.12.5. 仮想サーバサービス上における OS、ミドルウェアなどのログ収集が可能なこと。

4.12.6. ログの保管について、ストレージサービスなどに保管し、3 か月以上保管可能なこと。ただし、保管期間や保管場所は本学と協議すること。

4.13. 資産管理サービス

4.13.1. 現行ソフトウェアである「SKYSEA」を継続調達すること。

4.13.2. 本学で利用する端末（デスクトップ及びノート端末、計 450 台程度を想定）について管理可能なこと。

4.13.3. 端末の管理については、本学の部署ごとに管理が可能なこと。

4.13.4. 指定したネットワーク以外からの通信をブロックするなど、通信制御可能なこと。

4.13.5. ログを収集可能なこと。また、ログの保存期間や圧縮が可能なこと。

4.13.6. アラートを検知した際、メール通知が可能なこと。

4.13.7. 端末に接続する記憶媒体について使用制限が可能なこと。

4.14. 監視サービス

4.14.1. 収集した各リソースについて、グラフ化が可能なこと。

4.14.2. 閾値越え、異常が検出された際は、メール等で通知が可能なこと。

4.14.3. 提供するクラウドサービスに異常があった際、メール等で通知が可能なこと。

4.14.4. リソースデータの収集、閾値について設定し、監視が可能なこと。

4.14.5. サーバやサービスのリソースを監視し、スケールアウトやスケールアップなどのリソースの増減を、自動で行えること。

4.14.6. クラウドサービス上のログ、仮想サーバ中の OS やソフトウェアのログを収集し、監視可能なこと。また文言を細かくフィルタリング可能なこと。

4.15. 負荷分散サービス（ロードバランサーに相当するもの）

4.15.1. 冗長構成となっており、高可用性なサービスを選定すること。

4.15.2. 通信の種類により、適切なサービスを選定すること。

4.15.3. ロードバランサーに紐づくサーバ群について、ヘルスチェックの結果トラフィックの転送、停止が可能なこと。

4.15.4. SSL 通信での暗号化が可能なこと。

4.16. その他

4.16.1. 構成上必要な Microsoft Windows Server、Red Hat Enterprise Linux Server の各ライセンスを用意すること。ライセンス費用は本調達に含むこと。

Ⅳ.　設置・導入

1.　システムの設計及び構築に関する項目

1.1.　全体要件

1.1.1.　提案したすべてのシステムに関して、受注者は本学と協議の上設計を行うこと。

1.1.2.　導入にあたっては、作業予定及び進捗状況を日次及び週次で本学へ提示し、都度連絡調整を行うこと。

1.1.3.　既設電源の有無を確認し、電源工事を必要とする場合は、その工事費も本調達に含むこと。

1.1.4.　本学に設置する物理機器については、既存ラック内に搭載すること。

2.　現行システムからの移行に関する項目

2.1.　全体要件

2.1.1.　現行システムのデータを、基本的に運用無停止で新システムに移行する。ただし、本学と事前の調整の上、最低限のシステム停止を伴うことも可能とする。以下に係る項目に要する費用はすべて本調達に含まれる。

2.1.2.　既存のファイルサーバの領域を「Ⅲ.4.11.ファイル共有サービス」に移行すること。当該サーバにはユーザ ID に紐付いたホームディレクトリが含まれている。

・既存ファイルサーバ：Unity400

・プロトコル：CIFS/SMB

・使用容量：約 12 TB

2.1.3.　既存の事務用 Active Directory の動作環境及びデータを「Ⅲ.4.1.認証サービス及び 4.3.DHCP サービス」に移行すること。移行の際に、Active Directory のグループポリシーの見直しを行う。見直しにあたり、既存のグループポリシーの洗い出しと整理を受注者が行い、本学と協議の上、移行すること。また、当該サーバは、別途調達する「構成員情報及びサービス連携管理システム」とユーザ情報の自動連携を行う予定であるため、構築完了時点で接続テストも実施すること。

2.1.4.　既存の DHCP サーバのデータを「Ⅲ.4.1.認証サービス及び 4.3.DHCP サービス」に移行すること。なお、移行対象となるデータについては、本学と協議の上決定すること。

2.1.5.　既存の UTM（Unified Threat Management）装置（Fortinet 社製「FortiGate-500E」）の設定を「Ⅲ.2.2.ネットワーク機器（ファイアウォール）及び 3.11.セキュリティ要件」に移行すること。移行の際に、ファイアウォール ポリシールールの見直しを行う。見直しにあたり、不要なファイアウォール ポリシールールの洗い出しを受注者が行うこと。なお、既存 UTM 装置のファイアウォール ポリシールールは約 200 個である。

2.1.6.　現行のオンプレミス型プライベートクラウドからクラウド基盤への移行にあたり全体的なネットワークについて、再設計を行うこと。また、現行の基盤に搭載されていない業務システム（学務情報システム（CELS）及びグループウェア（HWP））の移行につい

ても、現行の環境を考慮してネットワークや UTM 装置及びファイアウォール等のセキュリティ機器の設計を行うこと。

2.1.7. その他、現行システムからのデータ移行について、別途本学と協議して実施すること。なお、各業務システムのデータ移行については、本調達に含まない。

2.1.8. 各運用システムの以下データ移行は対象外とする。

・現行サーバ、PC のローカルに保存されているユーザデータ

3. マニュアル、ドキュメント等に関する項目

3.1. 全体要件

3.1.1. 納品されるすべての機器、サービス、機能、ソフトウェア等について、その構成、設定、利用方法、保守等に関するマニュアル、ドキュメント等を作成し、紙媒体及び電子媒体（原本のファイル形式及び PDF 形式の 2 種）で提出すること。なお、ドキュメントの種類は以下のものとする。

・プロジェクト計画書
・基本設計書
・ネットワーク構成図（物理、論理）
・通信要件一覧（各サーバ・端末の通信制御情報（通信元/先、NAT 情報、用途等））
・詳細設計書（各機器、OS、ミドルウェア、等の設定単位）
・試験計画書及び結果報告書
・移行計画書及び結果報告書
・運用保守設計書（実施対象、体制、時期、項目、内容、方法等）
・各種運用手順書
・各種管理資料（IP 台帳、サーバ台帳、ラック図、諸元等）

3.1.2. 前項において受注者が作成する成果物は、原則としてマイクロソフト社の Office 製品のファイル形式とし、その著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、既存の製品付属のマニュアル、ドキュメント部分（受注者が既に著作権を保有しているもの（以下「受注者著作物」という。）が組み込まれている場合は、当該受注者著作物の著作権を含む。）を除き、本学に帰属するものとする。

なお、受注者は、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。

あわせて、前述の受注者著作物について、本システムへ利用する目的の範囲に限り、本学は受注者に権利留保された著作物を自由に複製し、及びそれらの利用を第三者に許諾することができるものとする。ただし、成果物に第三者の権利が帰属するときはこの限りでないものとし、この場合には複製等ができる範囲やその方法等について協議するものとする。また、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，受注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。

3.1.3. 使用言語は原則として日本語であること。

V. 保守・運用

1. 保守に関する項目

1.1. 全体要件

1.1.1. 本システム導入後の保守計画を提示すること。

1.1.2. 保守期間は本稼働後 5 年間とする。この間、本仕様書に記載の保守要件を継続すること。

1.1.3. 本システムに関するすべての保守・運用窓口を一本化すること。

1.1.4. 障害発生時に、故障の一元受付、切り分け、手配が実施可能な体制を有すること。

1.1.5. 本仕様の一部又は全部を他社の製品で満たしている場合にも、受注者が責任をもってそれらの製品の保守を行う体制をとること。

1.1.6. 平日（土・日祭日等の休日を除く）の午前 9 時から午後 5 時において故障受付が可能な連絡先を設定すること。

1.1.7. 本システムに障害が発生した場合に、連絡後 2 時間以内にその障害原因の調査に着手できる体制をとること。なお、学内に設置されるハードウェア障害に対する復旧措置は原則としてオンサイトで実施すること。

1.1.8. ソフトウェア（本調達に含む OS 及びミドルウェア等）の障害が発生した場合は、本学による障害一次切り分けの結果をもとに、更なる詳細切り分けを行い適切なサポート窓口へ保守対応依頼の連絡を行うこと。また、サポート窓口からの回答をもとに障害復旧策を本学に報告すること。

1.1.9. 本システムの障害等によりマイクロソフト社への調査依頼が必要となった場合は、受注者が窓口となり対応すること。なおマイクロソフト社のプロフェッショナルサポート等の購入に係る費用については、本学と協議の上、別途契約するものとする。

1.1.10. 無停電電源装置のバッテリー等、経年劣化の予想される機器はその機能、性能を最低 5 年間は維持すること。

1.1.11. 導入機器及びソフトウェアのセキュリティホール及びウィルスによる本システムの機能低下を未然に防ぐため、常に最新の情報を収集し、それらを提供すること。

1.1.12. 障害によるサービス中断は、故障連絡を受けてから休日を除く連続 2 日以内を原則とすること。障害復旧又は保守作業がこれを超えて長期に及ぶことが判明した場合には、本学にその旨を報告するとともに、受注者の負担により、障害の原因と考えられる物品及びサービスの同等又は同等以上の機能・性能を有する代替品を用いて障害箇所を交換する等の適切な処置を行うことによって、復旧までの間システムを利用するユーザに支障をきたさないようにすること。

2. 運用に関する項目

2.1. クラウド基盤等に求める運用要件

2.1.1. 受注者は、本稼動開始以降の保守・運用のため、専門知識を有する要員を確保し、遠隔保守又は現地対応の体制を保持すること。

2.2. 研修

2.2.1. 本学は、本学の情報システムに関する利用者からの問い合わせ及び不具合への対応（ハードウェア、ソフトウェア、支線ネットワーク等の障害に関する切り分け及び対応、ウィルス感染等への対応、ユーザ作業を前提とした本調達システムの調整及びカスタマイズへの対応、問い合わせへの対応又は適切な対応窓口への取り次ぎ等を含む）、及び本学の情報システムの運用支援（セキュリティパッチの適用作業、機器の故障や障害に関する連絡、各種マスタデータの作成・管理、事務用端末の管理等）を行う職員を配置するものとする。当該職員が適切に対応できるよう、受注者は本調達で導入する各種システムについて詳細なマニュアルを整備し、導入時に研修教育を実施すること。

2.3. 作業報告等

2.3.1. 受注者は、保守運用に関する作業内容について進捗リスト等の形でドキュメント管理し、随時報告を行うこと。また、１か月に１回程度の頻度で定例会を対面またはオンライン（web）等で開催し、進捗等について報告すること。定例会の議事録は受注者が案を作成し、本学の承認を得て確定するものとする。本定例会に係る費用は本調達に含める。

Ⅵ.　総合評価基準

1.　業務系情報基盤システム一式の総合評価基準

本調達に係る入札の評価に関する基準は次のとおりとする。

1.1.　落札方式

1.1.1.　次の各要件に該当する入札者のうち、以下に示す総合評価の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。

(1)　入札価格が、予定価格の制限の範囲内であること。

(2)　性能等が、仕様書において明らかにした性能等の要求要件のうち、必須とされた項目の最低限の要求要件を全て満たしていること。

1.1.2.　上記1.1.1.の数値の者が2人以上あるときは、当該者にくじを引かせて落札者を定める。

1.2.　総合評価の方式

1.2.1.　仕様書に記載する要件を満たしているか否かの判定及び総合評価基準に基づき付与する得点の判定は、複数の本学技術審査職員が仕様書その他の入札説明書で求めた提案資料の内容を審査して行う。

1.2.2.　入札価格に対する得点配分と、性能等に対する得点配分は等しいものとする。

1.2.3.　入札価格の評価方式については、以下のとおりとする。

入札得点は、入札価格を予定価格で除して得た値を一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。

$$入札価格に係る評価点 = \left(1 - \frac{入札価格}{予定価格} \right) \times 入札価格に係る得点配分$$

1.2.4.　性能等の要件については、本仕様書のⅡ.全体要件、Ⅲ.調達物品に備えるべき技術的要件、Ⅳ.設置・導入、Ⅴ.保守・運用に記載の全ての要件とし、これらの中で必要性を明記した（～すること。等）全ての要件を必須の要求要件とする。

1.2.5.　性能等の評価方法については、以下のとおりとする。

(1)　評価の対象とする要件については、当該調達の目的、内容に応じて必要性等の観点から評価項目を設定し、これを必須とする項目とそれ以外の項目とに区分する。

(2)　必須とする項目については、項目ごとに最低限の要求要件を示し、この要求要件を満たしていない者は不合格とし、要求要件以上の部分については評価に応じ得点を与える。

(3)　必須とする項目以外の項目は、項目ごとに評価に応じ得点を与える。

(4)　各評価項目に対する得点配分は、その必要度・重要度に応じて定める。

1.2.6.　総合評価は、入札者の入札価格の得点に当該入札者の申し込みに係る性能等の得点の合計を加えて得た数値をもって行う。

2. 性能等に対する評価項目と得点配分基準

2.1. 必須項目

項目	基礎点
本仕様書の要求要件（Ⅱ.全体要件、Ⅲ.調達物品に備えるべき技術的要件、Ⅳ.設置・導入、Ⅴ.保守・運用）の全てについて、最低限の必須とする要求要件を満たしていること。必須とする要求要件を満たしていない場合は、不合格とする。	50

2.2. 加点基準

項番	加点対象項目	加点
Ⅱ.5.2.2.	提出された提案書について、本学の仕様書の内容を十分理解し、調達の目的が正確に捉えられ、有効な提案がなされていると判断される場合は加点とする。	5
Ⅱ.5.2.2.10.	本調達のシステムを構築するに当たり、要員の体制図、経験年数、本調達と類似の案件（クラウド基盤）を構築した経験を証明する資料を添えて提出し、要員の体制、経験ともに充分と判断できる場合は加点とする。	5
Ⅱ.5.2.2.10.	提出された導入の作業スケジュール表に関し、作業順序、作業内容が妥当であり、そのスケジュールが合理的に計画され、納期を遵守できる日程であると判断できる場合は加点とする。	5
Ⅱ.5.2.2.11.	本稼動開始以降の保守・運用のため、専門知識を有する要員を確保し、遠隔保守又は現地対応の体制を具体的かつ充実して整備したと判断できる場合は加点とする。	5
Ⅱ.5.2.2.	ネットワーク設計図（物理環境及びクラウド環境）が合理的と判断できる場合は加点とする。	10
Ⅱ.5.2.2.	データベースを含むシステム全体（物理環境及びクラウド環境）について、コスト面及び運用面で本学にとって有益な提案と判断できる場合は加点とする。	12
Ⅱ.5.2.2.	セキュリティを考慮した設計、機器及びサービス選定であると判断できる場合は加点とする。	5
（下表参照）	ワーク・ライフ・バランス等の推進に関する指標（※）	3
計		50

※ワーク・ライフ・バランス等の推進に関する指標

加点対象項目　（認定等の区分 ※1）		加点
女性活躍推進法に基づく認定を受けている	プラチナえるぼし（※2）	3
	認定段階 3（※3）	3
	認定段階 2（※3）	2
	認定段階 1（※3）	1
	行動計画（※4）	0.5
次世代法に基づく	プラチナくるみん（※5）	3

認定を受けている	くるみん(令和 4 年 4 月以降基準) （※6）	2
	くるみん(平成 29 年 4 月-令和 4 年 3 月基準) （※7）	2
	トライくるみん（※8）	2
	くるみん(平成 29 年 3 月以前基準) （※9）	1
若者雇用促進法に基づく認定（ユースエール認定企業）		2
計		3

※1 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ものとする。

※2 女性の職業生活における活躍の推進に関する法律等の一部を改正する法律(令和元年法第 24 号)による改正後の女性活躍推進法第 12 条の規定に基づく認定

※3 女性活躍推進法第 9 条に基づく認定。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。

※4 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)。

※5 次世代法第 15 条の 2 の規定に基づく認定

※6 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 号の規定に基づく認定

※7 次世代法第 13 条の規定に基づく認定のうち、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 条又は令和 3 年改正省令附則第 2 条第 2 項の規定に基づく認定(ただし、※9 の認定を除く。)

※8 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 号の規定に基づく認定

※9 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 項の規定に基づく認定

以上