

「独立行政法人日本学術振興会業務基盤システム更新・保守業務 一式」に関する意見招請への回答

No.	頁	項番号等	仕様書（案）の記載内容	意見/質問内容	意見/質問の理由	回答（日本学術振興会記入）
1			(ISMAPに係る要件の記載が資料招請時の仕様書(案)と比較し削除されている)	クラウドサービスの選定にて、政府統一基準に基づいた一定水準以上のセキュリティが担保されているサービスの証明が必要であると考えます。そのため、以下のような記載の追加を願います。 「次期システムで利用するクラウドサービスは、原則としてISMAP又はISMAP-LIUに登録されていること。未登録サービスを利用する場合は、以下のいずれかを満たすこと。 ・ISO/IEC27017又はISMSクラウドセキュリティ認証制度に基づく認証を取得していること。または、同等以上のクラウドセキュリティ水準が第三者により保証されていること。なお、個人情報の利用においては、ISO/IEC27018又はプライバシーマーク、もしくは同等以上のプライバシー保護に関する第三者認証を取得していること。 ・SOC報告書を提出できること。ただし、当該報告書の対象範囲に当該クラウドサービスが含まれ、監査で選択した対象範囲/規準に「セキュリティ」が含まれること。」	クラウドサービスの選定について、政府統一基準に基づいた一定水準以上のセキュリティが担保されているサービスの利用が推奨されるため。 また、ISMAP登録サービスであることが望ましいが、採用可能なサービスの選択肢が限定されることを考慮し、ISO/IEC 27001（ISMS）、ISO/IEC 27017、ISO/IEC 27018、SOC2 Type II等の第三者認証・保証報告書を取得し、同等以上の情報セキュリティ水準が客観的に確認できるサービスについても提案可能としたいため。	クラウドサービスの選定においては原則ISMAP等（LIUを含む）に登録されていることとします。
2				総合評価落札方式の価格点：技術点配分について、長期的な業務継続、安全性、安定運用の観点から技術点を重視した1：3の配分の採用をご検討願います。	官公庁・外郭団体の基盤更改案件では、重要インフラ更改となるため技術点を重視した1：3を採用するケースが多くみられます。本案件においても、クラウド移行および移行後の長期的な業務継続、安定運用の実現を技術力の面から適切に評価するために、1：3の配分が望ましいため。	本調達の「総合評価基準及び加点付与基準」については、調達仕様書の別紙に記載しています。
3				加点についての記載ですが、機能の有無に関する内容が加点となっている認識です。機能の充足の評価だけでは、クラウド移行を含む基盤更改に関して、プロジェクト実行性や業務継続・安全性・安定運用について総合的な評価が困難と考えます。加点評価項目については、プロジェクト実行性や業務継続・安全性・安定運用について総合的に評価できるように、より定性的な内容への変更を願います。	前回調達時はオンプレミスからオンプレミスへの機器の更改ということで、機能充足の観点での総合評価基準書が適切であったと理解しています。 本調達のクラウド移行を含む基盤更改案件では、要件個々の充足も重要ですが、プロジェクト実行性や業務継続・安全性・安定運用について総合的に評価することが重要であり、総合評価基準書の加点評価項目についてもより定性的な内容が望ましいため。	本調達の「総合評価基準及び加点付与基準」については、調達仕様書の別紙に記載しています。
4	3	1.4.	業務サーバ(3環境を移行)	業務サーバについては調達仕様書、要件定義書の本文に記載がないため調達範囲外と認識しております。「本システムの概念図」では調達範囲に含まれるように見受けられるため、調達範囲外である場合は「本システムの概念図」の修正を願います。	「本システムの概念図」はまだ仮の記載の認識だが、業務サーバ移行については重要なポイントとなるため。	業務サーバは、今回の調達範囲外です。
5	2	1.4.(2)	FAT 端末（セキュアPCを含む）	ご提示いただいた要件から、ノート型クライアント端末は要件上すべてセキュアPCと理解しておりますが、FAT端末を併記している意図があれば、説明の追記を願います。 セキュアPCのみの場合は、FAT端末部分の記載を削除願います。	要件から、クライアント端末はすべてセキュアPC相当の想定だが、FAT端末の記載があり、貴会で想定している、FAT 端末、セキュアPCの違いについて、提案・見積の公平性確保の観点から確認するため。	本調達においては、ローカル処理を行うFAT端末の形態でありながら、強固なセキュリティ機能を備えたもの（セキュアPC）も対象に含まれるという意味で「FAT端末（セキュアPCを含む）」と記載しています。
6	3	仕様書 1.4（7） 別紙1 1.10.-2	「グループウェアは Microsoft 365 を基盤とし、ポータル、スケジュール、ファイル管理等を統合する。」 「Zoom、Teams 等を利用したオンライン会議」	Web会議サービス及びビジネスチャットの調達範囲について明記をお願いします。 資料提供招請時の導入説明書では、Web会議サービス及びビジネスチャットについてそれぞれ300ライセンス以上の提供が示されておりましたが、本仕様書（案）には該当する要件・数量の記載が見当たりません。 ① Microsoft Teams（Microsoft 365 に包含）をもって充足とするか ② 現行の Web会議サービスを継続利用する前提か ③ 継続する場合、当該ライセンスの調達が本調達の範囲に含まれるか	Web会議サービスを別途調達する場合、ライセンス費用が追加で発生するため。また Teams へ統合する場合は、既存の会議運用・外部招待運用の移行作業が必要となるため。	Microsoft Teams（Microsoft 365 に包含）を標準のWeb会議サービスとします。 既存の会議運用・外部招待運用の移行作業は調達範囲外です。
7	4	1.5.	本調達の契約期間は、以下のとおりとする。 ・設計・構築期間：2027年1月から2028年1月まで（予定） ・運用・保守期間：システム稼働開始後5年間（予定） なお、システムの納入期限は2028年1月31日、運用開始は2028年2月1日を予定している。	意見 ・クライアント端末について、「別紙1 要件定義書 1.10.ノートクライアント端末」の機能要件を満たす事を前提に、提案書提出段階より、納入する機種の後継機等他機器変更しても良い事とさせていただきますでしょうか。	・PCメーカー製品供給期間が新製品切替や部材供給の影響から同一機種で提供が困難となる場合があるため。	機能要件を満たしていて、かつ提案書記載のものと同等以上であれば、必ずしも同一機種でなくても構いません。
8	4	2.1. 4.3.	「（1）設計業務（要件定義の精緻化、基本設計、詳細設計）」 「内容について調整すべき事項があれば、本会と調整の上、結果に基づき要件定義書の修正を行うこと。」	要件定義工程について、受注者の対応は要件定義書の確認、検討および要件変更案の提示までとさせていただきますでしょうか。	デジタル庁の『デジタル・ガバメント推進標準ガイドライン』に要件定義書の作成および修正は発注者側で実施する旨が記載されているため。	

9	5、 19	2.2 表2.2.-1 8.2 (5)	「調達の種類：賃貸借」 「本システムの賃貸料には、ハードウェア及びソフトウェアの保守費用を含めること。また、構築期間中のハードウェア、ソフトウェア及び、通信回線費等の運用保守に係る費用も全て賃貸料に含めること。」	クラウドサービス利用料（Microsoft 365、Windows 365、Azure 等のサブスクリプション）の契約上の取扱いについて明記をお願いします。 ① 賃貸借（借入等）と役務の区分 ② 構築期間（2027年1月～2028年1月の13か月）に発生する利用料の計上方法及び支払開始時期 ③ 契約期間中にクラウド事業者による価格改定又は著しい為替変動が生じた場合の取扱い（変更契約の可否等）	クラウドサービスは、構築13か月＋運用5年の計約6年間を固定価格で引き受けることが困難であり、価格改定リスクの取扱いが不明な場合、応札者がリスク分を上乗せせざるを得ず、結果として調達価格が上昇するため。	8.2. (5) の記載に、以下を追加しました。「契約期間中に、クラウド利用料等の著しい価格改定が生じた場合等には、本会と協議を行うこと。」
10	5	2.2.-1	表2.2.-1 調達案件の概要 調達の種類 賃貸借	調達の種類「賃貸借」について、リース会社含む三社間契約での対応を考えております。問題ございませんでしょうか。	賃貸借における、リース会社含めた契約形態明確化のため。	三者間賃貸借であることのみをもって入札参加グループに該当するものではありません。調達仕様書における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」を指します。したがって、入札参加グループに該当するか否かは、三者間賃貸借であるか否かではなく、入札参加の形態が上記定義に該当するかにより判断します。
11	5,6,11, 20	2.4 表2.4.-1 No.8・No.9	「8 グループウェア Microsoft 365」「9 メールシステム Exchange Online」 (別紙1 1.13.-8「Microsoft 365 A3 又は A5 を 600 ライセンス」、1.7.-5「電子メール基盤として Microsoft Exchange Online を利用」)	表2.4.-1 のNo.8 (Microsoft 365) とNo.9 (メールシステム／Exchange Online) の関係について明記をお願いします。 Exchange Online は Microsoft 365 A3／A5 に包含されるため、No.9 を別途調達する必要はないものと理解しておりますが、別建てで数量計上を要する趣旨であればご教示ください。	同一ライセンスの二重計上を避け、正確な数量及び費用を積算するため。	ご理解のとおりですので、記載を整理しました。
12	5,6	2.4.	表2.4.-1 本会が調達する機器の一覧 Windows 11 Enterprise 350 式	「表2.4.-2」では調達となるクライアント端末は、 ・ 役職員用350台 ・ 管理者用・ 検証用15台 ・ 一時利用者用及び予備機50台 の計415台と記載されています。 一方で、「表2.4.-1」にて調達するOSが「Windows 11 Enterprise 350 式」と記載されています。 また、「1.4 次期業務基盤システムの概要」においても記載のシステム利用者は ・ 本会役職員：約350名 ・ 管理者：約15名 ・ 一時利用者等：約50名 計415人と記載されています。 誤記であれば「Windows 11 Enterprise 415 式」への修正願います。	システム利用者数および調達するクライアント端末の台数から Windows 11 Enterprise 415 式と認識しているため。	表2.4.-1を修正しました。
13	5,6	2.4.	BYOD端末（本調達外）	BYOD端末のOSは何を利用しているかご教示願います。	サービスを提供する上で動作環境を知る必要があるため。	「表2.4.-2 役職員等の端末の種類と数量」の「研究員用150 BYOD端末（本調達外）」はWindows11を想定しています。「海外研究連絡センター用70BYOD端末（本調達外）」はWindows11を想定しています。 なお、研究員のBYOD端末には、Macも含まれています。
14	6	2.4.	表2.4.-2 役職員等の端末の種類と数量 「海外研究連絡センター用」	海外研究連絡センター用と記載されていますが、海外の拠点からの接続を想定しているとの認識です。その場合、接続元の国（地域）ごとの内訳等についてご教示願います。	国（地域）によって通信品質やセキュリティ面、及び輸出管理の観点で考慮すべき事項が発生するため。	https://www.isps.go.jp/j-overseas/ に記載の9か国10か所に海外研究連絡センターを設置しています。
15	6	2.4.	表2.4.-2 役職員等の端末の種類と数量 管理者用・ 検証用15台	管理者用端末は役職員用端末とは異なる要件（主にインストール対象ソフトウェア）となるのか、あるいは役職員用端末と同一の要件となるかご教示願います。	検証用端末は、検証のため役職員用端末と同様の状態（要件）である必要があると考えております。 一方、管理者用端末は役職員用端末とは用途が異なると思われる、仕様や設定条件が異なる場合は設計規模に影響するため。	検証用端末も管理者用端末も、役職員用端末と同一の要件です。
16	6	2.4.	表2.4.-2 役職員等の端末の種類と数量 研究員用、海外研究連絡センター用のBYOD端末	BYOD端末に対する端末管理（ログ収集、MDM登録、パッチ管理、EDR導入等）はIntuneでの管理対象端末としてデバイス状態に基づくアクセス制御を行う想定でしょうか。 仮想デスクトップの認証、DLP制御、ZTNA制御等によるセキュリティ対策としてBYOD端末へソフトウェアのインストールを実施することが可能か、ご教示願います。	BYOD端末は基本的に管理対象としない認識だが、セキュリティとして守るべき領域は守れるように対策をとるべきであるため。	研究員用、海外研究連絡センター用のBYOD端末については、申請は必要ですが、デバイス管理、BYOD端末へのソフトウェアのインストールは行わない想定です。

17	7	3.1.	納入期限は2028年1月31日(月)	設計構築等の導入工程の納入期限は2028年1月31日(月)と記載がございますが、導入工程の検収完了後、導入費用の一括支払いを予定されておりますでしょうか。もしくは稼働開始後月額でのお支払いを予定されてますでしょうか。	リースを含む見積において必要な情報となるため。 導入費用を全てリース対象とするか、リース対象外とするか判断するため。 導入費用を一括でお支払いいただくことで、総コストの低減が可能です。	稼働開始後、月額での支払いとします。
18	7	3.1. (2)	2027年12月29日(水)から2028年1月3日(月)までの間に切り替え作業を行い、2028年1月4日(火)から仮運用を開始する	全システムの一斉切り替え作業を年末年始に限定せず、段階的移行（先行できるシステムから順次移行）の容認や、12月前半または1月中旬以降の週末を利用した切り替えなど、スケジュールの柔軟な提案を認めていただけないでしょうか。	年末年始は、利用予定のSaaSベンダー、通信キャリア、ハードウェア保守窓口等が特別営業（縮小体制）となっていることが多く、万が一のトラブル発生時に外部へのエスカレーションや復旧対応が大幅に遅延する深刻なリスクを孕んでいます。より安全で確実な移行を実現するため、影響を分散する段階的移行等をご検討いただきたいからです。	3.1. (2) の記載を「導入するシステムは、原則として、2027年12月29日から2028年1月3日までの間に切り替え作業を行い、」のように、「原則として」を追加しました。 ただし、1月4日からの試行運転は必須であり、前倒しのみ可能である。
19	6	3.1.(1)	納入場所は、日本学術学振会 東京都千代田区麹町5-3-1、又は別途指定する場所とする。	「別途指定する場所」について、KBC以外に別途納入場所があればご教示願います。	納入対象であるネットワーク機器や端末を貴会の拠点である東京都千代田区麹町5-3-1以外への納入は想定されていないものと認識しているため。	SINETデータセンタ等のネットワー機器を除き、KBC本部への納入となります。
20	27	3.2.-6	契約満了時、契約解除後又は障害等で不要となった本システムのストレージデバイスのデータ消去は受注者の責任において行い、本会の承認を得た上で撤去すること。なお、データ消去は、NIST800-88 消去方式相当以上の強度で消去又は物理的に破壊を行うこと。また、データ消去後に消去に係る証明書を提出すること。	データ消去は受注者指定場所に移動させてからの作業でよろしいでしょうか。	正確な仕様・要件を確認するため。	オンプレミス又は物理ストレージデバイスに含まれているものを含めてデータの持ち出しや移動については、発注者の承認が必要です。
21	8,9	3.3 (10)	入札参加ループの構成員は、上記の「受注者に必要な要件」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。	①三者間賃貸借も「入札参加グループ」に該当するという認識で相違ないでしょうか。 ②三者間賃貸借の場合、入札資格の考え方は下記の通りで相違ないでしょうか。 (1) 代表者は、入札参加資格の全てを満たす者とする。 (2) 受注者の実績に関する要件は、「入札参加グループ」全体で満たせばよい。 (3) 品質マネジメント、情報セキュリティマネジメントに関する認証は、代表者が取得していればよい。 ③三者間賃貸借の場合、入札参加グループの結成に関する協定書は「第三者をして貸付をする」	正確な仕様・要件を確認するため。	① 三者間賃貸借であることのみをもって入札参加グループに該当するものではありません。調達仕様書における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」を指します。したがって、入札参加グループに該当するか否かは、三者間賃貸借であるか否かではなく、入札参加の形態が上記定義に該当するかにより判断します。 ② ご理解のとおりです。 ③ 入札参加グループとして参加する場合は、調達仕様書に記載のとおり、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）を提出してください。なお、提出書類がこれに類する書類に該当するかについては、その書類により入札参加グループの構成及び役割分担等が確認できる必要があります。※単に第三者をして貸付を行う旨を定めた書類のみでは、入札参加グループの交際及び役割分担等を確認できない場合があります。
22	9	3.3. (13)	ITIL準拠の体系化した社内運用標準を有していること。	当該要件の「有することの証明」について、具体的な提出書類（例：運用マニュアルの目次等）の指定はありますでしょうか。また、社内標準化の途上であっても「ITIL有資格者がプロジェクトの運用設計・管理に参画すること」をもって同等とみなすことは可能でしょうか。	「ITIL準拠の社内運用標準」という定義が幅広く、客観的な証明方法が不明確であると入札参加の可否判断に迷いが生じます。要件の明確化、あるいは有資格者の配置による実質的な運用能力の担保へと緩和いただくことで、参入検討がしやすくなるためです。	3.3. (13)の記載を以下のとおり修正しました。「運用保守業務について、インシデント管理、課題管理等の運用管理手順を定めた社内標準を有していること。なお、提案時に当該手順の概要が確認できる資料を提出すること。」
23	9	3.4.	「(5) 本システムクラウドサービスを導入する場合には、同等以上の規模での導入実績が5件以上あること。」	クラウドサービスについて、クラウド基盤・Microsoft 365・ゼロトラスト環境等の導入実績としていただけますようお願いいたします。	本調達は単純なクラウドサービス導入案件ではなく、ネットワーク、認証、セキュリティ、クライアント基盤を含む総合的な業務基盤システム更新案件であるため、クラウド導入件数のみでは事業者の遂行能力を十分に評価できない恐れがあります。 また、本業務を遂行可能な事業者の参入機会を確保しつつ、適切な競争環境の維持が期待できるため。	原案どおりとします。
24	9	3.4. (1)	ネットワーク、ハードウェア、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・構築方法論を受注者自身が有し、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。	完全な自社独自の方法論に限定せず、パブリッククラウドベンダー（AWS、Azure等）が提唱するベストプラクティス（Well-Architected Framework等）に準拠した設計アプローチを採用することで本要件を満たすものとして許容していただけないでしょうか。	現代のクラウドを中心とした基盤構築においては、自社独自の閉鎖的な方法論よりも、業界標準のベストプラクティスを活用の方が属人性を排除でき、柔軟かつ高品質なインフラ構築が可能となるためです。	パブリッククラウドベンダーのベストプラクティスに準拠することは問題ありません。
25	9	3.4. (2)	過去5年以内において、クライアントPC 400台以上のシステムの企画、設計、構築、保守、工程管理等のプロジェクトを一貫して請け負った経験があること。	本実績要件の「クライアントPC 400台以上」について、「300台以上」に要件を緩和していただけないでしょうか。あるいは、物理的なPC台数ではなく「利用ユーザー数（またはアカウント数）400名以上」のシステム構築実績をもって同等要件としてみなしていただけないでしょうか。	BYODや仮想デスクトップ（VDI）、クラウドサービスの普及により、物理PCの調達台数よりもシステムを利用するユーザー規模感がプロジェクト管理の難易度を示す指標として適切であるケースが増加しています。実態に即した指標へ緩和いただくことで、競争環境が促進されるためです。	3.4. (2) の記載を以下のとおり変更しました。「過去5年以内において、利用ユーザ数（またはアカウント数）400名以上の……」
26	9	3.4. (5)	本システムクラウドサービスを導入する場合には、同等以上の規模での導入実績が5件以上あること。	「同等以上の規模での導入実績が『1件以上』あること」または「規模を問わずクラウド環境の導入実績が『5件以上』あること」など、要件を緩和していただけないでしょうか。	本件と同等の大規模かつ複雑な次期業務基盤システムの導入実績を「5件以上」有する事業者は極めて限定的です。競争原理を適切に働かせ、コスト最適化と最適な提案を引き出すためには、実績の「件数」のハードルを下げて参入障壁を低くし、フラットな環境とすることが有益であると考えるためです。	3.4. (5) の記載を以下のとおり変更しました。「設計・構築を完了し、本稼働させた実績を1件以上有すること。」

27	9	4.1.	(1) 搬入、据付、配線、調整、既存設備との接続に要するすべての費用は、本調達に含めること。また、関係事業者との調整が必要な場合は、本会と協議して対応を行うこと。	意見 ・既存設備との接続・関係事業者調整について、対象設備、作業範囲、想定回数、現地条件を開示し、仕様外・追加作業は別途協議といただきたい。	・未開示の既存環境や第三者都合による費用まで全て内包すると、受注者が制御できないコストを負担することになるため。	4.1. (6) の記載に以下を追加しました。「(6)☒会建物に搬入、据付、配線、調整、既存設備との接続を要する場合は、希望に応じ提案時に現地調査を承認する場合がある。」
28	9,10	4.1.	「(3) すべての調達機器に対して、本調達であることがわかるようにラベルを作成・貼り付けすること。」	「すべての調達機器」には、ノート型クライアント端末415台も含まれるとの理解であっておりますでしょうか。また、貼付するラベルの記載事項（管理番号、契約番号等）についてご教示ください。	対応範囲を明確化し、適切な工数算定を行うため。	4.1. (3) の記載に以下を追加しました。「ラベルの記載事項は、調達機器によって異なるが、管理番号、管理部署、契約番号等である」
29	30	4.1-5	「各サーバに対して行う脆弱性検査において指摘された事項について、設定変更やバージョンアップ作業を行うこと。」	保守運用フェーズで実施する脆弱性検査の回数について明記をお願いします。	正確な仕様・要件を確認するため。	保守運用フェーズで実施する脆弱性検査は発注者において年1回以上行う予定です。
30	37	4.6-7	「重大インシデント発生時には、必要に応じてフォレンジック調査を支援できること。」	本要件における「フォレンジック調査を支援」の範囲を明確化していただけますでしょうか。 例えば、証跡保全、ログ収集、ログ分析、調査報告書作成支援、外部専門ベンダーとの連携支援など、どこまでを本契約・本業務の対象とするのかについて明記をお願いします。	「フォレンジック調査を支援」の内容によって、必要な専門人材、ツール、対応時間、工数が大きく異なるため。	「フォレンジック調査を支援」の範囲は、ログ収集、証跡及び関連情報の提供までを本調達の対象とし、ログ分析等フォレンジック調査自体は対象外とします。 (参照：要件定義書4.6-7)
31	11	5.1.	項番 4 組織又は要員 システム設計・開発・保守班 役割 リーダはシステム設計・開発作業期間中、専任でこれに当たるものとする。	意見 ・「専任」とする要件について、本業務の遂行および責任体制に支障がない範囲で、他業務との兼任を認める要件に緩和いただけますでしょうか。	・専任要件は、必要な知識・経験を有するSEのアサインを制約し、提案可能な体制を狭める要因となるためです。連絡体制および責任者としての役割を明確にすることで、兼任であっても品質と円滑な業務遂行は確保可能と考えます。 ・各リーダーは長期間の専任が必要となり、業務量が少ない期間も他案件へ配置できず、人材確保・価格の両面で受入れが困難なため。	表5.1.-1の記載を以下のとおり修正しました。「ここでいう専任とは、本業務に主たる業務として継続的に従事することをいい、本業務の遂行に支障のない範囲で兼務を妨げるものではない。この場合、兼務の状況を作業体制図に明記すること。（以下、本表において同じ）」
32	11	5.1.	項番 5 組織又は要員 システム運用班 役割 リーダーはシステム運用期間中、専任でこれに当たるものとする。	意見 ・「専任」とする要件について、本業務の遂行および責任体制に支障がない範囲で、他業務との兼任を認める要件に緩和いただけますでしょうか。	・専任要件は、必要な知識・経験を有するSEのアサインを制約し、提案可能な体制を狭める要因となるためです。連絡体制および責任者としての役割を明確にすることで、兼任であっても品質と円滑な業務遂行は確保可能と考えます。 ・各リーダーは長期間の専任が必要となり、業務量が少ない期間も他案件へ配置できず、人材確保・価格の両面で受入れが困難なため。	同上。
33	11	5.1.	項番 3 組織又は要員 プロジェクト全体管理者（プロジェクトマネージャ） 役割 本業務の委託期間中、専任でこれに当たるものとする。	意見 ・「専任」とする要件について、本業務の遂行および責任体制に支障がない範囲で、他業務との兼任を認める要件に緩和いただけますでしょうか。	・専任要件は、必要な知識・経験を有するSEのアサインを制約し、提案可能な体制を狭める要因となるためです。連絡体制および責任者としての役割を明確にすることで、兼任であっても品質と円滑な業務遂行は確保可能と考えます。 ・PMは委託期間全体、業務量が少ない期間も他案件へ配置できず、人材確保・価格の両面で受入れが困難なため。	同上。
34	11	5.1.	プロジェクト統括管理責任者、システム設計・開発・保守班リーダー、システム運用班リーダーは業務委託期間中、専任でこれに当たるものとする。	各リーダーの「専任」要件について、「業務に支障のない範囲での兼任可」あるいは「プロジェクトのコア期間（要件定義～基本設計、移行・切替時など）のみ専任とし、他期間は兼任可」と緩和していただけないでしょうか。	複数領域を統括できる高度IT人材を数年単位で完全専任化することは非常に困難であり、過度なコスト増に直結します。組織としてのバックアップ体制を明示することを条件に兼任を認めていただくことで、より優秀な人材を配置しやすくなり、結果として品質と安定性が向上するためです。	同上。
35	11	5.1.	またパッチ適用、障害対応等において他事業者の支援を行う。	要件定義書には他事業者への支援についての記載がありません。他事業者支援について要件がある場合は、要件定義書への追記をお願いします。要件がない場合は本記載の削除をお願いします。	提案・見積の公平性確保の観点から、確認の必要があるため。	要件定義書4.1.-5の記載に以下を追加しました。「各サーバに対するセキュリティパッチの適用作業を行うこと。」
36	11	5.1.	作業実施体制と役割	・同一のシステム 設計・開発・保守班リーダーを設計構築から運用期間を通じて一貫してアサインすること。	品質を維持するため(トラブルを少なくする)。構築から運用へスムーズに移行。 運用中に設計・構築時の情報を踏まえたサポートを可能とするため。	原案どおりとします。

37	11	5.1.	作業実施体制と役割	・プロジェクト統括管理責任者、プロジェクト全体管理者、システム設計・開発・保守班リーダー、システム運用班リーダーを変更する場合、少なくとも変更の3ヶ月前までに委託者の承認を得ること。ただし、退職、傷病、事故等のやむを得ない事由により、事前に変更を予想することが困難な場合を除く。	人事異動や体制変更に伴い、受託者側の事情でプロジェクト統括管理責任者が容易に変更可能な体制では貴会の重要インフラを構築運用するには些か不安定と言わざるを得ません。プロジェクト統括管理責任者の変更には貴機構側の承認を得ることを提言いたします。	表5.1.-1に以下を追加しました。「要員の交代を希望する場合は、事前に本会へ報告し、承認を得ること。」
38	12	5.2.	(3) システム設計・開発・保守班（クラウドサービスの設計・開発担当者） クラウドサービスの設計・開発担当者は、次のいずれかに該当すること。 ・主として利用するクラウドサービスについて、当該クラウドサービスプロバイダが認定している 資格の中で、以下に例示する上級資格を保有している者。 AWS認定 ソリューションアーキテクト-プロフェッショナル AWS認定 DevOpsエンジニア-プロフェッショナル Google Cloud 認定 プロフェッショナルクラウドアーキテクト Google Cloud 認定 プロフェッショナルクラウドDevOpsエンジニア Microsoft 認定 Azure ソリューションアーキテクトエキスパート Microsoft 認定 DevOpsエンジニアエキスパート ・上記の試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者	クラウドサービスの設計・開発担当者全員に適用するには条件が厳しく、例えばM365関連サービス（ExchangeOnline、SharePoint、OneDrive等）の設計・開発担当者にはご指定の資格で求められるスキルとは異なるスキルを必要とすると考えております。そのため、本要件は削除いただくか、リーダーのみに要求するよう緩和をご検討いただけますでしょうか。	体制確保が困難となり、要員が限定されることでコスト増加につながるため。	特定の資格保有者だけではなく、「同等の能力を有することが、経歴等において、明らかな者」も要件に含めていますので、原案どおりとします。
39	12	5.2.	(4) システム運用班リーダー システム運用班リーダーは、運用の経験年数を5年以上有すること。また、その中でリーダークラスとしての経験を2年以上有し、次のいずれかに該当すること。 ・ITサービスマネージャ試験の合格者 ・ITIL4 マネージングプロフェッショナル ・上記のいずれかの試験合格者・資格保有者等と同等の能力を有することが、経歴等において、明らかな者	システム運用班リーダーの条件が厳しいため、以下の要件に緩和いただけないでしょうか。 システム運用版リーダーは、運用の経験年数を5年以上有すること。またその中でリーダークラスとしての経験を2年以上有し、次の能力を有すること。 ・共通用語としてITILベースで会話できること ・運用プロセス改善のPDCAを展開させること ・価値の拡大に向けたSLO,SLA等を推進できること その実績を示すこと。	体制確保が困難となり、要員が限定されることでコスト増加につながるため。	同上。
40	11, 12, 13	5.2.	「作業要員に求める資格等の要件 (1) プロジェクト全体管理者」	「プロジェクト統括管理責任者」に求める資格等の要件については記載がございませんが、本業務全体を統括する立場であることから、必要な経験年数、同規模案件の統括実績又は保有資格等の要件を明記いただくようお願いします。	「プロジェクト全体管理者」には資格要件が定義されている一方で、上位責任者である「プロジェクト統括管理責任者」には要件の記載がなく、役割と要求水準の整合性を図るため。	表5.1.-1に、受託者側のプロジェクト統括管理責任者の役割として、「受託者側として本業務全体を統括し、必要な意思決定を行い、本プロジェクトの円滑な遂行の責任を担う。」と記載しております。この役割を担える者であれば、資格要件は問いません。
41	11	5.2. (1)	プロジェクト全体管理者は、プロジェクトマネージャ試験、PMP等の資格保有者等であること。	「応用情報技術者試験合格等の要件に加え、同等規模のプロジェクト管理経験を十分有する者」、あるいは「有資格者が専門組織（PMO等）として当該管理者を組織的に支援する体制がある場合」も「同等の能力を有する」ものとして認めていただけないでしょうか。	プロジェクトを成功に導くためには、個人の特定資格のみならず、実務に即したマネジメント経験や組織的なPMO体制によるバックアップが不可欠です。実質的な管理能力をフラットに評価可能にいただくことで、経験豊富な人材をアサインしやすくなるためです。	同等であることの証明を提案書で説明してください。
42	12	5.2. (2)	システム設計・開発・保守班リーダーは、システムアーキテクト試験、データベーススペシャリスト試験等の資格保有者等であること。	高度情報処理技術者試験だけでなく、「応用情報技術者試験合格、かつ5年以上の設計・開発経験および3年以上のリーダー経験を有する者」も「同等の能力を有する」として認めていただけないでしょうか。	高度資格の保有に限定するとアサイン可能な人材が過度に絞られ、調達コストの増大や体制構築の遅れを招く恐れがあります。豊富な実務経験を持つリーダーの参画を広く認めることで、より高品質で確実なシステム構築を実現するためです。	特定の資格保有者だけではなく、「同等の能力を有することが、経歴等において、明らかな者」も要件に含めていますので、原案どおりとします。 同等であることの証明を提案書で説明してください。
43	12	5.2. (3)	クラウドサービスの設計・開発担当者は、AWS 認定 ソリューションアーキテクト プロフェッショナル等の上級資格を保有している者	特定の最上位資格に限定せず、「ベンダー認定の中級（アソシエイト等）資格を保有し、かつ同等規模のクラウド基盤構築の実務経験を3年以上有する者」等を同等とみなし、広く認めていただけないでしょうか。	クラウド上級資格の保有者は限られており、特定の資格に限定すると特定のベンダーへの偏り（ベンダーロックイン）や参入企業の過度な絞り込みに繋がります。実践的な「実務経験」をフラットに評価可能な要件としていただくことで、幅広い事業者からの提案が期待できるためです。	同等であることの証明を提案書で説明してください。

44	12	5.2. (4)	システム運用班リーダーは、ITサービスマネージャ試験、ITIL4 マネージングプロフェッショナル等の資格保有者等であること。	上位資格だけでなく、「ITIL Foundation (v3/4) 等の基礎資格を保有し、かつ5年以上の運用経験および3年以上のリーダー経験を有する者」についても同等の能力を有するとして認めていただけないでしょうか。	ITIL上位資格（マネージングプロフェッショナル等）の取得者は市場でも少なく、要員確保が極めて困難です。基礎的なフレームワークを理解した上で豊富な現場運用経験を持つリーダーの配置を許容いただく方が、実践的で安定した運用体制の構築に繋がるためです。	特定の資格保有者だけではなく、「同等の能力を有することが、経歴等において、明らかな者」も要件に含めていますので、原案どおりとします。 同等であることの証明を提案書で説明してください。
45	12	5.2. (5)	情報セキュリティ責任者は、情報処理安全確保支援士、CISA、CISM、CISSP等の資格保有者等であること。	特定の高度セキュリティ資格保有者のみならず、「情報セキュリティマネジメント試験等の基礎資格を有し、かつ企業のセキュリティ専門組織（CSIRTやSOC）が当該責任者を組織的に支援・バックアップする体制」をもって同等要件として許容していただけないでしょうか。	高度なセキュリティ脅威に対応するためには、個人の資格やスキルに依存する属人的な体制よりも、企業の専門組織（CSIRT等）によるチーム体制での対応の方が確実性が高いためです。組織的支援を評価いただくことで、より盤石なセキュリティ体制を提案可能になります。	同上。
46	13	5.3.	(2) 諸設備、物品等資源 本会のセキュリティポリシーを遵守の上、本会の了承を得ること。	具体的にどの設備・物品等資源を対象として、どのような手続きにより貴会の了承を得る必要があるのか、ご教示いただけないでしょうか。あらかじめ定められた手続きや承認基準がございましたら、併せてご提示ください。	正確な仕様・要件を確認するため。 適正な費用見積のため。	本会セキュリティポリシーにより以下の対策を想定しています。具体的には、契約後協議することとします。「要管理対策区域の特性に応じて、以下の観点を全て含む対策の基準を運用規程として定めること。 (ア) 許可されていない者が容易に立ち入ることができないようにするための、施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。(イ) 許可されていない者の立入りを制限するため及び立入りを許可された者による立入り時の不正な行為を防止するための入退管理対策。」
47	13	6.1.	(4) 情報セキュリティインシデントが発生する等、万一の事故があった場合に直ちに本会に報告した上で、事故発生の経緯、対応、再発防止策等が具体的に分かる事故報告書を適時に提出すること。また、受託者の責に起因する事故であった場合は、損害に対する賠償等の責任を負うこと。	意見 ・損害賠償は受託者の帰責性がある直接かつ通常の損害に限定し、賠償上限、不可抗力及び発注者・第三者起因の免責を契約書で明確化いただきたい。	・賠償範囲と上限が不明なままでは、間接損害や逸失利益を含む無制限責任と解釈され得るため。	損害賠償については契約書に記載されます。
48	17	8.1.	提案に関する留意事項	提案書の作成にあたり、仕様書に記載がありませんでしたので、以下2点についてご教示願います。 ・提案書の体裁は縦横のご指定はありますでしょうか。 ・提案書の最大ページ数の目安はありますでしょうか。	貴会の想定に沿った提案書作成のため。	8.1. の記載に、提案書に関する詳細を追加しました。
49	18	8.1.-1 (6)	(ア) 第 5 章に記載した機器について、製品名、機能、性能、設置占有面積、設置高さ、重量、消費電力、発熱量等の一般的な仕様について記載する（又は資料を提供する）こと。	「第5章に記載した機器について」とありますが、第5章の記載内容と整合していないため、修正願います。	「第 5 章に記載した機器について」とありますが第 5 章は作業の実施体制・方法に関する事項の章であり、機器についての記載が見られなかったため。	8.1(7)の記載を見直しました。
50	19	8.3.	(1) 受注者は、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本会に無償で譲渡するものとする。	意見 ・無償譲渡の対象から受託者の既存知財、汎用部品、テンプレート、OSS及び第三者権利物を除外し、成果物固有部分のみを対象としていただきたい。	・既存ノウハウまで譲渡対象と解釈されると他案件で利用できず、第三者ライセンス上も譲渡できない場合があるため。	7.1の記載を見直しました。
51	20	9.1.	(2) 受託者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。	遂行責任者とは「表5.1.-1 本業務における組織等の体制と役割」のどちらに該当しますでしょうか。また、資本関係のあるグループ会社の出向社員は"契約社員"に含まれますでしょうか。	受注業者のシステム運用班のリーダーは、グループ内からの出向社員を想定しております。遂行責任者がシステム運用班のリーダーに該当し、出向社員が契約社員に含まれる場合、入札参加が難しくなるため。	遂行責任者とは、表5.1-1の「役割」欄に記載しているように、「受注者側のプロジェクト統括管理責任者」のことです。

52		Garoonワークフローイメージ	11.Garoonワークフローイメージ	合計12本のワークフローイメージが公開されておりました。 Q1. この12本は、ワークフローの総数でしょうか？ ワークフローは12本しかない、ということでしょうか？という意味の質問です。 Q2. この12本は、代表的なパターンを集約したものでしょうか？ 実際のワークフローは、もっと大量にあるが、この12本のパターンに集約可能であるという意図でしょうか？という意味の質問です。 Q3. この12本は、なんらかの特徴的があるものをピックアップされたのでしょうか？ 実際のワークフローは、もっと大量にあるが、何某かの理由で、この12本に注目して欲しいという意図から選択頂いたのでしょうか？という意味の質問です。 Q4. Q1～Q3 への回答がいずれも No（いいえ）ならば、どのような意味を持つ12本なのでしょうか？	正確な仕様・要件を確認するため。 適正な費用見積のため。	ワークフローは現時点で23本あります。イメージの12本は代表的なものの例示とご理解ください。
53		意見招請説明会 QA	質問：JVは可能か。 回答：可能である。	意見招請説明会 QAで、JVは可能と回答ありますが、JVではなく、第三者賃貸による三者間契約は可能でしょうか。（お客様、ベンダー、リース会社） ノート型クライアント端末等は、リース会社からリース。クラウドサービスはベンダーから提供 等。	事業者として、JVより第三者賃貸の方が契約が容易な場合が多いと思われ、参入障壁が下がるため。	三者間賃貸借であることのみをもって入札参加グループに該当するものではありません。調達仕様書における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」を指します。したがって、入札参加グループに該当するか否かは、三者間賃貸借であるか否かではなく、入札参加の形態が上記定義に該当するかにより判断します。
54				昨今の社会情勢の悪化など落札業者に起因しない事由により、全国的なサプライチェーンへの影響等により落札後納品までに物件価格の大幅な上昇があった場合、落札金額について別途協議が可能ですか。	適正な費用見積のため。	8.2(5)に、「契約期間中に、クラウド利用料等の著しい価格改定が生じた場合等には、本会と協議を行うこと。」を追加しました。
55				本業務を円滑かつ安全に実施するためには、契約後の現行調査だけでなく、意見招請時点においても、現行環境の前提を一定程度把握した上で、移行計画、リスク対策、体制、スケジュール、見積を検討することが重要と考えます。 そのため各種設計ドキュメントについて、資料閲覧の機会を設けていただくよう願います。	現時点で開示いただいている内容のみですと、現行環境を把握している事業者と、それ以外の事業者との間で、提案内容、リスク評価、移行計画及び見積精度に差が生じる可能性があり、競争性・公平性確保の観点から確認の必要があるため。	詳細は、別途資料提供を行います。無線LANの設置作業の詳細は、希望により公示後現地調査を行うことができます。
56	要件定義書	1.1.-1	・本会とクラウドサービス間の接続は、原則として、国立情報学研究所（NII）が提供する学術情報ネットワーク（SINET）を利用する。	KBCからインターネット及びMicrosoft Azureを含むクラウドサービスへの通信について、原則としてKBCからSINET経由とし、KBCから直接インターネットへ出る経路は設けないものと理解しております。当該認識に相違ないか、ご教示願います。	KBCから、SINET接続用の2系統の他にインターネット接続する回線が必要か、確認のため。 SINET接続に関する不明確な要件がスコープに含まれる場合、特定の既存ベンダ優位に働く恐れがあるため。	要件定義書1.3.-3に、詳細を記載しました。
57	要件定義書	1.11.-2	・利用者が業務に必要な情報へ迅速にアクセスできるポータル機能を提供すること。 ・ポータル画面には、少なくとも以下の情報を統合的に表示できること。 ①スケジュール情報 ②お知らせ・掲示板情報 ③規程・マニュアル等へのリンク ④業務システムへのショートカット ⑤その他本会が必要と認める情報 ・利用者の所属、権限その他の属性に応じて表示内容を変更できること。 ・ポータル画面のレイアウト及び表示内容を管理者が容易に変更できること。	質問： ・ポータル画面については、既に稼働しているページの移行という認識でよろしいでしょうか (画面作成は不要の認識で正しいでしょうか) 質問： ・ポータル画面の運用・管理（バージョンアップに係る修正、レイアウト変更、URLリンクやコンテンツ、メッセージの更新など）は役割範囲外と考えてよろしいでしょうか	ポータル画面の新規作成・移行及び運用管理の役割範囲を明確にし、必要な作業体制と費用を適正に見積もるため。	ポータル画面の初期画面は、現行ページに準拠して移行いただく想定です。「管理者が容易に変更できること」と記載のとおり。内容の修正等は調達範囲外です。
58	要件定義書	1.11.-1	「Microsoft 365 を中心とした統合グループウェア基盤を提供すること。」 （表1.11.-1 に掲げられた機能：ポータル、スケジュール、会内ファイル管理共有、ワークフロー、施設予約）	現行 Garoon で利用されている機能のうち、本仕様書（案）に明記のない機能の取扱いについて明記をお願いします。 具体的には、タイムカード（勤務時間管理）、ToDo 管理、電話メモ、アドレス帳（共有アドレス帳）等です。 特にタイムカード機能については、次期システムでの代替提供が本調達の範囲に含まれるか否か、明記をお願いします。	現行機能のうち次期システムでの提供対象が不明な機能があると、稼働後の機能欠落又は追加開発の発生を招くため。	記載のないものは調達範囲外です。
59	要件定義書	1.11.-1／1.11.-6 1.12.-1／1.12.-3	「データは原則として単一のシステムで管理し、二重管理を行わないこと。」 「ファイル管理は SharePoint Online 又は OneDrive for Business を利用して実現すること。」 「ファイルサーバは、KBC 内もしくはクラウド環境に一式設置すること。」	1.11.-6（グループウェアの会内ファイル管理＝SharePoint Online／OneDrive）と 1.12（ファイル共有基盤＝ファイルサーバ、実効容量 100TB）の役割分担について明記をお願いします。 両者を併設する場合、1.11.-1 の「二重管理を行わないこと」との整合（どの種類のデータをどちらに配置するかの基本方針）についてもご教示ください。	文書の配置先が二系統に分かれる場合、利用者の混乱、二重保管、権限管理の複雑化を招くため、設計方針の確定が必要であるため。また両者の容量配分が費用に直結するため。	グループウェアの会内ファイル管理は主に会内規程類の共有に使用しています。ファイルサーバ上の規程ファイルを利用者が閲覧できる方式でも構いませんので、ご提案ください。

60	要件定義書	1.11.-2／1.11.-3 1.11.-5	「ポータル画面には、少なくとも以下の情報を統合的に表示できること。① スケジュール情報 ② お知らせ・掲示板情報 ③ 規程・マニュアル等へのリンク ④ 業務システムへのショートカット」 「既読確認又は閲覧状況を確認できることが望ましい。」	現行 Garoon のポータル・掲示板について、以下を明記またはご開示をお願いします。 ① 移行対象とするポータル部品（他アプリへのリンク集・ランチャ等を含むか） ② 掲示板の運用実態（年間掲載件数、カテゴリ数、添付有無、掲載期間、過去分の移行要否） ③ 1.11.-5 の「既読確認」は、個人単位の既読管理を求める趣旨か、閲覧数等の集計レベルで足りるか	SharePoint Online の標準機能では個人単位の既読管理は提供されず、実現にはカスタム開発を要するため、要求水準により工数が変わるため。	要件定義書1.11.-7の記載に以下を追加しました。「現行ワークフローの詳細は、別途資料提供を行う。」 また、別途資料提供の中に入っているとおり、「既読確認又は閲覧状況を確認」は個人単位を想定しています。
61	要件定義書	1.11-2	ポータル機能 ・利用者の所属、権限その他の属性に応じて表示内容を変更できること。	① スケジュール情報 ② お知らせ・掲示板情報 ③ 規程・マニュアル等へのリンク ④ 業務システムへのショートカット ⑤ その他本会が必要と認める情報 ①～⑤のどのコンテンツに対して「利用者の所属・権限に応じて表示内容を変更できる」を実現する必要があるでしょうか？	正確な仕様・要件を確認するため。 適正な費用見積のため。	① スケジュール情報 ② お知らせ・掲示板情報 ③ 規程・マニュアル等へのリンク ④ 業務システムへのショートカット ⑤ その他本会が必要と認める情報 のそれぞれに対して、「利用者の所属、権限その他の属性に応じて表示内容を変更できること。」を想定しています。
62	要件定義書	1.11-3	ポータル機能 ・ポータル上に業務支援のための簡易ユーティリティ等を追加できる拡張性を有すること。	業務支援の為の簡易ユーティリティとはどのような機能を想定されておりますでしょうか。	ポータルについてはSharePoint 標準 Webパーツでの実装を想定しているが、その実現が可能なのか確認するため。 正確な仕様・要件を確認するため。 適正な費用見積のため。	現時点では、セキュリティポリシーに沿ったパスワードの生成ユーティリティなどを想定しています。
63	要件定義書	1.11.-4 1.11.-1	「スケジュール管理は Exchange Online（Outlook）を利用して実現すること。」 「以下の表示形式に対応すること。① 日表示 ② 週表示 ③ 月表示 ④ 年表示 ⑤ グループ日表示 ⑥ グループ週表示」 （1.11.-1「Microsoft 365 に標準機能として備わる機能については、独自開発によらず当該機能を優先的に利用すること。」）	④年表示は Outlook（Web版・デスクトップ版）の標準機能には備わっておりません。また⑤グループ日表示・⑥グループ週表示についても、現行グループウェアと同等の一覧性を有する表示は標準では提供されていません。 ① 標準機能による代替（予定表の重ね合わせ表示・分割ビュー、スケジュールビュー、予定表グループ等）をもって充足とみなすよう要件緩和のご検討をお願いします。 ② 緩和されない場合、当該表示のためのカスタム開発（Microsoft Graph API + SharePoint Framework 等）を許容いただけるかについて明記をお願いします。	1.11.-1 の「独自開発によらず標準機能を優先」との方針と、標準機能では実現できない表示要件が併存しており、いずれを優先するかで構成・工数・稼働後の保守性が大きく変わるため。	要件定義書1.11.-4は、以下のように修正しました。「スケジュール管理は Exchange Online（Outlook）を利用して実現すること。以下の表示形式に対応すること。 ① 日表示 ② 週表示 ③ 月表示 ④ グループ表示 なお、グループ表示については、Microsoft 365標準機能（予定表グループ、スケジュールビュー、重ね合わせ表示等）により複数利用者の予定を一覧で確認できること等による実装を提案するものとする。」 なお、標準機能で不足する場合、独自開発を妨げるものではありませんが、可能な限り標準的な機能の組み合わせ等により提案してください。
64	要件定義書	1.11-4	スケジュール管理機能 ・ポータル上から Outlook カレンダーを参照及び操作できること。	SPO には、グループのイベント表示をする Web パーツのみが存在し、個人のカレンダーを表示/操作可能な標準 Web パーツは存在しません。 ポータル上に Outlook カレンダーを表示するリンクを配置することで代替可能でしょうか？	正確な仕様・要件を確認するため。 適正な費用見積のため。	要件定義書1.11-7に、「現行ワークフローの詳細は、別途資料提供を行う。」を追加しました。 また、別途資料提供の中に入っているとおり、「1.11.-5・既読確認又は閲覧状況を確認」は個人単位を想定しています。
65	要件定義書	1.11.-5	既読確認又は閲覧状況を確認できることが望ましい。	区分が空欄となっておりますが、スケジュール管理機能に関する要件との認識で相違ないか、ご教示願います。	区分が空欄となっております、本要件の対象機能を特定できないため。	要件定義書1.11.-5の区分を記載しました。
66	要件定義書	1.11.-5	スケジュール管理機能 ・既読確認又は閲覧状況を確認できることが望ましい。	既読確認又は閲覧状況を確認できる対象は「② お知らせ・掲示板情報」のみでよろしいでしょうか？ また、既読確認又は閲覧状況を確認できるというのは、閲覧者本人が自身の既読・閲覧状況を確認できるということですか？あるいは管理者が利用者全体の既読確認、閲覧状況を確認したいということでしょうか？	正確な仕様・要件を確認するため。 適正な費用見積のため。	「1.11.-5・既読確認又は閲覧状況を確認」は個人単位を想定しています。

67	要件定義書	1.11.-7	・Microsoft 365と連携可能なワークフロー機能を提供すること。 ・申請、承認、差戻し、通知等の業務プロセスを電子化できること。 ・ワークフロー基盤は、Microsoft Power Platformその他同等の機能を有する製品又はサービスにより実現してもよい。 ・以下の機能を有すること。 ①申請 ②承認 ③差戻し ④段階承認 ⑤通知 ・申請状況及び承認状況を利用者が確認できること。 ・申請及び承認履歴を保存し、検索及び参照できること。	質問： ・ワークフローはあくまで基盤提供であり、ワークフローの構築自体は役務対象外の認識でよろしいでしょうか。また、左記を実現可能な最低限のものを実装する想定でよろしいでしょうか。	ワークフロー機能の提供範囲及び構築責任を明確にし、役務対象外又は過剰な実装要件が含まれていないか確認するため。	現在利用している23本のワークフローについては、令和8年度データを含めて移行いただく想定（ワークフロー自体の運用は調達範囲外）です。要件定義書の1.11-7に、「現行ワークフローの詳細は、別途資料提供を行う。」を追加しました。
68	要件定義書	1.11.-7	ワークフロー機能 ・Microsoft 365と連携可能なワークフロー機能を提供すること。	ワークフローの機能数について、おおよそでも構いませんので想定があればご教示ください。 汎用的なワークフローを1つだけ開発し、各申請内容は EXCEL ファイルなどで入力・添付する方法を想定していますが、各申請内容ごとに個別でワークフローを開発する必要があるでしょうか？	正確な仕様・要件を確認するため。 適正な費用見積のため。	同上。
69	要件定義書	1.11.-7	「Microsoft 365 と連携可能なワークフロー機能を提供すること。」 「① 申請 ② 承認 ③ 差戻し ④ 段階承認 ⑤ 通知」	現行グループウェア（Garoon）で稼働中のワークフローについて、以下を明記またはご開示をお願いします。 ① 一覧（名称・用途・年間申請件数・承認段数） ② 各フローの入力項目・承認経路・帳票が分かる資料又は画面の閲覧機会 ③ 本調達での移行対象範囲（フロー定義のみか、過去の申請・承認履歴データを含むか） ④ 実装分担（受注者が全数を設計・実装するのか、標準テンプレート提供のうえ本会が追加作成するのか）	移行対象フローの本数・複雑度・実装分担が工数を最も大きく左右する要素であり、これが不明な場合は適正な費用見積が困難であるため。	同上。
70	要件定義書	1.11.-7 1.15.-7	「ワークフロー基盤は、Microsoft Power Platform その他同等の機能を有する製品又はサービスにより実現してよい。」 「PowerApps や Power Automate 等のクラウドサービスを用いて自動化できることが望ましい。」	Power Platform の前提ライセンス範囲について明記をお願いします。 Microsoft 365 に同梱される範囲（標準コネクタ、Microsoft 365 内データ）を前提とするか、Premium コネクタ、Dataverse、オンプレミスデータゲートウェイ、AI Builder 等の利用を想定するかにより、Power Apps／Power Automate の Premium ライセンス（利用者単位）の追加調達の要否が変わります。	Premium ライセンスは利用者数×月額での追加費用となり、対象人数により5年間の総額が大きく変動するため。	要件を実現できる構成、ライセンス等を提案してください。
71	要件定義書	1.11.-7	ワークフロー機能 ・以下の機能を有すること。 ① 申請 ② 承認 ③ 差戻し ④ 段階承認 ⑤ 通知	③差戻しは必須の機能でしょうか？申請の却下および申請を再作成することで代替可能でしょうか。	③差戻しを実施する場合、追加のコストが発生するため。	要件定義書1.11.-7の記載に以下を追加しました。「ワークフローの上位者に差戻しされたことが下位者や申請者に通知されること。」
72	要件定義書	1.11.-8	「会議室等の施設予約は Exchange Online のリソースメールボックス機能を利用して実現すること。」 「必要に応じて承認フローを設定できること。」	予約対象の範囲及び規模について明記をお願いします。 ① 会議室等の施設数 ② 会議室以外の備品・貸出品（プロジェクト、貸出PC、公用車等）を予約対象に含めるか ③ 承認を要する施設・備品の件数	会議室の施設数や会議室以外の備品・貸出品数により、リソースメールボックス作成・設定作業の工数が変動するため。	要件定義書1.11.-8に記載したとおり、会議室等の施設予約の詳細については、別途資料提供を行います。
73	要件定義書	1.1.-2	・業務系サーバについては、業務アプリケーションの実行に必要な仮想サーバ（OS、ミドルウェアを含む）又は PaaS、SaaS を利用して業務機能をデプロイすること。その際、デプロイに必要な情報をあらかじめ整理・とりまとめること。デプロイ後は、必要に応じて運用開始までの支援を行うこと。	業務系サーバは仮想基盤上の業務サーバ(3環境)を指しているとの認識でよいか、ご教示願います。 業務サーバの移行については、業務要件を踏まえた全体設計が必要となり、検討範囲の拡大に伴う構成の複雑化および費用増加につながる可能性があるため、調達範囲外にすることが望ましいと考えますので記載削除を願います。 調達範囲内にする場合は、業務サーバ移行に関する要件詳細の追記を願います。	業務サーバ(3環境)の移行について不明確な部分があるため。 業務系サーバに関する不明確な要件がスコープに含まれる場合、特定の既存ベンダ優位に働く恐れがあるため。	業務サーバ(3環境)は調達範囲外です。業務系サーバは、ファイル共有基、外部ファイル共有基を指します。
74	要件定義書	1.1.-2	共通要件 ・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。	運用設計書は「表3.1.-1 成果物一覧」に成果物として追加いただけないでしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	表3.1.-1に記載の「基本設計書」の1セクションとして、「運用設計」等を含めてください。

75	要件定義書	1.12.-1	・スナップショット機能を有し、ファイル単位のバックアップ／リストアが可能であること。	以下のように記載要件の緩和をご検討願います。 「スナップショット機能又は同等のバージョン管理及び復元機能を有し、ファイル単位のバックアップ／リストアが可能であること。」	ファイル共有基盤の実現方式で、クラウド型サービスではスナップショットではなく、バージョン管理及びファイル復元機能により同等のデータ保護を実現する方式が一般的であるため、どちらでも提案できる柔軟性を確保するため。	要件定義書1.12.-1の記載を、ご指摘のとおり修正しました。
76	要件定義書	1.12.-1	・ファイルサーバは、KBC内もしくはクラウド環境に一式設置すること。クラウド化するには物理ストレージに関する要件は適用しないが、クラウドサービスの公表スペックを明示すること。 ・ファイルサーバと外部向けファイル共有基盤の機能を分離して構成する場合において、Box等のクラウドファイルサーバを利用する場合は、当該サービスに必要なライセンス費用を本調達に含めること。 ・ファイルサーバにおいて、日本語を含む多言語のファイル名を扱えること。 ・Windows／macOS／Linuxなど複数OSから、公式クライアント又はWebブラウザで同一領域へアクセス可能であること。 ・Webベースの管理ツールを提供すること。 ・スナップショット機能を有し、ファイル単位のバックアップ／リストアが可能であること。 ・本会の指示に基づき、フォルダ単位のアクセス権設定が可能であること。 ・以下の2種類の領域を論理的に分離できること。 ① 役職員用領域 ② 研究員用領域 また、研究員用仮想デスクトップから役職員領域へアクセスできないよう制御できること。 ・ファイル共有サービス中の障害時に自動フェイルオーバーし、サービスが停止しないこと。 ・拠点障害が発生してもサービス継続可能な構成であること。 ・ファイルサーバ機能を停止せずにファイルシステムを拡張できること。	質問： ・フォルダ単位のアクセス権限設定について、受託者での作業実施を想定されておられますでしょうか。	アクセス権限設定の作業実施者と責任分界を明確にし、必要な作業工数及び運用体制を正確に見積もるため。	要件定義書1.12.-1の記載にある「本会の指示に基づき、フォルダ単位のアクセス権設定が可能であること。」は、構築作業時点での受託者による移行を想定しています。
77	要件定義書	1.12.-1	共通要件（クラウド / オンプレ共通） ・ファイルサーバと外部向けファイル共有基盤の機能を分離して構成する場合において、Box 等のクラウドファイル共有サービスを利用する場合は、当該サービスに必要なライセンス費用を本調達に含めること。	以下の内容に変更頂く事を提案します。 ----- ファイルサーバと外部向けファイル共有基盤を統合して構成する場合は、ファイルサーバとして利用するフォルダ構造やセキュリティに関する設計や設定等の見直しを実施すること。 なお、ファイルサーバと外部向けファイル共有基盤を分離して構成する場合においては、Box等のクラウドサービスが備えているセキュリティや機能を包含する形で導入すること。 どちらの構成の場合も、当該サービスに必要なライセンスについては本調達に含めること。	分離構成とする場合の要件に関する記載はあるが、統合した場合の要件がないため要件の理解を深めるため。 また、どちらの提案となってもセキュリティレベルや利便性の確保は重要な要素と考えるため同一水準となるような要件記載は必要と考えます。	要件定義書1.12.-1 の記載に、統合した場合の記載と、必要なライセンス費用は本調達に含めることを追加しました。
78	要件定義書	1.12.-1	共通要件（クラウド / オンプレ共通） ・Web ベースの管理ツールを提供すること。	提供される管理機能について想定されている機能がございましたらご教示いただけないでしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	要件定義書1.12.-1に以下の記載を追加しました。 「管理者がWebブラウザを利用して共有設定、アクセス権、容量及び運用状況の確認等の管理を実施できること。」
79	要件定義書	1.12-1	共通要件（クラウド / オンプレ共通） ・本会の指示に基づき、フォルダ単位のアクセス権設定が可能であること。	本会の指示に基づき、フォルダ単位のアクセス権設定が可能であること。アクセス権設定は、現在外部共有で利用している7段階の付与が可能であること。	現在利用されているアクセス権限は踏襲することが求められると思いますのでセキュリティの維持・向上となるように要件の追記をご提案します。	要件定義書1.12.-1の記載に以下を追加しました。「アクセス権設定は、現在外部共有で利用している7段階の付与が可能であること。」
80	要件定義書	1.12.-1	共通要件（クラウド / オンプレ共通） ・ファイルサーバ機能を停止せずにファイルシステムを拡張できること。	以下の内容に変更頂く事を提案します。 ----- ファイルサーバ機能を停止せずにファイルシステムを拡張できること。拡張で必要な課金が生じる場合は提案に含めること。	導入後にデータ容量の増加が著しく増えているケースも多く、従量課金の金額も大きく膨らむ可能性があるため。	要件定義書1.12.-1の記載を以下のように修正しました。 「ファイルサーバ機能を停止せずにファイルシステムを拡張できる機能を有すること。拡張が必要な場合は、発注者と協議すること。」

81	要件定義書	1.12.-2	共通要件（クラウド / オンプレ共通） ・ストレージ全体又はファイルシステムごとに暗号化が可能な場合は、加点として評価する。	以下の内容に変更頂く事を提案します。 ----- ストレージ全体又はファイルシステムごとに暗号化が可能な場合は、加点として評価する。暗号化については政府推奨の暗号化リストに掲載されているものを活用することを前提とする。	暗号化の強度を明確にするため。	要件定義書1.12.-2の記載に以下を追加しました。 「保存データ及び通信経路の暗号化に使用する暗号アルゴリズムは、CRYPTREC（暗号技術検討会及び関連委員会）が公表する最新の「電子政府推奨暗号リスト」に掲載された方式を採用すること。 また、将来の耐量子計算機暗号（PQC）への移行に対応できるよう、暗号方式の変更又は追加が可能な構成（Cryptographic Agility）を有すること。」
82	要件定義書	1.12.-3	・KBC側及びクラウド側の仮想サーバが全て稼働している状況でもストレスなく動作すること。 ・クラウドサービスの公表スペックに基づき、仮想サーバ40TB、ファイルサーバ100TB相当の実効容量を確保できること。 ・クラウドサービスが提供する冗長機能により、高い可用性及び耐障害性を確保すること。 ・クラウドサービスの標準機能により、ファイル共有サービスが停止しない構成を実現できること。	質問： ・ストレスなくの表現を明確にしていけないでしょうか ・記載の容量は運用期間内の増加は考慮する必要はないでしょうか ・仮想サーバ40TBの使用用途をご教示いただけないでしょうか。（仮想化基盤サーバーに搭載するストレージの総容量が、またオンプレ、クラウドどちらも構築する場合は、合計のストレージ総容量という理解で良いか）	性能基準、必要容量及び40TBの対象範囲を明確にし、適切なシステム構成と費用を算定するため。	要件定義書1.12.-3の記載を以下のように修正・追加しました。 「・KBC側及びクラウド側の仮想サーバが全て稼働している状態においても、ファイルサーバの利用に必要な性能を確保し、ファイルの参照、保存及び検索を円滑に実施できること。なお、その根拠となるサイジング及び性能設計を提案書に記載すること。 ・ファイルサーバ機能を停止せずにファイルシステムを拡張できる機能を有すること。拡張が必要な場合は、発注者と協議すること。」
83	要件定義書	1.12.-3	クラウド利用の場合 ・クラウドサービスの公表スペックに基づき、仮想サーバ 40TB、ファイルサーバ 100TB 相当の実効容量を確保できること。	以下の内容に変更頂く事を提案します。 ----- クラウドサービスの公表スペックに基づき、ファイルサーバ100TB相当の実行容量を確保できること。なお、利用期間中に増加する容量は無制限で利用できるサービスであること。	仮想サーバの容量については、必要な管理サーバやスペックは提案構成により異なるため削除を提案します。また末尾の容量無制限の記載については、容量超過を避けるために提案します。近年のデータ容量のさらなる増大、クラウド利用時はバージョン管理の過去バージョンまで容量の対象となり、当初の想定を超えた容量超過による課金の事例が増えております。	同上。
84	要件定義書	1.12.-4	オンプレ利用の場合 ・以下の実効容量を満たすこと： 仮想サーバ：40TB ファイルサーバ：100TB	以下の内容に変更頂く事を提案します。 ----- ・以下の実効容量を満たすこと： ファイルサーバ：100TB	仮想サーバの容量については、必要な管理サーバやスペックは提案構成により異なるため削除を提案します。	同上。
85	要件定義書	1.12.-4	・KBC側及びクラウド側の仮想サーバが全て稼働している状況でもストレスなく動作すること。 ・EIA規格19インチラックに搭載可能であること。 ・物理ストレージはラックマウント型であること。 ・ストレージ専用OSを搭載していること。 ・以下の実効容量を満たすこと。 仮想サーバ：40TB ファイルサーバ：100TB ・ストレージプロセッサ（コントローラ）を2式搭載した冗長構成であること。 ・ストレージはRAID5又はRAID6相当の耐障害性を有すること。 ・ファイル共有サービス中のファイルサーバ障害時には、自動的にフェイルオーバーし、サービスが停止しないこと。	質問： ・全てをクラウドにする場合、オンプレ機器は必要ないという認識でよろしいでしょうか	クラウド構成を採用する場合のオンプレミス機器の要否を確認し、不要又は重複する設備費用を見積もりから除外するため。	ファイル共有基盤 については、ご理解のとおりです。
86	要件定義書	1.12.-5	・ファイルサーバは、ファイルサーバ機能を停止することなくファイルシステムを拡張する機能を有する場合は、加点として評価する。 ・主要コンポーネント（コントローラ、電源、冷却ファン、バッテリー、ディスク等）に関して、障害発生時にもサービスを停止せずに交換・修理できるオンラインメンテナンス機能を有する場合には、加点する。	質問： ・オンプレ利用した場合は加点对象となるが、クラウド利用の場合は加点对象とならない、という趣旨で認識っておりますでしょうか。	クラウド構成とオンプレミス構成の評価基準を正確に理解し、提案方式による評価上の不利益が生じないことを確認するため。	ご理解のとおりです。
87	要件定義書	1.13.	業務アプリケーション基盤	業務アプリケーション基盤ですが、1.9.クライアント端末管理基盤、1.10.ノート型クライアント端末に記載される要件と思われます。独立した業務アプリケーション基盤は無い認識ですので、それぞれの要件分野に分散整理した記載が望ましいと考えますので修正をご検討願います。	抜け漏れのない要件確認と提案検討をさせていただくため。	ご指摘の趣旨に従い、記載を見直しました。

88	要件定義書	1.13.-10	文書作成 ・業務に必要な文書作成ソフトウェアを利用できること。	既存では一太郎・ATOKを利用されていますが、次期システムでは不要の認識でお間違いないでしょうか。	調達範囲を明確にするため。	ご理解のとおりです。
89	要件定義書	1.13.-2	セキュリティ方式 ・RBI又はEnterprise Browser等の方式を採用し、Webアクセスの安全性を確保できること。	RBI及びEnterprise Browserについての仕様は削除いただけないでしょうか。	SSE及びEDRによりWebアクセスのセキュリティを確保可能と考えるため。また、RBI及びEnterprise Browserを採用した場合、導入・運用コストが増加するほか、一部Webアプリケーションの利用制限や操作性への影響が生じる可能性があるため。	要件定義書1.13.-2の記載は以下のとおり修正しました。 「Webアクセスにおいて、マルウェア感染、フィッシング、不正スク립ト実行その他の脅威から端末を保護できること。」 また、要件定義書の1.13.-3の記載を以下のとおり修正しました。 「RBI（Remote Browser Isolation）、Enterprise Browser又はこれらと同等以上の機能により、Webコンテンツを端末から分離された環境で実行し、端末へのリスクを低減する仕組みを提供する場合は加点とする。なお、この場合Microsoft Edge以外のブラウザも可とする。」
90	要件定義書	1.13.-3	・Webコンテンツを隔離環境で実行し、端末へは表示情報のみを転送できる構成（Web隔離：RBI）とすること。 ・Webアクセスの安全性を確保するため、RBIのほか、Enterprise Browser等の高度なセキュリティ対策機能を併用又は代替方式として採用できること。（RBI、Enterprise Browser等を使用する場合は加点） ・Webサイト閲覧時において、危険なサイトへのアクセスブロック、不正なプログラムの実行防止、及び端末側への不要なデータ保存（ローカル保存）を制限できる構成とすること。	質問： ・Web隔離環境利用時におけるブラウザについても、Microsoft Edgeのみでよろしいでしょうか ・Webブラウザの利用において、全てのコンテンツがWeb隔離の対象となるのでしょうか。例外としてWeb隔離の非対応コンテンツへのアクセスは、ローカル環境のブラウザでのアクセスする等 ・Microsoft EdgeのInprivateモードは利用していない認識で問題ないでしょうか 意見： ・必須項目と任意項目で同一の内容を記載しているため、明確に項目を分けて記載いただけないでしょうか。	Web隔離の対象範囲、利用条件及び必須・任意要件の区分を明確にし、適合する製品構成と費用を正確に見積もるため。	同上。
91	要件定義書	1.13.-3	・Webコンテンツを隔離環境で実行し、端末へは表示情報のみを転送できる構成（Web隔離：RBI）とすること。 ・Webアクセスの安全性を確保するため、RBIのほか、Enterprise Browser等の高度なセキュリティ対策機能を併用又は代替方式として採用できること。 ・危険なサイトへのアクセスブロック、不正プログラムの実行防止及びローカル保存を制限できる構成とすること。	質問： ・Enterprise Browserを利用する場合、インターネットアクセスには独自ブラウザを使用してもよろしいでしょうか。	Enterprise Browser採用時に許容されるブラウザと利用条件を明確にし、要件に適合する製品及び構成を選定するため。	同上。
92	要件定義書	1.13.-3	Web 隔離 ・Web コンテンツを隔離環境で実行し、端末へは表示情報のみを転送できる構成（Web 隔離／RBI）とすること。 ・Web アクセスの安全性を確保するため、RBI のほか、Enterprise Browser 等の高度なセキュリティ対策機能を併用又は代替方式として採用できること。（RBI、Enterprise Browser 等を使用する場合は加点） ・Web サイト閲覧時において、危険なサイトへのアクセスブロック、不正なプログラムの実行防止、及び端末側への不要なデータ保存（ローカル保存）を制限できる構成とすること。	RBI 及びEnterprise Browserについての仕様は削除いただけないでしょうか。	SSE及びEDRによりWebアクセスのセキュリティを確保可能と考えるため。また、RBI及びEnterprise Browserを採用した場合、導入・運用コストが増加するほか、一部Webアプリケーションの利用制限や操作性への影響が生じる可能性があるため。	同上。
93	要件定義書	別紙1 1.13.-8 仕様書 1.4	「Microsoft 365 A3 又は A5 を 600 ライセンス提供すること。」 （一方、仕様書 1.4 の利用者は「約 635 名」と記載）	600ライセンスの内訳（役職員350／研究員150／管理者15／海外研究連絡センター70／一時利用者等50のうち、どの範囲を対象とするか）について明記をお願いします。 併せて、利用者属性ごとに異なるライセンス種別を組み合わせる構成（例：役職員はA5、一時利用者・海外はA3／A1／F3等）を許容いただけるかも明記をお願いします。	利用者数（約635名）と提供ライセンス数（600）が一致せず、対象範囲を判断できないため。 また属性別に最適なライセンスを組み合わせることで、要求水準を維持しつつ5年間の総費用を抑制できる余地があるため。	要件定義書1.13.-8の記載を修正しました。 利用者属性ごとに異なるライセンス種別を組み合わせる構成は、セキュリティ等の要件のほか合理性があれば提案可能とします。 合理的である旨を提案書で説明してください。

94	要件定義書	1.13.-8	・Microsoft 365 A3又はA5を600ライセンス提供すること。 ・Microsoft 365 A3又はA5に含まれるOfficeアプリケーション（Word、Excel、PowerPoint、Outlook、OneNote等）を、デスクトップ版・Web版の双方で利用可能とすること。 ・Microsoft 365 A3又はA5は、本会のID基盤（例：Entra ID）と連携し、認証・アクセス制御・ライセンス管理を統合的に行えること。 ・Outlookを利用した電子メール環境（Exchange Online）を提供し、業務利用に必要な初期設定（プロファイル設定、接続設定等）を行うこと。 ・Microsoft 365アプリケーションの更新プログラムは、自動更新又は管理者による制御のいずれにも対応できること。 ・Microsoft 365の利用開始に必要な設定（ポリシー設定、アプリ配布、セキュリティ設定等）を実施し、業務利用が可能な状態とすること。 ・ライセンス管理、利用者追加・削除、トラブル対応等について、必要な運用支援を行うこと。	意見： ・M365の構築時、平行稼働時には現行環境の設定を変更する必要があります。テナントの設定を操作する際は、次期事業者が操作することを許可していただくことをお願いいたします。 ・M365の構築時、平行稼働時に次期事業者が現行環境へアクセスできるようにしていただくことをお願いいたします。（M365環境にアクセスできる端末の貸し出しや、NWに穴をあける許可設定等）	現行M365環境へのアクセス権限及び設定変更の可否は、並行稼働と円滑な移行を実施するための前提条件となり、現行事業者以外の構築作業に公平性を担保するため。	要件定義書3.2.-4の記載に以下を追加しました。 「・現行システムで稼働しているサービスが引き続き使用できるように、移行作業を行うこと。 ・移行作業は、本会及び現行事業者の協力の下で実施するものとし、移行に関する詳細な事項については、本会、現行事業者及び受注者が協議の上、決定するものとする。」
95	要件定義書	1.13.-8	「Microsoft 365 A3 又は A5 を 600 ライセンス提供すること。」	「A3 又は A5」のいずれを前提とするかを明記をお願いします。 別紙1に記載の 1.5.-2（EPP/EDR）、1.5.-6（CASB）、1.5.-7（メールのサンドボックス検査・URL防御）、1.5.-10（SSPM）、1.6.-3（IDリスク検知・異常行動分析）、1.6.-7（特権ID管理の期間限定付与）等の機能要件は、Microsoft 365 A3 では標準提供されず、A5 相当の機能が必要となります。 A3 を前提とされる場合は、これら不足機能を第三者製品等で補完する構成を許容いただけるかを併せて明記をお願いします。	A3 と A5 では単価差が大きく、600ライセンス×5年では総額への影響が極めて大きいため。 また前提が不明確な場合、応札者ごとに見積前提が不統一となり、価格比較の公平性が損なわれるため。	Microsoft365 については、SSEその他の構成によるところが大きいため、総合的に適切な構成、ライセンスを提案いただくため、原案どおりとします。
96	要件定義書	1.13.-9	日本語入力 ・日本語入力については、業務利用に適した日本語入力システム（例：Microsoft IME 等）を利用できること。また、将来的なデータ活用や AI 活用において支障が生じない標準的な日本語入力方式に対応していること。	既存では一太郎・ATOKを利用されていますが、次期システムでは不要の認識でお間違いないでしょうか。	調達範囲を明確にするため。	ご理解のとおりです。
97	要件定義書	1.14.-2	・本会及びパブリッククラウドに設置されたWindows Serverのログを1年以上保存すること。 ・本会及びパブリッククラウドに設置されたLinuxサーバ及びネットワーク機器のログを1年以上保存すること。 ・異なる種類のログを独自形式で一元管理し、収集したログを加工せず保管できること。（原本の状態に戻せること。） ・ログデータは常に圧縮された状態で保管・管理できること。 ・ログデータを暗号化して保存できること。また、ログの改ざんを検出する仕組みを持つこと。 ・収集した未加工のログテキストと、解析されたログ双方とも管理画面から分析ができること。 ・Webベースのインタフェースを介し、ユーザ定義の条件により、検索・集計・レポートが実行できること。 ・ログを定期的にアーカイブする機能を有すること。また、アーカイブしたログの復元も同様にできる機能を有すること。 ・ログ管理システムの利用ユーザのアクセス制限や機能権限の設定ができること。 ・ログの受信件数をダッシュボード形式に表示できること。 ・ログ管理システムへのアクセスを監査できること。 ・管理画面やマニュアル、サポートの提供が日本語であること。 ・市販のRDB製品を用意する必要なく、独自DBによりログを管理可能であること。 ・製品ライセンスの制限により、上限を超えたログが欠落、収集停止するライセンス体系ではないこと。 ・管理画面から受信したログのサイズを確認できること。 ・運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。 ・ログデータをCSV出力する機能を有すること。	質問・提案： ・全サーバーのログを解析する場合、費用高騰が想定されるため、一部サーバー等範囲を限定していただけないでしょうか。 ・ログの改ざん検知について、製品仕様上ログの改ざんを防止する仕組みとなっている場合は、検知は不要で問題ないでしょうか。上記問題がない場合は要件として記載いただきたく考えております。 質問 ・独自DBの記載について、クラウドサービスを利用した実装の場合は独自DBとの認識で問題ないでしょうか。	全サーバーのログ解析は従量課金の増大が想定され、改ざん検知は運用負荷が高く、クラウドサービス利用も考慮されていない可能性があるため、過剰な要件を避けつつ代替手段と対象範囲を明確にするため。	要件定義書1.14.-2の記載を以下のとおり追記・修正しました。 「・ログは、重要度、利用頻度、保存期間等に応じて、ホットストレージ及びコールドストレージ等を組み合わせた段階的な保存方式を採用できるものとする。なお、収集後一定期間（概ね4か月程度）を経過したログについては、コールドストレージ等への移行を可とする。 ・収集したログについて検索及び分析が可能であること。なお、ログの保存方式、解析対象範囲及び分析方法については提案に含めることとし、詳細は契約後に本会と協議の上、決定するものとする。」 質問については、ご理解のとおりです。

98	要件定義書	1.14.-2	・ 本会及びパブリッククラウドに設置されたWindows Serverのログを1年以上保存すること。 ・ 本会及びパブリッククラウドに設置されたLinuxサーバ及びネットワーク機器のログを1年以上保存すること。 ・ 異なる種類のログを独自形式で一元管理し、収集したログを加工せず保管できること。（原本の状態に戻せること。） ・ ログデータは常に圧縮された状態で保管・管理できること。 ・ ログデータを暗号化して保存できること。また、ログの改ざんを検出する仕組みを持つこと。 ・ 収集した未加工のログテキストと、解析されたログ双方とも管理画面から分析ができること。 ・ Webベースのインターフェイスを介し、ユーザ定義の条件により、検索・集計・レポートが実行できること。 ・ ログを定期的にアーカイブする機能を有すること。また、アーカイブしたログの復元も同様にできる機能を有すること。 ・ ログ管理システムの利用ユーザのアクセス制限や機能権限の設定ができること。 ・ ログの受信件数をダッシュボード形式に表示できること。 ・ ログ管理システムへのアクセスを監査できること。 ・ 管理画面やマニュアル、サポートの提供が日本語であること。	「異なる種類のログを独自形式で一元管理し、収集したログを加工せず保管できること。（原本の状態に戻せること。）」について、「原本の状態に戻せること」とは受信した生ログの完全保管の意味でしょうか？それともSIEM上で検索分析可能な状態での保管を意味しますでしょうか？	正確な仕様・要件を確認するため。	要件定義書1.14.-2の記載を、以下のとおり修正しました。 「・異なる種類のログを一元的に管理できること。また、収集したログについて、製品又はサービスが行う正規化、インデックス化その他の処理後においても、原本の内容を確認又は復元できること。 ・ ログデータは、製品又はサービスが提供する保存最適化機能を利用して保管できること。 ・ ログデータを暗号化して保存できること。また、ログの完全性を確保できることとし、改ざん検知、改ざん防止、アクセス制御その他同等の仕組みにより実現できること。」
99	要件定義書	1.14.-2	・ 市販のRDB製品を用意する必要なく、独自DBによりログを管理可能であること。 ・ 製品ライセンスの制限により、上限を超えたログが欠落、収集停止するライセンス体系ではないこと。 ・ 管理画面から受信したログのサイズを確認できること。 ・ 本会及びパブリッククラウドに設置されたWindows Serverのログを1年以上保存すること。 ・ 本会及びパブリッククラウドに設置されたLinuxサーバ及びネットワーク機器のログを1年以上保存すること。 ・ 異なる種類のログを独自形式で一元管理し、収集したログを加工せず保管できること。（原本の状態に戻せること。） ・ ログデータは常に圧縮された状態で保管・管理できること。 ・ ログデータを暗号化して保存できること。また、ログの改ざんを検出する仕組みを持つこと。 ・ 収集した未加工のログテキストと、解析されたログ双方とも管理画面から分析ができること。 ・ Webベースのインターフェイスを介し、ユーザ定義の条件により、検索・集計・レポートが実行できること。 ・ ログを定期的にアーカイブする機能を有すること。また、アーカイブしたログの復元も同様にできる機能を有すること。 ・ ログ管理システムの利用ユーザのアクセス制限や機能権限の設定ができること。 ・ ログの受信件数をダッシュボード形式に表示できること。 ・ ログ管理システムへのアクセスを監査できること。 ・ 管理画面やマニュアル、サポートの提供が日本語であること。 ・ 市販のRDB製品を用意する必要なく、独自DBによりログを管理可能であること。 ・ 製品ライセンスの制限により、上限を超えたログが欠落、収集停止するライセンス体系ではないこと。 ・ 管理画面から受信したログのサイズを確認できること。 ・ 運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。 ・ ログデータをCSV出力する機能を有すること。	「ログデータは常に圧縮された状態で保管・管理できること。」について、ご提案しているSentinelではデータ保存はクラウド上で最適化されておりますが、内部ストレージ実装は未公開であるため、本要件についての回答が難しいものとなります。そのため可能であれば本要件の緩和をお願いいたします。	正確な仕様・要件を確認するため。また、当社からのご提案の最適化のため。	同上。
100	要件定義書	1.14.-2	・ 運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。	「上記要件」の記載について、1.14.-2のどの要件を対象としているかご教示いただきたいです。 また、上記要件が「ログの一元管理」を指している場合、ログの収集・管理では単一のソフトウェアでの実現は困難な認識ですので「任意」要件へと変更を願います。	抜け漏れのない要件確認のため。	要件定義書1.14.-2の記載を見直しました。

101	要件定義書	1.15.		外部公開領域について、ファイルの保管期間及びライフサイクルをご教示願います。 また、外部公開領域として必要となるストレージ容量について、現時点で想定されている容量（初期容量および将来的な増加見込みを含む）がございましたらご教示願います。	外部公開領域を一時的なファイル受け渡し用途として利用するのか、または継続的な保管先として利用するのかにより、必要となるストレージ容量、保管方式および製品選定が異なるため。	要件定義書1.15.-1に記載の外部ファイル共有基盤としては、現在の使用状況は約900GBです。一時的なファイル受け渡し用途として利用するので、増加を見込んでも2倍以下と見込んでいます。
102	要件定義書	1.15.-1	・本システムは、外部機関・外部ユーザとの間で安全にファイル授受を行うための外部ファイル共有基盤を提供すること。 ・外部共有に利用するストレージは内部ファイル共有基盤と論理的に分離し、外部公開領域と内部領域が自動的に混在しない構成とすること。 ・外部公開領域へのアクセスは、内部ユーザとは分離された外部ユーザ管理（ゲストユーザ管理等）により制御できること。	質問： ・内部ファイル共有基盤とは、「1.12 ファイル共有基盤」の記載を指す認識で間違いないでしょうか。 ・オンプレまたはクラウドのどちらかを可とする記載がないがどちらでも可能という認識で間違いないでしょうか。また、使用可能領域の要件等あればご教示いただけないでしょうか。	新設された外部ファイル共有基盤の対象、配置方式及び利用可能領域を明確にし、既存のファイル共有基盤との役割分担を正確に理解するため。	内部ファイル共有は「1.12 ファイル共有基盤」を使用する構成も可とします。 要件定義書1.12.-1においては、ファイルサーバ及び外部向けファイル共有基盤は、統合又は分離して構成することを可としているので、いずれかの構成により、適切な提案をお願いします。 「原則としてクラウド上に構築することを前提とし」ていますが、合理的な理由があればオンプレでの提案も可とします。
103	要件定義書	1.15.-1	「外部共有に利用するストレージは内部ファイル共有基盤と論理的に分離し、外部公開領域と内部領域が自動的に混在しない構成とすること。」	「論理的に分離」の判定基準について明記をお願いします。 ① 同一 Microsoft 365 テナント内に外部共有専用のサイトコレクション（又は専用サイト群）を設け、外部共有ポリシー・秘密度ラベル・条件付きアクセスにより内部領域と分離する構成をもって充足とみなしてよいか ② 別テナント又は別サービス（外部共有専用サービス）による分離を求める趣旨か	分離レベルの解釈により、テナント構成、運用設計及び費用（別テナント／別サービスの追加費用）が大きく異なるため。	要件定義書1.15.-1の記載に以下を追記をしました。 「なお、論理的な分離とは、外部共有専用サイト、専用ライブラリ、専用ストレージ領域その他これらに類する仕組みにより、内部領域と外部共有領域を区分して管理できることをいう。同一テナント内での実現も可とする。」。
104	要件定義書	1.15.-1	共通要件 ・外部公開領域へのアクセスは、内部ユーザとは分離された外部ユーザ管理（ゲストユーザ管理等）により制御できること。	以下の内容に変更頂く事を提案します。 ----- 外部公開領域へのアクセスは、内部とは分離された外部ユーザ管理（ゲストユーザ管理等）により制御できること。なお、外部ユーザについては当会でライセンス消費を負担しなくて済むように外部のアカウントに対してアクセス権を付与し、共有できる仕組みとすること。 アクセス権については、フル操作や閲覧専用、アップロード専用、レビューとアップロードのみを可能とするといった操作制御を多段階で選択できること。	コストおよびセキュリティの観点から、外部ユーザに対してのライセンス消費がある場合は提案に含める要件することや、不要な操作を許容できるようになるとセキュリティレベルも下がるため現在利用されているアクセス権限の設定は必須とすることをご提案します。	実現方法はご提案によることとするため、原案どおりとします。 ※ ご理解は間違っていない。
105	要件定義書	1.15.-2	「外部ユーザの登録、認証（多要素認証を含む）及びアクセス権限管理が可能であること。」 「外部ユーザのアカウントライフサイクル（登録・有効期限・削除）を適切に管理できること。」	外部共有の想定規模及び運用前提を明記またはご開示をお願いします。 ① 同時に管理する外部ユーザ数の想定上限 ② 1対N共有におけるNの最大値及び代表的な件数 ③ 年間のファイル授受件数・容量 ④ 許容される外部ユーザの認証方式（ゲストアカウント発行、電子メールワンタイムパスワード、相手先組織アカウントによるフェデレーション等） ⑤ 外部ユーザ側に多要素認証アプリの導入を求めることの可否	外部ユーザ数・認証方式により、ライセンス（外部ID の従量課金等）、運用負荷及び相手方の受入可否が変わるため。認証方式の選定が実運用の成否に影響するため。	現状で外部サービスを利用しているため、詳細な数値の把握が困難です。 多要素認証については可否、方法について、ご提案に含めてください。
106	要件定義書	1.15.-2	外部ユーザ管理 ・外部ユーザの登録、認証（多要素認証を含む）及びアクセス権限管理が可能であること。	以下の内容に変更頂く事を提案します。 ----- 外部ユーザの登録、認証（多要素認証の強制を含む）及びアクセス権限管理が可能であること。	セキュリティレベルの維持・向上のため。	同上。
107	要件定義書	1.15.-3	・外部ユーザからのファイルアップロード機能を提供し、アップロードされたファイルを安全に保管できること。 ・外部ユーザへのファイル提供にあたり、共有リンクの発行、有効期限設定、パスワード保護、ワンタイムアクセス、ダウンロード禁止等の制御が可能であること。 ・外部ユーザがアップロードしたファイルに対し、ウイルススキャン等の安全性確認を自動で実施できること。	「ワンタイムアクセス」の定義についてご教示いただけますでしょうか。1回のダウンロードでリンクが自動失効する標準機能は提供していません。ワンタイムパスワードの発行による認証は可能です。	正確な仕様・要件を確認するため。	要件定義書1.15.-3の記載を以下のとおり修正しました。 「・外部ユーザからのファイルアップロード機能を提供し、アップロードされたファイルを適切なアクセス権管理及び暗号化等により保護し、本会が許可した利用者のみが参照又は取得できる状態で保管できること。 ・外部ユーザへのファイル提供にあたり、共有リンクの発行、有効期限設定、パスワード保護又はワンタイムパスワードによる認証等のアクセス制御が可能であること。 ・外部ユーザがアップロードしたファイルに対し、ウイルススキャンその他同等の安全性確認を自動で実施できること。」

108	要件定義書	1.15.-3／1.15.-4	「共有リンクの発行、有効期限設定、パスワード保護、ワンタイムアクセス、ダウンロード禁止等の制御が可能であること。」 「外部ユーザのアクセスに対し、閲覧のみ、コピー禁止、印刷禁止等の制御を適用できること。」 「外部ユーザがアップロードしたファイルに対し、ウイルススキャン等の安全性確認を自動で実施できること。」	「コピー禁止・印刷禁止」は秘密度ラベル（Microsoft Purview Information Protection）による権限制御での実現をする場合、外部ユーザ側にも対応アプリ又はサインインが必要となり、対象ファイル形式も限定されます。ブラウザ表示のみに限定する運用（Webビューアでの閲覧に限定し、ダウンロードを禁止）での代替を許容いただけますか。	実現方式により、外部ユーザ側に求められる要件（サインインの要否、対応アプリの導入）及び必要ライセンスが変わり、利便性と費用の双方に影響するため。	要件定義書1.15.-3、1.15.-4の記載を見直しました。
109	要件定義書	1.15.-3	ファイル授受機能 ・外部ユーザからのファイルアップロード機能を提供し、アップロードされたファイルを安全に保管できること。	「ファイルを安全に保管」とは、具体的にどのようなセキュリティ要件を意味していますか？	正確な仕様・要件を確認するため。 適正な費用見積のため。	要件定義書1.15.-3の記載を以下のとおり修正しました。 「外部ユーザからのファイルアップロード機能を提供し、アップロードされたファイルを適切なアクセス権管理及び暗号化等により保護し、内部の権限を有する利用者のみが参照又は取得できる状態で保管できること。」
110	要件定義書	1.15.-3	ファイル授受機能 ・外部ユーザへのファイル提供にあたり、共有リンクの発行、有効期限設定、パスワード保護、ワンタイムアクセス、ダウンロード禁止等の制御が可能であること。	以下の内容に変更頂く事を提案します。 ----- 外部ユーザへファイル提供にあたり、共有リンクの発行、有効期限設定、パスワード保護、ダウンロード禁止等の制御が可能であること。	製品選択の幅を広げるため、ワンタイムアクセスの要件は、パスワード保護や有効期限があれば必須ではないという要件に緩和をお願いします。	同上。
111	要件定義書	1.15.-4	情報漏洩対策（DLP） ・外部公開領域に保存されるファイルに対し、機密情報の検出、外部共有の制限、ダウンロード禁止等の情報漏洩対策（DLP）を適用できること。	こちらのDLPに関する仕様を削除いただけないでしょうか。	製品選択の幅を広げるため。製品および設計によっては追加ライセンスのコストが発生するため。	要件定義書1.15.-4の情報漏洩対策（DLP）については、ファイル共有基盤（ファイルサーバ）と統合構成の場合に限定した記載に修正しました。
112	要件定義書	1.15.-5	・外部共有に関する操作ログ（アップロード、ダウンロード、アクセス、削除等）を取得し、監査証跡として保管できること。 ・外部ユーザのアクセス状況を把握し、不正利用の兆候を検知できること。	操作ログの保持期限は、どの程度の期間を想定されていますでしょうか。操作ログの保持期間はMicrosoft 365 A5で利用できるAudit Premium で365日となります（Audit Standardでは180日）。それ以上の期間についてはSentinelにてご提案させていただきます。	正確な仕様・要件を確認するため。	ログの保存は政府統一基準群により1年間で推奨とされています。直近のログ以降をアーカイブ保存 といった階層化をすることは可能です。
113	要件定義書	1.15.-6	・内部領域と外部公開領域は論理的に分離しつつ、必要に応じて安全なワークフローによりファイル転送、承認、通知等の連携が可能であること。 ・外部公開領域にアップロードされたファイルを内部領域へ移動・コピーする際、DLPチェックや承認プロセスを適用できること。	実現可否がどのような承認プロセスを想定されるかに依拠するため、外部公開領域にアップロードされたファイルを内部領域へ移動・コピーする際の「承認プロセス」について、詳細をご教示いただけますでしょうか？	正確な仕様・要件を確認するため。	要件定義書1.15.-6の記載を以下のとおり修正しました。 「・部領域と外部公開領域は論理的に分離し、相互に自動的に混在しない構成とすること。」
114	要件定義書	1.2.	Firewall、基幹SW、サーバSW、フロアSW、管理SW	必要台数について記載がありませんので、各必要台数を明記願います。	提案・見積の公平性確保の観点から、明示いただきたいため。	詳細は、別途資料提供を行います。
115	要件定義書	1.2.-10	・ギガビットポートを48ポート以上搭載すること。 ・管理専用セグメントに接続し、全NW／サーバ機器の管理・監視に利用できること。 ・スイッチング容量はワイヤレートを満たすこと。 ・パケットバッファ容量は十分な容量を有すること。 ・管理アクセスは暗号化通信及びアクセス制御により保護されていること。	質問： ・48ポート以上搭載とありますが、スイッチのスタックによって24ポート2台でも要件を満たせますでしょうか ・管理アクセスは暗号化通信及びアクセス制御により保護とありますが、スイッチ機能での通信暗号化ではなく、各機能での通信暗号化の認識でよろしいでしょうか	ポート要件及び管理アクセスの暗号化方式を明確にし、要件に適合するスイッチ構成とセキュリティ対策を正確に設計するため。	要件定義書1.2.-10の記載を以下のとおり修正しました。 「・ギガビットポートを合計48ポート以上搭載すること。 ・管理者によるアクセス及び管理・監視通信は、HTTPS、SSH、SNMPv3 その他同等の暗号化通信及びアクセス制御により保護されていること。」
116	要件定義書	1.2.-10	管理 SW	本仕様における「管理SW」とは、インターネット回線を収容するスイッチを指す認識でよいをご教示いただきたい。	正確な仕様・要件を確認するため。	管理SWはインターネット接続とKBC内の管理LAN収容を兼用するスイッチです。

117	要件定義書	1.2.-2	・SINETへの上流回線は、10Gbpsを前提とする。 ・KBC内バックボーンも、10Gbps以上の帯域を確保する。 ・クラウドネイティブ化、ユーザ通信量の増加を見込み、インターネット回線、Firewall、基幹SW、フロアSW間の通信帯域を十分に確保する。 ・プリンタ、後負荷TV会議システム（本調達外既存物品）は有線LAN接続とする。 ・有線LANは複数人で共有できるよう隣接するデスクの塊ごとに1口を用意する。	質問： ・以下記載は誤字と認識しましたが、認識相違ないでしょうか。 -後負荷×、高負荷○ ・プリンタおよび高負荷TV会議システムの設置場所は、貴会より指定される認識でよろしいでしょうか。 ・高負荷テレビ会議システムの設置台数をご教授ください 有線LANを設置するデスクの場所は、貴会より指定される認識でよろしいでしょうか。 会議室への設置は不要でしょうか、また、設置台数をご教授ください ・KBC内バックボーンについて、10Gbps以上の帯域とありますが、ネットワーク機器を10Gアップリンクが必須になるということでしょうか。バックボーンとはどこまでのことを指すのでしょうか - 例えば端末と末端SWの間で10Gbpsは過剰ではないでしょうか	設置対象、必要台数及び10Gbps要件の適用範囲を明確にし、配線・機器構成と費用を適正に見積もるため。	詳細は、別途資料提供を行います。
118	要件定義書	1.2.-2	「有線LANは複数人で共有できるよう隣接するデスクの塊ごとに1口を用意する。」	「隣接するデスクの塊」という表現があいまいであり、必要な配線規模を見積もることが困難であるため、数量や距離が定量的に把握できるよう、【意見招請_物品役務8】アクセスポイント詳細情報でいただいているようなレイアウト図に、ハブ設置位置およびケーブル引出位置のプロットを願います。	有線LANの設置を具体的に見積もるために、必要な情報ですが、現行施工事業者しか知りえない情報であり、公平性を保つため。	詳細は、別途資料提供を行います。
119	要件定義書	1.2.-2	帯域・性能要件 ・有線 LAN は複数人で共有できるよう隣接するデスクの塊ごとに 1口を用意する。	「有線 LAN は複数人で共有できるよう隣接するデスクの塊ごとに 1口を用意する」とあるが、「隣接するデスクの塊」の定義を明確化いただきたい。また、必要なローゼット数を算出するため、執務室等のレイアウト図又はローゼット取出し箇所をご提供いただきたい。	有線LANポート数及びフロアスイッチの必要台数を適切に算出するため。	同上。
120	要件定義書	1.2.-2	帯域・性能要件 ・SINET への上流回線は、10Gbps を前提とする。	主系統10Gbps、副系統1Gbpsでの構成でも要件を満たすものとして取り扱い可能かご教示いただきたい。	副系統は障害発生時の通信継続を目的とした回線であり、主系統と同一帯域を必須としない場合、副回線を1Gbpsとすることで回線費用及び収容するネットワーク機器の導入費用を抑制できるため。	ご理解のとおりです。要件定義書1.3.-3に記載しています。
121	要件定義書	1.2.-4	・KBC内ネットワークと外部ネットワーク（SINET／インターネット）間の通信を適切に制御するため、Firewallを設置すること。 ・Firewallは、以下の役割を担うものとする。 ① 不正アクセスの防止 ② 外部との通信制御（許可／拒否） ③ サーバセグメント等の内部ネットワーク間の通信制御 ④ ログ取得及び監査対応 ・Webベースの管理画面を備え、装置の稼働状況、セッション数、インターフェイス状態、脅威イベント等をダッシュボード形式で可視化できること。 ・リモート接続による設定・状態確認等の管理機能を有すること。 ・電源は200V対応であること。アクティブ／スタンバイ構成による冗長化をサポートし、障害発生時にセッション情報を維持したまま切り替えが可能であること。	質問： ・電源は200V対応であることと記載ありますが、200Vに限定されるのでしょうか。100V対応でもよろしいでしょうか。 ・適切な製品選定のためFirewallの要件をご提示お願いします。一般的には以下のような機能要件がございます。 -スループット -同時セッション数 -新規セッション数 -必要ポート数	電源条件及びファイアウォールの必要性能を明確にし、要件に適合する製品を適切に選定するため。	詳細は、別途資料提供を行います。
122	要件定義書	1.2.-4	Firewall ・電源は 200V 対応であること。 ・アクティブ／スタンバイ構成による冗長化をサポートし、障害発生時にセッション情報を維持したまま切り替えが可能であること。	「将来の増速に備え、25Gbps以上のインターフェイスに拡張可能であること」との要件について、インターフェースとThroughputについても25Gbps以上の性能を求める認識でよいかご教示いただきたい。 また、以下の項目を追記することを提案する。 ・10Gbps回線を収容可能であること。 ・Throughputは10Gbps以上であること。 ・冗長電源に対応すること。	インターフェイスのみ25Gbpsに対応している場合であっても、Firewall Throughputが不足する場合は回線性能を十分に活用できないため。	同上。

123	要件定義書	1.2.-5	・全ポートでワイヤレート転送が可能であること。 ・高負荷通信（クラウドアクセス、TV会議、サーバアクセス等）に耐えるスループットを有すること。 ・VLAN（IEEE 802.1Q）に対応し、用途に応じてネットワークを分離できること。 ・VLAN間通信は L3 ルーティングにより適切に制御できること。 ・リモート管理が可能であり、設定・状態確認・ログ取得が行えること。 ・管理アクセスは暗号化通信及びアクセス制御により保護されていること。 ・構成情報（Config）は自動バックアップされ、変更履歴を追跡可能であること。 ・ストームコントロール機能を有し、遮断通知・自動復帰が可能であること。 ・リンクアグリゲーション（LAG）に対応していること。 ・19インチラックマウント対応、1U以下であること。 ・電源ユニット及びファンユニットは冗長構成をサポートし、ホットスワップ可能であること。 ・将来の増速に備え、25Gbps以上のインターフェイスに拡張可能であること。	質問： ・25Gbps以上のインターフェイスに拡張可能とは、モジュール交換等により25Gbpsにアップグレードが可能であるという理解でよいでしょうか。また、25Gbpsに対応するポートの数量や対象となるリンク（上位ネットワーク接続部分）などご教示お願いします。 ・スイッチ要件について、基幹SWなど別途明記されているスイッチも含めた共通要件となりますでしょうか。 ・25Gbps以上の拡張インターフェースの搭載ポート数を明記願います。 ・25Gbps以上であればQSFPやSFP28など規格は問わない形で相違ないでしょうか。	25Gbps対応の対象機器、ポート数及び規格を明確にし、フロアスイッチ等に過剰な性能を求める構成を避け、適切な機器を選定するため。	要件定義書1.2.-5の記載を以下のとおり修正しました。 「将来の増速に備え、上位ネットワーク接続用として25Gbps以上のインターフェイスを2ポート以上実装可能であること（規格は問わない）。」
124	要件定義書	1.2.-5	スイッチ要件 ・将来の増速に備え、25Gbps 以上のインターフェイスに拡張可能であること。	25Gbps以上への拡張を想定している接続区間（インターネット回線収容区間、ファイアウォール接続区間、サーバ接続区間等）を明確化いただきたい。	一般的にフロアスイッチの下位接続は1Gbps又はマルチギガビットで運用されることが多く、25Gbps以上への拡張は上位スイッチ接続、ファイアウォール接続又はサーバ接続で想定されるため。	同上。
125	要件定義書	1.2.-5	スイッチ要件 ・電源ユニット及びファンユニットは冗長構成をサポートし、ホットスワップ可能であること。	「電源ユニットについては全てのスイッチを対象に冗長構成及びホットスワップ対応を必須とし、ファンユニットの冗長構成及びホットスワップ対応については、基幹SW及びサーバSWを対象とすること」へ変更することを提案します。	フロアSW及び管理SWについては、電源の冗長化及びホットスワップ対応により十分な可用性を確保できるため、ファンユニットの冗長化及びホットスワップ対応を必須要件とした場合、機種選定の制約や導入コストの増加につながるため。	要件定義書1.2.-5の記載を以下のとおり修正しました。 「電源ユニットについては全てのスイッチを対象に冗長構成及びホットスワップ対応を必須とし、ファンユニットの冗長構成及びホットスワップ対応については、基幹SW及びサーバSWを対象とすること。」
126	要件定義書	1.2.-6	・パケットバッファ容量は 32MB 以上とすること。 ・60,000 以上の MAC アドレスに対応すること。	パケットバッファ容量32MB以上およびMACアドレステーブル数60,000以上の要件について、機器選定の幅が限定されるため、想定される利用規模に応じた要件値への緩和をご検討願います。	想定される利用者規模に対して、要件を満たす製品が一部の上位機種に限定される可能性が高く、機器選定の自由度およびコストに影響を与えることが懸念されるため。 また、コスト最適化および製品選択肢確保の観点から要件値の見直しをご検討いただきたいと考えているため。	要件定義書1.2.-6の記載を以下のとおり修正しました。 「・パケットバッファ容量は16MB以上とすること。 ・32,000以上のMACアドレスに対応すること。」
127	要件定義書	1.2.-6	・マルチギガビットポートを48ポート以上搭載すること。 ・最大スイッチング容量は900Gbps以上とすること。 ・パケットバッファ容量は32MB以上とすること。 ・60,000以上のMACアドレスに対応すること。 ・経路障害時に自動切替が可能なL3ルーティング機能を有すること。 ・専用管理ポートを有するか、任意ポートを管理専用として設定可能であること。	意見： ・SWが全体的に高スペックで記載されておりますので、費用を低減するために機器ごとに最低限のスペックを記載いただけないでしょうか。 質問： ・48ポート以上搭載とありますが、スイッチのスタックによって24ポート2台でも要件を満たせますでしょうか ・スイッチング容量の算出根拠をご教示ください。 ・高スペック機器となりオーバースペックになる可能性があるため要件の緩和が可能かご検討ください。 ・参考までに現行機種名をご教示ください。	クラウド利用等による処理負荷の変化も踏まえてスイッチ性能の根拠と適用範囲を明確にし、一般的な利用規模に対して過剰な要件であると推察される仕様を適正化するため。	48ポート以上搭載とありますが、スイッチのスタックによって24ポート2台でも可です。 要件定義書1.2.-6の記載を以下のとおり修正しました。 「提案するポート構成において、全ポートを同時利用した場合でも性能低下が生じないノンブロッキング構成であること。」
128	要件定義書	1.2.-6／1.2.-7	「基幹SW及びサーバSWについて、それぞれ「16,000以上」「60,000以上」のMACアドレスへの対応が必須要件とされている。」	想定利用者数（約635名、クライアント端末415台）に対し、要求されるMACアドレス収容数の設定根拠（将来のIoT機器収容等の想定有無）についてご教示ください。 過大な場合は要件の見直しについてご検討をお願いします。	収容数要件により選定可能な機種及び価格が大きく変動し、過大なスペック要求はコスト増につながるため。	同上。
129	要件定義書	1.2.-6	基幹 SW ・マルチギガビットポートを 48 ポート以上搭載すること。	「マルチギガビットポートを48ポート以上搭載すること」を「マルチレート対応光インターフェースを48ポート以上搭載すること」へ変更することを提案いたします。	「マルチギガビットポート」の定義によってはRJ45マルチギガビットポート搭載機種に限定される可能性がある一方、サーバ接続、ネットワーク機器接続及び将来的な高速回線収容用途ではSFP/SFP+/SFP28等の光インターフェースを採用した機器が一般的のため。	要件定義書1.2.-6の記載を以下のとおり修正しました。 「1Gbps以上で利用可能なポートを48ポート以上搭載すること。」
130	要件定義書	1.2.-7	サーバSW	サーバSWはオンプレが存在する前提での要件であると思われ、サーバSWが必要となる条件を追記願います。	オンプレが存在する前提での要件であると思われ、必須とならない条件が存在するため。	「KBCにオンプレサーバを設置する場合」に限定しました。

131	要件定義書	1.2.-7	・マルチギガビットポートを48ポート以上搭載すること。 ・最大スイッチング容量は900Gbps以上とすること。 ・パケットバッファ容量は32MB以上とすること。 ・16,000以上のMACアドレスに対応すること。 ・サーバ・ストレージのバーストラフィックに耐えうる性能を有すること。	質問： ・48ポート以上搭載とありますが、スイッチのスタックによって24ポート2台でも要件を満たせますでしょうか ・容量の算出根拠をご教示ください。 ・高スペック機器となりオーバースペックになる可能性があるため要件の緩和が可能かご検討ください。 ・参考までに現行機種名をご教示ください。	必要ポート数及びスイッチング容量の根拠を明確にし、同等の収容能力を持つ複数台構成の可否を確認するとともに、過剰な要件を避けるため。	48ポート以上搭載とありますが、スイッチのスタックによって24ポート2台でも可です。 「KBCにオンプレサーバを設置する場合」に限定しました。
132	要件定義書	1.2.-7	サーバ SW ・マルチギガビットポートを 48 ポート以上搭載すること。	「マルチギガビットポートを48ポート以上搭載すること」を「マルチレート対応光インターフェースを48ポート以上搭載すること」へ変更することを提案いたします。	現行要件ではRJ45インターフェース搭載機種を前提とした解釈となる可能性があるが、基幹スイッチにおけるサーバ、ネットワーク機器及び上位スイッチとの接続では光インターフェースを用いる構成が一般的であるため。	同上。
133	要件定義書	1.2.-7	サーバ SW ・最大スイッチング容量は 900Gbps 以上とすること。	「最大スイッチング容量は900Gbps以上とすること」を「最大スイッチング容量は2Tbps以上とすること」へ変更することを提案いたします。	サーバ及びストレージ間通信において発生するバーストラフィックに対し、十分な通信性能及び将来的な拡張性を確保するため。	同上。
134	要件定義書	1.2.-7	サーバ SW ・パケットバッファ容量は 32MB 以上とすること。	「パケットバッファ容量は32MB以上とすること」を「共有パケットバッファ容量は40MB以上とすること」へ変更することを提案いたします。	サーバ及びストレージ間の大容量データ転送やバックアップ処理等に伴うバーストラフィック発生時においても、パケットロスを抑制し安定した通信品質を確保するため。	同上。
135	要件定義書	1.2.-7	サーバ SW ・サーバ・ストレージのバーストラフィックに耐えられる性能を有すること。	「サーバ・ストレージのバーストラフィックに耐えられる性能を有すること」については、「最大スイッチング容量」及び「パケットバッファ容量」の要件にて同様の性能を評価できるものと考えられるため、要件の明確化及び重複排除の観点から削除をご検討いただきたい。 以下の項目を追加することを提案する。 ・Jumbo Frame (9,000Byte以上) 対応	サーバ及びストレージ間の大容量データ転送時における通信効率の向上及び機器負荷の軽減を図り、安定した通信品質を確保するため。	原案どおりとします。
136	要件定義書	1.2.-8	・ギガビットポートを48ポート以上搭載すること。 ・10Gbpsポートを2ポート以上搭載すること。 ・最大スイッチング容量は100Gbps以上とすること。 ・パケットバッファ容量は6MB以上とすること。 ・16,000以上のMACアドレスに対応すること。 ・4台以上の論理統合構成（スタック）をサポートすること。	質問： ・48ポート以上搭載とありますが、スイッチのスタックによって24ポート4台以上でも要件を満たせますでしょうか	必要な総ポート数を満たす複数台構成の可否を確認し、柔軟かつ可用性を考慮した機器構成を検討するため。	要件定義書1.2.-8の記載を以下のとおり修正しました。「ギガビットポートを合計48ポート以上搭載すること。」
137	要件定義書	1.2.-8	フロア SW ・ギガビットポートを 48 ポート以上搭載すること。	以下の項目を追加することを提案いたします。 ・IEEE802.3at (PoE+) に対応すること。 ・PoE給電容量740W以上であること。	無線LANアクセスポイント等へのPoE+給電に対応するため。	要件定義書1.2.-8の記載に以下を追加しました。 「IEEE802.3at (PoE+) に対応すること。」
138	要件定義書	1.2.-8	フロア SW ・パケットバッファ容量は 6MB 以上とすること。	「パケットバッファ容量は6MB以上とすること」を削除することを提案いたします。	フロアスイッチにおいてパケットバッファ容量を要件として求めるケースは限定的であり、本調達で求める通信性能についてはスイッチング容量等の要件により評価可能と考えられるため。	要件定義書 1.2.-8の記載から削除しました。
139	要件定義書	1.2.-9	・全てのNW・サーバ機器について、管理接続、監視接続用のセグメントを用意し、接続すること。	質問： ・管理/監視用のセグメントの用意については、貴会内に設置するオンプレ機器類のみで、クラウド上に構築される機器については対象外との認識でよいでしょうか。 ・クラウド上の機器においては、同一機器に対する複数のIPアドレスの付与は推奨されないため。 クラウド上機器についてはセグメントを分けないことの懸念はほとんどないため。	管理・監視用セグメントの適用範囲を明確にし、クラウド環境の推奨構成に適合した設計とするため。	要件定義書 1.2.-9の記載を以下のとおり修正しました。 「KBC内に設置する全てのNW・サーバ機器について、管理接続、監視接続用のセグメントを用意し、接続すること。」
140	要件定義書	1.3.		既設の回線がある場合は回線業者や契約内容（ダークファイバ+伝送装置、専用回線、広域イーサネットサービス、その他適切な方式）についてご教示願います。	SINETに接続するための回線工事費を抑えられる可能性があるため。	次期業務基盤システムで利用できる回線等はありません。

141	要件定義書	1.3.	－	SINET利用に関する責任分界点としては貴会拠点のKBCからSINETデータセンターまでの経路が本調達の責任範囲となる認識です。 SINETデータセンターからAzureクラウドまでの経路やSINETデータセンターからインターネットまでの経路については貴会によるSINETの契約に基づくものとして、本調達の責任範囲外となる認識です。 当該認識に相違ないか、ご教示願います。	SINET契約に関する記載が見当たらず、調達範囲および責任分界点に抜け漏れがないことを確認するため。	ご理解のとおりです。
142	要件定義書	1.3.-1	・本システムは、国立情報学研究所（NII）が提供する学術情報ネットワーク（SINET）との接続に対応すること。 ・KBCとSINETデータセンタ間の接続に必要な回線、通信機器及び伝送装置を提供し、構築すること。 ・SINETが定める接続要件、インターフェイス仕様及び運用条件に適合すること。 ・本会拠点とSINETデータセンタ間を接続する回線は、異経路・異ルートによる2系統以上を確保し、単一障害点を排除すること。 ・本会拠点とSINETデータセンタ間を接続する回線に接続する通信機器及び伝送経路についても、同様に単一障害点を設けない構成とすること。 ・障害発生時には、待機系への自動切替が行われる構成とすること。	意見： ・異経路・異ルートによる2系統以上となる場合、コスト高となる可能性が高いと考えていますが必須要件となりますでしょうか。 ・SINETデータセンターとの接続ということですが、SINETデータセンタの所在地等（または位置に関する概要等）公開いただくことは可能でしょうか。	異経路・異ルートによる冗長化の必要性と接続先を明確にし、回線構成及び費用を適正に算定するとともに、過剰な回線要件を避けるため。 回線費用がどの程度となるかを積算するためとなります。	要件定義書1.3.-1の記載を以下のとおり修正しました。 「本会拠点とSINETデータセンタ間を接続する回線は、冗長化し、単一障害点を排除すること。」 SINETデータセンターは、東京都内の予定ですが未確定です。
143	要件定義書	1.3.-1	・本会拠点とSINETデータセンタ間を接続する回線は、異経路・異ルートによる2系統以上を確保し、単一障害点を排除すること。 ・本会拠点とSINETデータセンタ間を接続する回線に接続する通信機器及び伝送経路についても、同様に単一障害点を設けない構成とすること。	「本会拠点」はKBCの1拠点のみを指すものと認識しております。当該認識に相違ないか、ご教示願います。	キャリア回線の契約の見積もり内容に影響するため。	ご理解のとおりです。
144	要件定義書	1.3.-2	・SINETとの接続方式は、NIIが定める方式に準拠すること。 ・以下のいずれかの方式、又は同等以上の品質を有する方式に対応できること。 ① ダークファイバ+伝送装置 ② 専用回線 ③ 広域イーサネットサービス ④ その他適切な方式 方式選定にあたっては、帯域、遅延、冗長性、将来拡張性を考慮し、 <u>提案書に根拠を示すこと。</u>	質問： ・学術情報ネットワーク（SINET）との接続に際して、終端となる回線は光ケーブルとなるのでしょうか。UTP(メタル)ケーブルとなるのでしょうか。	SINET接続の終端インターフェースを明確にし、必要な回線終端装置及び接続機器を適切に選定するため。	SINET接続用アクセス回線は光ファイバーを想定していますが、詳細は提案に含めてください。。
145	要件定義書	1.3.-3	回線機能 ・回線帯域は10Gbps以上とし、将来的な回線増速が可能な構成とすること。	1.2-2に同様の記載があるため「1.2 ネットワーク基盤」にて記載いただけますでしょうか。	集約して記載いただいた方が仕様を理解しやすいため。	原案どおりとします。
146	要件定義書	1.3.-4	ルーティング ・BGP等のルーティングプロトコルに対応し、SINETが定める接続条件に適合すること。	経路制御ポリシーとしてフィルタリングやAS-PATH制御等の記載が求められていることから、将来的なマルチホーム構成を想定されているかご教示いただきたい。	マルチホーム構成を前提とした場合、回線障害時の冗長化や通信先に応じた経路選択を実現するためにはBGPの利用が一般的のため、対応するルーティングプロトコルをBGPに限定することが望ましい。	現時点でマルチホーム構成は想定していませんが、本要件はSINETとの接続に必要なルーティング機能を求めるものであり、具体的な実装方式は提案によることとします。 要件定義書1.3.-4の記載を以下のとおり修正しました。 「SINET接続における経路制御方針及びフィルタリング方針を提案書に記載すること。」
147	要件定義書	1.3.-4	ルーティング ・経路制御ポリシー（フィルタリング、AS-PATH制御等）を提案書に記載すること。	経路制御ポリシーとしてフィルタリングやAS-PATH制御等の記載が求められていることから、将来的なマルチホーム構成を想定されているかご教示いただきたい。	マルチホーム構成を前提とした場合、回線障害時の冗長化や通信先に応じた経路選択を実現するためにはBGPの利用が一般的のため、対応するルーティングプロトコルをBGPに限定することが望ましい。	同上。

148	要件定義書	1.4. 1.13.-8	・ Microsoft 365 A3 又はA5 を 600 ライセンス提供すること。	本システムの利用者数は「1.4 次期業務基盤システムの概要」より、 ・ 本会役職員：約350名 ・ 研究員：約150名 ・ 管理者：約15名 ・ 海外研究連絡センター：約70名 ・ 一時利用者等：約50名 の計約635名と記載がありますが、調達するライセンス数との差分についてご教示願います。	調達するライセンス数の意図を確認したいため。	表2.4.-1を修正しました。
149	要件定義書	1.4.-2	・ 執務室・会議室等において、業務に支障がない電波環境を整備すること。 ・ 特に会議室ではTV会議トラフィックに耐えうる通信品質を確保すること。 ・ 既存配線は利用可能とするが、必要に応じて増設すること。 (有線LANについて) ・ トラブル時に備え、有線LANも利用可能とすること。 ・ 有線LANは複数人で共有できるよう、隣接するデスク単位で1口以上を設置すること。 ・ プリンタ、高負荷TV会議システム（本調達外既存物品）は有線LAN接続とすること。 ・ 有線LANについても、既存配線は利用可能とするが、必要に応じて増設すること。	質問： ・ 有線LANについても、既存配線は利用可能とするが、必要に応じて増設すること。と記載がありますが、どこまで利用可能なのでしょうか。デスクへの配線部分のみでしょうか。 ※例えば、L3⇄L2間も利用可能なのか	既存配線の再利用可能範囲と新設対象を明確にし、配線工事の範囲及び費用を正確に見積もるため。	ご理解のとおりです。公示後、希望があれば現地調査が可能です。
150	要件定義書	1.4.-2	・ 執務室・会議室等において、業務に支障がない電波環境を整備すること。	無線LANの適切な設計及び収容計画を行うため、会議室、講義室、研修室等の利用者が集中するエリアの最大収容人数、想定同時接続端末数及び利用用途をご教示願います。 あわせて、現行無線LAN環境において認識している課題（通信品質、接続数不足、ローミング、Web会議品質等）がある場合はご教示願います。	無線LANの適切な収容設計及び品質確保にあたり、利用実態や現行環境の課題を把握する必要があるため。	詳細は、別途資料提供を行います。公示後、希望があれば現地調査が可能です。
151	要件定義書	1.4.-2	電波環境・有線 LAN ・ 有線 LAN は複数人で共有できるよう、隣接するデスク単位で 1口以上を設置すること。	1.2-2に同様の記載があるため「1.2 ネットワーク基盤」にて記載いただけますでしょうか。	集約して記載いただいた方が仕様を理解しやすいため。	原案どおりとします。
152	要件定義書	1.4.-2	電波環境・有線 LAN ・ プリンタ、高負荷 TV 会議システム（本調達外既存物品）は有線 LAN 接続とすること。	1.2-2に同様の記載があるため「1.2 ネットワーク基盤」にて記載いただけますでしょうか。	集約して記載いただいた方が仕様を理解しやすいため。	同上。
153	要件定義書	1.4.-3	・ 無線LANアクセスポイントは、既存のものから増強が必要であり設置台数を増やす。 ・ 無線コントローラ、RADIUSサーバ及びアクセスポイント等に関する詳細な情報は、別途提供を行う。	既存アクセスポイントの継続利用は、製品保守、更改予定他機器との互換性などから特定の既存業者が有利となる可能性があります。競争性・公平性、製品選択性の観点から、既存アクセスポイントの継続利用をする場合は、無線AP、コントローラ、RADIUSサーバを調達範囲外とするようご検討願います。 また、調達範囲内とする場合はアクセスポイント全数交換を前提条件とするよう修正願います。 既存アクセスポイントを継続利用する場合、既存機器の型番、ソフトウェアバージョン、保守期限、ライセンス、設定情報、RADIUS連携方式等の情報が、構成検討、互換性確認、移行方式、費用算定に大きく影響します。 公平性及び競争性を確保する観点から、これらの情報を全提案者に同一条件でご教示願います。	既存アクセスポイントの継続利用は、製品保守、更改予定他機器との互換性などから特定の既存業者が有利となるため。 既存アクセスポイントを継続利用を前提とした場合の、提案・見積の公平性確保の観点から、確認の必要があるため。	要件定義書1.4.-3の記載を以下のとおり修正・追加しました。 「・ 無線LANアクセスポイントの台数、設置場所については、別途資料提供を行う。 ・ 設置作業の詳細は、契約後、本会と発注者と協議の上決定するものとする。なお、希望により公示後現地調査を行うことができる。」
154	要件定義書	1.4.-3	システム要件 ・ 無線 LAN システムは、経路冗長化により単一障害発生時も自動復旧できること。	「無線LANシステム」とは、無線LANコントローラ、アクセスポイント、認証サーバ等を含むシステム全体を指すのか、又は無線LANコントローラを指すのか明確化いただきたい。 2また、「冗長構成」とは無線LANコントローラ機器本体の冗長化を指す認識でよいかご教示いただきたい。	冗長化の対象範囲により、必要となる機器構成及び費用積算が異なるため。	同上。

155	要件定義書	1.4.-4	・IEEE 802.1X 無線LAN認証（TLS/PEAP）に対応すること。 ・同時接続クライアント数 600台以上 をサポートすること。 ・ユーザ数に応じた無線LAN容量を確保できること。 ・無線LANコントローラ及びRADIUSサーバを新設し、これを利用すること。無線接続時の認証はRADIUSサーバを利用すること。 ・ゲストアカウント利用時はコントローラ内で認証できること。 ・複数アクセスポイント間をクライアント側で意識せずローミングできること。 ・無線LANクライアント間の通信をブロックできること。 ・複数のRADIUS／LDAPサーバでの認証が可能であり、ローカル認証・Web認証も有すること。 ・1台のコントローラで 50AP以上 をサポートし、必要なライセンスを提供すること。 ・管理用インターフェースはWebブラウザ及びSSHに対応すること。 ・GUI／CLIのいずれでもソフトウェアアップグレードが可能であること。 ・電波干渉やAP故障などの状況変化に応じて送信出力を自動調整できること。 ・1000BASE-T対応のポートを4つ以上有すること。 ・100V AC電源で動作すること。 ・N+1冗長構成またはクラスタ構成 がサポートされていることを推奨する。	質問： ・記載いただいた要件はオンプレミスのコントローラを想定されているものと思われますが、クラウド型のコントローラを提案することは可能でしょうか？可能な場合はクラウド型コントローラでも可能な要件に修正いただきたいです。	クラウド型コントローラも選択可能とすることでクラウド利用方針との整合性を確保し、オンプレミス設備や認証基盤の追加による過剰な構成を避けるため。	要件定義書1.4.-4の記載に以下を追記しました。 「管理基盤の障害時においても、既設アクセスポイントによる無線通信を継続できること。なお、オンプレミス型、クラウド型WLCのいずれも提案可能とするが、管理基盤との通信断が発生しても、アクセスポイントによる無線LANサービスが継続利用できること。」
156	要件定義書	1.5.	運用・保守期間 ーシステム稼働開始後 5 年間（予定）	昨今の社会情勢の悪化など落札業者に起因しない事由により、全国的なサプライチェーンへの影響等により納品が遅れた場合、賃貸借開始日について、別途協議が可能ですか。	適正な費用見積のため。	協議は可能です。
157	要件定義書	1.5.-10	アプリケーションセキュリティ（SaaS/CSPM） ・本システムは、SaaS 及びクラウドサービスの設定不備や権限過剰を防止するため、SSPM（SaaS Security Posture Management）及び CSPM（Cloud Security Posture Management）機能を備え、設定監査・リスク評価・是正提案を継続的に実施できること。	SSPM（SaaS Security Posture Management）及び CSPM（Cloud Security Posture Management）の要件を削除いただけないでしょうか。	大きな追加コストが発生し過剰投資になると考えているため。	要件定義書1.5.-10の記載を以下のとおり修正しました。 「本システムは、SaaS及びクラウドサービスの設定不備、権限過剰その他のセキュリティリスクを継続的に把握し、設定監査・リスク評価・是正提案を実施できること。」
158	要件定義書	1.5.-1	・本システムは、ゼロトラストアーキテクチャの考え方にに基づき、利用者、デバイス、ネットワーク、アプリケーション及びデータを保護するため、以下の要件を満たすこと。 ・侵害を前提とした設計（Assume Breach）とし、境界防御のみに依存しない多層防御を実現すること。 ・利用者の接続場所（KBC内、在宅、モバイル等）に依存せず、一貫したセキュリティポリシーを適用できること。 ・利用者、デバイス、通信状況及びアクセス先等のコンテキスト情報を継続的に評価し、リスクに応じたセキュリティ制御を実施できること。 ・ID、デバイス、ネットワーク、メール及びクラウドサービスに対するセキュリティ情報を統合的に管理・分析できること。 ・クラウドサービスを前提とした構成において、ゼロトラストの原則に沿った運用を実現できること。	提案： ・以下要件や内容を盛り込むのはいかがでしょうか。 -提供するリソースはサービス契約者で共有されるのではなく契約毎に専用環境が提供されること -ネットワークやセキュリティポリシー等の各種設定、ログの確認等は単一の管理UIで実施できること。 -インターネットへの通信だけでなくリモートユーザーから拠点および拠点間通信においてもセキュリティポリシーが適用できること。	専用環境、統合管理及び一貫したセキュリティポリシーに関する基準を明確にすることで、複数のサービスを公平に比較できるようにするとともに、運用負荷の軽減とセキュリティ水準の向上を図るため。	要件定義書1.5.-1の記載に以下を追加しました。 「・利用者及びシステムの情報は、他契約者の情報と論理的に分離して管理されること。 ・ネットワーク、アクセス制御及びセキュリティポリシーについて、統合的に管理及び監視できること。 ・インターネットアクセスに加え、リモートユーザから拠点への通信及び拠点間通信についても、一貫したセキュリティポリシーを適用できること。 ・管理及び運用に必要なログ、アラート及び設定情報を統合的に確認できること。」

159	要件定義書	1.5.-10	・本システムは、SaaS及びクラウドサービスの設定不備や権限過剰を防止するため、SSPM（SaaS Security Posture Management）及び CSPM（Cloud Security Posture Management）機能を備え、設定監査・リスク評価・是正提案を継続的に実施できること。 ・ゼロトラストの原則に基づき、SaaS・クラウドサービスの設定、アクセス権限、共有状況等を継続的に評価し、リスクに応じた制御を行えること。 ・SaaS利用時のセキュリティ設定（認証方式、共有設定、アクセス権限等）を監査・統制できること。 ・過剰権限、公開設定、外部共有等のリスクを検出し、是正措置を提案できること。 ・SaaSの設定変更（設定ドリフト）を検知し、アラートを生成できること。 ・クラウドサービスの設定不備を検出し、リスク評価及び是正措置の提案を行えること。 ・APIアクセスログの監査ログを取得できること。 ・SSPM/CSPMの検知情報をID基盤、SSE、ZTNA、SIEMと連携し、リスクベースアクセス制御に反映できること。 ・SaaSのリスク状態（共有設定、権限、公開範囲等）を継続的に評価し、必要に応じてアクセス制御を強化できること。	提案： ・SSPM（SaaS Security Posture Management）及び CSPM（Cloud Security Posture Management）機能について記載をお願いします。	SaaS及びクラウド環境の設定不備やセキュリティリスクを継続的に可視化・管理できる要件とし、適切なセキュリティ水準を確保するため。	要件定義書1.5.-10の記載を見直しました。
160	要件定義書	1.5.-10	・本システムは、SaaS及びクラウドサービスの設定不備や権限過剰を防止するため、SSPM（SaaS Security Posture Management）及び CSPM（Cloud Security Posture Management）機能を備え、設定監査・リスク評価・是正提案を継続的に実施できること。 ・ゼロトラストの原則に基づき、SaaS・クラウドサービスの設定、アクセス権限、共有状況等を継続的に評価し、リスクに応じた制御を行えること。 ・SaaS利用時のセキュリティ設定（認証方式、共有設定、アクセス権限等）を監査・統制できること。 ・過剰権限、公開設定、外部共有等のリスクを検出し、是正措置を提案できること。 ・SaaSの設定変更（設定ドリフト）を検知し、アラートを生成できること。 ・クラウドサービスの設定不備を検出し、リスク評価及び是正措置の提案を行えること。 ・APIアクセスの監査ログを取得できること。 ・SSPM/CSPMの検知情報をID基盤、SSE、ZTNA、SIEMと連携し、リスクベースアクセス制御に反映できること。 ・SaaSのリスク状態（共有設定、権限、公開範囲等）を継続的に評価し、必要に応じてアクセス制御を強化できること。	「SaaSのリスク状態（共有設定、権限、公開範囲等）を継続的に評価し、必要に応じてアクセス制御を強化できること。」についてリアルタイムでの評価までは不要という認識でよいでしょうか？	正確な仕様・要件を確認するため。	同上。
161	要件定義書	1.5.-10	アプリケーションセキュリティ（SaaS/CSPM） ・SSPM/CSPMの検知情報をID基盤、SSE、ZTNA、SIEMと連携し、リスクベースアクセス制御に反映できること。	以下の内容に変更頂く事を提案します。 ----- SSPM/CSPMの検知情報を管理者が参照可能であり、必要に応じてID基盤、SSE、ZTNA等のアクセス制御ポリシーに反映できること。	SSPM/CSPMの検知結果の自動連携は対応製品が限定されるため。製品選択の幅を広げるため。	同上。

162	要件定義書	1.5.-2	・本システムは、EPP（Endpoint Protection Platform）及びEDR（Endpoint Detection and Response）の双方の機能を備え、端末に対する多層防御及び侵害後の迅速な検知・対応を実現すること。 ・EPP/EDRはクラウドベースで動作し、最新の脅威インテリジェンスを自動的に取得・適用できること。 ・ファイル入出力をリアルタイムに監視し、既知・未知のマルウェアを検知・防御できること。 ・クラウド上の最新脅威インテリジェンスを参照し、定義情報を自動更新できること。 ・不正通信（C&Cサーバ等）を検知し、端末単位で通信遮断・隔離を行えること。 ・端末の挙動を分析し、正規プロセス（PowerShell、WMI等）の悪用を含む高度な攻撃を検知できること。 ・攻撃チェーン（感染経路、生成プロセス、通信先、影響範囲等）を可視化できること。 ・IOC（ファイル名、ドメイン、IP等）を指定して影響端末を特定できること。 ・検出した脅威をリモートで除去できること。 ・端末隔離後、脅威分析の完了をもって元の通信状態へ復帰できること。 ・EDRログを検索・分析し、CSV又はExcel形式で出力できること。 ・EPP/EDRの検知情報をSSE、ZTNA、ID基盤と連携し、端末リスクに基づくアクセス制御を実施できること。 ・端末のセキュリティ状態（脆弱性、隔離状態、EDRエージェントの稼働状況等）をZTNAのアクセス判定に反映できること。	質問： ・こちらはEPP/EDRにて検知した侵害情報やリスクスコアをもとにID基盤がコンプライアンス準拠レベルを確認。ID基盤の評価したデバイスのコンプライアンス準拠レベルに応じてZTNAのアクセス制御を行うと理解しましたが、認識相違ないでしょうか。	EPP・EDR、ID基盤及びZTNA間の連携方式とアクセス制御の判定条件を明確にし、必要なライセンス及び機能構成を適切に選定するため。	ご認識のとおりです。 本要件は、EPP/EDRが検知した侵害情報、脆弱性情報その他のセキュリティ状態を、ID基盤等を介して評価し、その結果をZTNAによるアクセス制御に反映できることを想定しています。 なお、隔離状態の端末については、EPP/EDR製品による通信遮断を前提とするため、本要件におけるZTNAのアクセス判定対象外として差し支えありません。 要件定義書1.5.-2の記載を以下のとおり修正しました。「端末のセキュリティ状態（脆弱性、セキュリティポリシー適合状況、EPP/EDRによる検知情報等）をID基盤、ZTNAその他のアクセス制御機能に連携し、リスクに応じたアクセス制御を実施できること。なお、隔離状態の端末については対象外とする。」
163	要件定義書	1.5.-2	・本システムは、EPP（Endpoint Protection Platform）及びEDR（Endpoint Detection and Response）の双方の機能を備え、端末に対する多層防御及び侵害後の迅速な検知・対応を実現すること。 ・EPP/EDRはクラウドベースで動作し、最新の脅威インテリジェンスを自動的に取得・適用できること。 ・ファイル入出力をリアルタイムに監視し、既知・未知のマルウェアを検知・防御できること。 ・クラウド上の最新脅威インテリジェンスを参照し、定義情報を自動更新できること。 ・不正通信（C&Cサーバ等）を検知し、端末単位で通信遮断・隔離を行えること。 ・端末の挙動を分析し、正規プロセス（PowerShell、WMI等）の悪用を含む高度な攻撃を検知できること。 ・攻撃チェーン（感染経路、生成プロセス、通信先、影響範囲等）を可視化できること。 ・IOC（ファイル名、ドメイン、IP等）を指定して影響端末を特定できること。 ・検出した脅威をリモートで除去できること。 ・端末隔離後、脅威分析の完了をもって元の通信状態へ復帰できること。 ・EDRログを検索・分析し、CSV又はExcel形式で出力できること。 ・EPP/EDRの検知情報をSSE、ZTNA、ID基盤と連携し、端末リスクに基づくアクセス制御を実施できること。 ・端末のセキュリティ状態（脆弱性、隔離状態、EDRエージェントの稼働状況等）をZTNAのアクセス判定に反映できること。	「端末のセキュリティ状態（脆弱性、隔離状態、EDRエージェントの稼働状況等）をZTNAのアクセス判定に反映できること。」について、ご提案しているEntraSuiteでは、EDRエージェントの稼働状況によるアクセス制限は機能的に対応できません。この部分について要件緩和は可能でしょうか。	正確な仕様・要件を確認するため。	同上。

164	要件定義書	1.5.-2	EPP/EDR ・端末のセキュリティ状態（脆弱性、隔離状態、EDR エージェントの稼働状況等）を ZTNA のアクセス判定に反映できること。	隔離状態の端末については、一般的なEPP/EDR製品において通信遮断を前提とした動作となるため、ZTNAによるアクセス判定の対象外とする記載をご検討いただけないでしょうか 端末のセキュリティ状態（脆弱性、EDRエージェントの稼働状況等）をZTNAのアクセス判定に反映できること。なお、隔離状態の端末については対象外とする。	隔離状態の端末は、EDRの制御により通信が遮断されることを前提とした動作となるため、ZTNAが当該端末へ到達してアクセス判定を実施できない場合がある。このため、隔離状態をアクセス判定要件として一律に求めると、製品仕様によっては要件を満たせない可能性があるため。	同上。
165	要件定義書	1.5.-3	・本システムは、SSE（Security Service Edge）基盤を備え、端末からインターネット、SaaS、KBC内リソースへの通信に対し、統一されたセキュリティ制御を適用できること。 ・ユーザの接続環境（KBC内、リモートワーク、モバイル等）に依存せず、通信の可視化・脅威検査・アクセス制御を継続的に実施し、ゼロトラストの原則に沿った保護を実現すること。 ・KBC内の端末からのインターネット、SaaS及びKBC内リソース（プライベートアプリケーション）への通信は、原則としてSSE（Security Service Edge）基盤を経由し、SWG、CASB、ZTNA等の機能により統合的に保護されること。 ・ユーザの接続環境に依存せず、同一のセキュリティポリシーを適用し、通信の可視化、暗号化トラフィックの検査、不正アクセスの防止を実現できること。 ・技術的制約や著しいパフォーマンス低下等により、例外的にSSEを経由しない通信（ローカルブレイクアウト等）を認める場合は、該当通信先及び理由を事前に定義し、承認を得た上で最小限の範囲で実装すること。 ・SSE、EPP、EDR、メールセキュリティ等のログを統合管理し、相関分析によりリスクを可視化できること。 ・単一コンソールで管理・監視が可能であること。	提案： ・SSEの詳細要件の記載をお願いいたします。	SSEに求められる機能、性能及び運用範囲を明確にし、要件に適合するサービス構成と費用を正確に見積もるため。	要件定義書1.5.-3の記載を以下のとおり修正・追加しました。 「・管理者が設定情報、ログ、アラート及びインシデント情報を統合的に確認できること。 ・送信元IPアドレスの固定化、経路制御その他のネットワーク機能については、必要に応じて提案に含めること。」
166	要件定義書	1.5.-3	・本システムは、SSE（Security Service Edge）基盤を備え、端末からインターネット、SaaS、KBC内リソースへの通信に対し、統一されたセキュリティ制御を適用できること。 ・ユーザの接続環境（KBC内、リモートワーク、モバイル等）に依存せず、通信の可視化・脅威検査・アクセス制御を継続的に実施し、ゼロトラストの原則に沿った保護を実現すること。 ・KBC内の端末からのインターネット、SaaS及びKBC内リソース（プライベートアプリケーション）への通信は、原則としてSSE基盤を経由し、SWG、CASB、ZTNA等の機能により統合的に保護されること。 ・単一コンソールで管理・監視が可能であること。	提案： ・以下要件や内容を盛り込むのはいかがでしょうか。 -外部SaaSのIPアドレス制限に対応するため、契約者占有のグローバルIPが割り当てられること。 -クラウドサービスから拠点へのトラフィックにQoSを設定できること。 -提供サービスと拠点間でBGPによる柔軟な経路制御が可能であること。 -拠点間のIPsecトンネルは1本当たり最大2Gbpsをサポートすること。 -モバイルユーザーのオートスケール時に、未登録の新規グローバルIPが払い出されないよう制御できること。 -すべてのTCP/UDPポートにセキュリティポリシーを適用し、アプリケーションを識別できること。	固定IP、帯域制御、経路制御、通信性能及び全ポートのセキュリティ制御について共通の評価基準を設けることで、複数のサービスを公平に比較し、安定した通信と安全なクラウド利用を実現するため。	同上。
167	要件定義書	1.5.-3	・本システムは、SSE（Security Service Edge）基盤を備え、端末からインターネット、SaaS、KBC内リソースへの通信に対し、統一されたセキュリティ制御を適用できること。 ・ユーザの接続環境（KBC内、リモートワーク、モバイル等）に依存せず、通信の可視化・脅威検査・アクセス制御を継続的に実施し、ゼロトラストの原則に沿った保護を実現すること。 ・KBC内の端末からのインターネット、SaaS及びKBC内リソース（プライベートアプリケーション）への通信は、原則としてSSE（Security Service Edge）基盤を経由し、SWG、CASB、ZTNA等の機能により統合的に保護されること。 ・ユーザの接続環境に依存せず、同一のセキュリティポリシーを適用し、通信の可視化、暗号化トラフィックの検査、不正アクセスの防止を実現できること。 ・技術的制約や著しいパフォーマンス低下等により、例外的にSSEを経由しない通信（ローカルブレイクアウト等）を認める場合は、該当通信先及び理由を事前に定義し、承認を得た上で最小限の範囲で実装すること。 ・SSE、EPP、EDR、メールセキュリティ等のログを統合管理し、相関分析によりリスクを可視化できること。 ・単一コンソールで管理・監視が可能であること。	「単一コンソールで管理・監視が可能であること。」について、運用監視およびインシデント対応はDefender Portalに統合可能ですが、すべての設定変更を単一画面で実施できるわけではありません。この場合でも本要件を満たすと考えてよろしいでしょうか。	正確な仕様・要件を確認するため。	同上。

168	要件定義書	1.5.-4	・本システムは、ZTNA（Zero Trust Network Access）機能を備え、利用者及び端末の状態に基づく動的アクセス制御を実現すること。 ・端末状態・認証結果・通信コンテキストを継続的に評価し、ゼロトラストの原則に沿ったアクセス制御を行えること。 ・管理端末の構成プロファイル（OSバージョン、セキュリティソフトの有無、EDR稼働状況、脆弱性情報等）を定期的に検査し、端末状態に応じたアクセス制御を行えること。 ・プロキシ設定（PACファイル）を自動配布でき、主要クラウドサービス（Microsoft 365、Google Workspace等）に対して適切なバイパス設定を行えること。 ・利用者及び端末の認証結果並びに端末状態に基づき、アプリケーション単位でアクセス制御を実施できること。 ・アクセス制御はログイン時だけでなく、通信中も継続的に評価し、リスクに応じて動的に制御できること。	質問： ・プロキシを利用せず、同等機能で実装する場合はプロキシ設定(PACファイル)を自動配布については不要という認識でよろしいでしょうか	プロキシを使用しない同等方式を採用する場合のPACファイル配布可否を明確にし、不要な設定作業や構成を避けるため。	要件定義書1.5.-4の記載を以下のとおり修正・追加しました。 「・管理端末のセキュリティ状態（OSの更新状況、セキュリティ対策ソフトの稼働状況、脆弱性情報、コンプライアンス状態等）を確認し、端末状態に応じたアクセス制御を実施できること。 ・クラウドサービスへの接続に当たり、必要に応じて通信の最適化、経路制御又は例外設定を実施できること。なお、PACファイルその他同等の方式による実現を可とする。」 なお、本要件は、PACファイルの利用を必須とするものではありません。利用者が適切な経路でクラウドサービスへ接続できることを求めるものであり、エージェント方式その他同等の方式による実現も可とします。
169	要件定義書	1.5.-4	・本システムは、ZTNA（Zero Trust Network Access）機能を備え、利用者及び端末の状態に基づく動的アクセス制御を実現すること。 ・端末状態・認証結果・通信コンテキストを継続的に評価し、ゼロトラストの原則に沿ったアクセス制御を行えること。 ・利用者及び端末の認証結果並びに端末状態に基づき、アプリケーション単位でアクセス制御を実施できること。	提案： ・以下要件や内容を盛り込むのはいかがでしょうか。 -オンプレミスのリソース（データセンター）への接続について、複数のパブリッククラウドプロバイダーを使用した冗長構成に対応できること。	特定のサービスに限定せず、冗長構成への対応可否を共通の基準で評価できるようにするとともに、障害発生時にも業務を継続できる可用性を確保するため。	同上。
170	要件定義書	1.5.-4	・本システムは、ZTNA（Zero Trust Network Access）機能を備え、利用者及び端末の状態に基づく動的アクセス制御を実現すること。 ・端末状態・認証結果・通信コンテキストを継続的に評価し、ゼロトラストの原則に沿ったアクセス制御を行えること。 ・管理端末の構成プロファイル（OSバージョン、セキュリティソフト有無、EDR稼働状況、脆弱性情報等）を定期的に検査し、端末状態に応じたアクセス制御を行えること。 ・プロキシ設定（PACファイル）を自動配布でき、主要クラウドサービス（Microsoft 365、Google Workspace等）に対して適切なバイパス設定を行えること。 ・利用者及び端末の認証結果並びに端末状態に基づき、アプリケーション単位でアクセス制御を実施できること。 ・アクセス制御はログイン時だけでなく、通信中も継続的に評価し、リスクに応じて動的に制御できること。	「管理端末の構成プロファイル（OSバージョン、セキュリティソフト有無、EDR稼働状況、脆弱性情報等）を定期的に検査し、端末状態に応じたアクセス制御を行えること。」について、ご提案しているEntraSuiteではEDRサービスプロセスの稼働状態そのものをアクセス制御条件とする機能は対応しておりません。この要件について緩和いただくことは可能でしょうか。	正確な仕様・要件を確認するため。	同上。
171	要件定義書	1.5.-4	・本システムは、ZTNA（Zero Trust Network Access）機能を備え、利用者及び端末の状態に基づく動的アクセス制御を実現すること。 ・端末状態・認証結果・通信コンテキストを継続的に評価し、ゼロトラストの原則に沿ったアクセス制御を行えること。 ・管理端末の構成プロファイル（OSバージョン、セキュリティソフト有無、EDR稼働状況、脆弱性情報等）を定期的に検査し、端末状態に応じたアクセス制御を行えること。 ・プロキシ設定（PACファイル）を自動配布でき、主要クラウドサービス（Microsoft 365、Google Workspace等）に対して適切なバイパス設定を行えること。 ・利用者及び端末の認証結果並びに端末状態に基づき、アプリケーション単位でアクセス制御を実施できること。 ・アクセス制御はログイン時だけでなく、通信中も継続的に評価し、リスクに応じて動的に制御できること。	「プロキシ設定（PACファイル）を自動配布でき、主要クラウドサービス（Microsoft 365、Google Workspace等）に対して適切なバイパス設定を行えること。」について、ご提案しているEntraSuiteの推奨構成としてはGlobal Secure Access Clientでの制御になります。こちらの機能での対応で本要件を満たすと考えてもよろしいでしょうか。	正確な仕様・要件を確認するため。	同上。
172	要件定義書	1.5.-4	アクセス制御（ZTNA） ・プロキシ設定（PAC ファイル）を自動配布でき、主要クラウドサービス（Microsoft 365、Google Workspace 等）に対して適切なバイパス設定を行えること。	プロキシ設定（PACファイル）の自動配布を必須要件とせず、同等の機能を実現可能な方式を許容する要件としていただきたい。 利用者端末へプロキシ設定を適用、または同等の機能を実現できること。また、主要クラウドサービス（Microsoft 365、Google Workspace等）に対して適切な通信制御を行えること。	製品によってはPACファイルの自動配布機能を有さず、エージェント方式等により同等の通信制御を実現する方式を採用しているため。要件を特定の実装方式に限定しないことで、提案可能な製品の選択肢を確保できるため。	同上。

173	要件定義書	1.5.-5	・ HTTP/HTTPS通信を復号し、脅威検査を実施できること。 ・ HTTPS復号後は再暗号化を行い、ブラウザ警告が発生しないこと。 ・ 機械学習により未知の脅威を検出できること。	提案： ・ 以下要件や内容を盛り込むのはいかがでしょうか。 -主要な検索エンジンを利用する際、SSL復号を行わずにセーフサーチが有効なサイトへ誘導できること。	実現方式を特定の製品に限定せず、プライバシーに配慮した検索時の安全対策を共通の基準で評価できるようにし、利用者の安全性と利便性を両立するため。	要件定義書1.5.-5の記載を以下のとおり修正しました。 「・ HTTP/HTTPS通信に対し、必要に応じて脅威検査を実施できること。 ・ HTTPS通信を検査する場合は、適切な復号及び再暗号化その他同等の方式により利用者への影響を抑制できること。 ・ 既知及び未知の脅威を検出できること。なお、当該機能はSSE単体又はEPP、EDR、XDR、CASBその他同等の機能との連携により実現できるものとする。」
174	要件定義書	1.5.-5	・ HTTP/HTTPS通信を復号し、脅威検査を実施できること。 ・ HTTPS復号後は再暗号化を行い、ブラウザ警告が発生しないこと。 ・ 機械学習により未知の脅威を検出できること。	・ 「機械学習により未知の脅威を検出できること」について、機能的にトラフィック検査による未知の脅威の検出は困難であるため、代替案として、 ・ 「Defender for Endpoint / Defender for Cloud Appsでの異常検知、リスク分析、不審な振る舞い検知を提供し、未知の脅威に対応する。」にて対応することは可能でしょうか？	当社からのご提案の最適化のため。	同上。
175	要件定義書	1.5.-6	・ 代表的なクラウドアプリに対し、アップロード／ダウンロードの制御が可能であること。 ・ 組織外テナントへのアクセスを制限し、個人向けクラウドサービスへのデータ漏えいを防止できること。	代表的なクラウドアプリについて、具体的に想定しているクラウドサービスがあればご教示ください。	正確な仕様・要件を確認するため。	要件定義書1.5.-6 に記載のとおりです。
176	要件定義書	1.5.-7	・ 本システムは、メールを経由したマルウェア感染、フィッシング、情報漏えい等の脅威を防止するため、クラウドベースのメールセキュリティ基盤を備え、受信・送信双方に対して多層的な検査・制御を実施できること。 ・ メールの内容・送信元・添付ファイル・URL等を継続的に評価し、リスクに応じた制御を行えること。 ・ 受信メール保護として、以下の機能を有すること。 ① 添付ファイルのスキャンを行えること。パスワード付きZIPの自動解凍・スキャンが可能であること。 ② ファイル及びURLに対するサンドボックス検査を行えること。 ③ 添付ファイルのサニタイズ（無害化）が可能であること。 ④ URLリライトにより、アクセス時に最新の脅威情報を用いて危険なURLへの接続を防止できること。 ⑤ スパム判定・隔離を行えること。 ⑥ ソーシャルエンジニアリング攻撃を脅威として検出できること。 ⑦ 送信元IPを複数のデータベースで評価し、スパム対策を実施できること。 ⑧ スパム判定メールの件名に識別用テキストを追記できること。	質問： ・ 「パスワード付きZIPの自動解凍・スキャンが可能であること」について、パスワードの入力を利用者または管理者の操作により行い、その後の解凍およびウイルススキャンを自動で実施する方式で要件を満たすものとしていただけないでしょうか。	パスワード付きZIPの処理について、セキュリティを確保しつつ実現可能な運用方式を認めていただき、特定の実装方式に限定されない構成とするため。	要件定義書1.5.-7の記載を見直しました。

177	要件定義書	1.5.-7	・本システムは、メールを経由したマルウェア感染、フィッシング、情報漏えい等の脅威を防止するため、クラウドベースのメールセキュリティ基盤を備え、受信・送信の双方に対して多層的な検査・制御を実施できること。 ・メールの内容・送信元・添付ファイル・URL等を継続的に評価し、リスクに応じた制御を行えること。 ・受信メールの保護として、以下の機能を有すること。 ① 添付ファイルのスキャンを行えること。パスワード付きZIPの自動解凍・スキャンが可能であること。 ② ファイル及びURLに対するサンドボックス検査を行えること。 ③ 添付ファイルのサニタイズ（無害化）が可能であること。 ④ URLリライトにより、アクセス時に最新の脅威情報を用いて危険なURLへの接続を防止できること。 ⑤ スпам判定・隔離を行えること。 ⑥ ソーシャルエンジニアリング攻撃を脅威として検出できること。 ⑦ 送信元IPを複数のデータベースで評価し、スパム対策を実施できること。 ⑧ スпам判定メールの件名に識別用テキストを追記できること。 ・利用者が隔離メールを確認し、配送処理を行えること。 ・隔離メールの概要を利用者へ通知できること。 ・SPF、DKIM、DMARC、ARC認証及びS/MIME暗号化・署名技術に対応していること。 ・無効アドレス宛メールを破棄できること。 ・機密データや個人情報を含むメールの外部送信を制限できること。 ・組織のデジタル資産がメール経由で漏えいすることを防止できること。 ・管理者が隔離メールに対し、配送・削除・ダウンロード等の処理を実行できること。 ・メール及びサンドボックス結果を統合管理できること。 ・スパム急増時においても、サーバ機器の追加やネットワーク構成変更を必要としないこと。 ・メールセキュリティの検知情報をEPP/EDR、SSE、ID基盤と連携し、リスクベースアクセスに反映できること。 ・メールボックス内の脅威を自動検査・隔離できること。	ご提案しているDefender for Office365において、 ・パスワード付きZIPの内容検査 ・添付ファイルのサニタイズ（無害化） は対応が難しい状況です。こちらについて、一部加点点目とする・項目の削除など要件を緩和いただくこと可能でしょうか？	当社からのご提案の最適化のため。	同上。
178	要件定義書	1.5.-7	メールセキュリティ ⑦ 送信元 IP を複数のデータベースで評価し、スパム対策を実施できること。	送信元IPアドレスの評価方法を特定の実装方式に限定せず、複数の情報源を用いてスパム対策を実施できる要件としていただきたい。 送信元IPアドレスを複数の情報源により評価し、スパム対策を実施できること。	スパム対策製品における送信元IPアドレスの評価方法は製品ごとに異なり、データベースによる評価に限定せず、脅威インテリジェンスやレピュテーション情報等を活用する製品も存在するため。	同上。
179	要件定義書	1.5.-7	メールセキュリティ ・隔離メールの概要を利用者へ通知できること。	メールの検知・隔離は可能製品は広くありますが、利用者ごとに隔離メールの概要をダイジェスト形式で通知する機能は製品が絞られるため削除いただけないでしょうか。	製品選定の幅を広げるため	同上。
180	要件定義書	1.5.-7	メールセキュリティ ・SPF、DKIM、DMARC、ARC 認証及び S/MIME 暗号化・署名技術に対応していること。	SPF、DKIM、DMARC、ARC 認証およびS/MIME暗号化・署名技術に関する要件については、メールセキュリティ製品の要件ではなく、Microsoft 365の標準機能により実現される要件として整理いただきたい。 本要件をメールセキュリティ機能要件から除外し、オフィスのメール要件へ移設いただけないでしょうか	求められる機能は基本的に、Microsoft 365の標準機能により実現される要件になります。 もし、こちらに記載する場合、機能を阻害なく利用できることになると思います。	同上。
181	要件定義書	1.5.-7	メールセキュリティ ・無効アドレス宛メールを破棄できること。	無効アドレス宛メールを破棄できることに関する要件については、メールセキュリティ製品の要件ではなく、Microsoft 365の標準機能により実現される要件として整理いただきたい。 本要件をメールセキュリティ機能要件から除外し、オフィスのメール要件へ移設いただけないでしょうか	求められる機能は基本的に、Microsoft 365の標準機能により実現される要件になります。 もし、こちらに記載する場合、機能を阻害なく利用できることになると思います。	同上。

182	要件定義書	1.5.-7	メールセキュリティ ・スパム急増時においても、サーバ機器の追加やネットワーク構成変更を必要としないこと。	クラウドサービス型のメールセキュリティ製品を採用する場合は、本要件を適用対象外としていただけないでしょうか。	本要件は、オンプレミス型製品においてスパム急増時の処理能力を確保するため、利用者側でサーバ機器の追加やネットワーク構成変更を行わないことを求めるものと考えます。 一方、クラウドサービス型製品では、サービス提供事業者側のクラウド基盤において処理能力の確保、負荷分散、冗長化等が実施されるため、利用者側でサーバ機器の追加やネットワーク構成変更を行う必要がありません。 このため、クラウドサービス型製品については、本要件の適用対象外とすることが適切と考えます。	同上。
183	要件定義書	1.5.-7	「受信メールの保護として、以下の機能を有すること。 ③ 添付ファイルのサニタイズ（無害化）が可能であること。」	添付ファイルのサニタイズ（無害化）とは、マクロ除去、PDF変換、危険拡張子の除去等の無害化が実現できればよいとの認識しております。当該認識に相違ないか、ご教示願います。	添付ファイルの無害化に関してどのレベルまで実現すればよいかが不明確なため。	ご理解のとおりです。
184	要件定義書	1.5.-8	・本システムは、SIEM/SOARを含む統合ログ管理基盤を備え、ID、端末、ネットワーク、メール、クラウドサービス等のログを統合的に収集・保管・分析し、ゼロトラストの原則に基づく継続的監視及び自動対応を実現すること。 ・統合ログ管理基盤は、Syslog、Windowsイベントログ、クラウドサービスAPI等、複数のログ形式に対応し、必要に応じてSIEM製品又は同等の機能を提供できること。 ・収集したログの保持期間や利用頻度に応じ、ストレージコストを最適化するため段階的な保管管理（Hot / Warm / Cold等のデータ階層化、又は外部ストレージへの自動退避）が行えること。 ・収集したログについて、検索、分析及びインシデント調査に利用できること。 ・複数のログ種別や条件を組み合わせて関連性を評価し、脅威を検知できること。 ・自動対応機能（SOAR又は同等機能）により、アラート発生時の端末隔離、通知、復旧等の自動対応が可能であること。 ・自動対応ルールをGUI上で作成・編集できること。 ・誤検知時のロールバック（復旧）が可能であること。 ・統合ログ管理基盤の検知情報をEPP/EDR、SSE、ZTNA、ID基盤と連携し、リスクベースアクセス制御に反映できること。 ・各セキュリティ製品のログを単一コンソールで可視化できること。	質問： ・ログの保持期間と現在のログ量についてご教授おねがいします。 質問： ・SOARで実装すべき自動対応機能についての要件はありますでしょうか。シナリオ構築となるため、実装シナリオ数、シナリオ内容によって大きく費用が異なります。	ログ量、保持期間及びSOARの実装シナリオ数・内容により必要な容量と構築工数が大きく変動するため、構成及び費用を正確に見積もるため。	ログの保持期間については、別途定めるログ管理基盤要件に従うものとします。 収集対象ログ及びログ量については、提案する製品構成や設計により大きく異なるため、本会として一律には指定しません。本調達で導入するID基盤、EPP/EDR、SSE、ZTNA、メールセキュリティ及び関連システムのログを基本対象として想定しています。 想定ログ量、保存容量、保存方式及び対象ログについては提案に含めるものとし、詳細は契約後に本会と協議の上決定するものとします。 また、本要件は、専用SOAR製品の導入を必須とするものではなく、SIEM製品の標準機能、Microsoft 365関連機能、ワークフロー機能その他同等の機能により実現することを可とします。 自動対応の対象については、通知、チケット発行、端末隔離、アカウント制御その他の対応を想定していますが、実装するシナリオ数及び内容は指定しません。 自動化対象及びシナリオについては提案に含めるものとし、詳細は契約後に本会と協議の上決定するものとします。なお、完全自動化を必須とするものではなく、半自動又は承認を伴う運用による実現も可とします。
185	要件定義書	1.5.-8	「統合ログ管理基盤は、Syslog、Windows イベントログ、クラウドサービス API 等、複数のログ形式に対応し、必要に応じて SIEM 製品又は同等の機能を提供できること。」	収集対象として想定しているログの種別、及びSIEMへ取り込む想定ログ量（日次GB量又は月次GB量）について、ご教示ください。	ログ収集対象及びログ容量によりSIEMライセンス費用及びストレージ容量が大きく変動するため。	同上。

186	要件定義書	1.5.-8	・本システムは、SIEM/SOARを含む統合ログ管理基盤を備え、ID、端末、ネットワーク、メール、クラウドサービス等のログを統合的に収集・保管・分析し、ゼロトラストの原則に基づく継続的監視及び自動対応を実現すること。 ・統合ログ管理基盤は、Syslog、Windowsイベントログ、クラウドサービスAPI等、複数のログ形式に対応し、必要に応じてSIEM製品又は同等の機能を提供できること。 ・収集したログの保持期間や利用頻度に応じ、ストレージコストを最適化するための段階的な保管管理（Hot / Warm / Cold等のデータ階層化、又は外部ストレージへの自動退避）が行えること。 ・収集したログについて、検索、分析及びインシデント調査に利用できること。 ・複数のログ種別や条件を組み合わせて関連性を評価し、脅威を検知できること。 ・自動対応機能（SOAR又は同等機能）により、アラート発生時の端末隔離、通知、復旧等の自動対応が可能であること。 ・自動対応ルールをGUI上で作成・編集できること。 ・誤検知時のロールバック（復旧）が可能であること。 ・統合ログ管理基盤の検知情報をEPP/EDR、SSE、ZTNA、ID基盤と連携し、リスクベースアクセス制御に反映できること。	「誤検知時のロールバック（復旧）が可能であること。」について、ユースケースごとに復旧自動化設計する、という認識であっておりますでしょうか？	正確な仕様・要件を確認するため。	本要件は、復旧処理の自動化を必須とするものではありません。 誤検知により自動対応を実施した場合に、対象となった処理について復旧又はロールバックを実施できることを求めるものであり、自動復旧、半自動復旧又は運用手順による復旧のいずれでも可とします。 復旧方法及び対象範囲については提案に含めるものとし、詳細は契約後に本会と協議の上決定するものとします。
187	要件定義書	1.5.-8	・各セキュリティ製品のログを単一コンソールで可視化できること。	一部クラウドサービスにおいては、製品仕様上、外部SIEMへのログ連携機能が提供されていない、又は特定SIEM製品への連携に限定されている場合があります。そのため、すべてのセキュリティ製品のログを単一コンソールへ集約することが困難な場合があります。公平な競争環境の確保及び提案製品の選択肢拡大の観点から、以下のとおり要件の緩和を願います。 「各セキュリティ製品のログについて、取得可能な範囲で集約し、統一的な監視及び分析が可能であること。」	一部のクラウドサービスでは、製品仕様上、ログ連携先が特定のSIEM製品に限定されている場合があり、提案可能な製品構成が不必要に制約されるため。	ログの保持期間については、別途定めるログ管理基盤要件に従うものとし、 収集対象ログ及びログ量については、提案する製品構成や設計により大きく異なるため、本会として一律には指定しません。本調達で導入するID基盤、EPP/EDR、SSE、ZTNA、メールセキュリティ及び関連システムのログを基本対象として想定しています。 想定ログ量、保存容量、保存方式及び対象ログについては提案に含めるものとし、詳細は契約後に本会と協議の上決定するものとします。
188	要件定義書	1.5.-8 1.14.-1／1.14.-2 1.11.-1	「1.5.-8：…SIEM/SOARを含む統合ログ管理基盤を備え…必要に応じてSIEM製品又は同等の機能を提供できること。」 「1.14.-2：市販のRDB製品を用意する必要なく、独自DBによりログを管理可能であること。」「管理画面やマニュアル、サポートの提供が日本語であること。」「運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。」	1.5.-8（SIEM/SOARを含む統合ログ管理基盤）と1.14（ログ管理基盤）の関係について明記をお願いします。 両者を別個の基盤として構築する必要があるか、単一の基盤（クラウド型SIEM等）で双方の要件を満たすことをもって充足とみなしてよいかが教示ください。 併せて、1.14の「独自DBによる管理」「単一のソフトウェアで実現」等は、要件の趣旨（ログの原本性確保、検索性、費用の予見性等）に照らした適合判定を可能としていただけないかご検討をお願いします。	1.11.-1の「同一機能を複数のシステムで重複して実装しないこと」との整合を図る必要があるため。	同上。
189	要件定義書	1.5.-8	監視・ログ統合（SIEM/SOAR） ・本システムは、SIEM/SOARを含む統合ログ管理基盤を備え、ID、端末、ネットワーク、メール、クラウドサービス等のログを統合的に収集・保管・分析し、ゼロトラストの原則に基づく継続的監視及び自動対応を実現すること。	SIEM/SOARに関する本要件について、対象とするログ、監視対象システム、自動化対象となるインシデント及び運用範囲が明確でないため、提案製品、構成及び運用体制の算定が困難です。 そのため、SIEM/SOARの対象範囲を明確化し、実装及び運用スコープを限定していただけないでしょうか。 ※別紙「意見補足資料.pptx」も併せてご参照ください。 代替案①：仕様書記載システムに限定 本要件の対象を、仕様書に記載されている特定のセキュリティ基盤（EPP/EDR、SSE、ZTNA、ID基盤）が収集・検知するログ及びアラートに限定し、当該製品の標準機能の範囲で統合監視及び対応を実施するものとしていただけないでしょうか。 代替案②：今回導入範囲まで拡張 仕様書に記載されている特定のセキュリティ基盤に加え、本調達において導入する機器・システムから取得可能なログをSIEMへ取り込み、統合監視を実施するものとしていただけないでしょうか。 なお、SOARについては完全自動対応を必須とせず、アラート発生後に管理者が内容を確認し、必要な対応を実施する手動または半自動運用を基本としていただけないでしょうか	SIEM/SOARは、収集対象となるログの種類・量、保存期間、相関分析ルール、監視時間、インシデント対応範囲、SOARによる自動化内容等により、必要となる製品ライセンス、基盤構成、設計・構築工数及び運用体制が大きく変動します。 現行仕様では「ID、端末、ネットワーク、メール、クラウドサービス等のログを統合的に収集・保管・分析し、継続的監視及び自動対応を実現する」とされていますが、具体的な対象システム、ログ量、監視・対応範囲が明確でないため、入札時点で各社が同一条件による費用算定を行うことが困難と考えます。 また、自動対応についても、完全自動での遮断・隔離等を求めるのか、管理者判断を介した手動または半自動対応を求めるのかによって、設計及び運用内容が大きく異なります。 公平な価格比較及び確実な履行を可能とするため、対象範囲を明確化することが適切と考えます。 代替案①にしていただけないでしょうか。代替案②だと非常に高額になるからです。	同上。

190	要件定義書	1.5.-8	監視・ログ統合（SIEM/SOAR） ・統合ログ管理基盤は、Syslog、Windows イベントログ、クラウドサービス API 等、複数のログ形式に対応し、必要に応じて SIEM 製品又は同等の機能を提供できること。	代替案のみ記載させていただきます。 代替案①：仕様書記載システムに限定 統合ログ管理基盤は、 EPP/EDR、SSE、ZTNA、ID基盤が生成するログ・検知データに対応し、リアルタイム可視化、脅威検知・相関分析を提供できること。 代替案②：今回導入範囲まで拡張 統合ログ管理基盤は、Syslog、Windows イベントログ、クラウドサービス API 等、複数のログ形式・第三者製品対応し、SIEM 製品又は同等の機能（ログ取り込み、リアルタイム可視化、脅威検知・相関分析）を提供できること。	公平な価格比較及び確実な履行を可能とするため、対象範囲を明確化することが適切と考えます。 代替案①にしていだけないでしょうか。代替案②だと非常に高額になるからです。	同上。
191	要件定義書	1.5.-8	監視・ログ統合（SIEM/SOAR） ・収集したログの保持期間や利用頻度に応じ、ストレージコストを最適化するための段階的な保管管理（Hot / Warm / Cold 等のデータ階層化、又は外部ストレージへの自動退避）が行えること。	代替案①：仕様書記載システムに限定 収集したログの保持期間について、標準の分析用データ保持期間(30日)を基本とし、追加の保存期間が必要な場合は、別途、オプション費用が必要となることを前提に、必要最小限の範囲で設計すること。 代替案②：今回導入範囲まで拡張 収集したログについて、保持期間（30日、90日／180日／1年に延長可能とする）及び利用頻度に応じた保管管理を行い、データ使用状況の監視を通じて、ストレージコストを最適化できること。	公平な価格比較及び確実な履行を可能とするため、対象範囲を明確化することが適切と考えます。 代替案①にしていだけないでしょうか。代替案②だと非常に高額になるからです。	同上。
192	要件定義書	1.5.-8	監視・ログ統合（SIEM/SOAR） ・収集したログについて、検索、分析及びインシデント調査に利用できること。	以下の変更を提案いたします。 収集したログについて、検索、相関分析及びインシデント調査に利用できること。	SIME機能のため、相関分析を盛込みが適切と考えます。	同上。
193	要件定義書	1.5.-8	監視・ログ統合（SIEM/SOAR） ・複数のログ種別や条件を組み合わせる関連性を評価し、脅威を検知できること。	代替案①：仕様書記載システムに限定 収集した検知情報を相関評価し、脅威を検知できること。 代替案②：今回導入範囲まで拡張 AI・機械学習による高度な相関分析を用いて複数のログ種別・条件を組み合わせる関連性評価を行い、脅威を検知できること。	公平な価格比較及び確実な履行を可能とするため、対象範囲を明確化することが適切と考えます。 代替案①にしていだけないでしょうか。代替案②だと非常に高額になるからです。	同上。
194	要件定義書	1.5.-8	監視・ログ統合（SIEM/SOAR） ・自動対応機能（SOAR 又は同等機能）により、アラート発生時の端末隔離、通知、復旧等の自動対応が可能であること。	自動対応機能により、アラート発生時の端末隔離、通知、アカウント無効化、強制サインアウト、パスワードリセット、スクリプト実行等の自動対応（セミオートメーション／フルオートメーション）が可能であること。	自動対応機能として、端末隔離のみでは弱いため、アカウント無効化などが必要と考えます。	同上。
195	要件定義書	1.5.-9	コールドストレージやアーカイブ等に退避させた過去のログについて、必要に応じて比較的容易な手順で検索・分析対象として再ロード（復元）できること。	質問： ・アーカイブからの再ロードについては、別途費用と考えてよろしいでしょうか。	アーカイブからの再ロードに必要な作業及び費用の扱いを明確にし、運用費用の算定条件を確認するため。	要件定義書1.5.-9の記載を以下のとおり修正しました。 「・一定期間経過後の過去のログについて、コールドストレージ、アーカイブその他の保存領域に保管することも可とする。そのようにした場合でも、必要に応じて検索又は分析対象として利用できること。 ・コールドストレージ、アーカイブその他の保存領域からの復元又は再ロードを行う場合は、本会と協議の上で実施するものとする。なお、復元又は再ロードに条件、処理時間の制約又は追加費用を要する場合は、ログ退避の設計と併せて、その内容を提案書に明記すること。」
196	要件定義書	1.5.-9	監視・ログ統合（SIEM/SOAR） ・コールドストレージやアーカイブ等に退避させた過去のログについて、必要に応じて比較的容易な手順で検索・分析対象として再ロード（復元）できることが望ましい。	クラウドサービス型の製品を採用する場合は、利用者側で実施するバックアップ要件について、適用対象外としていただけないでしょうか。	クラウドサービス型の製品では、システムを構成するサーバ、データベース等の基盤はサービス提供事業者が管理しており、利用者側で個別にバックアップ処理を実施できない、または実施する必要がないサービス形態となっています。 また、データ保全、冗長化、障害時の復旧等については、サービス提供事業者が定めるサービス仕様、可用性設計及び運用体制に基づき実施されます。	同上。

197	要件定義書	1.6.-1	本システムは、ゼロトラストアーキテクチャの中核となるIDをセキュリティ境界として位置付け、認証、認可及びIDライフサイクル管理を統合的に実施するため、以下の要件を満たすこと。 ・利用者及び管理者のIDを一元的に管理し、認証・認可を統合的に実施できること。 ・最小権限の原則に基づき、利用者、管理者及びアプリケーションに対し必要最小限の権限を付与できること。 ・利用者属性、デバイス状態、接続元及びリスクレベル等に基づき、動的なアクセス制御を実施できること。 ・認証情報、権限情報及びIDライフサイクルを適切に管理し、不正利用及び権限の残存を防止できること。 ・認証及び権限管理に関する操作履歴を記録し、監査証跡を確保できること。	「最小権限の原則に基づき、利用者、管理者及びアプリケーションに対し必要最小限の権限を付与できること。」について、アプリケーションに対する権限付与は、アプリケーションインスタンス自体の権限設定という認識でよいでしょうか？アプリケーション内の権限についてはEntraIDでは管理できません。	正確な仕様・要件を確認するため。また、当社からのご提案の最適化のため。	要件定義書1.6.-1の記載を以下のとおり修正しました。 「最小権限の原則に基づき、利用者、管理者、アプリケーション及びサービスアカウントに対し必要最小限の権限を付与できること。アプリケーションについては、可能な限り認証・ID管理基盤と連携した権限管理を行えること。」
198	要件定義書	1.6.-2	・利用者認証において、多要素認証（MFA）を適用できること。	AVD環境への接続時において、BYOD端末（PC端末）ではどのような多要素認証を想定しているか、ご教示願います。	納入端末には顔認証のカメラの要件があるものの、BYOD端末にはどのようなデバイスがあるか定かではなく、機器に依存した認証方法を採れないため。	要件定義書1.6.-2の記載を以下のとおり修正しました。 「・利用者認証において、多要素認証（MFA）を適用できること。 ・多要素認証は、認証アプリ、SMS、音声通話、ワンタイムコード、セキュリティキー（YubiKey等のFIDO2対応デバイス）その他同等の方式に対応できること。 ・特に、BYOD端末からクラウドPCへの認証について、セキュリティキー（YubiKey等）による認証を主な認証方式とし、利用方法、前提条件、必要ライセンス及び費用を提案に含めること。なお、セキュリティキー自体は調達範囲外とする。」。
199	要件定義書	1.6.-3	・認証基盤と連携し、アカウントの挙動を分析し、成りすまし・侵害リスクを自動評価できること。 ・機械学習等を用いて、通常と異なる行動を異常値として検知できること。 ・高リスクと判断されたアカウントに対し、自動的にアクセス制御（強制サインアウト、アカウント無効化、パスワードリセット等）を実施できること。	「高リスクと判断されたアカウントに対し、自動的にアクセス制御（強制サインアウト、アカウント無効化、パスワードリセット等）を実施できること。」について、アカウント無効化は誤検知・過検知時のインパクトが大きいため、要件からの削除をご提案いたします。	正確な仕様・要件を確認するため。	要件定義書1.6.-3の記載を以下のとおり修正しました。 「高リスクと判断されたアカウントに対し、リスクレベルに応じて、強制サインアウト、アクセス制限、パスワードリセット、アカウント無効化等の対策を実施できること。なお、対策は管理者の承認を経て実施できること。」
200	要件定義書	1.6.-4	・端末認証、ユーザ認証等に利用する証明書については、有効期限管理及び自動更新（自動登録・更新・失効）が可能な仕組みを備えること。 ・証明書の配布及び更新は、Active Directory又はクラウドベースの証明書管理機能と連携し、自動化されていること。 ・証明書の発行・管理・失効を行う証明書基盤（CA）を構成すること。	CAの構築が、完全新規構築となるのか既存CAとの連携を想定しているのかご教示いただけますでしょうか？	正確な仕様・要件を確認するため。	要件定義書1.6.-4の記載を以下のとおり修正しました。 「証明書の発行、管理及び失効管理を行う証明書基盤（CA）を提供すること。なお、既存の証明書基盤又はクラウドベースの証明書管理サービスの活用による実現を可とする。具体的な実現方式については提案に含めることとし、詳細は契約後に本会と協議の上決定する。」 なお、本要件は、証明書の発行、配布、更新及び失効管理を実現するための証明書基盤（CA）の提供を求めるものであり、必ずしも新規のCA構築を求めるものではありません。 既存の認証基盤、Active Directory、Microsoft 365テナント、既存CA等を活用できる場合は、その利用を妨げるものではありません。
201	要件定義書	1.6.-4／1.6.-6 1.6.-7	「アクセスレビュー（棚卸）及び承認ワークフローに対応可能であること。」 「職務分離（SoD）ルールの定義及び違反検知に対応可能であること。」 「証明書の発行・管理・失効を行う証明書基盤（CA）を構成すること。」	これらの要件充足に必要な追加ライセンス（例：Microsoft Entra ID Governance、Microsoft Intune Suite／Microsoft Cloud PKI 等）が本調達の範囲に含まれるか明記をお願いします。 Microsoft 365 A5 に標準包含されない機能が含まれるため、包含関係の前提について明記をお願いします。 併せて第三者製品による代替の可否もご教示ください。	アドオンライセンスの要否により費用が変動するため。また代替手段の許容範囲により構成が変わるため。	本要件は、アクセスレビュー（棚卸）、承認ワークフロー、職務分離（SoD）、証明書管理等の機能を実現できることを求めるものであり、特定のライセンス又は製品の採用を求めるものではありません。 Microsoft 365のライセンス体系については、A3又はA5を含め提案者が適切な構成を提案するものとします。 また、第三者製品による代替構成も可とします。 提案に当たっては、各要件を実現するために必要となるライセンス、製品構成及び前提条件を明示することとし、その内容を含めて評価するものとします。

202	要件定義書	1.6.-5	・IDライフサイクル管理については、本会が保有する ADMS（Account and Directory Management System）との連携を前提とし、当該ライセンスを利用すること。 ・ADMSと連携し、入社、異動、退職等の人事イベントに応じたアカウントの自動プロビジョニング及びデプロビジョニングができること。 ・HRシステムとの連携（CSV、API、SCIM等）に対応可能であること。	質問： ・ADMS側の連携処理やHRシステムの設定については役務対象外と考えてよろしいでしょうか ・ADMSとの連携内容について明記願います。 ・受託者がアカウント作成・変更・削除に対応する場合、ADMSに対して作業する必要がありますでしょうか。	ADMS・HRシステムとの連携方向、連携情報及びアカウント管理の責任分界が不明確であるため、必要な作業範囲、工数及び費用を正確に見積もるため。	要件定義書1.6.-5の記載を見直しました。
203	要件定義書	1.6.-5	「IDライフサイクル管理については、本会が保有するADMS（Account and Directory Management System）との連携を前提とし、当該ライセンスを利用すること。」	ADMSのライセンス名、バージョン、連携対象ID(Active Directory, LDAP, Box等)、連携方式（API、LDAP、CSV、DB連携、SCIM等）をご教示ください。 また、受注者側で追加開発が必要となる可能性があるため、公開されているインターフェース仕様書の有無についてもご教示いただくことは可能でしょうか。	ADMS連携方式により設計方針、開発工数及び構築費用が大きく変動するため。	同上。
204	要件定義書	1.6.-5 3.2.-1	・IDライフサイクル管理については、本会が保有するADMS（Account and Directory Management System）との連携を前提とし、当該ライセンスを利用すること。 ・現行システムで利用しているデータ及び設定情報について、本システムへの移行又は継承を行うこと。 ③ Exchange Online、Microsoft 365、Active Directory、ADMS については、現行テナント、ライセンス、設定、データを継承すること	貴会の保有するADMSについて、以下のどちらの認識であるかご教示願います。 ①次期システムへの移行対象ではなく、貴会の保有する現行のADMSを継続利用とする。ライセンス等は継承とする。 ②次期システムへの移行対象となり、新規で調達しオンプレ又はクラウドへ移行とする。ライセンス等は継承とする。	貴会の保有するADMSについて、移行対象であるか継続利用であるかが不明確であるため。	同上。
205	要件定義書	1.6.-5	・IDライフサイクル管理については、本会が保有するADMS（Account and Directory Management System）との連携を前提とし、当該ライセンスを利用すること。	貴会が保有するADMSとの連携を前提とありますが、提案対象範囲を明確にするため、下記についてご教示願います。 ・ADMSの製品名及びバージョン ・ライセンス体系(基本ライセンス及び導入オプション一覧) ・ライセンス形態(貴会保有/現行事業者契約) ・現在利用中の機能及び外部システム連携機能 ・現行ADMSライセンスの契約状況(契約期間、保守契約の有無) ・次期システム運用期間中におけるライセンスの利用条件及び契約期間	ご利用中のADMS及びライセンスの仕様によって提案する内容に影響するため。	同上。
206	要件定義書	1.6.-5	・IDライフサイクル管理については、本会が保有するADMS（Account and Directory Management System）との連携を前提とし、当該ライセンスを利用すること。	貴会の保有するADMSについて、次期システムへの移行対象ではなく、現行のADMSを継続利用とする場合、本調達の対象は、貴会が保有するADMSと受注者にて構築するADとの連携に係る作業のみとの認識です。当該認識に相違ないか、ご教示願います。	貴会が保有するADMSとの連携に係る作業範囲及び責任分界点が不明確なため。	同上。
207	要件定義書	1.6.-6	・アクセスレビュー（棚卸）及び承認ワークフローに対応可能であること。 ・職務分離（SoD）ルールの定義及び違反検知に対応可能であること。	Entra ID Governanceはアクセスレビューや権限管理機能を有しますが、本要件はEntraIDのみではなく、専用IGA製品との連携を想定されていますでしょうか？	正確な仕様・要件を確認するため。	要件定義書1.6.-6の記載を見直しました。
208	要件定義書	1.6.-6	ID ガバナンス ・アクセスレビュー（棚卸）及び承認ワークフローに対応可能であること。	アクセスレビューは必須の機能でしょうか？	実装する場合、追加のコストが発生するため。	同上。
209	要件定義書	1.6.-6	ID ガバナンス ・職務分離（SoD）ルールの定義及び違反検知に対応可能であること。	IT権限（Entra ID管理者ロール等）の職務分離を想定されていますか。もしくは、業務システムを含めた業務権限の職務分離(例：申請者と承認者の兼務禁止など)を想定されていますでしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	同上。

210	要件定義書	1.6.-7	特権 ID 管理 ・管理者権限は最小権限の原則に基づき付与し、必要に応じて期間限定で付与及び解除が可能であること。	「必要に応じて期間限定で付与及び解除が可能であること」は必須の機能でしょうか？	実装する場合、追加のコストが発生するため。	要件定義書1.6.-7の記載を以下のとおり修正しました。 「管理者権限は最小権限の原則に基づき付与し、期間限定の権限付与その他適切な運用により特権IDを管理できること。」 なお、本要件は、期間限定の権限付与をシステム機能により必須とするものではありません。 最小権限の原則に基づき特権IDを管理し、必要に応じて期間限定の権限付与及び解除を運用又はシステム機能により実施できることを求めます。
211	要件定義書	1.7.-1	共通要件 (オンプレミス利用の場合) ・クラウドサービスは、本会の ID 基盤（例：Entra ID）と連携し、認証・アクセス制御・ログ管理を統合的に行えること。 ・クラウドサービスの構築にあたり、必要な情報（ネットワーク、セキュリティ、アプリケーション要件等）を整理し、適切な設計を行うこと。 ・オンプレミス構成をそのまま踏襲するのではなく、クラウド構成に最適化した設計・構築・運用設計を行うこと。	こちらはクラウド利用の場合の要件でしょうか。	正確な仕様・要件を確認するため。	要件定義書1.7.-1の記載に以下を追加しました。 「・クラウドサービスは、本会の ID 基盤（例：Entra ID）と連携し、認証・アクセス制御・ログ管理を統合的に行えること。 ・クラウドサービスの構築にあたり、必要な情報（ネットワーク、セキュリティ、アプリケーション要件等）を整理し、適切な設計を行うこと。」
212	要件定義書	1.7.-2	・クラウドPC環境は、Windows 365、Azure Virtual Desktop (AVD)、又は同等のクラウドベース仮想デスクトップサービスにより、合計220ユーザ分の利用環境を提供できること。 ・Windows 365を採用する場合は、Frontline 150ライセンス及びEnterprise 70ライセンス構成 で提供されるサービスレベル（同時利用ユーザ数、処理性能、可用性）と同等以上であること。 ・クラウドPCは、外部のBYOD端末から利用できること。 ・BYOD端末からの利用に際しては、ゼロトラストの原則に基づき、デバイス状態・認証・ネットワーク等に応じたアクセス制御を行えること。 ・クラウドPC上で業務データが完結し、利用端末にデータを保存しない構成とすること。 ・クラウドPCの初期設定（ネットワーク、セキュリティ、ポリシー、アプリケーション等）を実施し、業務システムが利用可能な状態とすること。 ・クラウドPCの利用に必要なネットワーク設計（SINET経由の接続を含む）を行うこと。 ・クラウドPCの運用（ライセンス管理、利用者追加、削除、トラブル対応等）について、必要な支援を行うこと。	質問： ・BYOD端末に対するMDM管理、コンプライアンスポリシー等によるアクセス制限を行う認識でよいでしょうか ワイプやアプリケーション配信等必要な要件があれば明示ください。 ・Frontline150ライセンスは、研究員用、Enterprise70ライセンスは海外研究連絡用という認識でよろしいでしょうか。 また、Frontline150ライセンスについては、利用者が150人の場合は、Enterpriseでも問題ないと思えるが、Frontlineを利用したい旨があれば教えていただきたい。 ・BYOD端末の管理については不要との認識で問題ないでしょうか。 上記認識が問題ない場合はアクセス制御の条件となるデバイスの状態については記載を改めていただきたい。	デバイス状態の取得にはBYOD端末の管理が前提となるため、管理範囲、アクセス制御条件及び必要ライセンスを明確にし、実現可能な運用方式を検討するため。	要件定義書1.7.-2の記載を以下のとおり修正しました。 「・BYOD端末からの利用に際しては、ゼロトラストの原則に基づき、利用者認証、多要素認証、端末状態及び接続元情報等に応じたアクセス制御を行えること。 ・端末状態の判定に当たっては、OSバージョンその他セキュリティ上必要な条件を確認し、条件を満たさない端末からのアクセスを制限できること。」 なお、BYOD端末に対するMDM管理、ワイプ、アプリケーション配信は想定していませんが、クラウドPCへのアクセスに当たっては、利用者認証、多要素認証、端末情報その他の条件に基づくアクセス制御を実施できることを求めます。接続BYOD端末によりコンプライアンスポリシー等によるアクセス制限を行えることを想定しています。 Frontline150ライセンスは、研究用、Enterprise70ライセンスは海外研究連絡用、合計220ユーザについては、ご認識のとおりです。 研究員150名は、必ずしも業務時間対中常時接続しているわけではないので、役職員への流用可能性も考慮しFrontline150ライセンスとしています。 なお、数値には若干の余裕を含んでいるので、検証用等の利用には問題ないという理解です。 端末情報としては、OSのバージョン、OSのサポート状況、ブラウザのバージョンその他セキュリティ上必要な条件を確認し、条件を満たさない端末からのアクセスを制限できることを想定しています。 具体的な判定項目及び制御方法については、提案内容を踏まえ、本会と協議の上決定するものとします。
213	要件定義書	1.7.-2	・クラウドPC環境は、Windows 365、Azure Virtual Desktop (AVD)、又は同等のクラウドベース仮想デスクトップサービスにより、合計 220 ユーザ分の利用環境を提供できること。	220ユーザ分の内訳についてご教示願います。調達仕様書2.4にある研究員用150ユーザと海外研究連絡センター用の70ユーザーであると認識しております。 一時利用端末を研究員に一時貸与する場合や、検証用端末にて検証のために検証用のクラウドベース仮想デスクトップサービスを使う場合も想定されるため、これらの利用者の取り扱いについてご教示願います。	他の利用者がクラウドベースデスクトップ環境を利用する想定への抜け漏れ確認のため。	同上。
214	要件定義書	1.7.-2	BYOD 端末からの利用に際しては、ゼロトラストの原則に基づき、デバイス状態・認証・ネットワーク等に応じたアクセス制御を行えること。	BYOD端末はKBCのネットワークには直接接続せず、KBC内でBYOD端末を利用する場合はモバイルルータなどを使用してインターネット経由で利用すると認識しております。当該認識に相違ないか、ご教示願います。	BYOD端末をKBC内のネットワークに接続するのはセキュリティの懸念があり、その懸念点を把握することで、強いセキュリティの構成を検討するため。	ご理解の通りです。
215	要件定義書	1.7.-2	「Windows 365 を採用する場合は、Frontline 150 ライセンス及びEnterprise 70 ライセンス構成で提供されるサービスレベル（同時利用ユーザ数、処理性能、可用性）と同等以上であること。」	Windows 365 Frontlineは、Windows 365 Flexを指すとの理解で相違ないかご教示ください。	Frontlineは旧称となっているため念のためのご確認です。	ご指摘のとおり、Windows 365 Frontlineは、Windows 365 Flexへと名称が変更されましたので修正しました。。

216	要件定義書	1.7.-2	クラウド PC ・クラウド PC の利用に必要なネットワーク設計（SINET 経由の接続を含む）を行うこと。	「SINET経由の接続」の部分について確認させてください。 本要件は、クラウドPC（Windows 365）から貴会のシステムへアクセスする際、SINETを経由したネットワーク構成とすることを求める意図でしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	要件定義書1.7.-2の記載に以下を追加しました。 「・利用者はインターネット経由でSSE及び認証基盤を介してクラウドPCへ接続できること。 ・クラウドPCから本会システム及び業務利用するクラウドサービスへの通信は、原則としてSINET及びSSEを経由する構成とし、必要な接続設計及び設定を実施すること。」
217	要件定義書	1.7.-3	セキュリティ要件 ・クラウドサービスのログを適切に取得し、監視基盤（SOC／SIEM等）と連携できること。	以下の内容に変更頂く事を提案します。 ----- クラウドサービスのセキュリティ監視に必要なログを適切に取得し、監視基盤（SOC／SIEM等）と連携できること。	クラウドサービスで出力されるすべてのログを収集・分析する場合は、専用SIEM基盤の追加導入や運用コストの増加が見込まれるため。	要件定義書1.7.-3の記載を以下のとおり修正しました。 「クラウドサービスのセキュリティ監視、インシデント対応及び監査に必要なログを適切に取得し、監視基盤（SOC／SIEM等）と連携できること。対象とするログ及び連携方法については提案に含めること。」
218	要件定義書	1.7.-5	電子メール基盤 ・Exchange Online は Entra ID と連携し、多要素認証（MFA）条件付きアクセス デバイス準拠性（Intune／EDR）を利用したアクセス制御が可能であること。	デバイス準拠性（Intune／EDR）についてはEDRによる判定も必須でしょうか。 またその場合、EDRについてはMicrosoft Defender for Endpoint P2を指している認識で良いでしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	要件定義書1.7.-5の記載を見直しました。
219	要件定義書	1.7.-5	・本システムは、電子メール基盤として Microsoft Exchange Online を利用し、安定したメールサービス、認証連携、アーカイブ、監査を提供すること。 ・Exchange Onlineは、本会のID基盤（Entra ID）と連携し、認証・アクセス制御・ログ管理を統合的に実施できること。 ・メールクライアントとして Outlook（デスクトップ版／Web版）を利用できること。 ・メールボックス容量は利用者あたり 50GB以上 とし、アーカイブメールボックスを利用可能とすること。 ・1通あたりのメール容量は50MB程度とすること。 ・メール保持ポリシー、アーカイブ、訴訟ホールド等の設定を業務要件に応じて構成できること。 ・添付ファイルは分離添付又は安全なストレージ連携（OneDrive／SharePoint）により送信可能とすること。 ・誤送信防止機能（送信前確認、遅延送信等）を利用できること。 ・Exchange OnlineはEntra IDと連携し、多要素認証（MFA）、条件付きアクセス、デバイス準拠性（Intune／EDR）を利用したアクセス制御が可能であること。 ・ゼロトラストの原則に基づき、ユーザ属性・端末状態・接続元等に応じた動的アクセス制御を適用できること。	質問： ・添付ファイルは分離添付又は安全なストレージ連携（OneDrive／SharePoint）により送信可能とありますが、自動的な添付ファイル分離は必要ないという認識でよろしいでしょうか。また（OneDrive／SharePoint）に限定されないという認識でよろしいでしょうか	添付ファイルの安全な送信方式及び利用可能なストレージサービスの範囲を明確にし、特定の製品・方式に限定されない実現方法を検討するため。	同上。 自動分離は必須とはしません。
220	要件定義書	1.7.-5	・SPF、DKIM、DMARCを設定し、送信ドメイン認証を適切に構成できること。 ・ARC（Authenticated Received Chain）を有効化し、メール転送時における認証結果の維持及び正当性評価の向上を図ること。 ・S/MIMEにより、暗号化・署名を提供すること。 ・ウイルス対策、スパム対策、URL防御、サンドボックス等の機能を実装すること。 ・Outlookの初期設定（プロファイル設定、接続設定等）を行い、利用者が業務利用可能な状態とすること。 ・メールボックス管理、配布グループ管理、共有メールボックス管理等の運用を実施できること。 ・Exchange Onlineの監査ログ、メッセージトレース、アーカイブ機能を利用できること。 ・ログはSIEMと連携し、相関分析に利用できること。 ・トラブル対応、設定変更、利用者サポート等、必要な運用支援を提供すること。	質問： ・S/MIMEによる暗号化・署名の提供は、全役職員を対象とする要件でしょうか。また、S/MIMEを実現するために必要なユーザー証明書は受託者側の調達に含まれますでしょうか	S/MIMEの対象者数及びユーザー証明書の調達範囲を明確にし、必要なライセンス、証明書及び費用を正確に見積もるため。	同上。

221	要件定義書	1.7.-5	・本システムは、電子メール基盤としてMicrosoft Exchange Onlineを利用し、安定したメールサービス、認証連携、アーカイブ、監査を提供すること。 ・Exchange Onlineは、本会のID基盤（Entra ID）と連携し、認証・アクセス制御・ログ管理を統合的に実施できること。 ・メールクライアントとしてOutlook（デスクトップ版／Web版）を利用できること。 ・メールボックス容量は利用者あたり50GB以上とし、アーカイブメールボックスを利用可能とすること。 ・1通あたりのメール容量は50MB程度とすること。 ・メール保持ポリシー、アーカイブ、訴訟ホールド等の設定を業務要件に応じて構成できること。 ・添付ファイルは分離送付又は安全なストレージ連携（OneDrive／SharePoint）により送信可能とすること。 ・誤送信防止機能（送信前確認、遅延送信等）を利用できること。 ・Exchange OnlineはEntra IDと連携し、多要素認証（MFA）、条件付きアクセス、デバイス準拠性（Intune／EDR）を利用したアクセス制御が可能であること。 ・ゼロトラストの原則に基づき、ユーザ属性・端末状態・接続元等に応じた動的アクセス制御を適用できること。	「誤送信防止機能（送信前確認、遅延送信等）を利用できること。」について、遅延送信機能はOutlook機能にございますが、ポップアップ画面表示するような送信前確認の機能は標準ではございませんので、もしM365標準機能での実装を想定される場合にはこちらの機能の削除をお願いいたします。	当社からのご提案の最適化のため。	同上。
			・SPF、DKIM、DMARCを設定し、送信ドメイン認証を適切に構成すること。 ・ARC（Authenticated Received Chain）を有効化し、メール転送時における認証結果の維持及び正当性評価の向上を図ること。 ・S/MIMEにより、暗号化・署名を提供すること。 ・ウイルス対策、スパム対策、URL防御、サンドボックス等の機能を実装すること。 ・Outlookの初期設定（プロファイル設定、接続設定等）を行い、利用者が業務利用可能な状態とすること。 ・メールボックス管理、配布グループ管理、共有メールボックス管理等の運用を実施できること。 ・Exchange Onlineの監査ログ、メッセージトレース、アーカイブ機能を利用できること。 ・ログはSIEMと連携し、相関分析に利用できること。 ・トラブル対応、設定変更、利用者サポート等、必要な運用支援を提供すること。			
222	要件定義書	1.7.-5	電子メール基盤 ・誤送信防止機能（送信前確認、遅延送信等）を利用できること。	遅延送信や外部宛メール送信時の注意喚起等、Exchange Online標準機能による誤送信対策をもって要件を満たすこととし、送信前確認機能は必須要件から除外いただけないでしょうか。	送信前確認機能を実装する場合、専用ソリューションの追加導入が必要となり、コスト増加につながるため。Exchange Online標準機能でも一定の誤送信リスク低減が可能であるため。	同上。
223	要件定義書	1.7.-5 2.5.-2	「メール保持ポリシー、アーカイブ、訴訟ホールド等の設定を業務要件に応じて構成できること。」 「保存期間は1ヶ月以上とすること。」	メール及びMicrosoft 365データの保持要件について明記をお願いします。 ① メールの保持年数（法令・内部規程に基づく年数） ② アーカイブ対象（全利用者／特定利用者） ③ 訴訟ホールドの適用範囲 ④ 2.5.-2の「保存期間は1ヶ月以上」は、バックアップの保持期間を指すのか、データそのものの保持期間を指すのか	保持年数はアーカイブ容量及びバックアップ費用に直結するため。また保持期間が1か月の場合、ランサムウェア被害や誤削除の発覚が遅れた際に復元できない懸念があるため。	「2.5.-2の保存期間は1ヶ月以上」については、利用者が利用するメールデータ及びシステムデータについて、障害、誤削除その他の事象発生時に復旧又は参照可能な状態で保持する期間を指すので、バックアップとは異なります。

224	要件定義書	1.8.-1	・本システムはクラウド利用を原則とし、可能な限りパブリッククラウド上にサーバ群を配置するものとする。 ・ただし、クラウド上での運用が困難な機能（例：オンプレAD、ADMS、ネットワーク制御系、オンプレ接続が必要な管理サーバ等）については、KBC内の仮想化基盤上に配置するものとし、オンプレミス側は最小限の構成とすること。 ・本仮想化基盤上には、上記クラウド非適合サービスを安全かつ高可用に運用するための仮想マシン群を配置すること。 ・本システムは、オンプレミス及びパブリッククラウド環境において仮想化基盤を構築し、サーバ資源の有効活用、可用性向上、運用効率化を実現すること。 ・仮想化基盤は、ゼロトラストアーキテクチャに基づき、ID・ネットワーク・ログ管理基盤（SIEM/SOAR）と連携できること。	質問： ・全てをパブリッククラウド(IaaS)にサーバ群を配置する場合、オンプレミスの仮想基盤は必要ないという認識でよろしいでしょうか ・本仮想化基盤は今回調達の機能利用目的で構築し、他システムの構築のためにリソース（仮想マシンなど）を個別に提供するものではない理解でよいでしょうか。 ・クラウド上での運用が困難と想定されている意図がありましたら教えてください。	例示された機器類は一般的にクラウド上でも稼働可能であるため、オンプレミス仮想基盤が必要となる特殊な条件や制約を明確にし、重複又は過剰な設備構成を避けるため。	本会はクラウドファーストを原則としており、可能な限りパブリッククラウド上での実現を想定しています。 認証基盤（AD、DNSを含む）、ID管理基盤（ADMS）、監視系システムその他の機能についても、クラウドサービス又はパブリッククラウド上で合理的に実現できる場合は、クラウド環境への配置を可とします。 一方、業務上又は技術上の理由によりクラウド配置が適さない機能、又はオンプレミス環境への構築がより合理的な機能については、オンプレミス環境に配置することを想定しています。 そのため、提案する構成において全ての要件をクラウド上で実現できる場合は、オンプレミス仮想化基盤の構築を必須とするものではありません。 また、本仮想化基盤は本調達で導入するシステムの構築及び運用を目的とするものであり、他システム向けの共用基盤やリソース提供を必須とするものではありません。 クラウドサービスを利用する場合は、Azure、AWSその他のクラウドサービスが提供するコンピューティング基盤及び管理基盤を本要件における仮想化基盤として取り扱うことを可とします。 この場合、ライブマイグレーション、管理サーバ等の要件については、オンプレミス仮想化基盤を構築する場合に適用されるものとし、クラウドサービスにおいては同等以上の可用性、運用性及び拡張性を備えていることを求めます。可用性要件については、可用性ゾーン、リージョン冗長化等のクラウド標準機能による実現を可とします。 また、ベアメタルサーバ又は物理アプライアンスを利用する構成についても、本要件で求める可用性、運用性及び保守性を同等以上に満たす場合は提案を可とします。
225	要件定義書	1.8.-1	・本システムはクラウド利用を原則とし、可能な限りパブリッククラウド上にサーバ群を配置するものとする。 ・ただし、クラウド上での運用が困難な機能（例：オンプレ AD、ADMS、ネットワーク制御系、オンプレ接続が必要な管理サーバ等）については、KBC 内の仮想化基盤上に配置するものとし、オンプレミス側は最小限の構成とする。	「クラウド上での運用が困難な機能」と記載がありますが、困難と判断された意図や背景があればご教示願います。 要件を確認するかがり、すべてパブリッククラウドへの移行が可能な認識ですが、貴会で想定する懸念点がありましたら合わせてご教示願います。	パブリッククラウド上へのサーバ配置によって運用が困難となる理由について確認したいため。	同上。
226	要件定義書	1.8.-1	共通要件 ・仮想化基盤は、ゼロトラストアーキテクチャに基づき、ID・ネットワーク・ログ管理基盤（SIEM/SOAR）と連携できること。	以下の内容に変更頂く事を提案します。 ----- ・仮想化基盤のセキュリティ監視に必要なログを適切に取得し、監視基盤（SOC／SIEM等）と連携できること。	連携対象や取得対象ログを明確化するため。 仮想化基盤で出力されるログには多くの種類があり、すべてのログを収集・分析対象とした場合、専用SIEM基盤の追加導入や運用コストの増加が見込まれるため。	同上。
227	要件定義書	1.8.-3	・サーバ仮想化を行うため、物理マシン又はクラウドサービスを活用し、仮想化基盤を構築すること。 ・仮想マシンは、稼働したまま異なるホストへ移動できるライブマイグレーション機能を有すること。 ・仮想マシングループを指定し、特定の仮想マシン同士を同一ホストに配置しない設定が可能であること。 ・仮想化基盤は、KBC及びパブリッククラウド内にそれぞれ一式設置すること。	質問 ・クラウドサービス利用時における仮想化基盤の構築をするとは、何を意味するか具体的にご教示ください。パブリッククラウド(IaaS)環境自体が仮想化基盤と認識しており、必須要件となっている意図をお聞きたいです。	クラウドサービス利用時に求められる仮想化基盤の具体的な構成と目的を明確にし、重複する基盤構築や過剰な要件を避けるため。	同上。
228	要件定義書	1.8.-3	「仮想化基盤は、KBC内及びパブリッククラウド内にそれぞれ一式設置すること。」	クラウドサービスにより同等以上の可用性及び機能を実現できる場合には、オンプレミス仮想化基盤の設置を必須としない構成のご提案を可能としていただけますようお願いします。	本調達はクラウド利用を原則とし、オンプレミス環境は必要最小限とする方針が示されています。 クラウドネイティブな構成においてはオンプレミス仮想化基盤を必要としない場合があるので、提案の自由度及び最適なシステム構成の実現のため。	要件定義書1.8.の記載を見直しました。
229	要件定義書	1.8.-3	・サーバ仮想化を行うため、物理マシン又はクラウドサービスを活用し、仮想化基盤を構築すること。 ・仮想マシンは、稼働したまま異なるホストへ移動できるライブマイグレーション機能を有すること。 ・仮想マシングループを指定し、特定の仮想マシン同士を同一ホストに配置しない設定が可能であること。 ・仮想化基盤は、KBC内及びパブリッククラウド内にそれぞれ一式設置すること。	「ライブマイグレーション機能」および「仮想化基盤をKBC内とクラウド内にそれぞれ一式設置」との要件は、オンプレミス仮想化基盤を前提とした記載であり、クラウドサービス提案の場合は対象外という理解であっておりますでしょうか？	正確な仕様・要件を確認するため。	同上。

230	要件定義書	1.8.-3	仮想化サーバ ・仮想化基盤は、KBC 内及びパブリッククラウド内にそれぞれ一式設置すること。	パブリッククラウド上で冗長を取る構成(東西リージョン)も可でしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	同上。
231	要件定義書	1.8.-5	仮想化基盤の機能 ・サービスを停止せずに物理ホスト間で仮想マシンのライブマイグレーションが可能であること。 ・ストレージはデータ圧縮機能及び重複排除機能を有し、書き込み時にリアルタイムで処理されること。 ・ストレージベースのスナップショット機能を有し、任意タイミングのほか、毎時・日次・週次・月次で自動取得できること。 ・10Gbps のネットワークインターフェイスを必要数有すること。	本要件は、ベアメタルや物理アプライアンスの場合は緩和いただけないでしょうか。	製品選択の幅を広げるため。	同上。
232	要件定義書	1.8.-5	仮想化基盤の機能 ・ハイパーバイザー型で構築すること。	ベアメタルや物理アプライアンスの構成も許容いただけないでしょうか。	オンプレ側に配置する機能が少ない場合、ハイパーバイザー型ではなくベアメタルや物理アプライアンスを利用した方がコストメリットが出るケースがあるため。 製品選択の幅を広げるため。	同上。
233	要件定義書	1.8.-7	物理ホスト ・物理ホストは 1 台障害が発生しても残りのホストで全ての仮想サーバがストレスなく動作可能な構成とすること。	本要件は、ベアメタルや物理アプライアンスの場合は緩和いただけないでしょうか。	製品選択の幅を広げるため。	同上。
234	要件定義書	1.8.-8	ストレージ ・データ圧縮・重複排除機能を有し、リアルタイムで処理されること。 ・スナップショット機能を有し、任意タイミング及び定期取得（毎時・日次・週次・月次）が可能であること。	本要件は、ベアメタルや物理アプライアンスの場合は緩和いただけないでしょうか。	製品選択の幅を広げるため。	同上。
235	要件定義書	1.8.-9	・仮想化基盤は、物理ホスト・電源・ネットワーク経路の冗長化を行い、単一障害時もサービスを継続できること。 ・ライブマイグレーションにより、負荷集中時や障害時にサービスを停止せずに仮想マシンを移動できること。 ・クラウド環境においても、可用性ゾーン等を活用し、単一障害点を排除すること。	「ライブマイグレーションによる無停止移行」はオンプレミス仮想化基盤を前提とした要件であり、クラウドサービスの場合には対象外という理解であっておりますでしょうか？	正確な仕様・要件を確認するため。	同上。
236	要件定義書	1.8.-9	冗長化・可用性 ・ライブマイグレーションにより、負荷集中時や障害時にサービスを停止せずに仮想マシンを移動できること。	本要件は、ベアメタルや物理アプライアンスの場合は緩和いただけないでしょうか。	製品選択の幅を広げるため。	同上。
237	要件定義書	1.8.-10	・管理サーバを通じて仮想化基盤を一元管理できること。 ・仮想化基盤のログをSIEMに送信し、相関分析に利用できること。 ・仮想マシン・ホスト・ストレージの状態をリアルタイムに監視できること。 ・GUI及びCLIによる管理操作が可能であること。 ・将来的な仮想マシン・ホスト・ストレージの増設に対し、ライセンス又は構成追加により拡張可能であること。	「管理サーバを通じて仮想化基盤を一元管理できること。」については、オンプレミス仮想化基盤を前提とした要件であり、クラウドサービスの場合には対象外という理解であっておりますでしょうか？ Azureの場合は、Azure Portalというクラウドサービスから管理する形となります。	正確な仕様・要件を確認するため。	同上。
238	要件定義書	1.8.-10	管理 ・管理サーバを通じて仮想化基盤を一元管理できること。 ・仮想マシン・ホスト・ストレージの状態をリアルタイムに監視できること。 ・GUI 及び CLI による管理操作が可能であること。	本要件は、ベアメタルや物理アプライアンスの場合は緩和いただけないでしょうか。	製品選択の幅を広げるため。	同上。
239	要件定義書	1.8.-10	管理 ・仮想化基盤のログを SIEM に送信し、相関分析に利用できること。	以下の内容に変更頂く事を提案します。 ----- ・仮想化基盤のセキュリティ監視に必要なログを適切に取得し、監視基盤（SOC／SIEM等）と連携できること。	仮想化基盤で出力されるログには多くの種類があり、すべてのログを収集・分析対象とした場合、専用SIEM基盤の追加導入や運用コストの増加が見込まれるため。	同上。

240	要件定義書	1.9.-1	・クライアント端末に対し、OS設定、セキュリティポリシー、アプリケーション、更新プログラム等を一元的に管理・配布できること。 ・端末のインベントリ情報（ハードウェア情報、ソフトウェア情報、更新状況等）を収集し、管理者が参照できること。 ・端末紛失・盗難時に、リモートワイプ又はアカウント無効化等の遠隔操作による保護措置を実施できること。 ・BitLocker等のディスク暗号化の鍵管理が可能であること。 ・端末に適用するセキュリティ設定（ローカルデータ残存禁止、USB制御、アプリケーション制御等）を集中管理できること。 ・管理基盤はクラウドベース又はオンプレミスペースのいずれの方法でもよいものとし、上記要件を満たす方式を提案者の裁量により選定できること。	質問： ・業務用モバイル端末（スマホ）の運用はスコープ外という理解でよいでしょうか。	業務用モバイル端末に関する運用・保守の対象範囲を明確にし、必要な体制及び費用を正確に見積もるため。	ご理解のとおりです。
241	要件定義書	1.9.-10	・DNS機能は冗長構成とし、可用性を確保すること。 ・DNSは内部及び外部公開用で分離すること。 ・DNSSECを有効化し、ドメインのなりすましを防止すること。 ・DNSの変更は承認フローに基づき実施されること。 ・DNSクエリログを取得し、監査及び分析に利用可能であること。	質問： ・DNSSECの有効化については、外部公開用のみである認識でよろしいでしょうか ・本記載は運用として満たされるべき要件であり、システムとしてDNS変更時の承認フローを実現する必要はないとの認識でよいでしょうか。 上記認識が問題ない場合はその旨を記載いただきたい。	DNSSEC及び変更承認フローの適用範囲を明確にし、標準的なDNS機能を超える過剰なシステム要件を避けつつ、適切な製品・構成を選定するため。	要件定義書1.9.-10の記載は、1.9.-9の記載として、以下のように修正しました。 「・DNSの変更は、本会が定める変更管理手順及び承認手続に従って実施できること。 ・DNSクエリログその他運用管理及びセキュリティ監視に必要なログを取得可能であること。 ・取得したログは、必要に応じて監査、障害解析及びセキュリティ分析に利用できること。」
242	要件定義書	1.9.-10	DNS ・DNSSECを有効化し、ドメインのなりすましを防止すること。	以下の内容に変更頂く事を提案します。 ----- 外部公開用のDNSについては、DNSSECを有効化し、ドメインのなりすましを防止すること。	内部DNSの場合は、基本的に会内からの通信であり、通信経路やアクセス元が管理されているためDNSSECの必要性が低く、テレワーク時もZTNAにより認証・暗号化された経路からのみ利用するため、外部公開DNSに限定した記載を提案いたします。	同上。
243	要件定義書	1.9.-10	DNS ・DNSクエリログを取得し、監査及び分析に利用可能であること。	こちらは内部用DNSに関する要件の認識でよいでしょうか（外部公開用は対象外）。 また、DNSクエリログについては、常時取得を必須とせず、セキュリティ監視上必要な場合に取得可能であること、としていただけないでしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。 DNSクエリログを常時取得する場合、ログ量の増加に伴い、ログ保管容量に係るコスト増加が見込まれるため。	同上。
244	要件定義書	1.9.-2	・KBC内PCのローカルドライブにファイルを保存できる領域を、特定の領域(以下、「特定領域」という。)のみに制限可能なこと。 ・管理者が特定のKBC内PCに対して、遠隔で特定領域に保存されたファイルの削除命令を発行可能なこと。	ローカルの特定領域への保存の目的および利用用途（オフライン環境での作業等）についてご教示願います。	セキュリティおよび運用管理の観点からはローカルドライブ上の保存領域を設けない構成が望ましいと考えているため。 また、ローカル保存を認める要件の必要性および想定用途を確認するため。 （ファイル暗号化等のセキュリティ対策はファイルサーバ上でも実施可能と考えております。）	要件定義書1.9.-2の記載を、以下のとおり修正しました。 「1.10.-1に定めるノート型クライアント端末について、管理者が特定の端末に対して遠隔で業務データ（ファイル、設定情報、キャッシュ等）の削除を実施できること。当該削除機能は、端末の紛失、盗難、利用終了その他セキュリティ上必要な場合に実施できること。」
245	要件定義書	1.9.-2	・アプリケーションの起動を制限可能なこと。 ※起動の許可・制限は、アプリケーション名、ファイルパス、ハッシュ値の組合せにより設定可能なこと。	以下のように記載要件の緩和を願います。 「・アプリケーションの起動を制限可能なこと。 ※起動の許可・制限は、アプリケーション名、プロセス名、ファイルパス、ハッシュ値のいずれかによる設定が可能なこと。」	製品選定の幅を広げるため。	ご指摘のとおり修正しました。

246	要件定義書	1.9.-3	・KBC内領域／会外領域を管理者が定義できること。KBC内領域は、ローカルドライブ、ファイルサーバ、業務アプリ、指定クラウドストレージ等をホスト名・IP・URL等で指定可能であること。 ・KBC内領域に保存されるファイルは、既存システムへの影響を避けるため、平文で利用可能であること（ドライブ暗号化を除く）。 ・会外領域（USB、メール添付、Webアップロード等）へ持ち出す際は、ファイル形式に依存せず自動的に暗号化されること。暗号化に際し、ユーザによるパスワード入力を不要とすること。 ・暗号化されたファイルがKBC内領域に戻された場合は、自動的に復号化され、ユーザ操作を必要としないこと。 ・管理者が許可したプログラムのみ、会外領域への持ち出しを許可できること。 ・持ち出し専用フォルダを経由した場合、パスワード付きZIP等の形式に強制できること。 ・AES256bit以上 の暗号強度を利用できること。	提案： ・要件として、詳細な機能要求が記載されておりますが、想定される脅威や守りたい情報の内容について記載いただき、その方法については提案にゆだねていただきたい。	達成すべきセキュリティ目的と保護対象を明確にした上で実現方式の選択肢を確保し、特定製品に限定される可能性のある過剰な機能要件を避けるため。	要件定義書1.9.-3の記載を以下のとおり修正しました。 「・本会が指定する機密情報、業務情報及び個人情報について、不正な持出し、漏えい及び外部共有を防止できること。 ・ファイル、電子メール、クラウドストレージ、USBデバイス、Webアップロードその他の経路を対象として、情報の持出し及び外部共有を制御できること。 ・利用者、端末、保存場所、情報区分、属性その他の条件に応じてアクセス制御又は持出し制御を実施できること。 ・情報の持出し、共有、ダウンロード、コピー等について監査ログを取得できること。 ・暗号化、アクセス制御、情報分類、権限制御、情報漏えい対策（DLP）その他同等の機能により情報保護を実現できること。 ・情報保護及び持出し制御の実現方式については提案に含むこととする。 ・本会が管理する領域及び外部領域の定義並びに制御対象については、提案内容を踏まえ、本会と協議の上決定するものとする。」
247	要件定義書	1.9.-3	・会外領域（USB、メール添付、Web アップロード等）へ持ち出す際は、ファイル形式に依存せず自動的に暗号化されること。暗号化に際し、ユーザによるパスワード入力を不要とすること。	以下のように記載要件緩和のご検討願います。 「会外領域（USB、メール添付、Web アップロード等）へ持ち出す際は、ファイル形式に依存せず必要に応じて暗号化できること。暗号化に際し、ユーザによるパスワード入力を不要とすること」	自動暗号化を前提とした場合、業務利用可能な製品やサービスが限定される可能性があるため、実現性及び運用性の観点から代替方式の適用可否を確認したいため。	同上。
248	要件定義書	1.9.5	・組織内のノート型クライアント端末の情報（OS、アプリケーション、Defenderの状態など）を自動収集し、一元管理できること。	提案： ・クライアントコンピューターを管理する管理画面で、セキュリティ診断結果を端末機別・診断項目別に確認できること。といった内容を盛り込むのはいかがでしょうか	端末ごとのセキュリティ状態を一元的に把握し、問題の早期発見及び管理業務の効率化を図るため。	原案通りとします。
249	要件定義書	1.9.-2／1.9.-3 1.9.-6／1.9.-7／1.9.-8	「運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。」 「会外領域（USB、メール添付、Web アップロード等）へ持ち出す際は、ファイル形式に依存せず自動的に暗号化されること。」 「収集されたファイル操作ログから、一つのファイルに対して、どのような操作…が行われたかを抽出して表示する機能を有すること。」	1.9.-6の「単一のソフトウェアで実現すること」について、要件緩和のご検討をお願いします。 1.9.-2（保存領域の制限、遠隔でのファイル削除、ハッシュ値によるアプリ起動制限）、1.9.-3（形式非依存の自動暗号化）、1.9.-7（ファイル単位の操作ログ追跡）、1.9.-8（USBデバイス台帳の自動作成・登録制限）は、Microsoft Intune 単体では実現できない、又は同等の運用性を確保できないものと考えられます。 Microsoft 365（Intune／Defender／Purview）を基盤とし、資産管理・詳細操作ログ・持出制御を補完製品で組み合わせる構成を許容いただけるかについて明記をお願いします。	「単一のソフトウェア」を厳格に適用すると、Microsoft 365 を中核とする方針（別紙1 1.11.-1 等）と両立せず、いずれかの要件を満たせなくなるため。	要件定義書1.9.-6 運用を削除しました。
250	要件定義書	1.9.-6	・運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。	「上記要件」とは1.9-5のみを指している認識でよろしいでしょうか。また、単一ソフトウェアの定義をご教示願います。	抜け漏れのない要件確認のため。	同上。
251	要件定義書	1.9.-8	デバイス管理 ・USB デバイスをクライアントコンピューターもしくは管理者のクライアントコンピューターに挿入した際、利用した USB デバイスのシリアルナンバー、ペンダ ID を自動で収集し、管理台帳を作成できること。（USB デバイスタ帳自動登録、台帳管理） ・シリアル番号やペンダ ID、及びプロダクト ID が取得できず、個体識別が行えない USB デバイスについては、台帳への登録を制限できること。（USB デバイス／メディア登録設定）	こちらのUSB管理台帳に関する仕様を削除いただけないでしょうか。	USBデバイスの資産管理・台帳管理を目的とした機能であり、デバイス利用制御や情報漏えい対策の実現には必須ではないため。 本機能を実現するためには複数製品を組み合わせた導入が必要となり、追加コストが発生するため。	原案どおりとします。

252	要件定義書	1.9.-9	・本システムにおける認証基盤として Active Directory を構築すること。 ・Active Directoryは、オンプレミス又はクラウド環境のいずれでも構築可能とする。 ・Active Directoryは、Entra ID と連携し、認証及びアカウント管理を統合的に実施できること。 ・ドメインコントローラは冗長構成とし、単一障害点を排除すること。 ・閉域網における名前解決は、Active Directoryに統合されたDNS機能を利用すること。 ・内部リソースの名前解決は Active Directory DNS により実施すること。	質問： ・認証連携の提供が必要なシステムの一覧とそれぞれの認証方式についてご教示ください。ADMSのみの認識でお間違いないでしょうか。	認証連携が必要なシステム及び認証方式を明確にし、連携設計、構築工数及び必要なライセンスを正確に見積もるため。	Active Directory については、「表1.6-1 認証・ID管理基盤の機能要件」に移動し、整理しました。
253	要件定義書	1.9.-9	「本システムにおける認証基盤としてActive Directory を構築すること。」	Active Directoryを必須要件としている背景及び利用想定（AD認証が必要な業務システム、LDAP連携、グループポリシー適用、証明書連携等）をご教示ください。 また、業務要件を満たす場合には、Entra IDを中心としたクラウドネイティブ構成での提案は許容されますでしょうか。	Active Directoryの必要性及び残存範囲を明確化し、最適なシステム構成及び適正な費用算出を行うため。	本会はクラウドファーストを基本方針としていますが、施設内DNSサービスの提供及び既存ID管理基盤（ADMS）との連携を考慮し、現時点ではActive Directoryの利用を想定しています。 ただし、これらの要件をクラウドサービス等により合理的に実現できる場合は、Active Directoryを必須とするものではありません。
254	要件定義書	1.10.	-	クライアント端末を会外へ持ち出して利用する際のインターネット接続方式としては自宅ネットワークやモバイルルータ、テザリング等を利用し、端末内蔵のSIM及びモバイル回線は不要との認識でよろしいでしょうか。 自宅や外出先から業務サーバおよびSaaSサービス等利用のため、KBC拠点外からのインターネット接続について確認願います。	仕様には貴会外からのクライアント端末からの接続方式に関する記載がないため。	ご理解のとおりです。要件定義書1.10.-1の記載に、以下を追加しました。 「ノート型クライアント端末を会外へ持ち出して利用する際のインターネット接続方式としては、自宅ネットワークやモバイルルータ、テザリング等を利用し、端末内蔵のSIM及びモバイル回線は不要とする。」
255	要件定義書	1.10.-2	・生成AIアシスタント（AIエージェント）や対話型AIサービス（例：Microsoft Copilot 等）の利用	生成AIアシスタント（AIエージェント）や対話型AIサービスについて、一般的なWebベースのAIチャットの利用ができれば良いとの認識です。当該認識に相違ないか、ご教示願います。	一般的なWebベースのAIチャットの利用のみ（例：Microsoft Copilot）であれば調達するMicrosoft 365ライセンスに含まれているが、Microsoft 365データを参照したAIサービスやoffice製品内でのAI機能の利用には追加ライセンスが必要なため。	同上。
256	要件定義書	1.10.-2	用途 ・PDFファイルの閲覧及び編集	本機能を実現するために必要となるソフトウェアライセンス（Adobe Acrobat等）は、受託者にて調達・提供する前提でしょうか。それとも委託者から提供されるライセンスを利用する前提でしょうか。	調達範囲を明確にするため。 資料招請の段階では「PDF 作成・編集のため、Adobe Acrobat（保有ライセンス）を利用できること。」といった記述であったため。	同上。
257	要件定義書	1.10.-2	「生成 AI アシスタント（AI エージェント）や対話型 AI サービス（例：Microsoft Copilot 等）の利用」	生成AI／AIエージェントの位置付けについて明記をお願いします。 ① Microsoft 365 Copilot 等の生成AIライセンスが本調達の調達範囲に含まれるか（含まれる場合は対象人数） ② 端末が当該用途に耐える性能を有することのみを求める趣旨か ③ 本会における生成AI利用に関するポリシー（利用可否、入力可能な情報区分、監査・ログ要件）の有無	生成AIライセンス及び利用統制（データ保護、監査ログ、DLP連携等）の要否により、必要ライセンス及び構築・運用作業が大きく変動するため。	要件定義書1.10.-2は端末の用途の例示ですので、一般的なWebベースで生成AIサービスが利用できること、Adobe Acrobat等を利用してPDFの閲覧および編集ができることを想定しています。
258	要件定義書	1.10.-3	OS ・Windows 11 Enterprise（64bit）を搭載していること。	Windows 11 Pro 64bit以上を搭載し、Microsoft 365 Education A3/A5のライセンスによりWindows 11 Enterprise相当の機能を利用可能であること。	Microsoft 365 Education A3/A5ライセンスによりWindows 11 Enterprise相当の機能を利用可能であるため、Windows 11 Enterprise搭載を必須とする必要性は低いと考えます。提案可能な機種を選択肢拡大およびコスト最適化の観点から、Windows 11 Pro（64bit）以上を要件とすることを提案します。	ご指摘のとおり修正しました。
259	要件定義書	1.10.-4	・性能の目安として、PassMark CPU Mark において15,000 以上を満たすこと。	「性能の目安として、PassMark CPU Markにおいて10,000以上を満たすこと」に緩和願います。	項番61の要件が緩和される場合、PassMark CPU Markの要件についても併せて見直しが必要と考えるため。 必要な業務性能を確保しながら、調達における製品選択の幅を広げるかつ調達費用低減が図れるため。	要件定義書1.10.-4の記載を見直しました。
260	要件定義書	1.10.-4	・Intel Core i7相当以上、又は AMD Ryzen 7 シリーズ相当以上の性能を有するプロセッサを搭載していること。	「Intel Core i5相当以上、又は AMD Ryzen 5 シリーズ相当以上」に緩和を願います。	一般的な業務利用においてはIntel Core i5相当またはAMD Ryzen 5相当でも十分な性能を有しており、提案可能機種の拡大および調達費用低減が図れるため。	同上。
261	要件定義書	1.10.-5	・調達後の長期利用（5年間）を見据え、標準構成は32GB以上とすること。	提案： ・コスト最適化の観点から、メモリ要件を16GB以上へ変更することを検討いただけないでしょうか。	一般的な事務業務やMicrosoft Office製品を中心とした利用であれば、16GBでも十分な性能を確保できると考えられる。また、昨今のメモリをはじめとした半導体価格の高騰により、端末調達コストへの影響も大きくなっているため。	本要件は調達時点の利用状況だけでなく、5年間の利用期間を通じた性能維持を目的として設定しているため、原案のとおり32GB以上とします。

262	要件定義書	1.10.- 8	「のぞき見防止ファイルタ(プライバシーフィルタ)を装着した状態で納品すること。」	PCと併せて送付させていただくことも許可いただけますでしょうか。	初期セットアップ、キitting作業、動作確認、資産管理ラベル貼付等の工程においてフィルターの脱着が必要となりますが、対応可能なメーカーが限定され、競争性を欠く懸念があるため。 また、あらかじめPC本体に装着した状態での納品ではなく、PCと同時に同梱納品の方が運用上合理的であるため。	装着作業場所は本会でも構いませんが、装着作業自体は受注者負担とします。
263	要件定義書	1.10.-9	・Thunderbolt 4（DisplayPort Alt Mode／USB Power Delivery対応）ポートを1 ポート以上搭載していること。	「USB Type-C（USB3.2以上）ポートを1ポート以上搭載していること。」に緩和願います。	USB3.2 Type-C以上であれば、映像出力および給電等の一般的な利用要件を満たすことができ、提案可能な機種幅を広げるかつ調達費用低減が図れるため。	要件定義書1.10.-9の記載を、以下のように変更しました。 「Thunderbolt 4（DisplayPort Alt Mode／USB Power Delivery対応）ポート又はUSB Type-C（USB3.2以上）ポートを1ポート以上搭載していること。」
264	要件定義書	1.10.-1	共通要件 ・ノート型クライアント端末は、FAT 端末又はセキュア FAT 端末とし、本会役職員用に 415 式提供すること。ローカルデータの取り扱いに関する要件は「1.5.-17 セキュリティ要件」区分に記載する。	ローカルデータの取り扱いに関する要件は「1.5.-17 セキュリティ要件」区分に記載する。 ⇒「1.10.-17 セキュリティ要件」区分に記載する。の誤りではないでしょうか。	要件の記載箇所について確認したいため。	ご指摘のとおり修正しました。
265	要件定義書	1.10.-11	・ネットワーク機能は以下の要件を満たすこと。 (1) 有線LAN ① IEEE 802.1X認証に対応していること。 ② RJ45ポートを搭載し、1000BASE-T／100BASE-TXに対応していること。 (2) 無線LAN ① IEEE 802.1X認証に対応していること。 ② IEEE 802.11ax/ac/a/b/g/nに準拠していること。 ③ 高密度接続時においても、Web会議、VDI利用等を安定して実施できること。	質問： 「③高密度接続時においても、Web会議、VDI利用等を安定して実施できること。」に關し、クライアント端末に求められるハードウェア仕様をお教えいただけますでしょうか。	ハードウェア仕様・機能に必要な仕様を明確にしたいため。	高密度接続とは混雑に強いIEEE 802.11ax（Wi-Fi 6）以上に対応していることを指しているので、③は削除しました。
266	要件定義書	1.10.-13	・業務データの恒久的な保存先は、クラウドストレージ又は本会が指定するファイルサーバとすること。 ・保存先は、以下の要件を満たすものとする。 (1) ユーザがローカル端末にデータを恒常的に保存する必要がないこと。 (2) アクセス権限管理（ユーザー／グループ単位）が可能であること。 (3) バージョン管理又はバックアップ機能を有すること。 (4) 暗号化（保存時・通信時）が実装されていること。 (5) 外部媒体（USB等）への持ち出しを制御できること。 (6) 複数端末からのアクセスが可能であること。 ・保存先の具体的な方式（SharePoint、OneDrive、Azure Files、AWS S3、Box、オンプレミス SMB等）は問わないものとし、上記要件を満たす方式を提案者の裁量により選定できるものとする。	提案： ・本記載((4)の暗号化の記載)はデータ（ファイル等）自体の暗号化ではなく、ストレージ機器自体の暗号化やストレージとのデータ通信の暗号化の実装と認識している、本要件としても明確に記載していただけないでしょうか。	暗号化の対象及び実装範囲を明確にし、別項目に記載されたファイルの平文利用との整合性を確認するため。	要件定義書1.10.-13の記載を以下のように修正しました。 「(4) 保存先は、保存データの暗号化（ストレージ暗号化等）及び通信経路の暗号化（TLS等）を実装していること。なお、本要件は個々のファイルに対する暗号化機能を必須とするものではない。」
267	要件定義書	1.10.-13	ファイルサーバ ・保存先は、以下の要件を満たすものとする。 (5) 外部媒体（USB等）への持ち出しを制御できること	「(5) 外部媒体（USB等）への持ち出しを制御できること」とありますが、本要件はファイルサーバの機能として実現することを求めるものではなく、端末側の制御機能により要件を満たしていればよいとの認識で相違ないか、ご教示願います。	ファイルサーバに外部媒体への持ち出しを制御する機能を要するとなると、クラウドストレージをファイルサーバとして選択できなくなるため。	ご理解のとおりですので、(5)を削除しました。
268	要件定義書	1.10.-13 1.12.-1	「保存先の具体的な方式（SharePoint、OneDrive、Azure Files、AWS S3、Box、オンプレミス SMB 等）は問わないものとし、上記要件を満たす方式を提案者の裁量により選定できるものとする。」 「Windows／macOS／Linux など複数 OS から、公式クライアント又は Web ブラウザで同一領域へアクセス可能であること。」 「スナップショット機能を有し、ファイル単位のバックアップ／リストアが可能であること。」	1.12.-1 の各要件について、SharePoint Online／OneDrive で実現する場合の適合判定の考え方について明記をお願いします。 ① バージョン履歴・ごみ箱・保持ポリシーによる復元をもって「スナップショット」要件の充足とみなしてよいか ② 同期クライアント（OneDrive 同期クライアント／エクスプローラー統合）をもって「公式クライアント」要件の充足とみなしてよいか ③ SMB プロトコルによるアクセス及びフォルダ単位の任意のACL設定を必須とするか	1.10.-13 では方式選択が提案者の裁量とされる一方、1.12.-1 にはオンプレミス型ファイルサーバを前提とした要件が含まれており、方式ごとの適合判定基準が不明であるため。	要件定義書1.12.-1に、「クラウド化する場合には物理ストレージに関する要件は適用しない」としているので、原案どおりとします。

269	要件定義書	1.10.-15	・バッテリー駆動時間は JEITA バッテリー動作時間測定法（Ver.2.0 以上）において8時間以上であること。	バッテリー駆動時間の測定基準について、「JEITAバッテリー動作時間測定法（Ver.3.0以上）」への変更を検討願います。	JEITA Ver.3.0が最新の測定基準として広く採用されており、メーカー公表値との整合性や製品比較の公平性向上が期待できるため。	要件定義書1.10.-5の記載を、以下のように修正しました。「バッテリー駆動時間は JEITA バッテリー動作時間測定法（Ver.2.0）において8時間以上であること。または JEITA バッテリー動作時間測定法（Ver.3.0）、MobileMark® 30において同等以上の性能を有すること。」
270	要件定義書	1.10.-15	・バッテリー駆動時間は JEITA バッテリー動作時間測定法（Ver.2.0 以上）において8時間以上であること。	バッテリー駆動時間について、JEITAバッテリー動作時間測定法に加え、MobileMark® 30による測定結果も認める要件へ変更願います。	MobileMark® 30は業界標準の測定指標の一つであり、当該指標を採用するメーカーも存在するため。提案可能なメーカーの幅を広げるため。	同上。
271	要件定義書	1.10.-15	・バッテリー駆動時間はJEITAバッテリー動作時間測定法（Ver.2.0以上）において8時間以上であること。 ・バッテリーは保守期間内に交換可能であることが望ましい。	意見： ・JEITAバッテリー動作時間測定法はVer.3.0へ改定されているため、Ver.2.0ではなくVer.3.0に基づき、動画再生時及びアイドル時の各動作時間を記載していただけないでしょうか。	現行の測定規格に基づく統一的な評価条件とすることで、各端末のバッテリー性能を公平に比較するとともに、実際の利用状況に即した動作時間を確認するため。	同上。
272	要件定義書	1.10.-15	バッテリー ・バッテリー駆動時間は JEITA バッテリー動作時間測定法（Ver.2.0 以上）において 8 時間以上であること。	本要件は必須要件、任意要件のどちらでしょうか。 また、製品選定の幅を広げるため、JEITAバッテリー動作時間測定法に関する要件は削除いただけないでしょうか。	JEITAバッテリー動作時間測定法を条件とした場合、選定可能な製品が限定されるため。	同上。
273	要件定義書	1.10.-17	・端末内に業務データが恒常的に残存しない仕組みを実装すること。 実装方式（ローカル保存禁止、定時自動削除、暗号化領域の利用等）は問わない。 ・業務遂行上必要な一時的なローカル保存は許容するものとする。ただし、当該データは定時削除、ログオフ時削除、暗号化領域への限定保存等により、端末内に残存しないよう制御すること。 ・BitLockerの使用による暗号化ができること。 ・リモートワイプ、多要素認証、接続はSSE経由を必須とする。 （要確認）	・意見・質問： （要確認）の記載はどのようなイメージでしょうか。	「要確認」が示す具体的な確認事項及び必要な対応内容を明確にし、要求仕様を正確に理解するため。	（要確認）は削除しました。
274	要件定義書	1.10.-18	端末管理方式 ・端末管理ツール、資産管理方法及び運用体制について記載すること。	運用体制に関する記載は、別章（4.3. 体制及び方法）に記載いただけないでしょうか。	運用体制に関する内容は、集約して記載いただいた方が仕様を理解しやすいため。	運用体制に関する記載は、「4.3. 体制及び方法」に集約しました。
275	要件定義書	1.10.-11	ネットワーク機能 ③高密度接続時においても、Web会議、VDI利用等を安定して実施できること。	以下の内容に変更頂く事を提案します。 ----- 導入する無線LANシステムとの接続において、IEEE 802.11ax（Wi-Fi 6）以上及び2×2 MIMO等の機能を活用し、高密度接続環境においてもWeb会議、VDI利用等を安定して実施できること。	仕様を明確にするため。	同上。
276	要件定義書	2.1.-1	・本システムで利用するクラウドサービス（Microsoft 365、Azure、Windows 365 等）は、各サービス提供者が提示する SLA を前提とする。 ・受注者は、クラウドサービスの SLA を踏まえ、サービス停止時の影響範囲・復旧方針を明確化すること。	以下のように記載要件の緩和を願います。 「・本システムで利用するクラウドサービス（Microsoft 365、Azure、Windows 365 等）は、各サービス提供者が提示する SLA またはSLOを前提とする。 ・受注者は、クラウドサービスの SLAまたはSLO を踏まえ、サービス停止時の影響範囲・復旧方針を明確化すること。」	当社が採用を検討しているクラウドサービスの中にはSLOのみを提示している製品もございます。そのため、提案の幅を広げるためにも、停止時の影響範囲・復旧方針の明確化の前提をSLOとすることでも問題ないように要件の緩和をお願いいたします。	要件定義書2.1.-1の記載を、以下のとおり修正しました。 「・本システムで利用するクラウドサービス（Microsoft 365、Azure、Windows 365 等）は、各サービス提供者が提示するSLA又はSLOを前提とする。 ・受注者は、クラウドサービスのSLA又はSLOを踏まえ、サービス停止時の影響範囲、復旧方針及び代替手段について明確化し提案すること。」
277	要件定義書	2.1.-3	・オンプレミスに配置する最小構成（AD、DNS、証明書基盤等）は、冗長構成とし、障害時にもサービス継続が可能であること。 ・オンプレ機器の故障時は、定められた復旧時間内にサービスを再開できること。	提案： ・クラウド利用を原則とする要件があるため、本項目についてはオンプレミスに配置する場合のみの必須要件と想定しておりますが、認識に齟齬がないようでしたらその旨を記載いただけないでしょうか。	クラウド利用を原則とする要件とオンプレミス最小構成の必須要件が矛盾しているように読み取れるため、適用条件を明確にするため。	要件定義書2.1.-3の記載を、以下のとおり修正しました。 「・オンプレミス環境に配置する機能がある場合、必要に応じて冗長化を行い、障害発生時においても業務継続に必要なサービスを維持できること。 ・オンプレミス機器又はオンプレミス環境に障害が発生した場合は、定められた復旧目標に基づきサービスを復旧できること。」

278	要件定義書	2.1.-3	オンプレミス最小構成 ・オンプレミスに配置する最小構成（AD、DNS、証明書基盤等）は、冗長構成とし、障害時にサービス継続が可能であること。	要件では「AD、DNS、証明書基盤等」を冗長化対象としておりますが、証明書基盤については通常運用時に常時稼働を要するサービスではなく、障害が発生した場合でも直ちに利用者の業務継続に影響するものではないと考えております。このため、本要件における冗長化対象はADおよびDNSを想定し、証明書基盤は対象外とする認識でよいでしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	同上。
279	要件定義書	2.2.-1	ネットワーク性能 ・SINET 接続回線は 10Gbps 以上の帯域を安定的に提供できること。	1.3-3に同様の記載があるため削除いただけますでしょうか。	集約して記載いただいた方が仕様を理解しやすいため。	「2.2.-1 ネットワーク性能」は、「1.2. ネットワーク基盤」「1.3. SINET接続」に集約して削除しました。
280	要件定義書	2.2.-1	・SINET接続回線は10Gbps以上の帯域を安定的に提供できること。 ・SINET接続回線の遅延及びパケットロスは業務利用に支障のない水準であること。 ・クライアント端末を収容する有線LANポートは1Gbps以上に対応すること。 ・アクセススイッチと上位ネットワーク間は10Gbps以上で接続すること。 ・無線LANは想定利用者数及び想定トラフィックにおいて安定した通信性能を確保できること。	質問： ・上位ネットワークとは、最初のバックボーンの内容と同一でよいでしょうか。 ・無線LANは想定利用者数及び想定トラフィックにおいて安定した通信性能について、想定トラフィックを明記いただけないでしょうか。	上位ネットワークの範囲及び想定トラフィックを明確にし、必要な帯域・機器性能を適切に設計するため。	同上。
281	要件定義書	2.2.-4	・ポータル画面、お知らせ画面及びスケジュール画面は業務利用に支障のない応答性能を有すること。 ・ファイル検索及び文書参照は合理的な時間内に処理できること。 ・会議室予約、ワークフロー申請及び承認処理は円滑に実行できること。	質問： ・会議室予約、ワークフロー申請及び承認処理は円滑に実行の内容を明確にいただけないでしょうか。	「円滑に実行」の具体的な性能水準を明確にし、受入基準及び提案構成の妥当性を判断するため。	要件定義書2.2.-3の記載を、以下のとおり修正・追加しました。 「・会議室予約、ワークフロー申請及び承認処理は業務利用に支障のない応答性能を有すること。 ・上記は、数値的な性能水準を求めるものではない。」
282	要件定義書	2.2.-4／2.2.-5	「ポータル画面、お知らせ画面及びスケジュール画面は業務利用に支障のない応答性能を有すること。」 「ファイル検索及び文書参照は合理的な時間内に処理できること。」 「Microsoft 365 及びその他クラウドサービスとの連携において、業務利用に支障のない応答性能を確保すること。」	「業務利用に支障のない応答性能」「合理的な時間内」の判定方法について明記をお願いします。 SaaS（Microsoft 365）の応答性能は Microsoft のサービス水準に依存し受注者による保証が困難であるため、① 受注者の責任範囲を設計・設定の適切性及び SINET 側の帯域確保までとする、② 数値目標を設ける場合は測定条件（測定端末、回線、対象操作）を併せて定める、のいずれかとしていただけないかご検討をお願いします。	SaaS の応答性能について受注者に数値保証が求められる場合、実質的に履行不能な要件となり得るため。	同上。
283	要件定義書	2.2.-5	・Microsoft 365及びその他クラウドサービスとの連携において、業務利用に支障のない応答性能を確保すること。 ・ファイル同期、メール送受信及び予定表連携は安定して動作すること。	質問： ・メール送受信及び予定表連携は安定して動作するという内容を明確にいただけないでしょうか。 通常の利用時においては安定して動作という認識でよいでしょうか（サービス提供するMicrosoft社の不具合については考慮外ということ）	クラウドサービスの安定動作に関する責任範囲と性能基準を明確にし、サービス提供者側の障害を受託者の責任から除外するため。	本要件は数値的な性能水準を求めるものではありません。
284	要件定義書	2.2.-6	性能監視 ・システム全体の性能状況を継続的に監視できること。	主要なコンポーネントの監視が対象という認識でよいでしょうか。 2.4-1監視「・主要コンポーネントの死活監視、性能監視、ログ監視が可能であること。	正確な仕様・要件を確認するため。 適正な費用見積のため。	ご理解の通りです。

285	要件定義書	2.3.-2	・Microsoft 365の追加サービス又は新機能を容易に利用できる構成とすること。 ・新たなSaaSサービスとの連携に対応できること。	提案： ・記載の内容については構築時点で約束できるものではないため、記載を改めていただくか、想定されるSaaSサービスの連携方式について記載していただけないでしょうか。	将来提供されるサービスの仕様は提案時点で確定できず、連携可否を保証することは過剰な要件であると推察されるため、現時点で実現可能な連携方式に要件を適正化するため。	要件定義書2.3.-2の記載を、以下のとおり修正・追加しました。 「・Microsoft 365の追加サービス又は将来的な機能拡張に対応しやすい構成とすること。 ・認証連携（OpenID Connect、OAuth2.0、SAML等）、API連携その他一般的な連携方式により、新たなSaaSサービスとの連携が可能な構成とすること。 ・将来的な機能追加又はサービス連携を阻害しない拡張性を有すること。 ・機能拡張又は新たなSaaSサービスとの連携を実施する場合は、別途本会と協議の上、その実施内容、実施方式、費用及びスケジュールを決定するものとする。」
286	要件定義書	2.5.-1	・Microsoft 365（Exchange Online、SharePoint Online、OneDrive for Business等）のデータ、ファイルサーバのデータ（アクセス権限情報（ACL）を含む）、業務アプリケーションデータ及びネットワーク機器設定情報等を保護対象とすること。 バックアップ又は同等のデータ保護機能により、誤削除、障害発生時等にデータを復元可能な状態で保管できること。 ・データ保護方式及び取得スケジュールを提案すること。	質問： ・オンプレサーバについても拠点外でバックアップ取得が必要でしょうか。	オンプレミスサーバーのバックアップ保管場所と対象範囲を明確にし、必要な回線、保管容量及び運用費用を正確に見積もるため。	要件定義書2.5.-1の記載に、以下を追加しました。 「・Microsoft 365その他のクラウドサービスについては、サービス標準の保持機能、バージョン管理機能、復元機能その他同等のデータ保護機能による実現を可とする。 ・バックアップの世代管理、保持期間及び取得スケジュールについては提案すること。 ・BCP及びDR対策として、保護対象データは、最低1世代分を当該システムとは異なる場所又は異なる障害影響範囲に保管できること。 ・クラウド環境を利用する場合は、異なるリージョンへの保管、リージョン冗長化、LTR（Long Term Retention）、コールドバックアップその他同等の方法により、災害又は広域障害発生時に復旧できること。 ・オンプレミス環境を利用する場合は、拠点外保管その他同等の方法により、災害又は施設障害発生時に復旧できること。 ・データ保護方式、保管場所、保持期間、取得スケジュール及び復元手順について提案すること。」
287	要件定義書	2.5.-1	「Microsoft 365（Exchange Online、SharePoint Online、OneDrive for Business等）のデータ…を保護対象とすること。バックアップ又は同等のデータ保護機能により、誤削除、障害発生時等にデータを復元可能な状態で保全できること。」	Microsoft 365 データの保護方式に関する前提について明記をお願いします。 ① Microsoft 365 標準機能（ごみ箱、バージョン履歴、保持ポリシー、回復可能なアイテム）による復元をもって充足とみなしてよい か ② テナント外へのバックアップ（第三者バックアップ製品等）を要するか。②の場合、対象容量（メールボックス総容量、SharePoint／OneDrive 総容量）をご開示願います。	テナント外バックアップを要する場合、製品ライセンス及び保管容量に応じた費用が別途発生し、総額への影響が大きいため。	同上。
288	要件定義書	2.5.-1 2.5.-2	・Microsoft 365（Exchange Online、SharePoint Online、OneDrive for Business等）のデータ ・バックアップ又は同等のデータ保護機能により、誤削除、障害発生時等にデータを復元可能な状態で保全できること。 ・保存期間は1ヶ月以上とすること。	Microsoft 365（Exchange Online、SharePoint Online、OneDrive for Business）については、標準で提供される保持機能、バージョン管理機能及び削除データ復元機能を、「バックアップ又は同等のデータ保護機能」として評価対象に含む認識です。当該認識に相違ないか、ご教示願います。 また、Microsoft 365のデータの保存期間について「30日以上」への緩和をご検討願います。	Microsoft 365は、サービス標準機能として保持ポリシー、バージョン管理、削除データ復元機能等を備えており、誤削除、上書き及び利用者操作によるデータ消失時の復旧に対応可能であり、提案の柔軟性につながるため。 また、保存期間を『1か月以上』とした場合、31日が必要と解釈できるため、実質的な要件意図である『約1か月間の復元・保護』を満たしていても不適合と判断される懸念があるため。	同上。
289	要件定義書	2.5.-1	バックアップ対象・方式 ・Microsoft 365（Exchange Online、SharePoint Online、OneDrive for Business等）のデータ、ファイルサーバのデータ（アクセス権限情報（ACL）を含む）、業務アプリケーションデータ及びネットワーク機器設定情報等を保護対象とすること。 バックアップ又は同等のデータ保護機能により、誤削除、障害発生時等にデータを復元可能な状態で保全できること。	要件に記載の「障害発生時等にデータを復元可能な状態で保全できること」における「障害発生時」について、想定される障害の範囲をご教示ください。 例えば、利用予定のEntra ID、Windows 365およびBox等のクラウドサービスについては、サービス提供事業者による冗長化および可用性確保が実施されておりますが、クラウドサービスの全面停止や広域障害からの復旧までを求める場合には、別途バックアップソリューションの導入が必要となる可能性があります。 Microsoft 365およびBoxの標準機能（保持機能、バージョン管理機能、ごみ箱機能等）による復元機能をもって本要件を満たすとの認識でよいか、ご教示ください。	正確な仕様・要件を確認するため。 適正な費用見積のため。	同上。

290	要件定義書	2.5.-6	・広域障害発生時のデータ保全及び復旧方針（DR構成等）を提示すること。	災害対策におけるRTOおよびRPO要件について、貴会として特段の要件はないとの認識で相違ないか、ご教示願います。 バックアップの地理的冗長化のみが明示されている認識です。	クラウドサブリージョンでの災害対策の構成を検討する際、RTO、RPO要件により採用すべきサービスや構成が異なるため。	業務基盤システムについて、業務の目標復旧時間（RTO）5時間としています。
291	要件定義書	2.6.-4	・認証ログ、操作ログ、アクセスログ、セキュリティログ等の監査証跡を提供可能であること。 ・監査要求に応じたログ抽出・提供方法の概要を提示すること。	質問： ・監査対応(ログ提出)の想定発生頻度をご教示いただけないでしょうか。	監査対応の発生頻度によりログ抽出・提出に必要な運用工数変動するため、体制及び費用を適正に見積もるため。	監査対応（ログ提出）の頻度は現時点では定めていません。 要件定義書2.6.-4の記載に、以下を追加しました。 「法令対応、内部監査、外部監査、インシデント対応その他必要な場合において、監査証跡を抽出及び提供できること。」
292	要件定義書	3.1.-1	KBC内の既設ラック、配線設備及び電源設備を可能な限り活用すること。 機器設置に必要な電源設備は、原則として既設設備を利用すること。 既設設備の利用が困難な場合は、本会と協議の上で対応すること。	質問 ・ラック新設や電源設備工事における費用は調達外でしょうか。	ラック新設及び電源設備工事の費用負担範囲を明確にし、調達費用の算定漏れや重複計上を防止するため。	ラック新設・更新や電源設備工事が必要な場合は、調達範囲内です。
293	要件定義書	3.1.-3	搬入・設置 ・ラックへの機器等の搭載が必要な場合は、情報セキュリティ、耐震性、重量、消費電力及び保守性を考慮すること。 ・KBC内サーバ室の耐荷重は、500kg/m2 である。サーバ等の設置が必要な場合については、この値を十分に考慮すること。	現在のラックの状態（ラック数、空きユニットの場所、PDUの場所、他の機器の搭載位置）の情報をご教示願います。	ラックの状況は現行システムに係る事業者でなければ知りえない情報であり、ラック搭載図（提案書提出の際の一資料）の作成に公平性を保つため。	詳細は、別途資料提供を行います。
294	要件定義書	3.2.-1	・現行システムで利用しているデータ及び設定情報について、本システムへの移行又は継承を行うこと。 具体的には、以下を含むものとする。 ① 現行ファイルサーバのデータ移行 ② 現行グループウェアサーバのデータ移行 ③ Exchange Online、Microsoft 365、Active Directory、ADMSについては、現行テナント、ライセンス、設定、データを継承すること	質問 ・継承は契約等の変更により現行テナントを継続利用し運用主体だけ変更するという意図で間違いないでしょうか。 ・現行グループウェアサーバの移行するデータについては、本要件定義書にてグループウェア機能として記載されているデータの範囲との認識でよいでしょうか。 上記認識に問題ない場合はその旨も記載していただけないでしょうか。	既存テナントの継続利用可否及び移行対象データの範囲が不明確であり、移行方式、工数及び費用を正確に見積もるため。	③については継承ということでご理解の通りです。 ②については、後段のとおりです。
295	要件定義書	3.2.-1	「① 現行ファイルサーバのデータ移行」	現行ファイルサーバについて、移行方式・所要期間の検討に必要な以下の情報のご開示をお願いします。 ① 移行対象の実効容量及び総ファイル数 ② フォルダ階層の最大深度及び最長パス長 ③ アクセス権（ACL）の設定箇所数及び設定方式（グループ／個人） ④ 100MB超の大容量ファイル、260文字超パス、記号を含むファイル名の有無 ⑤ 移行時に許容される業務停止時間	40TB規模のデータ移行は、所要期間・回線帯域・移行ツール構成が費用及びスケジュールに直結するため。また Microsoft 365 側には最長パス長・禁止文字等の制約があり、事前の実態把握が不可欠であるため。	現行ファイルサーバのデータ、現行グループウェアサーバのデータの詳細は、別途資料提供を行います。
296	要件定義書	3.2.-1	「② 現行グループウェアサーバのデータ移行」	現行グループウェア（Garoon）からの移行対象データの範囲について明記をお願いします。併せて各データの現行件数・容量のご開示もお願いします。 ① スケジュール（過去何年分・将来予約分） ② ToDo ③ 掲示板（過去何年分・添付含むか） ④ ファイル管理（規程関連ファイル：容量・件数） ⑤ ワークフロー（定義／過去申請履歴） ⑥ 設備予約 ⑦ アドレス帳	移行対象データの種類・件数・容量により、移行方式（ツールによる自動移行／手作業／移行対象外）及び工数が大きく変わるため。	同上。
297	要件定義書	3.2.-1	・現行システムで利用しているデータ及び設定情報について、本システムへの移行又は継承を行うこと。 具体的には、以下を含むものとする。 ① 現行ファイルサーバのデータ移行 ② 現行グループウェアサーバのデータ移行 ③ Exchange Online、Microsoft 365、Active Directory、ADMS については、現行テナント、ライセンス、設定、データを継承すること	現行グループウェアサーバにおける移行は「1.11.-2」の範囲と認識しております。当該認識に相違ないか、ご教示願います。	移行対象範囲によって移行作業内容および見積金額が変動する可能性があるため。	同上。

298	要件定義書	3.2.-1	データ移行 ・現行システムで利用しているデータ及び設定情報について、本システムへの移行又は継承を行うこと。 具体的には、以下を含むものとする。 ① 現行ファイルサーバのデータ移行 ② 現行グループウェアサーバのデータ移行 ③ Exchange Online、Microsoft 365、Active Directory、ADMS については、現行テナント、ライセンス、設定、データを継承すること	「② 現行グループウェアサーバのデータ移行」の具体的なデータの内容をご教示いただけないでしょうか。 お知らせ・掲示板・施設・スケジュール など・・・	正確な仕様・要件を確認するため。 適正な費用見積のため。	同上。
299	要件定義書	3.2.-4	・現行システムで稼働しているサービスが引き続き使用できるように、移行作業を行うこと。なお、移行についての詳細な事項は、本会と受注者が協議するものとする。	項番が「2.2.-4」となっていますので、ご確認のうえ修正を願います。 また、現行システムで稼働中のサービスは継続利用を前提としているとの認識ですが、移行対象範囲は「3.2.-1」に記載のサービスのみとの認識で相違ないか、ご教示願います。	移行対象範囲が見積金額および提案内容に影響するため、公平性確保の観点から明確化が必要であるため。	ご指摘の通り修正しました。 移行対象範囲は「3.2.-1」に記載のサービスです。
300	要件定義書	3.4.-1	・教育訓練は2回実施すること。 ・実施期間は、各機器等の稼働開始前とすること。 ・教育訓練の内容を以下に示すが、詳細は本会と協議すること。 (1) 現行システムからの変更点を含む業務基盤システムの概要 (2) 業務基盤システムの基本操作 ① FATPC、仮想デスクトップ利用方法 ② グループウェア、ファイル共有の利用方法 ③ 電子メールシステムの利用方法 ④ 上記以外で説明が必要なこと	質問： ・教育訓練の2回は、役員および一般職員へ各2回(計4回)を想定されておりますでしょうか。 ・教育訓練は、システム稼働前のみであり、稼働後の実施は要件に含まれない認識でよろしいでしょうか	教育対象者ごとの実施回数及び実施時期を明確にし、講師体制、教材準備及び必要工数を正確に見積もるため。	教育訓練は、役職員に対しシステム稼働前に同様の内容を2回です。 本システムの利用者約635名を想定していますが、対面およびウェブ会議による配信は本会役職員約350名、それ以外は2回のいずれかを録画した内容を提供することとします。
301	要件定義書	3.4-1	役員及び一般職員に対する教育訓練 ・教育訓練は 2 回実施すること。	同様の内容を2回に分けて、実施するイメージであっておりますでしょうか。 対象者数をご教示いただけないでしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	同上。
302	要件定義書	3.4.-2 4.4.-11も同様	・教育訓練の内容を以下に示すが、詳細は本会と協議すること。 (1) 現行システムからの～(略) (2) 業務基盤システムの～(略) (4)業務基盤システム全般に～(略) (5)業務基盤システムにおける～(略)	項番の誤記と思われますが、（3）の記載が漏れている場合は、ご確認のうえ追記もしくは修正を願います。	抜け漏れのない要件確認のため。	ご指摘の通り修正しました。
303	要件定義書	3.4.-4	・2028年1月4日から2028年3月31日までの間、本システムの運用に関する内部定例会を、以下の要領で実施すること。 ① 本会及び仮想デスクトップ問い合わせ要員での内部定例会を週1回行うこと。 ② 本会役職員等からの問合せ、運用定着の進捗に関するレポートを週次で作成し、内部定例会で報告を行うこと。 ③ 運用上の課題管理、課題に関する解決策を提案すること。 ④ 対応中の障害に関する進捗を報告すること。 ・問い合わせ要員は、本システムに係る障害対応の1年以上の経験、又は本システムに係る障害対応の技術や知識を認定するベンダ公認の資格を有すること。	質問： ・問い合わせ要員は、本調達の構築に関わった要員も体制に入れるようにすることは可能でしょうか。 ・受託者へ直接問い合わせをするのは、貴会情報システム課の職員のみである理解でよいでしょうか。	問い合わせ要員の条件及び問い合わせ可能な利用者の範囲を明確にし、過剰な要員配置を避けて適切なサポート体制を設計するため。	ご理解のとおりです。
304	要件定義書	4	本章では、次期システムの安定的かつ継続的な運用を実現するため、保守体制、システム監視、セキュリティ監視、障害対応、脆弱性管理、サービスレベル（SLA）及び運用報告等に関する要件を示す。 なお、監視体制、障害対応手順、エスカレーションルール、報告内容その他の詳細については、本会と受注者が協議の上で確定するものとする。	意見： ・本調達の成否は、システム構築後の運用品質に大きく依存すると考えられるため、提案評価において運用体制、運用プロセス及び運用実績に関する評価観点を明確化いただくことをご検討願います。	システム稼働後の安定性と継続性を確保するため、提案段階で運用体制、プロセス及び実績を客観的に評価できるようにするため。	本調達の「総合評価基準及び加点付与基準」については、調達仕様書の別紙に記載しています。

305	要件定義書	4.1.-1	・機器等の保守対応時間帯について、以下に示す。なお、24時間365日のサービスレベルを提供できる場合は、加点として評価する。 ① サーバ ハードウェア 平日 9:00-17:00 オンサイト ソフトウェア 平日 9:00-17:00 オンサイト又はリモートサポート ② クライアント端末 ハードウェア 後出しセンタードバック ソフトウェア 平日 9:00-17:00 オンサイト又はリモートサポート ③ ストレージ 平日 9:00-17:00 オンサイト ④ バックアップ 平日 9:00-17:00 オンサイト ⑤ ネットワーク ネットワーク機器 平日 9:00-17:00 オンサイト	質問 ・ハードウェア、ソフトウェア保守の対応範囲をご教示いただけないでしょうか。 例： -貴会にて一次切り分けを行いハードウェア交換が必要と判断された場合のオンサイト対応 -ハードウェア一斉切り分けを含むハードウェア交換対応 -ソフトウェアにて発生したエラーに対する問合せ対応 -障害時のバックアップ復旧 -クライアント端末リカバリー対応 等	ハードウェア及びソフトウェア保守の責任分界と具体的な対応範囲を明確にし、必要な保守体制及び費用を正確に見積もるため。	要件定義書4.1.-2に、以下を追記しました。 「・受託者は、障害発生時において、本会から提供される障害情報を基に、受託者において原因究明及び復旧方法の検討を行い、必要に応じてオンサイト又はリモートにより対応すること。障害の一次切り分け、原因調査、復旧対応及び技術支援を実施すること。 ・ハードウェア障害が発生した場合は、受託者において障害箇所の特定及び交換部品の判断を行い、必要な部品交換作業を実施すること。 ・バックアップデータからの復旧が必要となった場合は、受託者はデータ復旧作業を行うこと。 ・クライアント端末に障害が発生した場合は、OS及び導入ソフトウェアの復旧支援並びに必要な技術支援を行うこと。 ・なお、業務アプリケーション固有の不具合修正やデータ入力誤り等、機器等の保守範囲を超える事項については対象外とする。」
306	要件定義書	4.1.-2	・機器等の障害及びトラブル発生時、その解決のために迅速に対応できる体制として、障害対応コール並びに技術サポートを一括で受け付けるサポート窓口（電話、FAX、電子メール）を提供すること。 ・機器等の障害発生時には、HW交換作業が必要と判断された時点から、4時間以内に保守員が到着できる体制を有すること	質問 ・上記のハードウェア対応時間を過ぎた場合は、4時間以内対応の対象外との認識でよろしいでしょうか	4時間以内対応が適用される時間帯を明確にし、保守員の待機体制及びサービスレベルを適切に設計するため。	要件定義書4.1.-2の記載を以下のとおり修正しました。 「オンサイト保守対象機器について、機器等の障害発生時には、HW交換作業が必要と判断された時点から、保守対応時間帯内において4営業時間以内に保守員が到着し、交換作業を開始できる体制を有すること。」
307	要件定義書	4.1.-2	・機器等の障害及びトラブル発生時、その解決のために迅速に対応できる体制として、障害対応コール並びに技術サポートを一括で受け付けるサポート窓口（電話、FAX、電子メール）を提供すること。 ・機器等の障害発生時には、HW交換作業が必要と判断された時点から、4時間以内に保守員が到着できる体制を有すること	意見： ・4.1.-1でクライアント端末はハードウェア後出しセンドバックが記載されております。本項目では、クライアント端末は対象外である旨を記載頂く事をご検討頂けますでしょうか。 ・FAXを対象外としていただくことは可能でしょうか。	クライアント端末のセンドバック保守との整合性を明確にするとともに、連絡内容の正確性及び迅速な受付・対応を確保できる連絡手段とするため。 FAXは番号の押し間違えによる誤送信や、文字のかすれによる読み間違いが起きる、受領場所が限定されることによる対応遅延のリスクがあるため。	同上。 また、要件定義書4.1-2を、以下のように修正しました。「機器等の障害及びトラブル発生時、その解決のために迅速に対応できる体制として、障害対応コール並びに技術サポートを一括で受け付けるサポート窓口（電話、電子メールその他受託者が提供する受付手段）を提供すること。」
308	要件定義書	4.1.-2	障害発生時の対応 ・機器等の障害及びトラブル発生時、その解決のために迅速に対応できる体制として、障害対応コール並びに技術サポートを一括で受け付けるサポート窓口（電話、FAX、電子メール）を提供すること。	電話および電子メールによる受付を必須要件とし、FAXは削除していただけないでしょうか。	FAX受付については運用上の利用が限定的であり、提供にあたり追加コストが発生するため。	同上。
309	要件定義書	4.1.-4	その他保守要件 ・賃貸借期間内に無停電電源装置のバッテリーの交換の必要が生じた場合、サービスを停止させることなく当該バッテリーの交換を行うこと。	本項目にしか無停電装置の記述がないため、前段の機能要件に記載いただけないでしょうか。	正確な仕様・要件を確認するため。 適正な費用見積のため。	要件定義書1.2.-4、1.2.-10、1.8.-7に、それぞれ、以下の記載を追加しました。 「停電及び瞬時電圧低下によるサービス停止を防止するため、無停電電源装置（UPS）を介して給電すること。なお、管理・外部接続SWへの給電と共通であることも可とする。」 「停電及び瞬時電圧低下によるサービス停止を防止するため、無停電電源装置（UPS）を介して給電すること。」 「無停電電源装置（UPS）を設置し、商用電源断時に安全な自動シャットダウンが実施できる構成とすること。」

310	要件定義書	4.3.-2	「統括管理・設計構築・移行担当の要員要件として「過去5年以内において、仮想サーバ20台以上、FAT端末400台以上のシステムのプロジェクトマネジメント（又は設計・構築）実施経験」が必須とされている。」	本調達がクラウドサービス主体の構成であることを踏まえ、オンプレミス台数（仮想サーバ20台、FAT端末400台）を基準とした実績要件について、同等規模のクラウド中心プロジェクトの実施経験としていただけますでしょうか。	クラウド前提の調達において、オンプレミス台数基準の実績要件では要員の遂行能力を十分に評価できない恐れがあります。 また、本業務を遂行可能な事業者の参入機会を確保しつつ、適切な競争環境の維持が期待できるため。	要件定義書4.3.-2の記載を以下のとおり修正しました。 「・統括管理を担当する要員は、過去5年以内において、仮想サーバ20台以上、FAT端末300台以上のシステム又はこれと同等規模のクラウドサービスを活用したシステムのプロジェクトマネジメント経験を有すること。 ・設計・構築担当及び移行担当のうち、各分野の主任担当者は、5年以上の実務経験を有し、過去5年以内において、仮想サーバ20台以上、FAT端末300台以上のシステム又はこれと同等規模のクラウドサービスを活用したシステムの設計・構築又は移行を実施した経験を有すること。」
311	要件定義書	4.3.-2	要員に必要な要件 ・設計・構築担当、及び移行担当する要員は、各機器等の設計・構築担当者として5年以上の経験を有し、過去5年以内において、仮想サーバ20台以上、FAT端末400台以上のシステムの設計・構築を実施した経験を有していること。	全ての設計・構築担当者および移行担当者に適用するには条件が厳しく、要員確保が困難となる可能性があります。 そのため、本要件は削除をご検討いただけますでしょうか。	体制確保が困難となり、要員が限定されることでコスト増加につながるため。	同上。
312	要件定義書	4.4.-11	・監視状況、アラート発生状況、ログ分析結果及びセキュリティイベントをリアルタイムに確認できるポータルを提供すること。 ・当該ポータルは、多要素認証等により適切に保護されていること。 ・監視結果を月次報告書として取りまとめ、翌月の指定日までに提出すること。報告書には、少なくとも以下の内容を含むこと。 ① 監視イベントの集計及び分析結果 ② セキュリティインシデント及び対応状況 ③ システム構成及びセキュリティ設定の評価結果 ④ 改善提案及び今後の対応事項 ・誤検知及び過検知を低減するため、継続的なチューニングを実施すること。 ・リアルタイムに監視状況やログ分析結果、不正アクセス状況等を確認できる専用のGUI（ポータル画面等）を提供すること。 ・当該ポータルは、適切なアクセス制御（多要素認証、ID／パスワード等）により保護されていること。 ・監視結果を月次レポートとして取りまとめ、翌月指定日までに提出すること。レポートには以下の内容を含むこと。 ① 監視イベントの集計及び分析 ② 不正アクセス・脅威の検知状況と対応結果 ③ システム設定やセキュリティポリシーの妥当性評価及び改善提案 ・運用の過程で誤検知（過検知）が発生する場合、適切なポリシーチューニング（ホワイトリスト登録等）を継続的に実施すること。	質問： ・こちらは貴会のシステム管理者向けに提供するものであり、一般的な監視の画面と考えてよろしいでしょうか。	監視結果を表示するポータルの利用者、機能及びレポート範囲を明確にし、必要なサービス構成と運用工数を正確に見積もるため。	ご理解のとおりです。
313	要件定義書	4.4.-13	高危険度のインシデントを検知した場合は、電子メールに加え電話等により24時間365日即時に通知すること。	高危険度インシデントの判定基準を確認したいため、現行システムにおいて高危険度と判断している事象の例および判定基準をご教示願います。	高危険度インシデントの判定基準により、24時間365日即時通知の対象範囲が異なるため、現行システムにおける判定基準を確認したいため。	要件定義書4.4.-13の記載を以下のように修正しました。 「高危険度のインシデントを検知した場合（受託者が重大な影響を及ぼす、又は及ぼすおそれがあると判断した場合を含む。）は、電子メールに加え電話等により24時間365日即時に通知すること。」 なお、高危険度インシデントについて、一律の定量基準は定めていません。 受託者において、発生した事象の内容、影響範囲、サービス継続への影響、情報セキュリティ上のリスク等を総合的に勘案し、重大な影響がある又はそのおそれがあると判断した事象については、高危険度インシデントとして速やかに通知してください。 なお、高危険度インシデントには、セキュリティインシデントに限らず、情報漏洩、システム停止、重要機器故障、冗長構成の喪失その他業務運営に重大な影響を及ぼす事象を含みます。

314	要件定義書	4.4.-2	・システムを構成する機器及びサービスについて、24時間365日の監視体制を提供すること。 ・障害又は異常を検知した場合は、速やかに本会へ通知するとともに、一次切り分けを実施すること。 ・障害の状況に応じて適切なエスカレーションを実施すること。	質問： ・監視の検知、通報(貴会へのメール通知) までという対応でも許容可能でしょうか。 障害の重大度を設計にて定義し、重大な障害については、連絡体制を用意し、オンコールによる夜間・休日対応する形でよいでしょうか。	障害の重大度に応じた合理的な監視・通知体制を設計し、全時間帯の有人対応による過剰な運用コストを回避するため。	要件定義書4.4.-2の記載を以下のように修正しました。「障害又は異常を検知した場合は、原因の一次切り分け（発生箇所、影響範囲、障害種別等の確認）を実施した上で、本会への通知及び必要なエスカレーションを行うこと。」 なお、監視業務は単なる検知及び通知に留まらず、障害又は異常を検知した場合は一次切り分けを実施した上で、必要に応じて適切なエスカレーションを行うことを想定しています。 ただし、障害の重大度に応じてオンコール体制等により対応することは妨げません。
315	要件定義書	4.4.-8	・監視状況をリアルタイムに確認できるポータル又はダッシュボードを提供すること。 ・月次報告書を作成し、翌月指定日までに提出すること。 報告書には少なくとも以下を含むこと。 ① 障害発生状況及び対応結果 ② リソース利用状況 ③ バックアップ及びジョブ実行状況 ④ システム性能の分析結果 ⑤ 改善提案	質問： ・こちらは貴会のシステム管理者向けに提供するものであり、一般的な監視の画面と考えてよろしいでしょうか。	提供する可視化画面の利用者、機能及び表示範囲を明確にし、必要な監視機能と構築工数を正確に見積もるため。	ご理解のとおりです。
316	要件定義書	4.4.-9	不正アクセス・脅威監視（セキュリティ監視） ・SIEM、XDR 等を活用し、各種ログ及びイベントを統合的に分析できること。	以下の内容に変更頂く事を提案します。 ----- SIEM、XDR 等を活用し、セキュリティ監視に必要なログ及びイベントを統合的に分析できること。	取得対象となるログ及びイベントを明確化するため。 すべてのログ及びイベントを収集・分析する場合は、専用SIEM基盤の追加導入や運用コストの増加が見込まれるため。	要件定義書4.4.-9に記載されている事項は、区分欄に示すように、「セキュリティ監視」に必要なログ・イベントを対象としています。
317	要件定義書	4.4.-9	不正アクセス・脅威監視（セキュリティ監視） ・エンドポイント（EDR 等）、ネットワーク、メール、クラウドワークロード等、複数のセキュリティレイヤを横断した脅威監視（XDR や SIEM 等による監視）を行えること。	上段に同様の文章があるため統合いただきたい。 「・エンドポイント、ネットワーク、メール、クラウドサービス等の複数のセキュリティレイヤを横断して脅威監視を実施できること。」	集約して記載いただいた方が仕様を理解しやすいため。	ご指摘のとおり修正しました。
318	要件定義書	4.4.-9	不正アクセス・脅威監視（セキュリティ監視） ・不正アクセス、マルウェア感染、異常通信等を検知し、攻撃の全体像やタイムラインを可視化できること。	上段に同様の文章があるため統合いただきたい。 「・攻撃の全体像、侵入経路、影響範囲及びタイムラインを可視化できること。」	集約して記載いただいた方が仕様を理解しやすいため。	ご指摘のとおり修正しました。
319	要件定義書	4.4.-9	不正アクセス・脅威監視（セキュリティ監視） ・セキュリティインシデント発生時には、以下を実施・支援すること。 ① 初動対応（通知・一次切り分け、ネットワーク隔離時の一時対処） ② 攻撃手法・原因の分析及び影響範囲の特定 ③ 残存脅威の根絶支援 ④ 再発防止策の提示及び適切な助言	上段に同様の文章があるため統合いただきたい。 「セキュリティインシデント発生時には、以下を実施又は支援すること。 ① 初動対応（通知、一次切り分け及び応急措置） ② 原因分析及び影響範囲の特定 ③ 残存脅威の調査及び排除支援 ④ 復旧支援及び再発防止策の提案」	集約して記載いただいた方が仕様を理解しやすいため。	ご指摘のとおり修正しました。
320	要件定義書	4.5.-1	受注者は、本システムに導入するEDR、SSE、ZTNA、CASB、メールセキュリティ、SIEM、SOARその他のセキュリティ機能から出力されるログ及びイベント情報を活用し、サイバー攻撃、不正アクセス及び情報漏えい等の脅威を早期に検知するためのセキュリティ監視を実施すること。 ・セキュリティ監視業務は、日本国内に設置されたSOC又は同等の体制により実施すること。 ・監視業務に従事する要員は、十分な知識及び経験を有すること。	提案： ・セキュリティ監視運用の有効性を確保するため、自社又はグループ会社においてSOCを保有し、24時間365日のセキュリティ監視サービスを運営している実績についても評価項目としていただくことをご検討願います。	継続的かつ実効性のあるセキュリティ監視を確保するため、SOCの運営体制及び24時間365日の監視サービスに関する実績を客観的に評価できるようにするため。	原案どおりとします。

321	要件定義書	4.5.-1 4.5.-2	・セキュリティ監視業務は、日本国内に設置されたSOC又は同等の体制により実施すること。 ・24時間365日のセキュリティ監視体制を提供すること。 ・高危険度又は重大なセキュリティイベントを検知した場合は、速やかに本会へ通知すること。 ・緊急性が高い場合は、電子メールに加え電話等による即時連絡を行うこと。	意見： ・SOC又は同等の体制による監視及び24時間365日のセキュリティ監視を一律の必須要件とする記載について、削除をご検討願います。 なお、対象システムの重要度及び想定されるセキュリティリスクに応じ、監視時間帯、検知対象、通知方法及び緊急時の連絡体制を協議の上で定める要件とすることをご提案します。	SOC及び24時間365日の常時監視を必須とした場合、専任要員や監視サービスの確保が必要となり、運用費用が大幅に増加する可能性があります。一方、本システムの重要度、取扱情報、想定脅威及び既存のセキュリティ対策を踏まえると、一律の常時監視は過剰要件となる可能性があります。要件をリスクベースの監視・通知体制へ見直すことで、必要なセキュリティ水準を確保しつつ、過度な費用負担を回避し、競争性及び経済合理性を確保するため。	要件定義書4.5.-2の記載を以下のとおり修正しました。 「24時間365日セキュリティイベントを検知可能な体制を提供すること。」 なお、本要件は、SOC要員による24時間365日常時有人監視を必須とするものではなく、24時間365日のセキュリティイベントの検知及び重大イベント発生時の通知体制を求めるものです。したがって、24時間365日の監視要件については変更を予定していません。なお、重大インシデント発生時の詳細分析及び復旧支援については、4.4.-13に定めるSOC又はCSIRT等の専門要員による対応を求めています。
322	要件定義書	4.6.-4	・攻撃手法、不正挙動及び侵入経路を分析できること。 ・感染経路、通信先及び影響を受けたシステム又は利用者を特定できること。 ・影響範囲及び被害状況を調査し、本会へ報告すること。 ・必要に応じてログ分析その他の調査を実施できること。	質問： ・原因分析及び影響調査の対象として、アラートが発生したEDRに関する範囲のみやEDRで分析可能な範囲のみなど対象範囲を制限いただけないでしょうか。	原因分析及び影響調査の対象が無制限では過剰な役務となる可能性があるため、EDRで検知・分析可能な範囲に限定し、責任範囲を明確にするため。	要件定義書4.6.-4の記載を以下のとおり修正しました。 「・受託者が監視対象とするEDR、SIEMその他のセキュリティ関連ログを用いて、攻撃手法、不正挙動並びに侵入・感染経路、通信先及び影響を受けたシステム又は利用者を分析すること。 ・上記の分析に基づき、影響範囲及び被害状況を調査し、本会へ報告すること。 ・必要に応じてログ分析その他の調査を実施すること。」
323	要件定義書	4.5.-6	・SOAR等を活用し、通知、チケット起票、情報収集その他の対応を自動化又は半自動化できること。 ・事前に本会と合意したプレイブックに基づき、自動対応又は半自動対応を実施できること。	質問： ・自動対応又は半自動対応の実施に係る実現方法について、SOC環境にログを取り込みSOCに構築した独自の自動化技術で分析を自動化する形を想定しております。このような実現方法が確認いただけないでしょうか。	実現方式と責任範囲を明確にするため。	ご理解のとおりです。 なお、提案に当たっては、自動化の対象範囲、実施内容及び運用方法を明確に示してください。
324	要件定義書	4.6.-7	・重大インシデント発生時には、必要に応じてフォレンジック調査を支援できること。 ・調査に必要なログ及び証拠を保全できること。 ・調査結果を報告書として取りまとめること。	提案： ・フォレンジック調査支援は一般的なSOCの役務外なので、対象外とすることをご検討いただけないでしょうか。	フォレンジック支援は一般的なSOC役務の範囲を超える専門業務であり、過剰な要件であると推察されるため。	要件定義書4.6.-7の記載を以下のとおり修正しました。 「・重大インシデント発生時には、本会又は本会が指定する調査機関による原因調査及びフォレンジック調査に協力し、必要なログ、証拠及び関連情報を提供できること。 ・調査に必要なログ、設定情報その他の証拠を保全できること。 ・対応経緯及び調査結果を報告書として取りまとめること。」