「令和９年度基幹 LAN システム契約 仕様書」へのご意見に対する回答

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
1	P3	ア. 認証基盤の適正化及び棚卸し	現行 Active Directory から Microsoft EntraID へ移行	移行対象外の現行環境において、Active Directory に依存するシステムが存在する場合、移行後に当該システムへ影響が生じる可能性があります。移行対象外のシステムについては、お客様側にてご対応いただく旨を仕様書等に明記していただくようご検討ください。	現時点において、現行 Active Directory に依存し、Microsoft Entra ID への移行対象外として継続利用する業務システムは想定していません。なお、移行作業の過程で現行 Active Directory との連携又は依存関係が確認された場合は、受注者から機構へ報告の上、対応方針について機構と協議するものとし、その旨が明確となるよう仕様書を修正します。
2	P3	オ. 現行の通信サービス提供事業者、LAN 事業者及びサーバー保守業者との調整 P.3 カ. 現行の通信サービス、LAN サーバーに対する作業	「受注者がその費用を負担すること」	現行の仕様書の記載内容では、詳細な要件を想定することが困難であり、適正な費用積算が難しい状況と考えます。つきましては、記載内容をより具体化していただくか、現時点で要件の明確化が難しい場合には、当該記載の削除をご検討ください。	ご意見を踏まえ、費用負担の範囲が明確となるよう仕様書を修正します。 現行の通信サービス提供事業者、LAN 事業者及びサーバー保守業者との調整及び連携に係る受注者自身の作業費用は、本業務に含むものとします。なお、現行事業者側で別途費用が発生する場合の取扱いについては、当該費用の発生原因、作業内容及び責任分界を踏まえ、機構と受注者で協議の上決定するものとします。
3	P25	イ. PC・プリンタに関する保守サービス	・ 紛失・盗難時の緊急対応端末の紛失又は盗難が発生した場合、受注者は「（３）ヘルプデスクサービス」の対応時間外（夜間・休日・年末年始等を含む）であっても、２４時間３６	24 時間 365 日体制で緊急連絡を受け付け、リモートワイプ又はリモートロックを実行する体制を構築することを実施するためには、24 時間 365 日体制で有人での対応体制を敷くことが必要となり、リソース状況等より対応が難しいことが想定されすため、平日 9 時から 17 時まで等への仕様の緩和をご検討く	端末の紛失又は盗難については、発生時点で情報漏えい等のリスクが生じ得ることから、夜間、休日及び年末年始等を含め、必要に応じてリモートワイプ又はリモートロックを実施できる体制が必要であると考えています。 このため、平日業務時間内に限定することは

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			５日体制で緊急連絡を受け付け、直ちにMicrosoft Intune を用いたリモートワイプ又はリモートロックを実行する体制を構築すること。	ださい。	適当ではないと考え、本要件については原案のとおりとします。
4	P40	２．３．２ 標準インストールソフト ２．３．３ 個別インストールソフト	（年間ライセンスのものについてはリース満了まで購入すること）	契約期間中に製品やサービスの価格改定が生じた場合、当初の契約金額では履行が困難となる可能性があります。つきましては、価格改定が生じた際には、変更契約により契約金額を見直すことができる旨を仕様書等に明記していただくようご検討ください。	価格改定が生じた場合の取扱いについて、個別の仕様項目として記載することは想定していません。 契約締結後に契約内容の変更が必要となる場合は、契約書の定めに基づき、必要に応じて協議の上対応することとなります。このため、本項目については原案のとおりとします。
5	P47	（５） クラウドサービス	利用するクラウドサービスは、ISMAP 管理基準の管理策基準が求める対策と同等以上の水準を満たすこと。	ISMAP サービスリストへ登録されていることを要求されていることは理解しておりますが、幅広くかつ安価なサービスを提案する余地がなくなるため、仕様緩和をご検討ください。	クラウドサービスの利用にあたっては、政府機関等のサイバーセキュリティ対策のための統一基準群及び ISMAP の原則利用の考え方を踏まえる必要があります。 本要件は、ISMAP 管理基準の管理策基準が求める対策と同等以上の水準を確保するためのものであることから、原案のとおりとします。
6	P3	仕様書/第 2 章/(4)/ア		Active Directory から Entra ID への移行対象となるユーザー数、サービスアカウント数、グループ数、GPO 数を仕様書内に記載いただくことは可能でしょうか。 もしくは、公示時には資料閲覧にて上記数量を確認可能な状況にしていただけますでし	現行Active Directoryから Microsoft Entra ID への移行対象となるユーザー数、サービスアカウント数、グループ数及び GPO 数等については、公示時の資料閲覧において、移行規模を把握するための概況資料として確認可能とすることを想定しています。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				ょうか。	なお、当該数量は概数であり、移行作業における棚卸し、整理及び設計内容により変動する可能性があるため、仕様書本文への個別数量の記載は行わないこととします。
7	P3	仕様書/第 2 章/(4)/イ	特権 ID	ここで指す記載とは、グローバル管理者などの Microsoft Entra ロールを示しているという理解で相違ございませんでしょうか。	特権 ID は、Microsoft Entra ID のロールに限るものではなく、本業務で導入又は運用するシステム、サービス、機器等における管理者権限又はこれに準ずる権限を付与された ID を想定しています。 ご意見を踏まえ、特権 ID の範囲が明確となるよう仕様書を修正します。
8	P3	仕様書/第 2 章/(4)/イ	>特に核心的な強い権限（アカウント管理者、権 限管理者等）は常時付与せず	上記記載いただいておりますが、こちらは原則ルールとして取り扱い、一部例外的にグローバル管理者を常時付与するアカウントを設ける形を許容いただけませんでしょうか。 承認者の不在などロールのアクティブ化ができない状況など、誤って Entra 組織からロックアウトされないようにするため、組織内に緊急アクセスアカウントを作成することが Microsoft より推奨されておりますため、となります。	特権 ID については、業務上必要な場合に限定し、必要最小限の権限を付与することを原則とします。 ただし、システム、サービス又は機器の仕様等により一部の措置を適用することが困難な場合は、機構と受注者で協議の上、取扱いを決定することとします。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
9	P3	仕様書/第 2 章/(4)/イ	>管理者権限を行使できる端末を、システム管理者等の専用端末に限定すること。	上記記載について、グローバル管理者等、任意の Entra ロールを付与されたアカウントは、特定の PC からのみ Entra 管理センターなどの管理ポータル（権限を行使する場）へのアクセスを実施できないように制御を実現されたいというご要件の理解で相違ない	管理者権限を行使できる端末については、システム管理者等の専用端末に限定することを原則として想定しています。 ただし、システム、サービス又は機器の仕様等により一部の措置を適用することが困難な場合は、機構と受注者で協議の上、取扱い

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				でしょうか。	を決定することとします。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
10	P3	仕様書/第 2 章/(4)/ウ	>現行サーバー（SKYSEA Client View）で行っている資産管理、パッチ適用管理、USB デバイス制御等の機能を Microsoft Intune へ移行すること。移行にあたっては、既存の制御ポリシーを精査し、Microsoft Intune 上で同等のセキュリティレベルを確保すること。	上記記載の「既存の制御ポリシー」という記載については、ポリシー一覧で提供いただく想定の意味にも捉えられます。そのため、まずは受注者にて現状調査をしたうえでの実装する形への代替案への修正を推奨いたします。	ご意見を踏まえ、仕様書を修正します。
11	P7	仕様書/第 3 章/(3)/ウ	>· 本仕様に定めるパケットフィルタリング、NAT、通信ログ取得、アプリケーション単位のポリシー制御、アンチウイルス、アンチスパイウェア、IPS、サンドボックス等の各機能については、当該機能の設定及び運用により検知または検出された通信状況、セキュリティイベント、脅威情報等を整理し、定期的に発注者へ報告すること。 ·当該報告内容や運用状況を踏まえ、不正通信、マルウェア感染、情報漏洩その他のセキュリティインシデントの被害予防及	上記記載ございますが、貴機構としては SOC（Security Operation Center）に相当する監視・分析運用を想定されておりますでしょうか。また、本要件は次世代ファイアウォールの運用管理要件内に記載されておりますが、対象範囲は当該機器で取得するログ及びイベントに限定される認識でよろしいでしょうか。SIEM 等を活用した横断的な監視・分析を想定している場合は、対象範囲をご教示ください。	本項は、次世代ファイアウォールの運用管理に関する要件であり、報告及び運用の対象範囲は、次世代ファイアウォールにより取得又は検知されるログ、イベント及び脅威情報等を基本とします。 複数システムを横断した監視・分析の取扱いについては、別途本仕様書に定めるログ管理、エンドポイントセキュリティ及び保守報告等の各要件に基づくものとします。 このため、本項目については原案のとおりとします。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			び被害拡大防止の観点から、受注者は、必要に応じて機構と協議のうえ、ポリシー設定の見直し、ルールの追加・変更、検知条件の最適化等を 行い、対策の実効性向上及びセキュリティ水準の継続的な強化を図ること。		
12	P9	仕様書/第 3 章/(7)	>本業務にて導入する Microsoft365 Business Premium のライセンス機能を最大限に活用し、庁舎内に物理的な管理サーバーを配置しない構成を基本とする。	上記記載ございますが、正確には「Microsoft365 Business Premium」＋「Microsoft 365 セキュリティ・コンプライアンスアドオン」となるため記載修正を推奨いたします	ご意見を踏まえ、仕様書を修正します。
13	P10	仕様書/第 3 章/（7）/イ	>検知した端末の脅威情報に基づき、安全性が確保できない端末からの内部ネットワークやクラウドサービスへのアクセスを制限できる仕組みを検討・構築すること。	上記記載においてアクセス制御の対象とする端末は、Microsoft Defender for Endpoint および Intune により管理されている端末を想定されていますでしょうか。管理対象外端末やネットワーク機器等も制御対象とする場合は、追加製品の検討が必要となるため、想定される対象範囲をご教示ください。	本要件におけるアクセス制御の対象は、本業務にて調達し、機構の管理基盤により管理する端末を想定しています。
14	P10	仕様書/第 3 章/（7）/ウ	>重大な脅威を検知した場合、インシデント検知から 30 分以内に機構が指定する連絡先へ通報を行うこと。	上記記載で、30 分以内通報とございますが、本運用は 24 時間 365 日対応を想定されておりますでしょうか。また、一次対処とは具体的にどこまでの対応（隔離、調査、駆除等）を期待されていますか。	本要件は、24 時間 365 日の対応を想定しています。 一次対処については、被害拡大防止を目的とした初動措置を想定しており、対象端末の隔離、通信遮断、検知対象のブロック、脅威の削除又は駆除等、製品機能及び運用上実施可

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
					能な対応を含みます。 一方、原因の詳細分析、侵入経路の特定、周辺機器等のログを含めた詳細調査、恒久対策、再発防止策の検討、復旧支援及び報告書作成については、本項に定める監視、通報及び一次対処の範囲には含まないものとし、必要が生じた場合は、機構と受注者で別途協議の上、対応の要否、範囲、方法及び費用負担等を決定するものとします。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
15	P10	仕様書/第 3 章/(8)	>リモートアクセス設定、ブラウザ設定、セキュリティ設定等の端末構成をポリシーとして定義し、全端末へ一括適用できること。	上記記載ございますが、「リモートアクセス」はリモートアシスタンス(リモートヘルプ)機能を指しておりますでしょうか。その場合、調達されるライセンス(Intune P1)の範囲内での実現が難しいため、要件緩和もしくはライセンス追加の要件見直しいただけますでしょうか。	本項における「リモートアクセス設定」は、リモートアシスタンス又はリモートヘルプ機能を指すものではなく、VPN 接続等に係る端末側の接続設定を想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう、VPN クライアント設定、条件付きアクセスに必要となる端末設定、ブラウザ設定、セキュリティ設定等の端末構成をポリシーとして定義し、本業務における管理対象端末へ一括適用できる旨に仕様書を修正します。
16	P12	仕様書/第 3 章/(10)	＞機構が DNS レコードの参照・編集を行えるように、機構専用のウェブページを提供すること。また、これらの変更は、DNS サーバーにおいて速やかに反映されること。また、その際の通信	上記にて「機構専用のウェブページ」と記載ございますが、ID・パスワード等による認証後に利用可能となる管理画面（コントロールパネル等）を提供する構成であれば、本要件を満たすものとしてよろしいでしょうか。	ご認識のとおり、認証後に利用可能となる管理画面又はコントロールパネル等により、機構が DNS レコードの参照及び編集を行える構成であれば、本要件を満たすものとします。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			は TLS にて暗号化すること。		
17	P12	仕様書/第 3 章/(10)	>上記ウェブページへのアクセス管理は、個人を特定可能な個別の ID にて行い、多要素認証等による適切な認証を行うこと。また、設定の参照、追加、変更、削除等の操作記録を適切に記録し、機構の求めに応じて提出できること	上記にて多要素認証の要件がございますが、ワンタイムパスワードアプリ等で要件を満たすものとしてよろしいでしょうか。	本要件では、政府統一基準群等における考え方を踏まえ、多要素認証方式による適切な認証を想定しています。 ID・パスワード等による認証に加え、認証アプリ等を用いた別要素による認証を行うことにより、2 つ以上の異なる認証方式を組み合わせる構成であれば、本要件を満たすものとします。
18	P12, 13	仕様書/第 3 章/(11)/ア 仕様書/第 3 章/(11)/イ	> IPv6 によるアクセスが可能であること。(IPv4 による場合は契約後において機構から IPv6 への変更を指示することがあるので無償で更新に応じる こと) >SQL インジェクションやクロスサイトスクリプティング等の攻撃を防御する機能を備えること。	上記記載ございますが、資料閲覧を踏まえて IIJ 様のサービスを利用されていると認識しています。 現在のサービス仕様では、上記の 2 つを満たすことが難しいため要件緩和をご検討いただけますでしょうか。「SQL インジェクションやクロスサイトスクリプティング等の攻撃を防御する機能を備えること。」 →WAF オプションにて対応可能です。 ただし、WAF オプションをご利用の場合は、IPv4 のみの対応となりますので、IPv4 への要件緩和をご検討いただければと考えております。	ご意見を踏まえ、IPv6 によるアクセスを必須とする記載は削除します。 Web サーバーについては、インターネットから HTTPS によるアクセスが可能であることを要件とし、SQL インジェクション、クロスサイトスクリプティング等の Web アプリケーションに対する代表的な攻撃を防御する機能を備えることを求める記載に修正します。
19	P14	仕様書/第 4 章/(1) /ア	>ア. パーソナルコンピュータ及び周辺機器 ・モバイルノート型 PC：125 台（予備在庫含む） ・省スペースデスクトップ型 PC：13 台（予備在	上記記載ございますが、運用期間中に予備在庫が不足した場合の補充方法や対応方針について、ご教示いただけますでしょうか。	運用期間中に、予備在庫が不足し、仕様書に記載の台数を超えて追加調達が必要となる場合は、変更契約の手続により対応することを想定しています。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			庫含む)		
20	P14	仕様書/第 4 章/(1) /ア	>ネットワークプリンタ:14 台以上	上記記載ございますが、想定される調達台数を明記いただく、もしくは 14 台を基本台数とし、追加で必要となる場合は別途調達または契約変更にて対応する旨をご記載いただくことをご検討いただけますでしょうか。	ご意見を踏まえ「14 台」に記載を修正いたします。
21	P14	仕様書/第 3 章/(11)/ウ	>設定変更、コンテンツ更新及び管理者ログインの操作ログを適切に記録し、1 年間以上保管すること。	上記記載ですと、保管対象となるログの範囲について各ベンダー間で解釈の余地があるかと存じますので、管理者操作・設定変更・管理者ログイン等のセキュリティ関連操作ログに限定する記載にするべきではないかと考えます。	本項は、設定変更、コンテンツ更新及び管理者ログイン等、管理者操作に係る操作ログについて、1 年間以上の保管を求める趣旨です。 一方、一般利用者のアクセスログについては、1 年間以上の保管を必須とするものではありませんが、障害調査、不審アクセス確認その他運用上必要な調査に利用できるよう、サービス又はシステムの標準機能により、90 日程度確認又は取得できることを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
22	P15,P16	仕様書/第 4 章/(7)/イ	>Microsoft Edge 等のブラウザにおけるお気に入り、パスワード等の設定を新PCに引き継ぐ手順	上記記載について、ブラウザ設定の同期における対象ブラウザは、組織の Microsoft アカウントのプロファイルに紐づいた Microsoft Edge のみかと思われましたが、後述章にて「googlechrome」のインストールも記載がございましたので、対象ブラウザを明示すべきと考えておりますが、いかがでしょうか。	Microsoft Edge を標準ブラウザとして想定していますが、現行端末において Google Chrome を利用している職員もいるため、Google Chrome についても利用実態を踏まえ、必要に応じて移行対象とすることを想定しています。 ただし、Google Chrome については、Google アカウントによる同期を前提とするものではなく、取得・移行可能な範囲及び方法につ
23	P15,P16	仕様書/第 4 章/(7)/イ	>Microsoft Edge 等のブラウザにおけるお気に入り、パスワー	上記記載について、ブラウザ設定の同期におけるご要件として「お気に入り、パスワード	

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			ド等の設定を新PCに引き継ぐ手順	等の設定」と記載いただいておりますが、移行対象とするデータはMicrosoft Edge標準同期機能で取得可能な範囲とする記載に修正すべきと考えております	いて、機構と受注者で協議の上決定することとします。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
24	P16	仕様書/第4章/(13)/イ	>ＬＡＮケーブルは原則として既存のものを流用するものとする。	上記をはじめとしたファシリティ部分の要件に関しては、事前調査、下見が必須と思われます。そのため、公示には資料閲覧の他、建屋の現地調査を許容する記載を推奨いたします。	ご意見を踏まえ、LANケーブルその他ファシリティ部分の確認に必要となる資料閲覧及び現地確認の取扱いについては、公示において示すこととします。
25	P17	仕様書/第4章/(13)/ウ	>床下でのケーブルの絡まりを整理し、マジックテープ等を用いて適切に結束することで、保守性を向上させること。	上記記載の範囲について、ケーブルの捕縛は見える範囲のケーブルに対して実施する認識でよろしいでしょうか。	本項は、ハブ周辺及び各接続ケーブルの両端へのラベル貼付により接続先を識別しやすくするとともに、床下の確認可能な範囲において、ケーブルの絡まり、たるみ、交差等を整理し、保守性を向上させる趣旨です。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
26	P17	仕様書/第4章/(13)/エ	>更新された床下配線図及び、新しいハブの各ポートと端末（又は情報コンセント）との対応関係を示すポート収容図を電子データにて提出すること。	上記記載で指すものは、配線図に記載されるポート番号に対応するケーブル番号記載の接続表の認識でよろしいでしょうか。	ご認識のとおり、配線図に記載されるハブ等のポート番号と、これに対応するケーブル番号、端末又は情報コンセント等との接続関係を示す表を想定しています。
27	P17,P18	仕様書/第5章/(1)	>さらに、本番環境への設定反映やポリシー変更、OSアップデート等の手順確認及び事前検証を安全に行うため、受注者は本番環境の運用に影響を与えない検証環境を構築・整備すること	上記記載ございますが、当該検証環境は、現行環境においても本番環境とは別に整備されているものとの理解でよろしいでしょうか。(OSアップデート等については、初期設定に限らず、継続して運用期間中も事前検証を実施されていると読み取れるため)	現行環境において、本番環境とは別の検証環境は整備されていません。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				またその場合、現行受託者にて既に検証環境が整備されている場合には、新たに検証環境を構築する方式に限定せず、既存の検証環境を引き継いで利用する方式や、グループを分けて構築する方式についても許容いただけるかご教示ください。	
28	P18	仕様書/第 5 章/(2)/ア	>また、多要素認証（MFA）及びデバイスの準拠（Microsoft Intune 連携）を組み合わせたアクセス制御を実装すること。	上記記載について、多要素認証(MFA) のアクセス制御をご要件のとして記載いただいておりますが、MFA のアクセス制御の対象とするユーザー130 名様分は全て、スマートフォンが支給されているご状況の理解で宜しいでしょうか。	MFA のアクセス制御については、予定ユーザー数 130 名を対象として実装することを想定しています。 職員向けスマートフォンの利用に限定するものではなく、具体的な認証方式については、対象ユーザーの利用環境、端末配備状況、認証方式の安全性及び運用方法を踏まえ、機構と受注者で協議の上決定するものとします。
29	P18	仕様書/第 5 章/(2)/イ	>受注者は人事異動に伴うユーザー数の変動に対応するため、ユーザー1 人あたりの単価を算出すること。	上記記載いただいておりますが、こちらは、ユーザー１人が追加された際にMicrosoft のライセンス費用を算出するというご要望の理解で相違ないでしょうか	ご認識のとおりです。
30	P18	仕様書/第 3 章/(9)/ア 仕様書/第 5 章/（１）/ウ	>特定のウェブサイトやクラウドサービス(生成AI サービスを含む)に対し、機密情報の貼り付け、書き込み、ファイルのアップロードを制限できる機能を有すること。 >組織的なＡＩ活用を安全に実現するため、上記イ.で調達する	上記記載ございますが、DLP の制御はCopilot およびWeb サイトのみの認識で問題ないかご教示ください。	ご意見を踏まえ、Microsoft Purview 等を活用した情報保護及び AI 利用時の安全対策について、対象範囲及び実装内容が明確となるよう仕様書を修正します。 DLP（データ損失防止）による制御については、Microsoft 365 Copilot の利用並びにWeb ブラウザを介した特定の Web サイト又はクラウドサービスへの機密情報の貼り付け、書

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			アドオンを活用し、感度ラベルや DLP（データ損失防止）を用いたアクセス制御を実装すること。		き込み及びファイルアップロード等を対象として実装することを想定しています。具体的な制御対象、制御内容、検知条件及び適用条件については、機構と受注者で協議の上決定するものとします。 感度ラベルの適用対象は、主としてSharePoint Online 及び OneDrive に保存されるファイルを想定しています。 また、Microsoft 365 Copilot に係るプロンプト及び回答内容については、Microsoft Purview eDiscovery 等により検索、収集及びエクスポートできる環境を整備し、Copilot の利用状況及び操作履歴については、Microsoft Purview Audit 等の Microsoft 365 標準の監査ログ機能により記録及び確認できることを想定しています。 なお、Microsoft 365 側で保持、検索又は確認可能なログについては、別紙 4 に定める統合ログ管理基盤への集約を必須とはしないものとします。
31	P18	仕様書/第 5 章/（1）/ウ	>ユーザーが入力したプロンプト（指示内容）及び、それに対する AI の回答内容を、MicrosoftPurview の監査ログとして保持すること。また、管理者がセキュリティ調査等の目的で、特定のユーザーの対話履歴を検索・抽出（eDiscovery 等）できる環境を整備すること。	上記記載ございますが、実現されたい内容と製品機能の紐づけを追記・修正いただくことは可能でしょうか。 弊社認識では下記となりますので、認識齟齬がないよう要件修正を実施いただきたいと考えております。 Microsoft Purview Audit → 利用履歴・操作履歴 Microsoft Purview eDiscovery → プロンプトと回答本文の保持・検索	
32	P18	仕様書/第 5 章/（1）/ウ	>組織的なＡＩ活用を安全に実現するため、上記イ.で調達するアドオンを活用し、感度ラベルや DLP（データ損失防止）を用いたアクセス制御を 実装すること。	上記記載ございますが、ラベル適用先のファイルは、SharePointOnline および、OneDrive 上に保存されるファイルを想定しているとの理解でよろしいでしょうか。	
33	P18,45,46	仕様書/第 5 章/(1)/ウ 別紙 4/(1)/エ/①/⑤	>ユーザーが入力したプロンプト（指示内容）及び、それに対する AI の回答内容を、Microsoft Purview の監査ログとして保持すること。また、管理者がセキュリティ調査等の目的で、特定のユーザーの対話履歴を検索・抽	上記記載ございますが、Microsoft Purview による監査ログについては、Microsoft 365 の標準機能により保持・検索・監査が可能であることから、別紙 4(1)エに記載の統合ログ管理の対象外とし、Microsoft Purview（Microsoft 365）の標準監査ログ機能および eDiscovery 機能等により要件を満たす	

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			出（eDiscovery 等）できる環境を整備すること	構成を可としていただきたく存じます。	
34	P18,P19	仕様書/第 5 章/(2)/ウ	>以下のアプリケーションについてはユーザーに割り当てること。	上記記載に含まれるユーザーに割り当てるアプリケーションとは、Microsoft のライセンス割り当てを指しており、本要件は指定の機能群（Exchange/SharePoint/Intune 等）を網羅するベースライセンスを全 130 名へ割り当て、うち 90 名には Microsoft 365 Copilot ライセンスを追加付与する"割り当て設計"を行う、という理解で相違ないでしょうか。	ご認識のとおりです。
35	P19	仕様書/第 5 章/(3)/ア	>組織の設定において、データの保存場所（データ主権）を日本国内に指定すること。	上記記載要件について、念のため確認となりますが、データ保存先リージョンの指定要件は Microsoft Teams のみでよろしいでしょうか。それ以外になる場合は、別途ライセンスが必要のため、対象の確認をさせていただきます。	ご認識のとおりです。
36	P19	仕様書/第 5 章/(3)/ウ	>サードパーティ製アプリの追加を制限する。	上記記載の要件について、管理対象に Copilot エージェントを含めた表現への修正を推奨いたします。現在の Microsoft 365 および Teams では、従来のアプリに加えて Copilot エージェントや各種 AI エージェントも利用可能となっております。そのため、「サードパーティ製アプリ」のみを制限対象とした場合、サードパーティ製エージェントが管理対象外と解釈される可能性があります。意図するセキュリティ統制を実現するた	ご意見を踏まえ、仕様書を修正させていただきます。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				めには、アプリだけでなくエージェントも含めた管理対象として定義することが望ましいと考えます。	
37	P19,20	仕様書/第 5 章/(4) /ア	>既存のデータ及び各部署の組織単位のアクセス権限を、最新の勤務実態に合わせて整理・継承すること。	上記記載がありますが、現行と同じようにアクセス権限を継承させたいという理解で正しいでしょうか。 また、その場合の現状のアクセス権限管理の考え方についてをご確認させていただくか、仕様書側にも記載するかを推奨いたします。	本項は、現行の SharePoint Online 等におけるアクセス権限設定を基本とし、最新の勤務実態に合わせて整理した上で継承することを想定しています。アクセス権限は、原則として部、課等の組織単位又はグループ単位で管理するものとします。 また、外部ユーザーへのファイル共有機能は原則として禁止します。ただし、機構が業務上必要と認めた受注者、業務委託先その他の外部関係者との情報共有については、機構が指定又は承認する専用の共有領域に限り、必要最小限の範囲で利用できるものとします。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
38	P19,20	仕様書/第 5 章/(4) /ア	>外部ユーザーへのファイル共有機能は原則禁止とする	上記記載がありますが、例外有無に関する記載が無かったようにお見受けしております。 仮に例外ルールが現状が無い場合は、外部ユーザーへのファイル共有機能は禁止とする記載を推奨いたします。例外がある場合は、例外の内容を明記いただくことを推奨いたします。	
39	P19,20	仕様書/第 5 章/(4) /イ	>SharePoint Online → 9TB	上記記載がありますが、9TB は現状の利用状況をもとに算出したものでしょうか。また、本調達が 4 年間を対象としたものと理解しておりますが、4 年分を想定した容量という理解で問題ないでしょうか。必要に応じてご提言させていただきたいと思います。	ご意見を踏まえ、現行環境の使用状況及びデータ増加傾向を考慮し、次期環境において確保するストレージ容量を 15TB とするよう仕様書を修正します。
40	P21	仕様書/第 5 章/(5)/ア	>機構のメールサーバー機能は引き続き Exchange Online を利用し、既存環境からの移行及び最適化を行うこと。	上記記載の「最適化」の記載が曖昧であるため、あらかじめ定義していただくか、現時点で難しい場合には、状況の確認後に協議が可能な余地での記載をすべきかと思われます。	本項は、Exchange Online 自体の移行を求める趣旨ではなく、引き続き Exchange Online を利用する前提で、既存環境の設定内容、利用状況及び運用上の課題等を確認・整理した

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
					上で、必要な設定調整を行うことを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
41	P21	仕様書/第 5 章/(5)/イ	>利用可能な最大限のセキュリティ機能を構成すること。	上記記載がございますが、「最大限」の記載が曖昧であるため、あらかじめ定義していただくか、現時点で難しい場合には、状況の確認後に協議が可能な余地での記載をすべきかと思われます。	本項における「最大限」は、本業務で調達するライセンス及びサービスに含まれる送信セキュリティ機能について、機構の利用環境及び運用への影響を確認した上で、利用可能な範囲で有効に活用できるよう設定する趣旨です。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
42	P21	仕様書/第 5 章/(5)/ア	>機構のメールサーバー機能は引き続き Exchange Online を利用し、既存環境からの移行及び最適化を行うこと。	上記記載がありますが、M365 テナントは既に構築（利用）されている理解のため、継続利用する方針ではないでしょうか。その場合は記載を修正すべきを考えます。	本項は、Exchange Online 自体の移行を求める趣旨ではなく、引き続き Exchange Online を利用する前提で、既存環境の設定内容、利用状況及び運用上の課題等を確認・整理した上で、必要な設定調整を行うことを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
43	P21	仕様書/第 5 章/(5)/イ	>現行で適用している DMARC ポリシー（p=reject）の設定値を継承すること	上記記載がありますが、現行は _dmarc.jehdra.go.jp は、p=quarantine となります。p=reject への強化を想定していますでしょうか。	本要件は、なりすましメール対策の強化を目的として、次期環境において適切な DMARC ポリシーを維持することを想定しています。
44	P22	仕様書/第 5 章/(6)/ア	>本業務において調達する端末及び機構が独自に調達するスマートフォンを Microsoft Intune	上記記載を詳細化し、Windows PC およびスマートフォンを Microsoft Intune 管理化対象とする旨記載することを推奨いたします。	ご認識のとおり、Microsoft Intune の管理対象は、本業務において調達する Windows PC 及び機構が別途調達する Android 端末を想

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			の管理下に置くこと		定しています。iPhone 等の iOS 端末は、本要件の対象外とします。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
45	P22	仕様書/第 5 章/(6)/ア		Microsoft Intune 管理化のスマートフォンは Android のみ認識でよいでしょうか。（iPhone 等 の iOS は含まれない）	
46	P22	仕様書/第 5 章/(6)/ウ	>端末の初期設定にあたっては、WindowsAutopilot 等の最新手法の活用又は効率的なキッティング手法を提案し、実施すること。	上記記載において、端末のセットアップおよび展開については Windows Autopilot への言及から Windows PC を対象とされている認識ですが、スマートフォンについても同様の要件でしょうか。含まれる場合には範囲を揃えるため、記載を修正すべきと思われます。	本項における端末の初期設定及び展開は、本業務において調達する Windows PC を対象とすることを想定しています。 機構が別途調達するスマートフォン（Android 端末）については、受注者によるキッティング作業の対象外とし、第 5 章 (7) イに定める一般ユーザー向けマニュアルにおいて、Microsoft Intune への登録に関する手順を作成することを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
47	P22	仕様書/第 5 章/(6)/ウ	>いずれの手法においても、職員が最小限の操作でポリシーが自動に、又は確実かつ迅速に適用される環境を構築すること。	上記記載がございますが、「迅速」の記載が曖昧であるため、あらかじめ定義していただくか、現時点で難しい場合には、状況の確認後に協議が可能な余地での記載をすべきかと思われます。	ポリシー等の適用については、運用上支障が生じないよう、可能な限り速やかに適用される構成とすることを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
48	P22	仕様書/第 5 章/(6)/エ	>HID デバイスの利用を妨げず、「取り外し可能ストレージ」のみを対象とした読み書きの制限を実装すること。なお、機構が個別に許可した媒体に限り、接続を可能とする例外設定用ポリシーを用意すること。	上記記載について、個別に許可した媒体に限りとの記載がございますが、利用許可予定の外部記憶媒体は現時点でどの程度の量を想定しておりますでしょうか。	外部記憶媒体については、原則として利用を制限する運用を想定しており、例外的に許可する媒体については必要最小限に限定することを想定しています。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
49	P24	仕様書/第 7 章/(1)/イ	>CD-ROM 等の媒体及びこれに類するものを 使用する際に発生した障害	上記記載につきまして、「CDROM 内に含まれるマルウエア感染等による論理的な障害」か「物理的に酷く破損された CDROM 等の読み込みによるドライブ等の物理的な障害」のどちらを想定されている記載か、具体的なシナリオ等ついてご教示頂けないでしょうか。	本項は、CD-ROM 等の媒体及びこれに類するものの使用に起因して、ドライブ等の機器に物理的な故障が発生した場合の対応を想定しています。
50	P24	仕様書/第 7 章/(1)/イ	>PC については故障機器の交換、代替機の手配、付随する必要なセットアップ作業を受注者側で行い、原則として使用者が利用できない期間が生じないように対応するものとする。セットアップ作業については可能な限り交換前の状態に復旧すること。	上記記載ですが、利用できない期間とは故障してから即日中に代替機を使用者に引き渡す要件となりますでしょうか。例えば、交換連絡をいずれかの形でお問い合わせいただき、代替機を先にお送りしてからの返送をする先出しセンドバックのような状況にて満たす理解で宜しいでしょうか。	本項は、PC 故障時に、受注者において代替端末を手配し、必要なセットアップを行った上で使用者が利用できる状態とし、その後、故障端末を返送する運用を想定しています。 故障発生後、即日中に代替端末を使用者へ引き渡すことを必須とする趣旨ではありません。
51	P24,P25	仕様書/第 7 章/(1)/ウ		Microsoft Intune の活用のうち、USB 制御等、申請ベースで日常運用が発生する項目等の記載がございませんでした。ソフトウェア更新プログラムの展開については記載がございましたが、以下の運用は発生しない想定で問題ございませんでしょうか。 ・USB メモリ等の外付け USB デバイスの使用不可設定変更作業 ・更新ソフトの配布および共通ソフトウェアの一括配信	USB メモリ等の外付け USB デバイスについては、原則として使用を制限する運用を想定しており、日常的な申請に基づき例外設定を追加又は変更する運用は想定していません。 更新ソフトの配布及び共通ソフトウェアの一括配信については、Microsoft Intune 等を活用した端末管理運用の範囲として実施することを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
52	P28	仕様書/第 8 章/(2)	>LAN 配線図（竣工図）、情報コンセント及びL2スイッチのポー	当該成果物の配線図については、既存のレイアウト図面をいただいたうえで、今回の作業	ご認識のとおりで問題ございません。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			ト収容図（第４章（１３）に基づく）。	に伴うアップデートを行う形でよろしいでしょうか。	
53	P36,P37	別紙 2/1	>1.1 モバイルノート型 >1.2 省スペースデスクトップ型	モバイルノート型および省スペースデスクトップ型 PC においては、同一メーカーでのご提案が必須か、そうではないかご確認させてください	モバイルノート型 PC と省スペースデスクトップ型 PC は、同一メーカーであることを必須とするものではありません。 ただし、管理、保守及び利用者対応の効率性を確保するため、モバイルノート型 PC 内及び省スペースデスクトップ型 PC 内では、それぞれ原則として同一メーカーの機器で統一することを想定しています。 また、提案する各機器については、仕様書に定める性能、機能、保守、管理及び動作確認等の要件を満たすものとしてください。
54	P40	別紙 2/2.3.1/③	>別紙 3 に基づきプリンタドライバを各 PC にモノクロレーザー１台、複合機１台２台分インストールするものとする。	上記記載のプリンタドライバを各 PC へ配布する要件について、端末導入時にプリンタドライバのインストールのみを対象とする認識で相違ないでしょうか。また、各部門・各拠点で利用するプリンタの選択やプリンタ追加設定については、手順書を提供した上での利用者による手動設定を想定しているかご教示ください。	本項は、各 PC に対し、機構が指定する複合機及び各課に設置されるモノクロプリンタを利用できるよう、必要なプリンタドライバをあらかじめインストールすることを想定しています。 プリンタの選択及び設定対象については、機構が指定する内容に基づき対応することを想定しており、利用者による手動設定を前提とするものではありません。また、部署、設置場所又は利用者ごとに異なるプリンタ設定を自動的に割り当てる仕組みの構築を求める趣旨ではありません。
55	P41	別紙 2/2.6/③	>1PC に対し、機構が指定する Microsoft Entra	上記記載部分ですが、原則として１台の PC に対して１アカウントとなる一対一での利用を	ご認識のとおりです。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			ID アカウントで利用可能とすること。	想定している認識で相違ないでしょうか。	
56	P45	別紙 4/(1)/ア	>機構外からリモートアクセスを行う場合及びクラウドサービスの管理者権限等を用いてアクセスを行う場合は、2 つ以上の方式を組み合わせた多要素主体認証（フィッシング耐性を有する認証方式）を用いること	上記記載ございますが、職員向けスマートフォンの配備状況についてご教示いただけますでしょうか。	MFA のアクセス制御については、予定ユーザー数 130 名を対象として実装することを想定しています。 職員向けスマートフォンの利用に限定するものではなく、具体的な認証方式については、対象ユーザーの利用環境、端末配備状況、認証方式の安全性及び運用方法を踏まえ、機構と受注者で協議の上決定するものとします。
57	P45	別紙 4/(1)/イ/②	>アカウント管理者による不正を防止するため、アカウントの管理を行う権限を制御する機能（同一人物による権限の付与と執行の分離や、強い権限の都度承認等の仕組みを含む）を備えること。	上記記載の中で、「強い権限の都度承認等の仕組み」とございますが、特権アクセス管理（PIM）を利用した権限昇格および承認フローを想定されている認識であっておりますでしょうか。	ご認識のとおりです。
58	P45	別紙 4/(1)/エ/①	>システムの特性に応じて想定される脅威を分析し、システムの利用記録、例外事象の発生に関するログを取得すること。取得したログを最低４年間保管すること。	上記記載の「システムの特性に応じて」とございますが、ログの取得対象を明確化していただく、もしくは取得対象となる条件や定義などを明確にしていただくことは可能でしょうか。	本項は、政府機関等のサイバーセキュリティ対策のための統一基準群に基づき、情報システムの特性、想定される脅威、情報セキュリティインシデント発生時の原因調査、影響範囲の確認及び監査対応等の観点を踏まえ、必要となるログを取得、保管、確認及び点検・分析できる仕組みを求める趣旨です。 具体的なログの取得対象、ログ項目、保管方法、保管場所、集約範囲、点検・分析方法及

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
					び利用する機能については、本業務の設計段階において、機構と受注者で協議の上決定するものとします。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
59	P46	別紙4/(1)/エ/⑤	>収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施できる機能を備えること。	上記記載ですが、一元管理となりますとSIEM製品と呼ばれる一元的にログ管理、分析を行う製品の導入で実現可能と思われます。その場合は、実装したい要件に応じた緩和、もしくは明確化をお願いできればと思います。ただ、この要件においては事前の定義、記載が非常に多岐に渡るため、要求期待度合に応じた取捨選択からぜひご検討いただきたいと思います。	すべてのログを一律に取得することや、単一のログ管理基盤又は特定のSIEM製品に集約することを必須とする趣旨ではありません。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
60	P46	別紙4/(1)/エ/⑤		No.59の関連となります。SIEM製品によっては取得可能なログの種類が様々となるため、最低限の記載もしくは許容可能な記載としていただきたいと思います	
61	P45	別紙4/(1)/エ/②	>② ログの不当な消去や改ざんを防ぐとともに、許可された管理者のみがアクセスできるよう、アクセス制御機能を備えること。	上記記載がございますが、アクセス制御のみでは管理者による誤操作や、管理者アカウントの侵害によるログの削除・改ざんリスクがあると考えます。 ログの暗号化、改変防止、改ざん検知を組み合わせる要件を加える点について、ご検討いただければと存じます。	ログの保全については、アクセス制御に加え、対象となるログの性質及び保管方法に応じて、改ざん防止、改ざん検知、暗号化等の適切な保全措置を講じることを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
62	P46	別紙4/(1)/エ/③	>ログに記録される時刻にずれが生じないよう、システム内の	上記記載ございますが、時刻同期の実現方法を特定の機能要件に限定せず、システム全体	ログ取得対象となる機器、サービス及びシステムについて、適切な時刻同期を行うことを

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			機器の時刻を同期する機能を備えること。	として適切な時刻同期を実現できる構成を許容いただくことをご検討いただけますでしょうか。	想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
63	P46	別紙4/(1)/エ/④	›④ 容量の不足や障害の発生等により、ログが取得できなくなるおそれのある事象が発生した場合又はログが取得できなくなった場合、速やかにシステム管理者及びシステム運用担当者に通知する機能を備えること。	上記記載について、ログが取得できなくなった場合の解釈を明確にすべきと考えます。	容量不足、障害その他の理由により、ログの取得、保存、転送又は確認等のログ管理に支障が生じるおそれのある事象が発生した場合又は支障が生じた場合は、速やかにシステム管理者及びシステム運用担当者が把握できる仕組みを設けることを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
64	P46	別紙4/(1)/カ	›不正プログラム対策機能を使用し、ファイルアップロードをする機能にはチェック機能を付加すること。	こちら、本調達範囲における「ファイルのアップロード」が間接的も含めて関係するであろう該当箇所はMicrosoft365部分の一部(ファイルサーバとしてのSharePoint Online、送信セキュリティアドオンを管轄するExchange Online)となりますが、これら2つの領域への要求事項となりますでしょうか。 現状記載ですと、対象の範囲が不明瞭であり、希望される「不正プログラム対策機能」という部分が、アップロードファイルへのウイルスチェック等なのか、何か上長や決められた先への共有通知が行いたい機能なのか、要求事項も不明瞭かと思われます。そのため、要求と範囲を明確にしていただきたく思います。	本項は、ファイルアップロード機能を有する製品、サービス又は機能を本業務で新たに導入又は構築する場合に、アップロードされたファイルについて不正プログラム感染等の有無を確認できる機能を求める趣旨です。 ご意見のとおり、本項でいう「チェック機能」は、アップロードされたファイルに対するウイルスチェック等の不正プログラム対策機能を指しており、上長、管理者又は特定の宛先への共有通知、承認フローその他の通知機能を求める趣旨ではありません。 Microsoft 365及び送信セキュリティアドオン等については、各サービスに標準的に備わる不正プログラム対策機能又は契約範囲内で提供される機能を活用することを想定しており、本項により追加のセキュリティ製品

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
					の導入を当然に求める趣旨ではありません。ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
65	P50	別紙 4/(5)/⑤	>暗号化に用いる鍵の保管場所等の管理を適切に行えること。	上記記載について、利用者による管理を求める要件として解釈される可能性があります。一部のクラウドサービスでは利用者による鍵管理を前提としていないため、管理主体についての表現の見直しをご検討いただけますでしょうか	本項は、暗号化に用いる鍵について、管理主体に応じて適切に管理されることを求める趣旨です。 Microsoft 365 等のクラウドサービスにおいて、サービス提供者が暗号鍵を管理する方式の場合は、機構又は受注者が暗号鍵そのものを取得、保管又は直接的にライフサイクル管理することを必須とする趣旨ではありません。 一方で、サービス提供者、受注者又は機構等、いずれの主体が管理する場合であっても、暗号鍵については、生成、保管、利用、更新、失効及び廃棄等のライフサイクルにおいて適切に管理されることを求めるものです。 ご意見を踏まえ、管理主体に応じた暗号鍵管理の趣旨が明確となるよう仕様書を修正します。
66	P50	別紙 4/(5)/⑤	>クラウドサービスで利用する暗号鍵に関する生成から廃棄に至るまでのライフサイクルにおける適切な管理を行うこと。	上記記載ございますが、Microsoft 365 等の主要な SaaS では、暗号鍵をサービス提供者が管理する方式が一般的であるため、利用者による鍵ライフサイクル管理を前提としない表現への見直しをお願いいたします	
67	P8	第３章（５）無線 LAN 環境の整備 ウ. 配置設計及び事前調査		無線 LAN の導入にあたっては以下の作業を必須とすることで通信品質を担保することを推奨します。 ＜記載例＞ 無線 LAN の電波測定は専用の測定器または測定ソフトウェアを使用して、ヒートマップと測定結果の説明を明記した報告書を提出す	ご意見を踏まえ、無線 LAN 機器の配置設計及び設置後の確認内容が明確となるよう仕様書を修正します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				ること。想定エリアにおいて外来波、管理外APの有無、電波強度を確認した上で、最適なチャネル設計を実施すること。導入前においては、機器設置予定位置にAPを仮設したうえで電波測定を実施して、想定エリアに適切な電波強度で電波が到達しているか確認すること。 導入後にも同様に電波測定を実施して、必要に応じてチャネルの調整、電波出力の調整を実施すること。	
68	P9	第３章 （６）VPN環境の整備 ア.構成及び認証要件		制約を満たせない場合は、キッティング時に事前に設定もしくはキッティングのマニュアルに明記する等、受注者側による運用と環境の整備を実施することで、職員のスマートフォン運用に影響が出ないようにすることを前提として、スマートフォンにおける条件の緩和を検討頂きたい。	本項は、VPN 利用時において、Microsoft Entra ID の条件付きアクセス及び準拠デバイス判定に必要な情報が適切に連携され、機構が求める認証制御を実現することを求める趣旨です。 アプリ独自の認証画面又は組み込みブラウザ等を利用する方式であっても、Microsoft Entra ID の条件付きアクセス及び準拠デバイス判定に必要な情報を正しく連携でき、機構が求める認証制御を実現できる場合は提案可能とします。 また、設定反映にあたり、事前に一度接続に成功しなければ必要な設定が適用されない等の仕様がある場合についても、受注者において事前設定、初期展開方法又は代替手順等により、機構の運用に支障が生じないことを担保できる場合は、当該仕様を許容する方向
69	P9	第３章 （６）VPN環境の整備 ウ.集中管理及び自動構成		制約を満たせない場合は、キッティング時に事前に設定もしくはキッティングのマニュアルに明記する等、受注者側による運用と環境の整備を実施することで、職員の運用に影響が出ないようにすることを前提として、条件の緩和を検討頂きたい。	

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
					で要件を緩和します。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
70	P10	第３章（７）エンドポイントセキュリティ ウ.運用管理		運用管理として通常のヘルプデスク、監視の運用とは別に、セキュリティ対処の専門チームとして SOC(Security Operation Center)の配置を明記することを推奨します。	監視体制の実現方法については、特定の SOC サービスの利用を必須とするものではなく、受注者の自社体制又は SOC 等の外部監視サービスの活用により、仕様書に定める監視、通報及び一次対処の要件を満たすことを想定しています。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
71	P10	第３章（７）エンドポイントセキュリティ ウ.運用管理		EDR が検知するアラートに対する監視体制を整備することの記載がありますが、次世代 FW、EDR、Microsoft Entra ID、Intune、Microsoft365 監査ログ等のセキュリティログについても、SIEM又は SOC サービス等を用いた相関分析、重大度判定、一次通知及び月次報告を実施することを推奨します。	ご意見を踏まえ、エンドポイントセキュリティに係る監視状況等の報告事項が明確となるよう、第 7 章（4）の定例会における報告事項へ追記します。
72	P10	第３章（７）エンドポイントセキュリティ ウ.運用管理		監視又は分析によりセキュリティインシデントを検知した場合、重要度の高いものは検知後 30 分以内を目安に通報すること。また、通報時には重要度、緊急度、影響範囲、一次対処方法を含めることを推奨します。	ご意見を踏まえ、仕様書を修正します。
73	P14	第３章（１１）ウェブサーバーの運用管理 ウ.管理機能		サービス側で保存可能な期間が 1 年未満である場合、定期的に手動取得するなど運用によって、1 年以上を保存する方法を認めて頂きたい。サービスやログの種類によって保存可	ご意見を踏まえ、サービス側で保存可能な期間が 1 年未満であっても、受注者が提供する機能により補完する方式を認めるよう、仕様書を修正します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				能な期間が異なることも多く、サービスの選択幅を狭める可能性がある	
74	P14	第３章（１１）ウェブサーバーの運用管理 ウ.管理機能		「IPv6 によるアクセスが可能であること。」について、IPv6 が必須となる見込みではない場合、要件の削除を検討頂きたい。IPv6 の要件は IPv6 の普及状況を踏まえると、不要であると考えます。	ご意見を踏まえ、IPv6 によるアクセスを必須とする記載は削除します。
75	P21	第５章（５）メールサーバー イ.サーバー設定		DMARC ポリシー（p=reject）の設定値を継承することと記載されておりますが、現状の「jehdra.go.jp」の DNS 設定を確認したところ隔離（p=quarantine）となっておりますので、確認の上、どちらの設定を採用するか決定することを推奨します。	本要件は、なりすましメール対策の強化を目的として、次期環境において適切な DMARC ポリシーを維持することを想定しています。
76	P24	第７章 （１）保守サービス ア.インターネットサービス		調達機器に関する脆弱性情報への対応について、受注者による対象機器への影響確認、調査結果の整理及び機構への報告を想定している場合は、業務内容として明記いただきたい。 ＜記載例＞受注者は、調達機器等に関する脆弱性情報を確認した場合、対象機器・ソフトウェアへの該当有無、影響有無、対応要否を整理し、影響がない場合を含めて機構へ報告すること。	ご意見を踏まえ、仕様書に脆弱性への対応について追記します。
77	P25	第７章 （１）保守サービス イ.PC・プリンタに関する保守サービ		職員の異動等に伴い、端末の返却、再セットアップ、再配備等の作業が発生する場合は、PC・プリンタに関する保守サービスの範囲として仕様書に明記いただきたい。	ご意見を踏まえ、人事異動時の対応について追記します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
		ス		＜記載例＞職員の異動等により端末利用者の変更が発生した場合、受注者は端末の回収、初期化、再セットアップ、必要な設定変更、動作確認及び再配備を実施すること。	
78	P25	第７章 （１）保守サービス イ. PC・プリンタに関する保守サービス		端末交換及び代替機手配等に伴い発生する配送費用の負担区分について、仕様書へ明記いただきたい。 ＜記載例＞ 端末交換、代替機手配その他保守サービスの実施に伴い発生する配送費用については、受注者にて負担すること。	ご意見を踏まえ、配送費用の負担区分について追記します。
79	P25	第７章 （２）障害時の対応 エ. 技術的助言		機構、監督官庁、関係機関又はベンダ等から提供されるセキュリティ関連情報に対する調査、影響確認、回答及び報告対応を受注者に求める場合は、ヘルプデスクサービスの業務内容として仕様書へ明記いただきたい。 （記載例） ・セキュリティ関連情報に係る調査・回答対応機構、監督官庁、関係機関又はベンダ等から提供されるセキュリティ関連情報について、内容確認、調達機器等への影響確認、必要な調査、回答及び報告を実施すること。対象には、脆弱性情報、セキュリティインシデント関連情報、監査及び点検対応に伴う確認依頼等を含むものとする。	ご意見を踏まえ、仕様書を修正します。
80	P25	第７章 （２）障害時の対応 エ.		監査対応、ペネトレーションテスト対応において受注者の協力が必要となる場合、想定す	

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
		技術的助言		る対応内容と回数を記載頂くことを推奨します。	
81	P26	第７章 （２）障害時の対応 【新規】セキュリティインシデントへの対応		セキュリティインシデント発生時における受注者の対応範囲として、一次切り分け、影響範囲確認、端末隔離、証跡保全、暫定対処、復旧支援、報告書作成の要否を仕様書へ明記することを推奨します。	ご意見を踏まえ、仕様書を修正します。
82	P27	第７章 （３）ヘルプデスクサービス		脆弱性情報の収集、影響確認、リスク評価及び早期報告について、受注者に実施を求める場合は、要求する業務内容及び報告内容を仕様書へ明記いただきたい。 （記載例） 受注者は、調達機器等に関する脆弱性情報を継続的に収集し、対象機器への影響有無及びリスク評価を実施すること。また、重要度の高い脆弱性を確認した場合は、機構へ速やかに報告を行うこと。報告に際しては、脆弱性概要、関連情報、影響範囲、重要度評価及び対処方法を含めること。	ご意見を踏まえ、仕様書を修正します。
83	P27	第７章 （４）保守サービス等の記録整理		セキュリティインシデントの検出状況、対応状況、傾向分析、改善提案を含む月次 SOC レポートを作成し、定例会での報告を求めることを推奨します。	No.71 と同様
84	P30	第１０章（２）入札参加要件 【新規】SOC の体制		SOC の要件を明記頂く場合、を提供する事業者又は協力会社について、IPA「情報セキュリティサービス基準適合サービスリスト」の「セキュリティ監視・運用サービス」登録、	本仕様書では、特定の SOC サービスの利用又は SOC 事業者の配置を必須とすることは想定していません。 エンドポイントセキュリティに係る監視体

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				又は同等のサービス品質を有することを確認条件として追加することを検討頂きたい。	制については、受注者の自社体制又はSOC等の外部監視サービスにより実現することを可能としますが、いずれの場合であっても、仕様書に定める監視、通報及び一次対処の要件を満たすことを求めるものです。 このため、SOCサービスの利用を前提とした入札参加要件又は資格要件は追加しないこととします。
85	P36	別紙２　１．ハードウェア　１．１　モバイルノート型		モバイルノート仕様内 【仕様書案】 電源　AC100V　及びリチウムイオンバッテリパック。ACアダプタはUSB Type-C（PD　対応）を推奨。 【変更案】 電源の電圧は AC100V に対応していること。ACアダプタはUSB　Type-C（PD　対応）に対応している純正品を選定すること。リチウムイオン製またはリチウムポリマー製バッテリパックをモバイルノート本体に内蔵しており、JEITA3.0　準拠計測を利用し動画再生約 10 時間/アイドル時 20 時間以上のバッテリ駆動性能を有すること。	ご意見を踏まえ、電源及びバッテリに係る要件が明確となるよう仕様書を修正します。 ACアダプタについては、USB　Type-C（PD対応）のメーカー純正品又はメーカーが動作保証するものを付属することとします。 バッテリについては、リチウムイオン電池又はリチウムポリマー電池を内蔵することとし、駆動時間については、メーカー公表値において、動画再生時、業務利用を想定したベンチマーク又はこれらに準ずる条件で 6 時間以上であることを求める趣旨に整理します。 ご意見を踏まえ、当該趣旨が明確となるよう仕様書を修正します。
86	P37	別紙２　１．ハードウェア　１．２　省スペースデスクトップ型		省スペースデスクトップ型　仕様内 【仕様書案】 表示方式 TFT カラー液晶ディスプレイ、メーカー純正品であること、PC　との接続にあたっては	ご意見を踏まえ、DisplayPortケーブルを含めるように仕様書を修正します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				HDMI ケーブルを使用できること表示サイズ 23.8 インチワイド以上グラフィック表示解像度 ：1920×1080 ドット以上、表示色 ：1677 万色以上 【変更案】 表示方式 TFT カラー液晶ディスプレイ、メーカー純正品であること、PC との接続にあたっては HDMI ケーブルまたは DisplayPort ケーブルを使用できること 表示サイズ 23.8 インチワイド以上 グラフィック表示 解像度 ：1920×1080 ドット以上、表示色 ：1677 万色以上	
87	P37	別紙２ １.ハードウェア １．２ 省スペースデスクトップ型		省スペースデスクトップ型 仕様内 【仕様書案】 最大消費電力 最大構成時 260W 以下 【変更案】 最大消費電力 最大構成時 400W 以下	ご意見を踏まえ、最大消費電力に係る要件を見直します。 機器構成やメーカーごとの表示方法により、通常消費電力、最大構成時の消費電力、定格電流、電源容量等の値が異なる場合があり、最大消費電力の数値を一律に定めると、提案可能な機器が不必要に限定されるおそれがあります。 環境への配慮については、既に国際エネルギースタープログラム基準を満たしていることを要件としているため、最大消費電力に係る個別の数値要件は削除します。
88	P14	第 4 章 (1) ア		予備在庫の保管数について、契約締結後の協	No.19 と同様の回答となりますが、契約締結

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				議結果や運用実績を踏まえ、必要に応じて見直しを行うことは可能でしょうか。	後に保管台数を変更する場合には、変更契約により対応させていただきます。
89	P19	第5章（4）ア		SharePointOnline 及び OneDrive Online 等のアクセス権限整理・継承にあたり、最新の勤務実態に基づく情報連携の頻度または実施タイミング（月次、都度、人事異動時等）の目安をご提示いただくことは可能でしょうか。	ご意見を踏まえ、情報連携の頻度及び実施タイミングの目安が明確となるよう仕様書を修正します。 通常の人事異動に伴う権限変更については、機構から提供する人事異動情報等に基づき、対象ユーザーのグループへの追加、削除又は所属変更により対応することを想定しています。 人事異動に関する情報連携は、大規模な人事異動が年１回程度、その他必要に応じて少人数の異動が発生した都度行うことを想定しています。なお、権限設定全体の棚卸しについては、第２章（４）アに記載のとおり実施することを想定しています。
90	P24	第7章（1）イ		PC 及びプリンタ故障時の修理・交換対応について、過去実績又は想定件数をご提示いただくことは可能でしょうか。	ご意見を踏まえ、過去実績を仕様書に追記させていただきます。
91	P25	第7章（1）イ		端末の紛失・盗難時に実施するリモートワイプ又はリモートロックについて、過去実績又は想定件数をご提示いただくことは可能でしょうか。	ご意見を踏まえ、過去実績を仕様書に追記させていただきます。
92	P25	第7章（1）イ		Windows 11 更新プログラムの運用管理保守について、品質更新プログラム（月次）及び機能更新プログラム（年次等）が対象と記載されていますが、仕様書記載のア～エ（情報	ご認識のとおりです。仕様書に記載のア～エまでの具体的な作業内容は、「機能更新プログラムの適用にあたっての具体的な作業内容」として記載しているものです。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				収集、先行適用、展開管理、ロールバック等）の具体的な作業については、機能更新プログラムのみを対象としているとの理解でよろしいでしょうか。	
93	P26	第7章（2）エ		技術的助言について、過去実績又は想定件数、及び主な相談内容の例をご提示いただくことは可能でしょうか。	技術的助言については、過去実績又は想定件数を一律に示すことは困難です。 主な相談内容としては、調達機器等の障害又は不具合に関する技術的助言、設定変更の要否に関する確認、セキュリティ関連情報への対応等を想定しています。
94	P30	第10章（2）ウ		受注実績において、「100ユーザー以上が利用する基幹システムを 48 カ月以上継続して賃貸借した実績があること。」とありますが、証明時、具体的な顧客名・システム名は伏せても問題ないでしょうか。	契約上又は守秘義務上の理由により、具体的な顧客名及びシステム名を開示できない場合は、当該部分を伏せた資料の提出でも差し支えありません。
95	P30	第10章（2）ウ		受注実績において、「100ユーザー以上が利用する基幹システムを 48 カ月以上継続して賃貸借した実績があること。」とありますが、貴機構が想定しております「基幹システム」についての判断基準をご教示いただけますと幸いです。	本要件における「基幹システム」とは、組織の主要業務を継続的に支える業務システムであり、停止又は利用不能となった場合に、業務遂行に大きな影響を及ぼすものを想定しています。
96	P3	（4）現行サービスからの移行 オ. 現行の通信サービス提供事業者、LAN事業者及びサーバー保守	各事業者との調整及び連携が必要となる場合には、受注者にて対応すること。また、これに伴い発生した費用は、受注者にて負担すること。	左記要件に「発生した費用は、受注者にて負担すること。」とありますが、負担する範囲は、受注者分という認識でよろしいでしょうか。	No.2と同様です。 現行の通信サービス提供事業者、LAN事業者及びサーバー保守業者との調整及び連携に係る受注者自身の作業費用は、本業務に含むものとします。なお、現行事業者側で別途費用が発生する場合の取扱いについては、当該

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
		業者との調整			費用の発生原因、作業内容及び責任分界を踏まえ、機構と受注者で協議の上決定するものとします。
97	P3	（４）現行サービスからの移行 カ.現行の通信サービス、LAN及びサーバーに対する作業	受注者の都合により現行システムに対する設定変更をはじめとする作業を実施する場合、受注者がその費用を負担すること。	左記要件に「発生した費用は、受注者にて負担すること。」とありますが、負担する範囲は、受注者分という認識でよろしいでしょうか。	No.2と同様です。 受注者の提案内容、作業方法その他受注者の都合により、現行システムに対する設定変更その他の作業を実施する必要が生じた場合における、受注者自身の作業費用は本業務に含むものとします。なお、現行事業者側で別途費用が発生する場合の取扱いについては、当該費用の発生原因、作業内容及び責任分界を踏まえ、機構と受注者で協議の上決定するものとします。
98	P9	（６）VPN環境の整備ア.構成及び認証要件	VPN クライアントは認証時にアプリ独自の組み込みブラウザ（WebView等）を使用せず、OS 標準のブラウザ（Microsoft Edge等）を呼び出して認証を完結させる構成であること。認証基盤へデバイス ID 等の情報を正しく伝達できない製品は認めない。	左記要件を満たす構成として、「P7 （３）次世代ファイアウォールの運用管理」で提案予定の機器と Entra ID を連携することで実現することは可能であると認識しております。ただし、「P11 （９）ウェブ閲覧規制サービス」の要件との整合性を確認したところ、ゼロトラストネットワークを求めているように見受けられました。VPN 環境についても、ゼロトラストネットワークとして提供することを許容いただけないでしょうか。ただし、クライアントソフトのインストールが必要となります。	（９）ウェブ閲覧規制サービスは、Web閲覧制御、ログ記録及び情報持ち出し制御に関する要件であり、VPN環境をゼロトラストネットワーク方式として提供することを求める趣旨ではありません。 VPN環境については、機構外部から機構内LANリソースへ安全に接続するための環境を求めるものです。 本項目については、原案のとおりとします。
99	P12	（１１）ウェブサーバーの運用管	上記の既存 CGI システム及びメールフォーム等の移行にあた	昨今の公共市場における入札調達においては、公平性の観点からインフラ基盤業務とア	本業務は、基幹LANシステム全体の一元的な整備及び保守サービスを目的としており、ウ

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
		理① 経営努力事例検索システム	っては、移行先サービスが提供する標準のフォーム機能や検索機能又は次期環境で動作する汎用的なプログラム等を用いて同様の機能を構築又は機能適合することとし、これに伴う必要な設定調整やコンテンツの改修は全て本業務に含めるものとする。	プリ開発業務は分割調達となるケースが多い傾向にあると認識しております。そこで、本調達においても分割調達を検討してみてはいかがでしょうか	ェブサーバーの運用管理についても、インターネット接続サービス、DNS サーバー、ドメイン管理、移行作業及び運用上の調整等と関連するため、本業務の中で一体的に取り扱うことが適当であると考えています。 経営努力事例検索システム及び問い合わせフォーム等の既存機能についても、現行ウェブサイトの移行及び運用管理と密接に関連するため、本業務に含めることとし、本項目については原案のとおりとします。
100	P12	（１１）ウェブサーバーの運用管理 ②問い合わせフォーム		昨今の公共市場における入札調達においては、公平性の観点からインフラ基盤業務とアプリ開発業務は分割調達となるケースが多い傾向にあると認識しております。そこで、本調達においても分割調達を検討してみてはいかがでしょうか。	
101	P28	第８章 提出書類 （２）完了届と同時に提出する書類		左記要件には、設定定義書以降に係る成果物が定義されておりますが、以下の成果物を明示的に追加してみてはいかがでしょうか。 ・要件確認書、基本設計書、運用保守計画書、運用保守実施要領書等	設定定義書その他仕様書に定める提出書類により、本業務の履行に必要な設計内容、設定内容、運用方法及び保守に係る事項を確認できるものとすることを想定しています。 ご意見にある書類については、事業者により名称や構成が異なる場合があるため、個別の成果物名称としては追加せず、本項目については原案のとおりとします。
102	P4	第３章 （１）インターネット接続サービス	利用可能な固定 IPv4 アドレスを割り当てること。アドレス数は、冗長構成の維持及び管理に必要な数（/30 以上等）を確保	「IPv6 による接続環境」とは LAN 側で IPv6 を利用する想定でしょうか。 ※その場合、固定 IPv4 アドレスを割り当てつつ、固定 IPv6 アドレスも割り当る必要が	ご意見を踏まえ、インターネット接続サービスについては、利用可能な固定 IPv4 アドレスを割り当てることを要件とし、「IPv6 による接続環境の提供が可能であること」との記

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			すること。また、IPv6 による接続環境の提供が可能であること。	ございます。	載は削除します。
103	P4	第３章 （１）インターネット接続サービス	冗長構成の維持及び管理に必要な数	ここでの「冗長構成」とは”インターネット回線”と”WAN サービス”この２つでの冗長構成でよろしいでしょうか。 ※インターネット回線は２拠点にそれぞれ１回線ずつでよろしいでしょうか。もしくは２拠点にそれぞれ 2 回線ずつ(メイン、バック)でしょうか。	本要件における冗長構成は、インターネット接続サービス及び WAN サービスを組み合わせ、障害発生時にも業務継続に必要なインターネット接続を確保する構成を想定しています。 各拠点に複数のインターネット回線を設ける構成や、バックアップ回線として別の回線サービスを利用する構成を必須とするものではありません。
104	P4	第３章 （１）インターネット接続サービス		・インターネット回線を(メイン､バック)2回線の場合、メイン、バックはそれぞれ冗長性を考慮して別の回線サービスを利用するという仕様はいかがでしょうか。※バック回線には、メイン回線に求められている SLA は除外していただけますと幸いです。	