

「情報・研修館情報基盤システムの設計・構築及び運用・保守業務 一式」の意見招請に対する意見の回答について

項番	文書名	頁	項目	意見概要	提出の理由	補足資料	修正有無	意見への対応(回答)
1	1_調達仕様書	5	1.6 情報基盤システムの環境構築・設置期日 (2)機密性情報系ネットワーク ウ	調達仕様書(案)には、ウ「平成 31 年 3 月 31 日までに、特許庁普及支援課職員、特許庁特許室職員および知財総合支援窓口担当者が利用する環境の構築・設置を完了すること。」との記載がございますが、 要件定義書(案) 39 頁 5 平成 31 年 4 月:知財総合支援窓口の利用に係る要件の補足 「知財総合支援窓口における機密性情報系 NW の利用について、その利用に伴う構築作業等は本業務の調達範囲外とし、別途調達を行う予定である。」との記載と異なります。 どちらの記載が正しいかご確認をお願いします。	要件の明確化のため		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
2	1_調達仕様書	5 ～ 6	1.6 情報基盤システムの環境構築・設置日	調達時期が平成 30 年 3 月 31 日開始とする知財総合支援窓口管理者様向けシステムについて、「図表 1-8-1 用語の定義 項番 3」には現行情報システムは、平成 30 年 1 月末まで使用できると記載があり、平成 20 年 2～3 月は、この対象のシステム自体が現行も新も両方利用できないこととなります。 知財管理窓口管理者様は、現行の情報基盤システムは、使用しないという解釈でよいでしょうか。	要件の理解のため。		無	知財総合支援窓口の管理者が利用する OA 系システムは、他の拠点・利用者が利用するシステム(=現行システム)とは異なる。なお、知財総合支援窓口の管理者が利用する OA 系システムは、平成 30 年 3 月末まで利用する。
3	1_調達仕様書	6	1. 7スケジュール	設計、構築・テスト、受入テストのスコープや作業内容を仕様書中に明記するか、具体的なテストシナリオやテストの方法、テストスケジュールを提案に含むよう明記し、提案時の評価で考慮すべきと考えます。	サービスインまでのスケジュールがタイトであり効率的なプロジェクト運営を行う必要があるため。 特にテスト作業の進め方において認識齟齬があるまま進めた場合、遅延リスクが高まるため。		無	意見のとおり、作業内容やスケジュールは評価対象とする。
4	1_調達仕様書	6	図表 1-7-1 想定する作業スケジュール	設計工程にてサーバ等の機器(台数・スペック等)やソフトウェアが確定し、構築するまでの間に機器を納入する必要がございます。想定する作業スケジュールでは機器の発注から納品までのリードタイムが考慮なされていないと思われます。これにより、実質的な構築・テストの期間が不足することが懸念され、サービス開始日に確実な納期の遵守が難しいと考えます。 従って、納期遵守を優先する場合、全体のスコープやスケジュールの見直し、または設計範囲を縮小する等の対応が必要と思われます。	実現可能性を高めるため		有	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにした。
5	1_調達仕様書	6	図表 1-7-1 想定する作業スケジュール	設計・構築フェーズの期間が対象システムに比してあまりにも短く、現行の仕様を熟知しているベンダが有	調達における公平性の確保のため		有	情報基盤システムの平成 30 年 1 月の稼働開始は必須であるため、スケジュールはこのままとする。ただし、調達範囲に関する意見を

				利となっているため、スケジュールの見直しをお願いしたい				踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることとした。
6	1_調達仕様書	6	図表 1-7-1 想定する作業スケジュール	スケジュール上、HW の仕様および数量が決定される設計フェーズの終了後、HW の確保(製造)にかかる準備が考慮されていないため、最低三カ月程度の製品準備期間を設けて頂きたい	実現性のあるスケジュールとするため		有	設計・構築期間中に、HW 等機器の準備を実施されたい。情報基盤システムの平成 30 年 1 月の稼働開始は必須であるため、スケジュールはこのままとする。ただし、調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることとした。
7	1_調達仕様書	7	2. 1 作業の内容 ア設計・構築実施計画書の作成	WBSの作成に関連し、費用は機器や回線費用(インシヤル、ランニング)の別に提示することはもちろん、役務については工程(WBSレベル 3~4 の粒度)ごとにコストを提示することを明記すべきと考えます。	投資におけるフェーズごとのコストを明確にし、後年度負担が増加することを抑制するため、また役務については、後述する通りEVMの実施が求められており、適切なコスト管理を行うことで説明責任を果たすため。		有	意見を踏まえ、受注者は EVM または WBS の作業項目・タスクごとに予定工数・実績工数(5 人日程度の単位)を示し、提示することとする。
8	1_調達仕様書	7	2. 1 作業の内容 ①コミュニケーション管理	①コミュニケーション管理は、その一環として、「レビュー計画を作成し、いつ(いつまでに)誰が、何をレビューするのかを明確にし、遅滞なく工程が進むよう管理すること。なお、レビューやその管理には発注者の工数(作業期間)に配慮するとともに作業負荷軽減の工夫をし提案すること」などを追記すべきと考えます。	短期間で設計に係る合意や各種テストを行う必要があり、効率的に合意形成を図る必要があるため。また、文書作成量を見込まずに進めるとレビューの工数が想定以上に増加することがあるため。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
9	1_調達仕様書	7	2. 1 作業の内容	②体制管理、③工程管理、④品質管理については、管理手法ではなく、管理作業の手順までを示すよう求めるべきと考えます。	手法だけでは概念的な提案に留まり、リスクの認識、管理の具体的な作業内容が把握できないため。		有	意見を踏まえ、調達仕様書の「2.1 作業の内容」の一部記載を以下に修正する。  ----- ② 体制管理 受注者における作業体制の管理手法、手順等について記載する。 ③ 工程管理 設計・構築の作業、その工程の管理手法、手順等について記載する。 ④ 品質管理 成果物の品質を確保するために、品質基準、品質管理方法、手順等について記載する。 -----
10	1_調達仕様書	8	2.作業の実施内容に関する事項 2.1 作業の内容 (1)設計・構築業務 ア 設計・構築実施計画書の作成 4 ポツ目	受注者から貴館への会議体の議事録の送付は 3 営業日、貴館側の議事録の確認と承認は、それ以降であり、手段は、メールや会議体という認識でよろしいでしょうか。	要件の理解のため。		無	認識のとおりである。

11	1_調達仕様書	8 (9 )	2. 1作業の内容 ⑤リスク管理	リスクの認識、リスクの管理は手法のみならず手順までを示すべきと考えます。	手法だけでは概念的な提案に留まり、リスクの認識、管理の具体的な作業内容が把握できないため。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
12	1_調達仕様書	8 (9 )	2. 1作業の内容 ⑦システム構成管理	システムの構成管理手法ではなく、システムの構成管理手順とし、また、CMDBの利用、セキュリティ対策への適応方法までを記載すべきと考えます。また、「設計段階で構成一覧を作成した後にテストや運用フェーズを経て変更が生じた場合は、アップデートを行うこと」などを追記すべきと考えます。	NISCの「高度サイバー攻撃対処のためのリスク評価等のガイドライン」が28年10月に発行され、これに記載された対策セットの導入が求められており、そのためには正確かつ詳細なシステム構成管理が必要であり、手法でなく具体的な構成管理手順までを提案評価に含む必要があるため。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。 システムの構成管理手順について、応札時の提案資料に記載することは求めないが、設計において構成管理手順も検討するものと想定している。
13	1_調達仕様書	8 (9 )	2. 1作業の内容 ⑨情報セキュリティ対策	「受注者のプロジェクト作業場所においては、発注者が行うセキュリティ対応状況の監査(現地視察を含む)を受け入れること」などを追記すべきと考えます。	通則法改正に伴い、独立行政法人においては内部統制強化が求められており、その一環として委託契約における発注先の管理徹底も求められているため。		有	意見のとおり修正する。
14	1_調達仕様書	8 (9 )	2. 1作業の内容 ア設計・構築実施計画書等の作成 ⑨情報セキュリティ対策	情報セキュリティ対策の一環として、「受注者は本件にア設計・構築実施計画書等の作成 ⑨情報セキュリティ対策 情報セキュリティ対策の一環として、受注者は本件にア設計・構築実施計画書等の作成 ⑨情報セキュリティ対策 情報セキュリティ対策の一環として、受注者は本件にア設計・構築実施計画書等の作成 ⑨情報セキュリティ対策 情報セキュリティ対策の一環として、受注者は本件にア設計・構築実施計画書等の作成 ⑨情報セキュリティ対策	通則法改正に伴い、独立行政法人においては内部統制強化が求められており、その一環として委託契約における発注先の管理徹底も求められているため。		有	意見のとおり修正する。
15	1_調達仕様書	8 (9 )	2. 1作業の内容 イ設計	基本設計及び詳細設計とありますが、工程の名称はベンダ各社によって定義が異なることがあるため、ベンダ独自の手法に偏ることのないよう、独立行政法人情報処理推進機構発行の共通フレーム2013を参照し、工程名称及び作業内容はこれに準ずるべきと考えます。	受発注者間での認識合わせのための時間や、それがなくままに手戻り時間をとられてしまうことで大きな遅延を起こすリスクがあるため。また、特定のベンダ依存を回避するため。		有	「調達仕様書 5.2 遵守する法令等」に記載の「政府情報システムの整備及び管理に関する標準ガイドライン」に基づいて作業を行うが、必要に応じて「共通フレーム2013」も参照してプロセスを可視化し、発注者及び応札者間における定義の齟齬が生じないようにすること。
16	1_調達仕様書	9	イ 設計	「以下に示す事項以外でも、必要と考えらえる作業については提案すること」について、委託開始後に作業が必要である旨が判明した場合の当該作業に関する契約上の取り扱いについてご教示頂きたい	調達範囲を明確にするため		無	契約締結後に作業が必要であることが判明した場合は、情報・研修館の職員と協議の上、契約変更等の必要な対応を決定する。
17	1_調達仕様書	9	2 作業実施内容に関する事項 2.1 作業内容 イ 設計	基本設計書として取りまとめる内容として、 ①～⑫を定義されていますが、この定義の中にアプリケーション開発で定義すべき内容があり、本調達には適合しない内容があると思われるので記載の見直しをお願いいたします。 ②画面設計、③帳票設計など			有	要件定義書(案)別紙2「提供サービス・機能一覧」[7.イントラサービス]における設定が画面設計の対象となるため、画面設計は現行の要件のままとする。帳票設計に関する要件は、意見を踏まえ、削除する。
18	1_調達仕様書	9	2. 作業の実施内容に関する事項 2.1 作業の内容 (1)設計・構築業務	「②画面設計」について、インフラ基盤の導入である本調達において、画面設計は必要となりますでしょうか。不要の場合、削除願います。	開発を伴う業務アプリケーションにおいては、要求事項として必須と考えますが、要求機能の仕様を満足するパッケージ製品を導入しコストを抑えるためには、不要と考えま		無	「要件定義書(案)別紙2 提供サービス・機能一覧 7.イントラサービス」における設定が画面設計の対象となるため、意見は採用しない。

			イ 設計 3 ポツ目		す。 必要な場合、画面に関する具体的な要件(要件定義書(案) 図表 3-1-2 ユーザビリティ要件項番 1 よりも具体的で定量的な要件)を記載いただけますでしょうか。パッケージ製品のカスタマイズとなり、コスト増のため適正な費用が見積もれないと考えます。		
19	1_調達仕様書	9	2. 作業の実施内容に関する事項 2.1 作業の内容 (1)設計・構築業務 イ 設計 3 ポツ目	「③帳票設計」について、要件定義書(案)には、不要と記載があります。 削除願います。 帳票設計が必要な場合、どのような設計・開発が必要になるか記載願います。	要件定義書(案)(P4 2.3)では、帳票設計は取り扱わない想定と記載があり本仕様との差異があります。 どちらを正とすべきか提案業者側では判断できないため、修正願います。		有 意見 No.17 を参照すること。
20	1_調達仕様書	9	2. 1 作業の内容 ウ構築・テスト	テスト体制、テスト環境のみならず、テストスコープ及びテストにおける詳細な作業と作業ごとの役割分担を含むテスト計画とすべきと考えます。	受発注者間での認識齟齬を避けるため、また作業のぬけ漏れを防ぐため。		有 意見を踏まえ、調達仕様書の「2.1 作業の内容」の一部記載を以下に修正する。 ----- ・ 受注者は、テスト体制、テスト環境、作業スケジュール、テストスコープ、テストシナリオ、役割分担、合否判定基準等を記載した「テスト計画書」を作成し、情報・研修館の了承を得ること。 -----
21	1_調達仕様書	9 (1 0)	2. 1 作業の内容 ウ構築・テスト	「テストシナリオ・スクリプト」とは何を示すのか説明が必要と考えます。	読み手により理解に差が出るおそれがあるため。		有 「テストシナリオ・スクリプト」とはテストの実手順を記述したものを意図しているが、「シナリオ」と「スクリプト」は類似の意味であり誤解を招く可能性があるため、意見を踏まえ「テストシナリオ」に修正する。
22	1_調達仕様書	10	2. 1 作業の内容 エ受入テスト支援	受入テストには、業務移行を含む運用テストも含めるのか検討のうえ明記が必要と考えます。	短期間で受入テストを行うことになるが、現実的な作業計画を立てるために仕様書にスコープを明示する必要がある。		無 受入テストには業務移行は含まず、提供サービス・機能が仕様どおり利用できるか確認を行う。業務データの移行は情報・研修館職員にて行う。
23	1_調達仕様書	10	2. 1 作業の内容 オ情報基盤システムの切替え	移行期間において、業務移行の支援を行うことも記載が必要と考えます。	発注者の組織体制に照らして、各拠点を含めて網羅的に業務移行を行うには受注者の支援が必要であるため。		無 業務移行の支援は、「3.13 移行に関する事項」の「(2)データ移行・システム切替え要件」「イ 個別要件」及び「教育に関する事項」で利用者等への説明会実施等の支援を行うこととしている。
24	1_調達仕様書	11	2. 作業の実施内容に関する事項 2. 1 作業の内容 (2) 運用・保守業務 ア 運用・保守作業	「受注者は、利用者数の増加による機器・ライセンス等の追加を運用作業として行うこと。ただし追加に伴う費用については、当該調達の単価を上限に、情報・研修館と協議の上で別途対応することとする。」について、「当該調達の単価を上限に、」を削除いただきたい。	ライセンスや機器を追加する場合、数ユーザの追加の場合でもおいても、一定単位での設備増強が必要となり、調達時の単価で提供することが難しい場合があるため。		有 意見 No.29 を参照すること。

			計画及び運用・保守実施要領の作成				
25	1_調達仕様書	12	2.1 (2)運用・保守業務	「利用者の増加」という記載について、想定する増加人数について、年度ごとにご教示ください。	どの程度の割合で増加するか、予測できないため。		無 利用者の増加は年間5名程度を想定している。なお、組織変更等によりそれ以上に増える場合は対応方法について別途協議を行うこととする。
26	1_調達仕様書	11	2. 1作業の内容 ア運用・保守作業計画及び運用・保守実施要領の作成	「「運用・保守計画」には、SIEMを活用した、システムの監視及び制御の方法及び緊急対応チーム(CSIRT)との連携方法と作業分担についても定義すること。」などの追記が必要と考えます。	NISCの「高度サイバー攻撃対処のためのリスク評価等のガイドライン」にある対策セットを導入し、適切な運用管理を行うためには、SIEMによるログの解析は必須であるため。 また、緊急時には通常の運用体制以外に緊急対応を行う体制を整えておく必要があるため。		無 本意見招請においては、意見は採用しない。「高度サイバー攻撃対処のためのリスク評価等のガイドライン」にある対策セットの導入については、段階的且つ別途調達をする方針である。
27	1_調達仕様書	11 (1 2)	2. 1作業の内容 ア運用・保守作業計画及び運用・保守実施要領の作成	⑨情報セキュリティ対策には、機密性に限らず可用性、信頼性への対策も含むことは追記が必要と考えます。	セキュリティ対策において可用性、信頼性の確保も求められるため。		無 可用性や信頼性要件は要件定義書に記載済であるため、追記は必要ないと判断し、意見は採用しない。
28	1_調達仕様書	11 (1 2)	2. 1作業の内容 ア運用・保守作業計画及び運用・保守実施要領の作成	⑨情報セキュリティ対策の、「管理体制について記載する。」について、管理体制のみならず意図せざる変更が加えられないようにするための規程作りが必要になると考えます。	管理体制だけでは不十分であるため。		無 外部委託における「委託先において不正プログラム等が組み込まれることへの対策」については、要件定義書の図表3-10-1「情報セキュリティ対策要件」を参照すること。また、変更管理の仕組み・プロセスを実施することで、意図せざる変更が加えられないようにする対策も実施されることと認識している。
29	1_調達仕様書	11	2. 1作業の内容 ア運用・保守作業計画及び運用・保守実施要領の作成	機器・ライセンス追加時の費用は、機器・ライセンスそのものの費用のみでなく、構築作業や運用・保守業務の費用も協議の対象とすべきと考えます。	機器やライセンスの追加には、相応の設計・構築作業が発生することが想定され、状況により人的リソースの追加も必要になると考えられるため。 また、機器の追加により運用範囲が拡大することが想定され、別途定義されるSLAを遵守するためにリソースの追加を含む体制変更が求められるケースが想定されるため。		有 意見を踏まえ、以下のとおり修正する。 ----- 受注者は、利用者数の増加による機器・ライセンス等の追加を運用作業として行うこと。ただし追加に伴う費用については、原則、当該調達の単価を上限に、情報・研修館と協議の上で別途対応することとする。 -----
30	1_調達仕様書	11 (1 2)	2. 1作業の内容 ア運用・保守作業計画及び運用・保守実施要領の作成	「運用・保守実施要領」について、インシデント管理、SLA管理を項目として追加するべきと考えます。	インシデント管理については、システム障害やセキュリティインシデントに対して、原状回復までの対応の管理と恒久対策のための対応の管理(問題管理)はわけて管理する必要があると考えられるため。 また、SLA管理については、SLA		有 意見を踏まえ、調達仕様書の「2. 1作業の内容 (2)運用保守業務 ア運用・保守業務計画及び運用保守実施要領の作成」に以下のとおり修正・追記する。 ----- (修正) ⑥ 課題管理

					の運用を効率的かつ効果的に実施するために必須であると考えられるため。			運用・保守において発生したインシデント及び解決すべき問題について、発生時の対応手順、管理手法等について記載する。  (追記) ⑩ SLA 管理 SLA 設定項目の計測方法及び達成状況の管理方法について記載する。 -----
31	1_調達仕様書	13	2.作業の実施内容に関する事項 2.1 作業の内容 (2)運用・保守業務 イ 定常時対応 6 ポツ目	月例の定期会議の出席者は、運用保守計画時に決定することよろしいでしょうか。	要件の理解のため。		無	認識のとおりである。遂行責任者及び運用・保守チームのチームリーダーは参加を必須とするが、それ以外の参加者については、運用保守計画時に決定する
32	1_調達仕様書	14	2. 1 作業の内容 エ 運用・保守の改善 提案	「受注者は、定常時対応や障害発生時対応の中で確認された課題の分析を行い、情報基盤システムの信頼性の向上を目的とし、積極的に改善提案を行うこと」と変更する必要があると考えます。	改善提案は日常的な運用業務の中で随時すべきものであり、それによりシステムの信頼性やセキュリティ面が向上され、さらに不要な運用コストの増加を抑える効果が期待されるため		有	意見のとおり修正する。
33	1_調達仕様書	15	2 作業実施内容に関する事項 2.2 成果物の範囲、提出期限等	本調達に向けた提案として、運用を含めたサービス型の提案は可能でしょうか？ その場合、定義された成果物を全て納品する事が難しいと考えます。成果物について調整する事は可能でしょうか？ ※調達仕様書に記載されている成果物の提出が必要であれば、サービス型の提案はできない物と判断します。			有	本調達はサービス型の調達であり、意見を踏まえて図表 2-2-1「成果物及び提出期日」を見なおすこととする。なお、成果物についての協議は可能である。
34	1_調達仕様書	15	2.作業の実施内容に関する事項 2.2 成果物の範囲、提出期日等 (1)成果物(ドキュメント類)	「図表 2-2-1 成果物及び提出期日 No.8 情報基盤システムの稼働開始に伴う切り替え計画書」について、提出期日は、貴館と相談とありますが、各拠点に対して提出ではなく、貴館本社(特許庁庁舎)に対して、取りまとめの上提出という理解でよろしいでしょうか。 さらに、各拠点毎に切り替え計画の決定のタイミングが異なることより、一度提出させていただいた切り替え計画書を随時更新していくという対応でよろしいでしょうか。	要件の理解のため。		無	認識のとおりである。
35	1_調達仕様書	15	2. 2 成果物の範囲、提出期日等 (1) 成果物(ドキュメント類)	No.20 運用・保守報告書(月次)の提出期日を 10 営業日後に変更いただきたい。	障害、問い合わせ、SLA 稼働実績等の多岐にわたる情報の集計・分析が必要となり、作業期間を確保することで、より有益な報告書とするため。		有	意見を踏まえ、No.20 の提出期日を以下のとおり修正する。 ----- 平成 30 年 1 月以降、毎月次(月初5営業日以内に提出。ただし、稼働開始後三ヶ月間は提出期日については、必要に応じて、情報・

								研修館と協議の上変更可能。 -----
36	1_調達仕様書	18	4. 1 作業実施体制	情報セキュリティ対策の一環として、「受注者は本件に関与する全ての要員の一覧を作成し提示すること。また要員を変更する場合は、情報・研修館の承認を得たうえとし、速やかに一覧を更新の上提出すること。」などを追記すべきと考えます。	通則法改正に伴い、独立行政法人においては内部統制強化が求められており、その一環として委託契約における発注先の管理徹底も求められているため。		有	意見 No.14 を参照すること。
37	1_調達仕様書	19	4.2 図表 4-2-1 No3	運用保守要員の資格追加  <変更案> 運用要員においては次の実績を有する事が望ましい ・運用保守の役割に該当する運用実績を 2 年以上有する事。 ・ITIL 資格を保有しているまたは当該資格者と同等の能力を有すること	記載内容だと全体的なスキル、運用品質が保たれない可能性がある		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
38	1_調達仕様書	19	4.2 作業要員に求める資格等の要件	<資格> 本業務を遂行するために必要な担当者として、以下に示す資格を 1 件以上を有する、もしくはその資格と同等以上のスキルを有する者を最低 1 名配置すること。ただし、資格または～(以下略)  ①経済産業省情報処理技術者試験のシステムアーキテクト資格 ②経済産業省情報処理技術者試験の情報セキュリティスペシャリスト資格	2 件の資格を持つ要員が業界的に充分に存在していない為、「2 件とも必要」としてしまうと本質的でない理由で要員確保を阻害してしまう為。	無し	無	一人の担当者が二つの資格を持っていることが必須ではなく、チーム内の複数の要員で資格を保有していれば要件を満たすことを指す。
39	1_調達仕様書	19	4.2 作業要員に求める資格等の要件	<経験等> 情報システムのセキュリティ全般と標的型攻撃対策に精通し ～(中略)～ といった一連の業務経験を有し、適切な対応が取れるような体制とすること。  <u>※上記文面を削除、又は経験者の確保ではなく体制として準備するレベルにとどめる</u>	セキュリティ対策の経験者については、会社として対応できる体制を用意することは可能ですが、運用・保守チーム要員として経験者をフルアサインする事は難易度が高く、またコストも増大してしまう為、体制として用意するレベルにとどめていただきたい。	無し	無	運用・保守チーム要員として専属である必要はない。
40	1_調達仕様書	20	4.2 作業要員に求める資格等の要件	図表 4-2-1 に記載のある、各要員に必要な経験等について、一部要件緩和をお願い致します。	当社において『情報基盤システムと同規模(端末 100 台以上かつ数十拠点以上)・・・』の要件を満たすのが困難であるが、同規模の定義を緩和することにより、要件を満たすことができるため。		無	「(端末 100 台以上かつ数十拠点以上)」の記載は、拠点ごとに 100 台以上の端末ではなく、端末数の合計が 100 台以上の設計・構築経験(運用・保守経験)、拠点数が数十拠点以上のシステムの設計・構築経験(運用・保守経験)のいずれも満たすことを指す。 なお、複数の業務実績で上記を満たすことも許容する。
41	1_調達仕様書	19	4. 4 作業の管理に関する要領	作業の進捗や出来高を管理するためにEVMを用いるべきと考えます。	通則法改正に伴い、独立行政法人においては内部統制強化が求めら		有	意見 No.7 を参照すること。

					れており、中期計画等の進捗状況のモニタリング(EVM(アードバリューマネジメント)手法を用いた計画管理が求められているため。			
42	1_調達仕様書	19(20)	4. 4作業の管理に関する要領	マイルストーン、各タスクの期間設定及び完了条件は単に定めておくだけでなく、情報・研修館の承認を得る必要があると考えます。	短期間で実施するプロジェクトであり、マイルストーン、各タスクの期間及び完了条件を受発注者双方で合意のうえ進めることで、遅滞ないよう管理を徹底する必要があるため。		無	意見のとおり、情報・研修館の了承を得る必要があると考える。
43	1_調達仕様書	21	5. 作業の実施に当たっての遵守事項 5.1 機密保持、資料の取り扱い及びセキュリティ対策	情報セキュリティ対策の実施計画(本業務に係る情報セキュリティ対策とその実施方法及び管理体制)は、設計・構築実施要領の中に記載でよろしいでしょうか。	図表 2-2-1 成果物及び提出期日に該当の資料の記載がないため、どのような形式で提出となるか明確にさせていただきます。		有	「設計・構築実施要領」とは別の成果物であるため、「図表 2-2-1 成果物及び提出期日」に「情報セキュリティ対策の実施計画(本業務に係る情報セキュリティ対策とその実施方法及び管理体制)」を追加する。
44	1_調達仕様書	21(22)	5. 2遵守する法令等 イガイドライン等	「高度サイバー攻撃対処のためのリスク評価等のガイドライン」(内閣サイバーセキュリティセンター)、の追記が必要と考えます。 <a href="http://www.nisc.go.jp/active/general/risk.html">http://www.nisc.go.jp/active/general/risk.html</a>	本意見招請前の 2016 年 10 月にリリースされたガイドラインであり仕様書に記載のあるガイドライン同様遵守する必要があるため。		有	当調達のスコープだけでは「高度サイバー攻撃対処のためのリスク評価等のガイドライン」の全ての対策を適用することはできないが、調達スコープに該当する対策は適用する必要があるため、参照する法令等として定めることとする。
45	1_調達仕様書	23	6. 2 瑕疵担保責任	「契約期間中の納入機器一式の瑕疵に関して」とありますが、瑕疵担保期間について期間を明示していないでしょうか。	通常、瑕疵担保責任に関しては、検収後、〇〇年などの期間を設定しているため。		有	情報基盤システムの稼働開始から平成 33 年 12 月 31 日(契約期間終了)までである。
46	1_調達仕様書	24	(2)公的な資格や認証等の取得	運用体制における ISO20000 の認定条件の追加  <変更案> 運用体制における ISO20000 の認定条件の追加	運用業務の品質確保の為		無	必須の要件とする必要はないと判断し、意見は採用しない。
47	1_調達仕様書	24	7. 1 入札参加要件 (2) 公的な資格や認証等の取得	「プライバシーマークの使用許諾の認定を受けていること」について、「プライバシーマークの使用許諾又は個人情報保護マネジメントシステム(JIS Q 15001)の認定を受けていること」に変更をお願い致します。	個人情報保護マネジメントシステム(JIS Q 15001)はプライバシーマークと同等の認証としての評価を得ており、企業の規模・組織・方針により取得資格は様々であるため。		有	意見のとおり修正する。
48	1_調達仕様書	27	3.11 (4)施設・設備要件	本業務に参加する部署が ISO9001、ISO/IEC27001 の認定を受けていれば、保管する倉庫自体は認証が不要という認識でよろしいでしょうか。	外部倉庫にも ISO 条件が必要か確認し、提案の幅を広げたいため。	P27、P28	無	認識のとおりである。
49	1_調達仕様書	27	9 調達・導入条件 ②	本調達に係る費用として、機器のリース期間終了時のハードディスク等記録媒体のデータ消去費用は含まないことでよろしいでしょうか。 データ消去作業が必要な場合、「リース期間終了後に、機器のハードディスク等記録媒体のデータ消去を行うこと。データ消去の形式としては、DoD 方式または NSA 方式とすること」等、データ消去方法についての	展開作業計画の立案・ご提案・試算に係るため。		有	データ消去は本調達に含む。意見を踏まえ、以下の要件を追記する。  ----- 運用期間終了後に、機器のハードディスク等記録媒体のデータ消去を行うこと(消去証明書を提出すること)。データ消去の方法は、米国防総省規格(DoD 5220.22-M)相当の方



				指定の有無を記載いただけますでしょうか。				式又は復元不可能な状態まで粉砕すること。 -----
50	1_調達仕様書	28	9. 調達・導入条件	⑥に契約変更が必要となる場合について記載がありますが、既に導入いただいた機器等の費用変更は不可であることをご承知ください。	左記事項は一般的な提供業者の考え方のため、貴機構への注意喚起として、念のため記載いたしました。		無	意見内容と同じ認識である。
51	1_調達仕様書	28	9. 調達・導入条件	⑫「平成 33 年 12 月 31 日以降も利用する場合の保守費用については、本契約の保守費用を原則超えないこと」とありますが、利用期間の用途などはございますでしょうか。	延長保守の可否と保守金額の検討が必要なため。		無	現時点で利用(利用期間)の目処はない。延長保守を求める場合には、別途協議することとする。
52	1_調達仕様書	28	9 調達・導入条件 ⑮	搬入、据付を行うにあたり、平日、休日、業務時間外等作業時間帯に制約がある場合、記載いただけますでしょうか。 また、現地との調整が必要な場合、その旨を記載いただけますでしょうか。	展開作業計画の立案・ご提案・試算に係わるため。		有	搬入・据付作業の作業時間帯については、以下のとおり。 特許庁庁舎・三井ビル・近畿統括拠点(仮称)は、原則、平日夜間(業務時間外)または土日祝祭日とする。 それ以外の拠点は、業務時間内が望ましい。 なお、受注者は、作業時間帯等について情報・研修館と調整を行う。
53	1_調達仕様書	29	10. 応札者が閲覧できる資料一覧	資料閲覧について、いつ閲覧が可能かご教示願います。	本システムの検討のため。		無	入札公告時に提示する。
54	1_調達仕様書	全般		「情報・研修館の確認を受ける」との表現が散見されますが、承認を受ける必要があるものが含まれているため、確認と承認の使い分けが必要と考えます。	確認だけでは内容について発注者は賛同していない場合も想定されるが、仕様書では内容を精査し、それでよいと認めて合意する必要があるものまで確認となっているものがあるため。		有	意見を踏まえ、「確認を受ける」⇒「了承を得る」に表現を修正する。
55	1_調達仕様書	なし	なし	データセンター及びクラウドサービス活用により、従来の利用状況と比較して、レスポンスがダウンすることも考えられます。この事項に対する貴機構の考え方や対策をご教示いただけますでしょうか。	左記事項についての、貴機構の考え方に合致するサービスを選定し、提案するため。		無	レスポンスについては、記載した性能要件を満たした提案を行うこと。
56	①要件定義書(案)  ②別紙5 運用保守作業項目一覧  ③要件定義書(案)	① 33 頁  ② 2 頁	① 3.12 テストに関する事項  ② 項番 36 端末回収	①要件定義書(案) 33 頁 3.12 テストに関する事項 「個別業務システム「相談データベース」及び「窓口イントラ DB」の移行におけるテストを支援すること。」との記載がございしますが、具体的な支援内容についてご教授いただけますでしょうか。  ②要件定義書(案) 別紙5運用保守作業項目一覧 2 頁 36 端末回収 「端末の返納を申請した者から、該当の端末を郵送にて回収すること。」との記載がございしますが、郵送の手配は申請者と受託者のどちらが行うか、ご教授いただけますでしょうか。  ③要件定義書(案) 1 頁 図表 1-1-1 業務ごとの場	見積もりに必要なため		有	①について 調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。  ②について 端末の返納時の郵送の手配は、情報・研修館にて行う。  ③について 運用・保守業務の実施場所は、受注者の用意する施設・設備(またはデータセンタ)とし、発注者が用意することは行わない。

		③ 1 頁	③ 1.1 業務実施手順に関する事項 (3)業務の実施に必要な体制 図表 1-1-1 業務ごとの場所・利用者情報	所・利用者情報 情報基盤システムの運用保守 「場所:特許庁庁舎、利用時間帯:24 時間 365 日、人数:数名程度」との記載がございますが、要件定義書(案) 42～43 頁 3.16 運用保守に関する事項 (1)運転管理・監視等要件 「運用業務の受付時間及び作業時間は、開館日の 8:30～18:15 とすること。運用業務は受注者の用意する施設・設備(またはデータセンタ)にて実施すること。」との記載と異なります。 運用業務の対応時間に関する責務について、開館日の 8:30～18:15 の人の常駐要件と緊急時の自宅待機(オンコール)体制が必要かにより見積もりの基準が異なりますので、具体的な要件を仕様書上に明記いただけますでしょうか。 また、施設・設備についても発注者、もしくは受注者のどちらが準備するか、仕様書上に明記いただけますでしょうか。			対応時間について、開館日の 8:30～18:15 は、受注者が用意する施設・設備で運用保守業務を行い、それ以外の時間(障害発生等の緊急時)は電話によるエスカレーション対応を行い、緊急対応の必要性等を情報・研修館職員と協議の上、必要な対応を実施する。
57	2_要件定義書	1	1.1 業務実施手順に関する事項 (2)業務フロー図	現行業務について、参照するフロー図があることですが、ないものに関しては今後のシステム構築に向けて整備が必要と思われます。また、作成に当たっては、特定ベンダの記述方法にとられないようにすべく、BPMN 等標準的な記述法による業務フロー作成が必要と考えられます。	業務フロー図は参照元の内容にとられず、今後の再利用性にかんがみて BPMN での記載が必要と思われます。貴法人の所管省庁である特許庁の最適化事業においても、WFA ではなく、BPMN でのフロー作成となっております。	有	情報・研修館にて BPMN 等標準的な記述法に基づき業務フローを作成するが、機密情報が含まれるため、落札後に受注者のみに開示することとし、閲覧資料から除外することとする。
58	2_要件定義書	3	1.6 情報化に関する事項 (1)情報システム化の範囲	本調達のスコープ外になるものを明記すべきと考えます。	作業の抜け漏れを防ぐため。	無	別紙 3「情報基盤システムの全体概要図」で示す構成図においては、外部 SOC が対象外である。
59	2_要件定義書	4	2.2 画面に関する事項	「利用者のユーザビリティ及びアクセシビリティに配慮した上で、設計及び構築を行うこと」について、「利用者のユーザビリティ及びアクセシビリティに配慮すること」に変更願います。	「利用者のユーザビリティ及びアクセシビリティに配慮した上で、設計及び構築を行うこと」という表現は、スクラッチ開発や個別カスタマイズを求める要件と捉えることができます。 ユーザビリティ及びアクセシビリティに配慮したパッケージ製品を選定することにより、短納期対応やコスト圧縮が見込めるため、文言の変更をお願いします。	有	意見のとおり修正する。
60	2_要件定義書	5	3.1 ユーザビリティ及びアクセシビリティに関する事項 (2)ユーザビリティ要件	「図表 3-1-2 ユーザビリティ要件 項番 1 画面の構成」に記載の各要件について、以下のように記載変更願います。 「以下について極力配慮した製品を提案すること。 ・無駄な情報、デザイン及び機能を排し、簡潔で分か	画面の構成の各要件について、“～すること”という記載は、必須要件と捉えることができます。提案の観点という主旨という点を明確にしたいため。	有	意見のとおり修正する。

				りやすい画面 ・十分な視認性のあるフォント及び文字サイズ ・画面の大きさや表示位置の変更が可能 」				
61	2_要件定義書	5	3.1 ユーザビリティ及びアクセシビリティに関する事項 (2)ユーザビリティ要件 図表 3-1-2 項番 2	下記の要件を「補足」等に追加願います。  「各システムの運用管理画面については、シングルサインオン対応の対象外とするが、複数の主体認証に対応していること。」	提供サービス・機能一覧の「1 認証基盤サービス」の中に「(1)運用管理および監視で利用するサービスにおいては、セキュリティ強度を高める必要があるため、シングルサインオンは行わないこと。」とあり、各システムの運用管理等に必要な画面については対象外と認識しておりますが、当該内容の記載をお願いいたします。		有	意見を踏まえ、「要件定義書 3.1 ユーザビリティ及びアクセシビリティに関する事項 (2)ユーザビリティ要件 図表 3-1-2 項番 2」に利用者向け画面と運用管理用画面の要件は異なることを追記する。 ----- 情報基盤システムに求めるユーザビリティについての要件を以下に示す。なお、本要件は「図表3-1-1 情報システムの利用者の種類、特性」に示す情報基盤システムの利用者を対象とし、受注者が実施する運用保守等に係るユーザビリティは対象としない。 -----
62	2_要件定義書	5	図表3-1-2 ユーザビリティ要件 項2	「ID・パスワードなどを入力し一度認証を受けるだけで複数の異なるアプリケーションやシステムへアクセスできるようにシングルサインオン機能を設けること」との記載がありますが、シングルサインオンの実現はActiveDirectory 連携可能なソフトウェア・ハードウェアについてであれば、その旨の記載をお願いします。	全てのハードウェア・ソフトウェアにおいてシングルサインオンの実現を満たす構成は現実的に難しいため。シングルサインオン対象を明確にするか、「可能な限り」といった仕様の緩和をご検討願います。		有	意見のとおり修正する。
63	2_要件定義書	5	3.1 ユーザビリティ及びアクセシビリティに関する事項 (2)ユーザビリティ要件	「図表 3-1-2 ユーザビリティ要件 項番 3 指示や状態のわかりやすさ」は、削除願います。	「指示や状態のわかりやすさ」の各要件について、“～すること”という記載は、必須要件と捉えることができます。「指示や状態のわかりやすさ」については、現在記載の要件以外の方法(運用で回避する等)で満たすことができると考えます。提案の観点という主旨という点を明確にしたいため、現在の文言を削除願います。		有	意見を踏まえ、以下のように修正する。 ----- 以下について配慮した製品を提案すること。 ・ 操作の指示、説明、メニュー等には、利用者が正確にその内容を理解できる用語が使用されている。 ・ システムが処理を行っている間、その処理内容を利用者が直ちに分かる。 -----
64	2_要件定義書	42	図表 3-1-2 ユーザビリティ要件、図表 3-1-3 アクセシビリティ要件	当該項目は設計・構築対象システムのうち、エンドユーザが利用するもの(メール、ポータル文書管理、ファイルサーバなど)が対象と考えて良いかご教示頂きたい	仕様を明確にするため		無	認識のとおり、アクセシビリティ要件は情報基盤システムの利用者が利用するサービス・機能が対象となる。
65	2_要件定義書	6	3.1 ユーザビリティ及びアクセシビリティに関する事項 (2)ユーザビリティ要件	「図表 3-1-2 ユーザビリティ要件 項番 4 エラーの防止と処理」は、削除願います。	「エラーの防止と処理」の各要件について、“～すること”という記載は、必須要件と捉えることができます。「エラーの防止と処理」については、現在記載の要件以外の方法(運用で回避する等)で満たすことが		有	意見を踏まえ、以下のように修正する。 ----- 以下について配慮した製品を提案すること。 ・ 利用者が操作、入力等を間違えないようなデザインや案内を提供すること。

					できると考えます。提案の観点という主旨という点を明確にしたいため、現在の文言を削除願います。			<ul style="list-style-type: none"> <li>重要な処理については事前に注意表示を行い、利用者の確認を促すこと。</li> <li>エラーが発生したときは、利用者が容易に問題を解決できるよう、エラーメッセージ、修正方法等について、分かりやすい情報提供をすること。</li> </ul>
66	2_要件定義書	6	3.2 システム方式に関する事項 (1)情報システムの構成に関する全体の方針	<p>図表 3-2-1 に下記の記載があります。</p> <ul style="list-style-type: none"> <li>両ネットワークは物理的に分離され、異なる環境とする。</li> </ul> <p>ネットワーク仮想化技術を利用した論理的なネットワーク分離においても、十分にセキュリティを確保した上でコストメリットのあるネットワークの構築が可能となりますので、ネットワークについては論理的な分離での提案を許容頂けますようお願いいたします。</p> <p>上記を認めて頂ける場合、本意見招請で公開されたドキュメント全般に物理的な分離の表現がありますので、論理的な分離を許容する表現として頂くようお願いいたします。</p>	コスト最適化のため		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
67	2_要件定義書	7	3.3 規模に関する事項 (2)データ量	共有ストレージに、個人ストレージの容量は含まれませんでしょうか。 共有ストレージの“担当単位”と個人ストレージの“個人”は、別の物を指しますでしょうか。	共有ストレージおよび個人ストレージの要件を正しく理解し、システムを提案させていただくために確認させていただければと思います。		無	共有ストレージに個人ストレージの容量は含まれない。ただし、ストレージの筐体を同一にすることは可能とする。また、共有ストレージの“担当単位”と個人ストレージの“個人”は、別の物を指す。
68	2_要件定義書	7	3.3 規模に関する事項 (2)データ量	今後増加することも想定するべきと考えます。 (制度変更による人員や拠点の増減など) 但し、その場合、応札時の見積もりが高額にぶれることが懸念されるため、「制度変更等に伴う人員や拠点の増減等についても配慮した設計とすること。ただし構築後の当法人都合による契約条件の見直しが発生するレベルの環境変更においては、契約内容の見直しも含めた対応とする。」等の記載が必要と考えます。	5 年間の契約期間において現状のデータ量のみを前提にした設計は不適切と思われ、柔軟な対応が必要なことを前提にする必要があるため。		有	意見のとおり修正する。なお、利用者の増加は年間 5 名程度を想定している。組織変更等によりそれ以上に増える場合は対応方法について別途協議を行うこととする。
69	2_要件定義書	8	3.3 規模に関する事項	業務用サーバ提供サービス(業務系 NW 用)について、当初必要となるリソースを教えてくださいませんか。	見積りにあたり必要となるため		無	業務用サーバ提供サービス(業務系 NW 用)については現在用途が確定していないため、不要とする。提案においては将来的な個別システムの統合を考慮した拡張性を期待する。
70	2_要件定義書	8	3.3 規模に関する事項	メールの利用について、使用するアカウントの数はいくつになりますでしょうか？(メーリングリスト、組織メール含む)	見積りにあたり必要となるため		無	現時点で個人メールアカウントは約 250、組織メールは約 10、メーリングリストは 0(現時点でアカウント数が 0 であるが、必要な機能である)を想定している。なお、今後利用者が増加した場合にはアカウントも増加する。

71	2_要件定義書	8	3.3 規模に関する事項 (3)処理件数 図表 3-3-2 No.4	Web プロキシのデータ量の“件数”は具体的に何の件数となりますでしょうか。	見積りにあたり必要となるため		無	利用者による WEB サイトの閲覧回数の件数を示している。
72	2_要件定義書	8	3.3 規模に関する事項 (3)処理件数 図表 3-2-2 処理件数	「図表 3-3-2 処理件数」に記載の電子メール(個人)のデータ量はユーザ全員の合計という認識でよろしいですか。 電子メール(組織)のデータ量は登録している組織すべての合計でよろしいですか。	1 ユーザ、1 組織あたりのデータ量として捉えることも可能なデータ量であるため明確にしていればと思います。		無	認識のとおりである。
73	2_要件定義書	8	3.4 性能に関する事項 (1)応答時間	認証基盤サービス目標値 1 秒以内、クライアント PC サービス目標値 15 秒、25 秒の根拠はありますか？	利用者の体感的には遅いと感じることが多いと思われるため。		無	現行システムでの処理時間を基に設定した数値である。
74	2_要件定義書	9	3.4 性能に関する事項 (1)応答時間	全文検索機能(グループウェアサービス)の目標値はご提示いただくべきかと考えます。	検索性能はハードウェアの構成やソフトウェアを含むシステム方式設計に影響するものであり、検索機能の目標値を加味したシステム構成及び方式になっているか、提案評価に含める必要があるため。(落札後に決めるのではリスクが高いと思われます。)		無	検索性能については検索条件に依存するため、明確な目標値は設定しない。検索の効率性については提案とする。
75	2_要件定義書	9	3.4 性能に関する事項 (1)応答時間	WAN 回線、インターネット回線の目標値の根拠はありますか？	回線の性能は、サービスに必要な速度とする必要がありますが、それらが加味されているものか確認するため。		無	情報・研修館で検討した結果であり、要件の修正はなしとする。
76	2_要件定義書	9	3.4 性能に関する事項 図表 3-4-1 応答時間 項番 5	インターネット網内に対する目標値のご要望については取り下げ頂けませんでしょうか。	インターネット網は任意 ISP 網の集合体であり、本調達範囲(情報基盤システム)に含まれません。調達範囲外に対するご要件となっておりますので、取り下げをお願い致します。		有	意見を踏まえ、インターネット網内における応答時間の目標値は削除する。
77	2_要件定義書	10	3.5 信頼性に関する事項	インターネット回線について、「パケット損失率の目標値が 0.1%以下であることを追加願います。	インターネット回線の品質指標として、一般的な ISP では「可用性」「遅延時間」の他に「パケット損失率」の SLA を設定することが通常となっているためです。 回線が常時利用できていても、パケットロスが多いネットワークであれば信頼性において非常に問題です。費用に影響が出るものではないため、本項目の追加をお願いします。		有	意見を踏まえ、「要件定義書 3.5 信頼性に関する事項」にパケット損失率に係る目標値を追加する。
78	2_要件定義書	10	3.5 信頼性に関する事項 (1)	「図表 3-5-1 可用性に関する目標値 2 項 インターネット回線(バックボーン網内)の目標値 99.99%以上(24 時間 365 日の稼働における年間停止時間の合	各キャリアのインターネット回線の SLA としてインターネット回線(バックボーン網内)の可用性を設定して		有	意見のとおり修正する。

			ア可用性に係る目標値	計:0.9 時間)」と記載がありますが、削除をお願い致します。	いるキャリアが少ないため、提案の幅を広げるためにも本仕様の削除をお願い致します。		
79	2_要件定義書	10	図表3-5-1 可用性に関する目標値	項番 2.「インターネット回線」項番 3.「帯域確保型アクセス回線」について、指標である回線の稼働率目標値を 99.9%以上として頂くことを希望いたします。	当該回線種類に関する当社が定める SLA 条件が 99.9%以上となっており満たしていない為。	有	意見のとおり修正する。
80	2_要件定義書	10	3.5 信頼性に関する事項 (1)可用性要件	『目標値:99.99%、24 時間 365 日の稼働における年間停止時間の合計:0.9 時間』は項番3の帯域保障型アクセス回線について 99.99%、0.9 時間の目標値を対象外として頂きたい	冗長化構成とした場合でも実現困難と思われるため。	有	意見 No.79 を参照すること。
81	2_要件定義書	10	3.5 信頼性に関する事項 (1)可用性要件 ア可用性に係る目標値	「図表 3-5-1 可用性に関する目標値 3 項 帯域確保型アクセス回線の目標値 99.99%以上」を 99.9%に変更をお願い致します。	各キャリアの帯域確保型アクセス回線の SLA として可用性を 99.99%で設定しているキャリアはありません。提案できる回線がないため、変更をお願い致します。	有	意見 No.79 を参照すること。
82	2_要件定義書	10	3. 5 信頼性に関する事項 (1)可用性要件	帯域確保型のアクセス回線の目標値については、冗長化された回線のどちらかが稼働していれば問題ない認識でよろしいでしょうか。	要件確認のため。	無	認識のとおりである。
83	2_要件定義書	10	3. 5 信頼性に関する事項 (1)可用性要件 イ 可用性に関する対策	下記の記載があります。  ・可能な限り単一障害点のないシステム構成とし、可用性に係る目標値を達成するため、サーバをクラスタ構成とし、冗長化する等の対策を講じること。ただし、パブリッククラウドサービスにより提供されるものについては、「図表 3-5-1 可用性に関する目標値」を達成できれば必ずしもクラスタ構成による冗長化は必要としない。  上記は、オンプレ環境ではサーバはクラスタ構成必須、パブリッククラウドサービスでは可用性に係る目標値を達成できればクラスタ構成不要との記載に見受けられます。オンプレ、パブリッククラウドサービスどちらを提案するにしろ、可用性に係る目標値に対して、どのような冗長化手法を採用するかは各社の提案内容に依存するものと考えますので、仕様の記載を以下に緩和願います。 「可能な限り単一障害点のないシステム構成とし、可用性に係る目標値を達成するため、冗長化する等の対策を講じること」	仕様明確化のため	有	意見を踏まえ、以下のとおり修正する。 ----- 可用性に係る目標値を達成するため、冗長化する等の対策を講じること、可能な限り単一障害点のないシステム構成とすること。 -----
84	2_要件定義書	10	3.5 信頼性に関する事項 (1)可用性要件	可用性目標値のうち、メール機能について、受信と送信は別々に定義すべきと考えます。	送信は一定時間できなくとも、受信は、可能なかぎり稼働していることが求められることが多く、各々メールシステムでは別々のサービスが動いているため。	無	意見は採用しない。導入を想定している日本マイクロソフト社の Office365 をはじめ、メールの送信と受信の可用性に係るサービスレベルを合わせて設定しているクラウドサービスもあ

								ることを鑑み、送受信を合わせた可用性目標値とする。
85	2_要件定義書	10	3.5 信頼性に関する事項 (1)可用性要件	可用性に係る対策のうちサーバのクラスタ構成について、仮想化の場合は仮想化技術に依存しますが RAID の場合はモードの指定が必要になると考えます。	冗長構成は、サーバーに組み込まれたRAIDアプリケーションへの依存性により、単一障害となってしまうケースがあります。求める可用性によりRAIDモードを指定しておく必要があります。		無	記載の可用性要件を満たす内容で、受注者が RAID モード等を含めた構成を設計するものとする。
86	2_要件定義書	10	3.5 (1) イ	サービスレベルを満たすための手段として、機能に応じた適切な冗長化の手段を講じる、という認識でよろしいですか。	可用性を達成するための方式は、自由に提案可能である認識です。		無	認識のとおりである。
87	2_要件定義書	11	3.5 信頼性に関する事項 (2)完全性要件 2 ポツ目	“異常な入力や処理を検出し”は、データの改ざん検知機能を本システムに実装させ人為的な作業による異常の検知を要件としているという認識でよろしいでしょうか。 それとも異常な入力や処理は、不正プログラム(ウイルス)による異常動作を指し示していますでしょうか。	要件の理解のため。		無	後者((不正プログラム(ウイルス))等)を示している。
88	2_要件定義書	10	3.5 信頼性に関する事項 (1) (2)完全性要件	差分バックアップの条件(時間差等)を定義する必要があると考えます。	データの完全性を担保するため。		無	バックアップの方法は差分バックアップに限定していないため、意見は採用しない。
89	2_要件定義書	10	3.5 信頼性に関する事項 (1) (2)完全性要件	ログ等の証拠を残すとありますが、ログの種類を指定する必要があります。	保管する対象を明確にすることで、バックアップの容量を明確にするため。		無	保管するログの種類と期間は、要件定義書の図表 3-9-2「バックアップ対象データに関する目標復旧時点と保管期間」を参照すること。
90	2_要件定義書	11	3.5 信頼性に関する事項 (2)完全性要件	本要件(5 個の要件)は、サーバ上のデータに対してのみの要件である認識でよろしいでしょうか。	要件の理解のため。		無	認識のとおりである。
91	2_要件定義書	11	6.拡張性に関する事項 (2)機能の拡張性	機能拡張性の必要性が生じた場合は、検討から別途契約という理解でよろしいでしょうか。	本調達範囲の確認のため。		無	認識のとおりである。
92	2_要件定義書	11	3.6 拡張性に関する事項	拡張に伴う作業を行う場合、稼働中の情報基盤システムに極力影響を与えないよう考慮致します。しかし必要に応じてシステム停止等が必要になる可能性もありますので、ご調整頂きたく思います。	拡張作業に伴うリスクについて、ご承知いただきたいと考え、記載いたしました。		無	情報基盤システムの拡張時のシステム停止が必要になる場合には、事前に情報・研修館職員と影響内容について協議した上で、実施すること。
93	2_要件定義書	12	3.8 中立性に関する事項	デファクトスタンダードの条件を追記する必要があると考えます。	何らかの条件提示がないと、主観的な評価に基づくデファクトスタンダードの定義も認められかねないため。		無	要件の内容は「政府情報システムの整備及び管理に関する標準ガイドライン」に同様の記載があり、応札者共通の理解があるため、意見は採用しない。
94	2_要件定義書	12	3.8 中立性に関する事項	「他社に引き継ぐことが可能なシステム構成」とはどのような場合に、どのような社に引き継ぐことを指すかご教示頂きたい	仕様を明確にするため		無	情報基盤システムの利用者がシステムが提供するサービス・機能を活用して格納するデータ(メール、ドキュメント等)及び受注者が活用する第三者の SaaS 系サービスは、次の情報基盤システム・サービスの提供者に引継ぐことを想定している。

95	2_要件定義書	13	3. 8 中立性に関する事項	「情報基盤システム更改の際に、移行の妨げや特定の装置やシステムに依存する事を防止するため、原則として情報基盤システム内のデータ形式は XML、CSV 等の標準的な形式で取り出すことができるものとする。」との記載ですが、「可能な限り」等の記載の緩和をお願い致します。	本システムにおける全てのデータを XML、CSV として取り出す機能を設けることは困難と考えますので「可能な限り」といった仕様の緩和をご検討願います。		有	意見のとおり修正する。
96	2_要件定義書	13	3. 非機能要件の定義 3.9. 継続性に関する事項	大規模災害時の復旧目標値(72 時間)について、DR 要件含めて再検討いただきたい。	大規模災害を考慮すると損壊・被害が激しくて同じ場所(DC など)での復旧が物理的に不可能なことが考えられ新たに機能を提供するデータセンタ等へのインフラの復旧が必要となり、指定された時間内の復旧は困難と考える。 また、クラウドサービスについては SLA はあるが復旧作業についてこちらでは関与できないので 72 時間以内という時間は確約できないため。		有	大規模災害発生時の復旧目標時間については、クラウドサービスの提供範囲を含め、災害の内容や情報基盤システムへの影響度合い等を踏まえ、協議の対象とすることとする。
97	2_要件定義書	13	3.9 継続性に関する事項(2) 継続性に係る対策	一つ目の「(コールドスタンバイ)」の表記について、下記の通り修正願います。  ・変更前: 共通化した単位で予備機を設置(コールドスタンバイ)すること。 ・修正案: 共通化した単位で予備機を設置(コールドスタンバイ等)すること。	予備機は必ずしもコールドスタンバイである必要は無いと考えます。(インターネット接続に利用する NW 機器等についてはホットスタンバイを想定しております) コールドスタンバイに限定すると、障害対応の迅速性への影響が出るだけでなく、コスト増の要因になる可能性もあるため、要件の修正をお願いします。		有	意見 No.98 を参照すること。
98	2_要件定義書	13	3. 9 継続性に関する事項 (2) 継続性に係る対策	下記の記載があります。  ・受注者が用意するデータセンタに設置する機器については可能な限り共通化し、共通化した単位で予備機を設置(コールドスタンバイ)すること。  可用性に関する要件で、冗長化などの対策を行うこととの記載がございますので、冗長化している装置に関しては予備機の設置は過剰な投資と考えられます。コスト面からも本仕様に関しては削除もしくは、冗長化されていない装置に限定した要件に仕様変更をお願いします。	コスト最適化のため		有	意見を踏まえ、以下の要件は削除する。 ----- ・受注者が用意するデータセンタに設置する機器については可能な限り共通化し、共通化した単位で予備機を設置(コールドスタンバイ)すること。 -----
99	2_要件定義書	13	3.9 継続性に関する事項 (1) 継続性に係る目標値	MTTR と RTO の別に記載する必要があると考えます。	現状の記載だと平均値なのか、絶対値なのかが不明瞭なため。		無	意見は採用しない。目標値に示したような長時間の停止の発生頻度は低いと考えるため、目標復旧時間(RTO)のみ設定する。



100	2_要件定義書	13	3. 9継続性に関する事項 (1)継続性に係る目標値	「なお、パブリッククラウドサービスを利用し、下記に示すサービスを提供する場合には、目標値は情報・研修館職員と協議の上で決定するものとする。」という文章を追加するべきと考えます。	IaaS や SaaS といったパブリッククラウドサービスで障害が発生した場合、サービスの復旧作業に運用・保守作業者が介在できないケースが多く、クラウドサービスの提供者側に依存してしまうため。		有	意見のとおり修正する。
101	2_要件定義書	13	3.9 継続性に関する事項 (2)継続性に係る対策	コールドスタンバイについて、「MTTR 及び RTO 達成に必要なコールドスタンバイとすること」との記載が必要と考えます。	コールドスタンバイは、電源を入れて即時に使えるようにする場合と、商品梱包したままの状態、一定の構築が必要な場合があり、復旧にもとめる条件によって、対応が違うため。		有	No.98 の意見を踏まえ、冗長化した機器の予備機の設置は不要とした。これを踏まえて、以下のとおり修正する。 ----- 予備機を設置する場合は、目標復旧時間を満たす方法で設置等の対応を行うこと。 -----
102	2_要件定義書	13	3.9 継続性に関する事項 (2)継続性に係る対策	バックアップ処理の設計について、オンラインバックアップが必要な構成を指定する必要があると考えます。	本調達のスコープに含まれるシステム全てにおいてオンラインバックアップが必要ではないと思われ、コスト抑制のため。		有	意見 No.103 を参照すること。
103	2_要件定義書	14	3.9 継続性に関する事項 (2)継続性に係る対策	下線の追加をお願いいたします 『情報システムの設置場所が完全に消失した場合に備え、テープ装置、ストレージ、クラウドサービスが提供するバックアップサービス等を利用し、バックアップデータを』	製品選定の幅を広げるため。 テープ装置に比べて復旧速度を早められる仕組みを利用できるため。		有	意見を踏まえ、バックアップ方法は応札者の提案とし、要件定義書の「3.9. 継続性に関する事項」の一部記載を以下に修正する。 ----- 障害や大規模災害等により情報システムの設置場所が完全に滅失した場合に備え、テープ装置、ストレージ、クラウドサービスが提供するバックアップサービス等を利用し、バックアップデータを月次で保管・取得すること。ただし、DR(Disaster Recovery)サイトの構築は不要とする。 -----
104	2_要件定義書	14	3.9 継続性に関する事項 (2)継続性に係る対策 図表3-9-2 5 ポツ目	「・・・テープ装置にバックアップデータを月次で保管・取得し、・・・」について、  上記項目のうち、Office365 等クラウドサービス (Exchange Online や Sharepoint Online 等)については、クラウド to クラウド等のバックアップでも可としていただけますでしょうか。	クラウドサービスのデータをオンプレミスに保存するソリューション等の実現方法が難しいため。		有	意見 No.103 を参照すること。
105	2_要件定義書	14	3.9 継続性に関する事項 (2)継続性に係る対策 図表3-9-2 6 ポツ目	「・・・テープ装置にバックアップデータを月次で保管・取得し、・・・」について、別添資料 1 に例示されている Office365(Exchange Online)のメールデータは、対象外としていただけますでしょうか。	別添資料 1 に例示されている Office365(Exchange Online)は、サービス契約者によるバックアップの取得が可能な仕様となっています。		有	意見 No.103 を参照すること。
106	2_要件定義書	14	3.9 継続性に関する事項	「・・・テープ装置にバックアップデータを月次で保管・取得し、・・・」について、別添資料 1 に例示されている	別添資料 1 に例示されている Office365(Sharepoint Online)は、		有	意見 No.103 を参照すること。

			(2) 継続性に係る対策 図表3-9-2  6 ポツ目	Office365(Sharepoint Online)のスケジュールデータは、対象外としていただけますでしょうか。	サービス契約者によるバックアップの取得が可能な仕様となっております。			
107	2_要件定義書	14	3. 9 継続性に関する事項 (2)継続性に係る対策	「テープ装置にバックアップデータを月次で保管・取得し、設置場所から 100KM 以上離れた場所に保持すること」との記載がございますが、テープ以外の媒体でもよければ、「不揮発な外部媒体に」という表現に変えることをお奨めします。	テープ媒体以外での BCP 対策についてのご提案の可能性を確認したいため。		有	意見 No.103 を参照すること。
108	2_要件定義書	14	3.9 継続性に関する事項 (2)継続性に係る対策	障害や大規模災害等により情報システムの設置場所から完全に消失した場合に備え、テープ装置にバックアップを月次で保管取得し、設置場所から 100km 以上離れた場所に保管することとあるが、距離の緩和をお願いいたします。	100kmの距離だと、災害時の交通網状況により復元が困難と考えるため。		無	意見 No.103 も踏まえ、バックアップ方法によらずバックアップデータは情報システムの設置場所から 100km 以上離れた場所に保管すること。なお、災害時の交通網状況については、「要件定義書 3.16 運用・保守に関する事項」にて「災害発生時における交通インフラの麻痺等に起因する、運用保守要員の保守拠点への不達」は免責事項としているため、意見は採用しない。
109	2_要件定義書	14	(2)継続性に係る対策	「ネットワーク機器については、基本的に冗長構成とする。ただし、内部的に冗長化の構成となっている機器を導入する場合は、冗長化部品の障害時における交換の際にも、システムを停止せずに行えること。」とありますが、記載中の「ネットワーク機器」について、回線終端装置、WAN ルータ、モバイル接続ルータも含みますでしょうか。	コールドスタンバイ機を用意する場合、費用が変更となる為。		無	回線終端装置、WAN ルータ、モバイル接続ルータは冗長構成の対象外である(WAN ルータ以下の NW 機器は冗長構成の対象とする。LAN の冗長構成は不要である)。
110	2_要件定義書	14	3.9 継続性に関する事項 (2)継続性に係る対策 9 ポツ目	ネットワーク機器の冗長化の適応範囲について、端末が直接接続されるハブや無線アクセスポイントは、冗長化の要求の範囲外という認識でよろしいでしょうか。	要件の理解のため。		無	認識のとおりである。
111	2_要件定義書	14	3. 9 継続性に関する事項 (2)継続性に係る対策	下記の記載があります。  ・電源、ハードディスク及びファンは基本的に冗長化構成とする。なお、負荷分散構成等により、機能が冗長化されている場合や、ファンレス等で物理的に部品が存在しない場合は冗長化構成としなくても良い。ただし、内部的に冗長化の構成となっている機器については、冗長化部品の障害時における交換の際にも、システムを停止せずに行えること。  ・ネットワーク機器については、基本的に冗長化構成とする。ただし、内部的に冗長化の構成となっている機器を導入する場合は、冗長化部品の障害時における交換の際にも、システムを停止せずに行えること。	仕様明確化のため 製品選定の幅を広げるため		有	意見を踏まえ、ネットワーク機器に関する要件を以下のとおり修正する。  -----  ・ネットワーク機器については、基本的に冗長化構成とする。ただし、内部的に冗長化の構成となっている機器であれば冗長化は必須としない。また、内部的に冗長化の構成となっている機器については、冗長化部品の交換の際に、システムを停止せずに行えること。  -----

				<p>上段がサーバ、ストレージに関する要件、下段がネットワーク機器に関する要件だと認識しており、サーバ、ストレージについては、下記の要件が記載されているかと思えます。</p> <p>○基本的に装置内部部品(電源、ハードディスク、ファン)の冗長化を行うこと</p> <p>○装置内部部品の障害時における交換作業はシステムを停止せず行えること。</p> <p>○負荷分散等により装置を冗長化している場合は、装置内部部品の冗長化は必須ではない。</p> <p>対して、下段のネットワーク機器に関しては、以下の記載に見受けられます。</p> <p>○基本的に装置を冗長化すること。</p> <p>○装置内部の部品(電源、ファンと想定しています。)を冗長化している製品を提案する場合、装置内部の部品の障害時における交換作業はシステムを停止せず行えること</p> <p>ネットワーク機器について、装置内部部品(電源、ファン)の冗長化が必須となるのか判断がつきませんでしたので、仕様への明記をお願いします。なお、ネットワーク機器については、装置の冗長化が基本要件となっておりますので、サーバやストレージと同様に装置内部部品(電源やファンを想定)の冗長化については必須ではないとした方が製品選定の幅が広がりますのでお勧めいたします。</p>			
112	2_要件定義書	14 (1 5)	3.10 情報セキュリティに関する事項	記載された対策を受注者が必ず実施することを求めている訳ではない、とありますが、必須項目と望ましい(提案審査において加点となる要素等)の別は定義する必要がありますと考えます。	要求の捉え方が応札者によって異なる結果となり、入札金額に大きく差が出て適切な評価が行えず、調達が成立しないおそれがあるため。	有	意見を踏まえ、図表 3-10-1「情報セキュリティ対策要件」を見直し、必須要件と望ましい要件が識別できるように記載することとする。ただし望ましい要件については、コストメリットを担保する対策を提案すること。
113	2_要件定義書	14 (1 5)	3.10 情報セキュリティに関する事項	準拠する対象に、NISCの「高度サイバー攻撃対処のためのリスク評価等のガイドライン」を含むべきと考えます。	本意見招請前の 2016 年 10 月にリリースされたガイドラインであり仕様書に記載のあるガイドライン同様遵守する必要があるため。	有	当調達のスコープだけでは「高度サイバー攻撃対処のためのリスク評価等のガイドライン」の全ての対策を適用することはできないが、調達スコープに該当する対策は適用する必要があるため、参照する法令等として定めることとする。
114	2_要件定義書	15	3.10 情報セキュリティに関する事項	将来的に利用を想定されている外部 SOC について、調達予定時期をご教示いただけますでしょうか。また利用予定のサービス内容を本頁に記載すべきだと考えます。	外部 SOC は本調達範囲外であると認識しておりますが、将来的に本システムとの連携が必要であり、それを踏まえたセキュリティ対策要件であることを本頁で提示すべきだと考えます。	無	平成 30 年 1 月の情報基盤システムの稼働時に、外部 SOC も同時に利用・稼働する予定である。なお、外部 SOC で利用予定のサービス内容は、セキュリティ上の観点から本仕様書上では公開しないが、落札業者決定

								後に情報・研修館が情報提供する。
115	2_要件定義書	15	3.10 情報セキュリティに関する事項	上記と関連して、外部 SOC 導入の際の改修作業については、本調達に含まない理解してよろしいでしょうか。	要件・作業が不確定のため、左記作業の提案は不可能であると考えたため。		無	外部 SOC 導入に際しては、受注者は要件定義書「3.11. 情報システム稼働環境に関する事項」の「(4)施設・設備要件」で示す内容に対応することとしている。
116	2_要件定義書	15	3.10 情報セキュリティに関する事項 図表3-10-1 対策区分:侵害対策 対策方針:通信回線対策 要件名称:通信経路の分離	『物理的に分離された業務系 NW から機密性情報系 NW』について、『物理的』だけではなく『論理的』な分離においても認めて頂きたい。	論理的な分離であってもセキュリティ面での効果としては同様と考えます。結果として、製品選定の幅、コスト削減の可能性を広げます。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
117	2_要件定義書	15	3.10 情報セキュリティに関する事項 図表 3-10-1 不正通信の遮断	下記内容を追加願います。  「ファイアウォールの通信ログを解析し、通信傾向を学習したうえで、通常の通信状況とは異なる変則的な通信が発生した場合に、異常として検知し、通知すること。」	一定のしきい値を設けてそれを超えたら異常と判断することは容易ですが、時間帯や平日・休日の違いなどでも組織毎の業務の特性により通信傾向は異なります。そのため、日常の通信傾向を学習し、通常と大きく異なるトラフィックがあった際は異常として検知することで、いち早く異常を検知することが可能です。 通常、ISP 等のサービスとして無償で提供される機能であるため、コストの増加もなく、セキュリティレベルを大きく向上させることが可能です。		無	必須の要件とする必要はないと判断し、意見は採用しない。
118	2_要件定義書	14 (1 5)	3.10 情報セキュリティに関する事項 図表 3-10-1 情報セキュリティ対策要件	不正通信の遮断については、通信経路において機器別に遮断方法として手動、自動の識別をしたうえで対策がをする必要があり、また遮断や隔離の設定を行う根拠をえるため、情報リスクアセスメントを行い、それに基づく設定が必要なことを追記すべきと考えます。	情報資産や情報流通経路(どんな情報がどこを流れているのか)を把握した上でないと、業務運用上無理のない遮断設計を行えないため。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
119	2_要件定義書	15	3.10 情報セキュリティに関する事項	「図表 3-10-1 情報セキュリティ対策要件 要件名称:不正通信の遮断」について、 「ファイアウォール等の機器を通過するパケットのデータを読み取り、内容により動的にポートを開放・閉鎖する機能を備えること」とありますが、下記の文言へ変更いただけませんか。 「ファイアウォール等の機器を通過するパケットのデータを読み取り、セキュリティ上の脅威を検出した場合に	当該項は不正通信の遮断を目的としているという理解です。 一般に UTM 製品では、パケットのデータ内にセキュリティ上の脅威を検出した場合、ポート単位ではなく通信そのもの(コネクション)を遮断する動きとなります。 ポート単位での遮断・閉鎖という動作の場合、脅威の含まれない通信		有	意見を踏まえ、図表 3-10-1「情報セキュリティ対策要件」の「不正通信の遮断」に以下のとおり修正する。 ----- ファイアウォール等の機器を通過するパケットのデータを読み取り、内容により動的にポートを開放・閉鎖する機能を備えること。 機器を通過するパケットのデータを読み取り、セキュリティ上の脅威を検出した場合に当該

				当該通信を遮断する機能を備えること」	まで遮断することとなり、業務への影響が懸念されるため、要件として避けるべきと考えます。		通信を遮断する機能を備えること。 -----
120	2_要件定義書	16	図表3-10-1 情報セキュリティ対策要件 サービス不能化の防止	「…なお、通信キャリア側での対策を行うなど、情報システムに対する広範囲かつ多様な DDoS 攻撃に対処可能であること」とありますが、DDoS 対策は公開サーバが LAN 内にない場合でも必要になるかどうか、明確なご記載を頂くことを希望いたします。	DDoS 対策付加が可能な回線サービス種別は限られる為。	有	意見を踏まえ、以下のとおり修正する。 ----- なお、通信キャリア側での対策を行うなど、情報システムに対する広範囲かつ多様な DDoS 攻撃に対処可能であることが望ましい。 -----
121	2_要件定義書	14 (1 6)	3.10 情報セキュリティに関する事項 図表 3-10-1 情報セキュリティ対策要件	サービス不能化の防止のうち DDoS 攻撃の対処には、ネットワークレベルとサーバ及びアプリケーションレベルの別に DDoS 攻撃への対処が必要なことを追記すべきと考えます。	近年はネットワークレベルの攻撃より Webサーバなどのアプリケーションレベルの攻撃が増えているため。	無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
122	2_要件定義書	16	図表 3-10-1 情報セキュリティ対策要件 侵害対策 不正プログラム対策 不正プログラムの感染防止	以下について、具体的にご教示ください。  不正プログラム(ウイルス、ワーム、スパイウェア、ボット等)による脅威に備えるため、想定される不正プログラムの感染経路の全て(サーバ装置及びエンドポイントを含む。対策に使用するソフトウェアはサーバとエンドポイントとは異なるものを使用すること。)  下線部にある”異なるもの”とは、メーカーが異なることを意味するのか或いは、製品が異なることを意味するのかご教示ください。	要求仕様を明確にする為です。	有	意見 No.125 を踏まえ、対策に使用するソフトウェアはサーバとエンドポイントとは異なるものを使用することは必須の要件からは削除し、記載を以下に修正する。 ----- 不正プログラム(ウイルス、ワーム、スパイウェア、ボット等)による脅威に備えるため、想定される不正プログラムの感染経路の全て(サーバ装置及びエンドポイントを含む。)において感染を防止する機能を備えるとともに、新たに発見される不正プログラムに対応するために機能の更新が可能であること。 -----
123	2_要件定義書	16	3. 10 情報セキュリティに関する事項 図表3-10-1 情報セキュリティ対策要件 不正プログラム対策の管理	「システム全体(サーバ及びエンドポイント)として不正プログラムの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。」とあるが、「不正プログラムの感染防止」にて、「対策に使用するソフトウェアはサーバとエンドポイントとは異なるものを使用すること」と記載されており一元管理が難しいと考えます。	要件確認のため。	有	意見 No.122 を参照すること。
124	2_要件定義書	16	図表3-10-1 情報セキュリティ対策要件 侵害対策 不正プログラム対策 不正プログラムの感染防止	「対策に使用するソフトウェアはサーバとエンドポイントとは異なるものを使用すること」と記載がございますが、NW 分離している背景もあり費用増となる一方、効果も薄いと考えられます。「サーバ及びエンドポイントとゲートウェイで異なる製品」としてはいかがでしょうか。	提示価格低減のため	有	意見 No.122 を参照すること。
125	2_要件定義書	16	3.10 情報セキュリティに関する事項	「図表 3-10-1 情報セキュリティ対策要件 要件名称:不正プログラムの感染防止」の「サーバとエンドポイントとは異なるものを使用すること」について、“異なるもの”は、“ソフトウェアが異なるもの”という認識でよろ	昨今のセキュリティ対策として標的型攻撃に対抗する仕組みの導入を考えると、入口/出口/内部の3点の対策が軸になると考えていま	有	意見 No.122 を参照すること。

				しいでしょうか。 “メーカーが異なる”という場合、セキュリティ対策の運用面および異常時のメーカー含む一連の対応について考慮した場合、サーバとエンドポイントの対策ソフトのメーカーを分けるべきではないと考えます。 複数メーカーによる対策で、不正プログラム対策の漏れを補うことを考えているならば、「入口出口対策と内部対策を行うソフトまたはハードを、異なるメーカーにすること」としたほうが効果的と考えます。	す。3点の軸に沿った仕様とすることで、提案の幅を広げると考えます。“マルチベンダでの対策”を適用する部分を変更いただきたいです。			
126	2_要件定義書	16	3.10 情報セキュリティに関する事項	「図表 3-10-1 情報セキュリティ対策要件 要件名称: 不正プログラムの感染防止」の「受信メールについて、未確認添付ファイルや～省略～対処する機能を備えること」について、Web アクセスについても同様の要件を追加いただいたほうがよいと考えます。	標的型攻撃への対抗としての手段を設けるための要件と認識しています。標的型攻撃への対抗としては、受信メールの添付ファイルの開封以外に、メールの添付ファイル以外に、メール本文の疑わしい URL へのアクセスも対策すべきと考えます。		有	意見のとおり修正する。
127	2_要件定義書	16	3. 10 情報セキュリティに関する事項 図表3-10-1 情報セキュリティ対策要件 不正プログラムの感染防止	未知のマルウェアなどを実行するサンドボックス環境をご要望の場合、その旨を追記いただきたい。自由提案の場合は不要です。	要件確認のため。		無	必須要件ではないため、要件の修正は行わないこととする。
128	2_要件定義書	16	図表 3-10-1 情報セキュリティ対策要件 侵害対策 不正プログラム対策 不正プログラムの感染防止	以下の文言を追加することをご提案いたします。  修正前) 受信メールについて、未確認添付ファイルや疑わしい添付ファイルの振る舞いをチェックし、対処する機能を備えること。  修正後) Web 及びメールウイルス対策について、サンドボックス機能を有する仕組みまたは、サービスを提供すること。	今日までに公表されているインシデント事例を鑑みますと、未知のウイルスが端末まで到達してしまった場合、端末側での対処がしきれず、組織内部に拡大感染してしまうケースが多い為、可能な限り事前に防御できる対策が必要です。		無	必須の要件とする必要はないと判断し、意見は採用しない。
129	2_要件定義書	16	図表 3-10-1 情報セキュリティ対策要件 侵害対策 不正プログラム対策 不正プログラムの感染防止	以下の文言を追加することをご提案いたします。  メールセキュリティについて拡張子やファイルタイプの制限ができる機能を提供すること。また、拡張子やファイルタイプの検査にあたっては Zip 形式等の圧縮ファイルに格納されていても検知できる機能を有すること。	標的型メールに添付される可能性がある拡張子やファイルタイプを予め制限しておくことで、サイバー攻撃からのリスクを低減する効果があります。また、新たな攻撃手法が見つかった際、早期に対策を図ることが可能になります。		無	必須の要件とする必要はないと判断し、意見は採用しない。
130	2_要件定義書	14 (2 0)	3.10 情報セキュリティに関する事項	委託先において不正プログラム等が組み込まれることへの対策について、対策の実施例として「導入時及び	委託先の体制を確認するだけでは、不正プログラム等が組み込ま		有	意見のとおり修正する。受注者は、システム稼働前に1度、稼働開始から稼働終了まで

			図表 3-10-1 情報セキュリティ対策要件	定期的なペネトレーションテストの実施」を追記すべきと考えます。	れることへの対処にはなっていないため。		年1回、脆弱性診断を行う。なお、第三者による検査も別途調達し実施予定である。
131	2_要件定義書	17	3.10 情報セキュリティに関する事項	「図表 3-10-1 情報セキュリティ対策要件 要件名称: 運用時の脆弱性対策」について、ソフトウェアを貴館にて予め指定されている「別紙 2 提供機能・サービス一覧 3.クライアントソフトウェアサービス」に記載のソフトウェアについては、明記願います。	検討の必要があるソフトウェア(特に貴館で指定されているソフトウェア)を明記いただくことで、提案の範囲を明確にさせていただきたいと考えます。	無	「別紙 2 提供機能・サービス一覧 3.クライアントソフトウェアサービス」に記載のソフトウェアだけでなく、サーバ機能を構成するソフトウェアも含め、導入する全てのソフトウェアを対象とする。
132	2_要件定義書	17	3.10 情報セキュリティに関する事項	「図表 3-10-1 情報セキュリティ対策要件 要件名称: 運用時の脆弱性対策」について、脆弱性対策としては、貴館が認めていないインターネット上の情報(URL等)へのアクセスをさせないことも必要と考えます。	必須とすべきセキュリティ対策の不足が見られるため、要件を追加願います。	有	意見 No.136 を参照すること。
133	2_要件定義書	17	図表 3-10-1 情報セキュリティ対策要件 侵害対策 脆弱性対策 運用時の脆弱性対策	以下の文言を追加することをご提案いたします。  重要サーバ(特に AD、DNS、ファイル)については、堅牢性と安全性を十分考慮すること。	昨今の標的型攻撃手法として PsExec コマンド等の Windows 標準のコマンドを利用して、アクセスを試みる為、気付きづらい状況にあります。その為、通常運用時よりもログイン試行の回数が多い、ログイン失敗の回数が多い等しきい値を決め、早期に異変に気付く機能が必要であると考えます。	無	特定のサーバではなく情報基盤システム全般に対する要件を記載済であるため、必須の要件とする必要はないと判断し、意見は採用しない。
134	2_要件定義書	17	図表 3-10-1 情報セキュリティ対策要件 侵害対策 脆弱性対策 運用時の脆弱性対策	以下の文言を追加することをご提案いたします。  アプリケーションの脆弱性が発覚し、メーカから正式なパッチが提供され、本番環境への適用が完了するまでの期間において、影響を極小化する方法がある場合は、積極的に採用すること。	ゼロデイ攻撃への対策として、アプリケーションの脆弱性を狙った攻撃に対して、メーカから提供される正式なパッチの適用完了までの間、一時的にでもセキュリティリスクを攻撃者にさらすことになる為、一次対処となる方法を積極的に取り入れる必要であると考えます。	有	意見を踏まえ、「図表 3-10-1 情報セキュリティ対策要件」の「運用時の脆弱性対策」に以下を追記する。 ----- アプリケーションの脆弱性が発覚し、メーカから正式なパッチが提供され、本番環境への適用が完了するまでの期間において、影響を極小化する方法がある場合は、積極的に採用すること。 -----
135	2_要件定義書	17	図表 3-10-1 情報セキュリティ対策要件 侵害対策 脆弱性対策 運用時の脆弱性対策	以下の文言を追加することをご提案いたします。  Microsoft Office、Aobe PDF、Flash などの一般的なアプリケーションに加え、一太郎などの日本独自のアプリケーションへの脆弱性対策を考慮した対策を講じること。	Microsoft Office 等の一般的なアプリケーションに加えて、一太郎等の公文書に利用されているアプリケーションに対する脆弱性コードを狙った攻撃への対策が必要であると考えます。	無	必須の要件とする必要はないと判断し、意見は採用しない。
136	2_要件定義書	17	図表 3-10-1 情報セキュリティ対策要件 侵害対策 脆弱性対策 運用時の脆弱性対策	以下の文言を追加することをご提案いたします。  業務上、許可されていないオンラインストレージサービスやファイル共有サービスへのアクセス、SNS への書	組織内部から組織外部への情報の持ち出し等による情報漏洩を防止する対策が必要だと考えます。	有	意見を踏まえ、「図表 3-10-1 情報セキュリティ対策要件」の「不正通信の遮断」の一部記載を以下に修正する。 ----- WEB フィルタリング機能により、業務上許可さ

				き込み等を制限する機能を提供すること。				れていない、または悪意のある WEB サイトとの通信を検知し、遮断すること。フィルタリングデータベースは定期的に最新化され、緊急性を要する場合には、即時に情報を反映させる緊急配信機能を備えること。 -----
137	2_要件定義書	17	3.10 情報セキュリティに関する事項	脆弱性対策の実施例について、「脆弱性診断」と記載がありますが、脆弱性診断は本調達外とし、別件として調達するべきだと考えます。	本調達システムは、平成 30 年 1 月に新たに稼働するシステムであり、適切な脆弱性対策という観点から、より第三者による検査実施が重要だと考えます。よって左記事項をご提案いたします。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。受注者は、システム稼働前に 1 度、稼働開始から稼働終了まで年 1 回、脆弱性診断を行う。なお、第三者による検査も別途調達し実施予定である。
138	2_要件定義書	17	図表 3-10-1 情報セキュリティ対策要件 不正監視・追跡 ログの管理	ログ管理の対策実施例として、補足資料①と②でご案内するクラウドを活用した脅威分析、システム保護に関する機能要件も検討すべきと考えます。	日々高度化する標的型攻撃に対し、防衛側もクラウドサービスを活用して随時防衛能力を向上させることができるため。	補足資料 ① Office 365 Advanced Security Management 概要 コミュニケーション系など監視 補足資料 ② Windows Defender Advanced Threat Protection 概要 クライアント PC 系の監視	有	①必須の要件としての変更の必要はないと判断し、意見は採用しない。 ②一部意見を採用し、修正する。
139	2_要件定義書	17	図表3-10-1 情報セキュリティ対策要件 不正監視・追跡 ログ管理 ログの蓄積・管理	「クラウドサービスを活用する場合は、クラウドサービスで記録し公開するログについて、保管期間中はデータセンターにコピー・保管するなどして退避させること。」と記載がございますが、「公開するログ」について、種類と想定データ量等の記載を仕様書にてご提示願います。	ディスクサイジング及び、クラウド利用料金に関連するため。		無	ログの種類と量は、受注者が活用するクラウドサービスにより異なるため、活用するクラウドサービスを踏まえてサイジングを行うこと。
140	2_要件定義書	18	3.10.情報セキュリティに関する事項 図表 3-10-1 内 主体認証	「PIN 及び生体認証の方式を採用し」とありますが、「PIN 及び生体認証等」の方式を採用しに変更をお願いします。	生体認証要件はコスト増に直結する要件であるうえ、複数要素の主体認証とした場合でもセキュリティレベルは下がらないと考えます。		無	当該認証方式については OS の機能を活用することを想定しており、必須の要件とする必要はないと判断し、意見は採用しない。
141	2_要件定義書	18	3. 10 情報セキュリティに関する事項 図表3-10-1 情報セキュリティ対策要件 機密性・完全性の確保	要件「通信経路上の盗聴防止」の対策要件にて「データセンター（業務系 NW）とクラウドサービス間の通信は、閉域網または IPsec 等により暗号化されたインターネット回線とする」とあるが、別紙 4 のとおりインターネット回線で接続する際の暗号化については SSL/TLS で問題ない理解でよろしいでしょうか。	インターネット接続にてクラウドサービスを利用する際は、IPsec ではなく SSL/TLS にて暗号化されるのが一般的と考えるため。		無	認識のとおりである。なお、意見 No.143 も参照すること。



142	2_要件定義書	18	3. 10 情報セキュリティに関する事項	要件「通信経路上の盗聴防止」の対策の実施例にて「IPsec による IP レベルでの暗号化」とあるが、こちらの記載は、アクセス回線にインターネットなどの公衆網を活用する場合を想定しており、主要拠点向けの閉域性を確保するアクセスの場合は、IPsec による暗号化は不要との理解でよろしいでしょうか。	アクセス回線部分を暗号化することで、閉域回線サービスとの機能重複が発生し、コスト増の要因となる。 各拠点に設置するネットワーク機器間で IPsec による暗号化を実施した場合、クラウドサービスを閉域接続した場合の通信経路が実現できない可能性があるため。		無	認識のとおりである。
143	2_要件定義書	18	対策区分: データ保護 対策方針: 機密性・完全性の確保 要件名称: 通信経路上の盗聴防止	「データセンター(業務系 NW)とクラウドサービス間の通信回線は、閉域網または IPsec 等により暗号化されたインターネット回線とする。」とありますが、セキュリティ強化の観点から閉域網での接続を必須とすることを推奨します。	業務データが流れる回線であり、セキュリティの確保が必要と考えます。  各拠点とデータセンター間は閉域網で接続するのに対して、パブリッククラウドとデータセンター間が IPsec で接続することはポリシーとして矛盾しており、業務用 NW の通信フロー全体としてはセキュリティレベルが著しく低下するため、閉域網の要件を必須とすべきであると考えます。		有	意見を踏まえ、図表 3-10-1「情報セキュリティ対策要件」の「通信経路上の盗聴防止」を以下のとおり修正する。 ----- ・データセンター(業務系 NW)とクラウドサービス間の通信回線は閉域網が望ましいが、IPsec 等により暗号化されたインターネット回線も許容する。 -----
144	2_要件定義書	18	図表3-10-1 情報セキュリティ対策要件 データ保護 機密性・完全性の確保 通信経路上の盗聴防止	「データセンター(機密性情報系 NW)と拠点間は、閉域網とする」と御座いますが、ここでのアクセス回線に対し地域 IP 網の使用が可能かどうかの記載を頂くことを希望します。 地域 IP 網とは、利用者が限られた地域に限定された公衆ネットワーク網(共有網)となります。共有網の為、当該区間での通信は IPsec による暗号化を施します。	地域 IP 網利用可否により費用が変更となる為。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
145	2_要件定義書	19	3.10 情報セキュリティに関する事項 図表3-10-1 対策区分: データ保護 対策方針: 機密性・安全性の確保 要件名称: 保存情報の機密性確保	『s/MIME 機能を備えること』については、メール本文ままで暗号化可能な数少ない仕組みではありますが、添付ファイルの暗号化と閲覧対象の限定ができれば十分と考えます。 要件を「添付ファイルの暗号化と閲覧対象の限定機能を備えること」に緩和をお願いします。	GPKI 以外から証明書を購入する場合、非常に高価な構成となります。また、メール送付先のメーラが s/MIME に対応し証明書を持つ必要があります。不特定多数の送付先を想定した場合、送付先に証明書が無い時には、暗号化できずデジタル署名によるなりすまし対策にしかありません。		無	「政府機関の情報セキュリティ対策ため統一基準(平成 28 年度版)」の「府省庁対策基準のためガイドラン(平成 28 年度版)」において、電子メールに関する基本対策事項のひとつとして、S/MIME 等の電子メールにおける電子署名の技術を利用する旨の記載もあり、必須の要件として変更する必要はないと判断し、意見は採用しない。なお、活用を想定している Office365 は S/MIME に対応している(機能を備えている)。
146	2_要件定義書	19	3.10 情報セキュリティに関する事項 図表 3-10-1 保存情報の機密性確保	・5 つ目について、下記要件の変更をお願いいたします。  ・現在: メール送信時に、誤送信防止のポップアップアラートの表示及びファイル暗号化の有無を選択する機	メール送信に関するポリシーは、組織内で統一する必要があると考えます。  現在の要件表記のままですと、ユ		有	意見を踏まえ、図表 3-10-1「情報セキュリティ対策要件」の「保存情報の機密性確保」を以下のとおり修正する。 ----- ・メール送信時における誤送信防止のための

				<p>能を備えること</p> <p>・変更案:管理者が、メール送信時における誤送信防止のための送信保留機能及びファイル自動暗号化の有無を選択する機能を備えること</p>	<p>一々が誤送信防止機能の利用やファイル自動暗号化の有無をメール送信の都度自由に選択可能であるように読み取れるため、セキュリティレベルの統一化および向上のため、管理者が一括で設定可能であるという形に変更をお願いします。</p>		<p>ポップアップアラートの表示又は送信保留機能を備えること。</p> <p>・メール送信時におけるファイル自動暗号化の有無を選択する機能を備えること。</p> <p>-----</p>
147	2_要件定義書	22	3.11 情報システム稼働環境に関する事項 (3) ネットワーク	<p>「図表 3-11-1 業務系ネットワークに係る回線要件」について、回線番号 5 の回線種別は「無線」ではなく「有線」としていただけますでしょうか。</p>	<p>無線回線は有線回線に比べて外部環境からの影響を受けやすく、定常的な業務利用に耐えるだけの品質は確保できないと考えます。</p> <p>&lt;想定される外部環境からの影響&gt;</p> <ul style="list-style-type: none"> <li>・同一回線を利用する外部ユーザの数</li> <li>・同一回線を利用する外部ユーザのトラフィック</li> </ul> <p>通常業務では有線回線の利用を推奨致します。</p>	無	<p>本システムの運用期間中に場所が変更する可能性がある拠点について、変更時の作業負荷を低減するために無線としている。そのため、意見は採用しない。ただし、現地調査の結果、無線では期待する帯域の確保が困難な場合においては、別途変更契約により、有線に変更する等の対応を実施する。</p>
148	2_要件定義書	22	3.11.情報システム稼働環境に関する事項 (3) ネットワーク イ ネットワーク回線の要件 ①回線帯域 (ア)業務系ネットワークにかかる回線要件 図表 3-11-1 「7 データセンタ(インターネット回線)」	<p>ベストエフォートではなく、帯域確保型に変更願います。</p>	<p>インターネット回線については、全ての利用者が接続する回線であるうえ、パブリッククラウドへの接続も想定されるならばなおさら、可用性のみならず、十分な帯域の確保が必要となります。</p> <p>ベストエフォートとはあくまで「最大値」ですので、その値が出る可能性は極めて低く、必要な時に回線が遅いといった事態になるケースが想定されるため、「帯域確保型」にされることを強く推奨いたします。</p> <p>また、帯域については、インターネット経由でのパブリッククラウド利用をどの程度利用するかにより必要帯域、設計が変わるため、提案者に導入時点で必要な保障帯域を提案させるべきと考えます。</p>	有	<p>本意見及び意見 No.308 を踏まえ、クラウドサービスへの接続回線の種別(インターネット回線または閉域網)を含め、回線構成については提案を妨げるものではない。</p>
149	2_要件定義書	22	図表 3-11-1 業務系ネットワークに係る回線要件	<p>冗長構成「必要」と記載の回線につきまして、冗長用回線の品質(正系と同等の回線種別・要求帯域が必要か等)の記載を仕様書にてご提示願います。</p>	<p>副系回線の要求帯域等を低くすることで、価格低減が見込めるため。</p>	有	<p>意見を踏まえ、情報・研修館が想定する回線要件を要件定義書に記載することとする。ただし、回線の冗長化や必要帯域は提案要求</p>

			図表3-11-2 機密性情報系ネットワークに係る回線要件				項目とする。  なお機密性情報系ネットワークについては、調達範囲に関する意見を踏まえ、設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
150	2_要件定義書	22	3.11 情報システム稼働環境に関する事項 (3)ネットワーク ①回線帯域	「図表 3-11-2 機密性情報系ネットワークに係る回線要件」について、回線番号 9、11、12、13、15 の回線種別は「無線」ではなく「有線」として頂けますでしょうか。	無線回線は有線回線に比べて外部環境からの影響を受けやすく、定常的な業務利用に耐えるだけの品質は確保できないと考えます。 <想定される外部環境からの影響> ・同一回線を利用する外部ユーザの数 ・同一回線を利用する外部ユーザのトラフィック  通常業務では有線回線の利用を推奨致します。		無  調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
151	2_要件定義書	23	②インターネット回線 (ア)基本要件	「インターネット回線を経由してパブリッククラウドへ接続する場合は、通信を暗号化すること」と御座いますが、暗号化の可否はパブリッククラウドの仕様依存しますので、インターネット回線要件からは削除頂くことを希望いたします。	インターネット回線サービス自体では通信を暗号化しない為。		無  回線を含む、情報基盤システム全体で実現すべき内容であると考え、必須の要件としての変更の必要はないと判断し、意見は採用しない。
152	2_要件定義書	23	(イ)インターネット接続に係る IP アドレス等要件	[データセンターで利用する IPv4 アドレスとして、最大 256 個割り当てること]とありますが、最大 256 個提供から最大 64 個割り当てることに変更頂くことを希望いたします。	IPv4 アドレス数により提供可能なサービス種別や料金が異なる為。		有  意見 No.159 を参照すること。
153	2_要件定義書	23	(イ)インターネット接続に係る IP アドレス等要件	「データセンターで利用する IPv6 による通信要件については必須としない」と御座いますが、今後 IPv6 の利用予定が御座いましたら、必要要件として頂くことを希望いたします。	IPv6 提供有無により提供可能なサービス種別や料金が異なる為。		無  必須要件とはしない。
154	2_要件定義書	23	3.11.情報システム稼働環境に関する事項 (3)ネットワーク イ ネットワーク回線の要件 ②インターネット回線 (ア)基本要件	下記の内容を削除願います  ・3 つ目 回線ごとのトラフィックが、情報・研修館職員とあらかじめ協議のうえ、設定したしきい値を超えた場合に指定のメールアドレスに通知が可能なこと。	本要件は特定の ISP サービスに限定する内容であると思われます。実現する場合はコストに大きく影響するうえ、本要件の削除によるセキュリティレベルへの影響は無いため、公平性の観点から削除をお願いします。		有  意見を踏まえ、「3.11.情報システム稼働環境に関する事項」(3)ネットワーク「イ ネットワーク回線の要件」②インターネット回線「(ア)基本要件」の一部記載を以下に修正する。 ----- 回線ごとのトラフィックが、情報・研修館職員とあらかじめ協議の上、設定したしきい値を超えた場合に指定のメールアドレスへ通知が可能なこと。なお、要件の実現方法は、データセンターのネットワーク機器等でトラフィックを監視する等、回線の提供者(通信業者)が提供

							するサービスに限らない。 -----
155	2_要件定義書	23	3.11 情報システム稼働環境に関する事項 (3) ネットワーク イ ネットワーク回線の要件 ② インターネット回線 (ア) 基本要件	「回線ごとのトラフィックが、情報・研修館職員とあらかじめ協議の上、設定したしきい値を超えた場合に指定のメールアドレスへ通知が可能なこと。」と記載がありますが、削除をお願い致します。	トラフィックのしきい値を決めそのしきい値を超えた場合に通知する機能を提供しているキャリアは少ないため、またその仕組みを造るとなると大幅なコストアップに繋がりますので、サービスの選択肢を広げる意味でも削除をお願い致します。		有 意見 No.154 を参照すること。
156	2_要件定義書	23	3. 11 情報システム稼働環境に関する事項 (3) ネットワーク ②(ア)	「インターネット回線を経由してパブリッククラウドへ接続する場合は、通信を暗号化すること。」とあるが、インターネット回線の機能ではなく、SSL 通信による接続を想定している理解でよろしいでしょうか。	要件確認のため。		無 認識のとおりである。
157	2_要件定義書	23	3.11 情報システム稼働環境に関する事項 (3) ネットワーク イ ネットワーク回線の要件 ② インターネット回線 (イ) インターネット接続に係る IP アドレス等要件	「データセンターで利用する IPv4 グローバルアドレスとして、最大 256 個割り当てること。」 上記仕様を以下へ変更をお願い致します。 「データセンターで利用する IPv4 グローバルアドレスとして、〇個以上割り当てること。」 ※〇個は実際に必要なグローバル IP 数	ベストエフォートのインターネット回線で IPv4 グローバル IP アドレスを 256 個割り当てられるサービスが少ないため、サービスの選択肢を広げる意味でも変更をお願い致します。		有 意見 No.159 を参照すること。
158	2_要件定義書	23	3.11 情報システム稼働環境に関する事項 (3) ネットワーク イ ネットワーク回線の要件 ② インターネット回線 (イ) インターネット接続に係る IP アドレス等要件	「データセンターで利用する IPv6 グローバルアドレスとして、/48 のアドレスブロックを 1 個割り当てること。ただし、IPv6 による通信要件については必須としない。」と記載がありますが、IPv6 に対応していないインターネット回線でも提案は可能でしょうか。	インターネットの仕様を確認するため。		無 意見のとおり IPv6 に対応していないインターネット回線でも提案可能である。
159	2_要件定義書	23	3. 11 情報システム稼働環境に関する事項 (3) ネットワーク ①回線帯域 (イ) インターネット接続に係る IP アドレス等要件	「データセンターで利用する IPv4 グローバルアドレスとして、最大 256 個割り当てること。」 「データセンターで利用する IPv6 グローバルアドレスとして、/48 のアドレスブロックを 1 個割り当てること。ただし、IPv6 による通信要件については必須としない」と記載がありますが、グローバルアドレスの必要数と IPv6 の利用有無については明示頂けないでしょうか。	「提案構成に対して必要数分のグローバルアドレスを割り当てること」としていただくことは可能でしょうか		有 意見のとおり、グローバル IP アドレスの必要数は提案構成に対して必要な数を用意すること。IPv6 対応は不要とする。
160	2_要件定義書	24	3.11 情報システム稼働環境に関する事項 (3) ネットワーク イ ネットワーク回線の	「有線及び無線ともにデータ通信量による速度制限を設けないこと」の仕様についてですが、削除をお願い致します。	無線を利用する場合、速度制限を設けないサービスが少ないため、またコストアップにも繋がりますの		有 意見 No.163 を参照すること。

			要件 ③ WAN 回線 (オ) アクセス回線		で、サービスの選択肢を広げる意味でも削除をお願い致します。		
161	2_要件定義書	24	3. 11 (3)ネットワーク ③WAN 回線 (オ) アクセス回線	「また、無線においては原則、LTE 又は WiMAX とすること。」について、「また、無線においては原則、LTE 又は WiMAX の対応機種で提供すること。なお、立地条件や屋内などで無線の電波状況が安定せず通信が不安定な場合は、有線回線を引くなどの対策・代替手段を受託者の負担で実施すること。」へ変更することをご提案いたします。	モバイル通信は立地や時間帯などで回線パフォーマンスが安定しないため、通信不可の場合の対策を考慮する必要があるため。		無 意見は採用しない。ただし、現調した結果、実行帯域等の品質が保てない場合には、変更契約等を含め、別途協議の上対応することとする。
162	2_要件定義書	24	3. 11 情報システム稼働環境に関する事項 (3)ネットワーク ③WAN 回線 (オ)アクセス回線	「無線においては原則、LTE 又は WiMAX とすること」「有線及び無線ともにデータ通信量による速度制限を設けないこと」と記載がございますが、LTE、WiMAX 共に速度制限が設けられているため記載内容を緩和頂けないでしょうか。	LTE、WiMAX 共にデータ通信量による速度制限のプランを用いたほうが、リーズナブルな提案ができる可能性がございますので、真に必要でなければ仕様の緩和をお願い致します。		有 意見のとおり修正する。
163	2_要件定義書	24	③WAN 回線 (オ)アクセス回線	「有線及び無線ともにデータ通信量による速度制限を設けないこと」と御座いますが、「直近 3 日の合計使用量上限超過による制限」だけはサービス提供上、制限がかかるため、その点について緩和頂くことを希望いたします。 また無線による提供の場合、お客様のご利用エリア・場所・環境により十分なデータ通信が利用できないこともあるため、その点について緩和頂くことを希望いたします。	無線サービスにおいて、データ通信量による速度制限のうち「直近 3 日の合計使用量上限超過による制限」はどのサービスであっても必ず発生してくる為。 また無線サービスでは電波次第で利用できない場合、業務影響が大きいと考えられる為。		有 意見を踏まえ、以下のとおり修正する。 ----- データ通信量による速度制限は設けないことが望ましい。ただし、提供サービスの仕様等により、止むを得ず制限が発生する場合には、端末の OS・セキュリティアップデート等による大量通信の発生を加味した上で、システム設計、運用設計を行うこと。 なお、回線を設置または利用する場所・環境により、業務を行う上で十分な品質が保てない場合には、契約変更を含め、別途情報・研修館職員と対応を協議し、決定すること。 -----
164	2_要件定義書	24	3.11.情報システム稼働環境に関する事項 (3)ネットワーク イ ネットワーク回線の要件 ③WAN 回線 (オ)アクセス回線	下記の内容を削除願います  ・4 つ目 帯域保証型回線については、回線ごとにトラフィックが情報・研修館職員とあらかじめ確認の上設定したしきい値を超えた場合、前日の状況を翌日の午前中までに指定のメールアドレスへ通知を行うこと。	本要件は特定のキャリアサービスに限定する内容であると思われます。 実現する場合はコストに大きく影響するうえ、本要件の削除によるセキュリティレベルへの影響は無いため、公平性の観点から削除をお願いします。		有 意見を踏まえ、「3.11.情報システム稼働環境に関する事項」「(3)ネットワーク」「イ ネットワーク回線の要件」「③WAN 回線」「(オ)アクセス回線」の一部記載を以下に修正する。 ----- 帯域保証型回線については、回線ごとにトラフィックが情報・研修館職員とあらかじめ確認の上設定したしきい値を超えた場合、前日の状況を翌日の午前中までに指定のメールアドレスへ通知を行うこと。なお、要件の実現方法は、データセンターのネットワーク機器等でトラフィックを監視する等、回線の提供者(通信業者)が提供するサービスに限らない。 -----

165	2_要件定義書	24	3.11 情報システム稼働環境に関する事項 (3) ネットワーク イ ネットワーク回線の要件 ③ WAN 回線 (オ) アクセス回線	「帯域確保型回線については、回線ごとにトラフィックが情報・研修館職員とあらかじめ確認の上設定したしきい値を超えた場合、前日の状況を翌日の午前中までに指定のメールアドレスへ通知を行うこと。」の仕様についてですが、削除をお願い致します。	トラフィックのしきい値を決めそのしきい値を超えた場合に通知する機能を提供しているキャリアは少ないため、またその仕組みを造るとなると大幅なコストアップに繋がりますので、サービスの選択肢を広げる意味でも削除をお願い致します。		有	意見 No.164 を参照すること。
166	2_要件定義書	25	(カ)WAN 接続ルータ	「・LAN 側ポートは 4 個以上を備えること」と御座いますが、「1 個以上を備えること」としてご変更頂くことを希望いたします。	LAN 側ポート 1 個の機器であれば、より安価に提供できる為。		有	意見を踏まえ、以下のとおり修正する。 ----- LAN 側ポートについては、提案するネットワーク構成を踏まえ必要な数を備えること。 -----
167	2_要件定義書	25	3.11.情報システム稼働環境に関する事項 (3)ネットワーク イ ネットワーク回線の要件 ③WAN 回線 (カ)WAN 接続ルータ	下記要件の変更をお願いいたします。  ・3 つ目 修正前: LAN 側ポートを 4 個以上備えること 変更案: LAN 側ポートを 3 個以上備えること	多くの拠点が、WAN ルータの配下に L2 スイッチを配置すると思いますので、各拠点において LAN ポート 4 つは数量が多いと考えます。  コストを大きく削減できる要素となりますので、本要件の修正をお願いいたします。(4 個以上必要な拠点がある場合は、必要拠点のみご指定されるのがよろしいかと思います。)		有	意見 No.166 を参照すること。
168	2_要件定義書	25	3. 11 情報システム稼働環境に関する事項 (3)ネットワーク ③WAN 回線 (カ)WAN 接続ルータ	以下の記載があります。  ・SNMPv1、SNMPv2 以上をサポートしていること。  SNMP でデファクトスタンダードとなっているバージョンは、v1,v2c,v3 となりますので、上記の SNMPv2 を SNMPv3 に緩和された方が製品選定の幅が広がります。	公平性及び製品選定の幅を広げるため。		有	意見を踏まえ、以下のとおり修正する。 ----- SNMPv1、SNMPv2c、SNMPv3 をサポートしていること。 -----
169	2_要件定義書	25	3.11.情報システム稼働環境に関する事項 (3)ネットワーク イ ネットワーク回線の要件 ③WAN 回線 (カ)WAN 接続ルータ	下記要件の変更をお願いいたします。  ・5 つ目 修正前: SNMPv1、SNMPv2 以上をサポートしていること 変更案: SNMPv1、SNMPv2 以上をサポートしていること、または SNMP で一般的に利用される監視やトラフィックグラフ等の情報を提供すること。	一般的にキャリア等のサービス機器の場合、お客様管理のシステムなどのサービス外機器と、SNMP 連携を許容していないことが多く、実現する場合は個別構築となりコストに大きく影響するうえ、本要件の削除によるセキュリティレベルへの影響は無いため、本要件の修正をお願いします。		有	意見 No.168 を参照すること。
170	2_要件定義書	25	3.11.情報システム稼働環境に関する事項 (3)ネットワーク	下記の要件を追加願います。  ・盗難時の設定情報漏洩防止のために、電源 OFF 時	全国の複数拠点に設置する機器となるため、盗難時の設定情報の漏えい、INPIT 様 NW 内の侵入対策		無	物理的に十分な対策が講じられていれば問題ないため、必須の要件とする必要はないと

			イ ネットワーク回線の要件 ③WAN 回線 (カ)WAN 接続ルータ	にコンフィグが揮発すること、あるいは、これに準じた方法で設定情報漏洩の対策が十分にとられていること	等の セキュリティの考慮が必要と 考えております。 ワイヤー等による物理的なセキュリ ティ対策と併せて、ケーブルの抜き 差し等で設定情報を消去するなど の機器側のセキュリティ対策も重 要だと考えます。  また、各拠点機器毎の設定管理工 数が不要となるため、コストの削減 にも寄与することができます。			判断し、意見は採用しない。
171	2_要件定義書	25	3. 11 情報システム稼働環境に関する事項 (3)ネットワーク ④LAN 要件 (ア)基本要件	「各拠点の LAN を構成すること。拠点の規模等に応じて適切なアドレス設計及びネットワーク機器の設置を行うこと」と記載がありますが、特許庁庁舎、三井ビル、近畿統括拠点については人数も多いことから L3 スイッチや L2 スイッチの導入が必要と考えています。その場合の各拠点及び、フロアに対するラック設置の有無をご教示ください。	ネットワーク設計及び工事有無等、 構成に関係するため。		無	ラックは設置可能で、受注者で用意する。
172	2_要件定義書	25	3.11.情報システム稼働環境に関する事項 (3)ネットワーク イ ネットワーク回線の要件 ④LAN 要件 (ア)基本要件	下記要件の削除をお願いいたします。  ・6 つめ 許可されないセグメント間通信が発生したときは、直ちにログに記録すると同時に、運用担当者へ通知する機能	本要件の上の項目に「LAN 回線のセグメント間の通信は、必要最低限の通信のみ許可する設計とし」とあるため、そもそも「許可されないセグメント間通信」は発生し得ないと考えます。(もしあった場合は、設計・構築時の大きな瑕疵です。)。  本要件を実現する場合は、コストにも大きく影響するため、削除をお願いします。		有	意見を踏まえ、以下のとおり修正する。 ----- 許可されないセグメント間通信が発生したときは、直ちにログに記録すると同時に、運用担当者へ通知する機能を持つことが望ましい。 -----
173	2_要件定義書	25	3.11 情報システム稼働環境に関する事項 (3) ネットワーク ④ LAN 要件 (ア) 基本要件	「許可されないセグメント間通信が発生した時は、直ちにログに記録すると同時に、運用担当者へ通知する機能を有すること」の仕様について、削除をお願いします。	セグメント間の通信は、拠点間の通信も含まれるという認識です。各拠点に通知する機能を有する機器の導入が必要となり、コストアップに繋がりますので、削除をお願い致します。		有	意見 No.172 を参照すること。なお、データセンターを経由しない拠点間の通信は想定していない。業務セグメントと管理セグメント間等における許可されないセグメント間通信の検知を想定している。
174	2_要件定義書	25	3. 11 情報システム稼働環境に関する事項 (3)ネットワーク ④LAN 要件	以下の記載があります。  ・拠点ごとに帯域の割合を変更できること。  上記は QoS の機能で、拠点から WAN に送られる通信について、通信種別により帯域割合を変更できることとの理解で宜しいでしょうか？	仕様明確化のため		無	認識のとおりである。
175	2_要件定義書	25	3.11.情報システム稼働環境に関する事項	下記要件の変更をお願いいたします。	(本要件は WAN ルータにも関連する要件であると想定し、)一般的に		無	システム全体として実現することを求めている要件であるため、意見は採用しない。QOS の

			(3)ネットワーク イ ネットワーク回線の要件 ④LAN 要件 (ア)基本要件	・7つ目 現在:各拠点におけるトラフィックは Diffserv 値、ToS もしくは CoS 値を利用して、優先度、帯域制御を設定できること。 変更案:各拠点におけるトラフィックは Diffserv 値、ToS もしくは CoS 値を利用して、優先度、帯域制御を設定できること。もしくは、十分な帯域を確保すること。	キャリア等のサービス機器の場合、お客様管理のシステムなどのサービス外機器との帯域制御設定に関する連携を許容していないことが多く、実現する場合は個別構築となりコストに大きく影響するうえ、本要件の削除によるセキュリティレベルへの影響は無いため、本要件の修正をお願いします。			機能は、ウェブ会議等で将来的に利用する可能性があり、機能は備えておく必要がある。
176	2_要件定義書	25	3. 11 情報システム稼働環境に関する事項 (3)ネットワーク ④LAN 要件 (ア)基本要件	以下の記載があります。  ・セキュリティの強化及び帯域資源の有効利用のため、マルチキャストパケットの不要な複製と転送を抑制するため、PIM パケット、IGMP パケットの動作を観察しインタフェースへのフラッティングを最適化する機能を提供すること。  PIM パケットの動作を観察し、インタフェースへのフラッティングを最適化する機能(PIM スヌーピング機能)については、特定メーカーの製品機能となりますので仕様緩和をお願いします。(上記の PIM パケットを削除)	公平性及び製品選定の幅を広げるため。		有	意見のとおり修正する。
177	2_要件定義書	26	3. 11 情報システム稼働環境に関する事項 (3)ネットワーク ④LAN 要件 (ウ)無線 LAN	特許庁庁舎、三井ビル、近畿統括拠点(仮称)については閲覧資料③「無線LAN拠点フロアレイアウト」にて確認が可能となっておりますが、それ以外の拠点レイアウトも仕様書にてご提示願います。	特許庁庁舎、三井ビル、近畿統括拠点(仮称)以外の拠点に関する建屋内構成の検討が必要なため。		無	拠点側は回線に無線を使用し、拠点側の回線工事は想定していないため、仕様書への追記・閲覧資料への追加は行わない。 近畿統括拠点(仮称)については、拠点が決定次第提示可能とする。
178	2_要件定義書	26	3. 11 情報システム稼働環境に関する事項 (3) ネットワーク ④ LAN 要件 (ウ) 無線 LAN	特許庁庁舎、三井ビル及び近畿統括拠点(仮称)以外の各拠点の LAN 工事も本調達に含まれる認識でよろしいでしょうか。	各社の見積もり条件を均質化するため。		無	認識のとおりである。ただし、拠点側は回線に無線を使用し、拠点側の回線工事は想定していない。
179	2_要件定義書	26	④LAN 要件 (ウ)無線 LAN	地域相談窓口拠点においても無線 LAN が必要な場合は、その要件をご記載頂くことを希望いたします。	地域相談窓口拠点の無線 LAN 機器を選定する為。		有	意見を踏まえ、要件定義書の「3. 11 情報システム稼働環境に関する事項」「(3) ネットワーク」「イ ネットワーク回線の要件」「④LAN 要件」「(ウ) 無線 LAN」に、以下を追記する。 ----- 特許庁庁舎、三井ビル、近畿統括拠点(仮称)以外の拠点についても、無線 LAN を使用することとするが、今後拠点が変更になる可能性も考慮して、拠点変更時の機器の撤去や移設がしやすい機器構成とすること。 -----



180	2_要件定義書	26	④LAN要件 (ウ)無線 LAN	「特許庁庁舎、三井ビル及び近畿統括拠点(仮称)においては端末との接続に無線 LAN を使用すること。」との記載がございますが、無線 LAN アクセスポイントについては設計段階で無線の干渉等のサーベイ作業を行う必要があり、設計期間が不足する可能性がございます。サーベイ結果による機器台数の決定とその構築が作業スケジュール全体上のクリティカルなパスと考えます。 従って、無線 LAN アクセスポイントについて、提案期間中にサーベイ作業を実施させていただくことは可能でしょうか。	実現可能性を高めるため		無	提案期間中のサーベイ作業は可能である。作業時間等は情報・研修館職員と相談すること。
181	2_要件定義書	26	3.11 情報システム稼働環境に関する事項 (3) ネットワーク ④ LAN 要件 (ウ) 無線 LAN	「無線特有の DoS 攻撃(RF Jamming、認証失敗等の攻撃)、ブロードキャストを利用した無線アクセスポイントの偵察行為等を検知する機能を有していること。」の仕様について、削除をお願いします。	コスト増につながる要件のため削除をお願い致します。		有	意見のとおり修正する。
182	2_要件定義書	26	3.非機能要件の定義 3.11 情報システム稼働環境に関する事項 (3)ネットワーク ④LAN 要件 (ウ)無線 LAN	「無線を利用したリソースへのアクセス権限のない不正アクセスを防ぐため、コア/ディストリビューションレイヤ等で無線 LAN コントローラからの意図しない通信による不正トラフィックを検知し、通信の遮断を行うこと。」に関して、「無線を利用したリソースへのアクセス権限のない不正アクセスを防ぐため、コア/ディストリビューションレイヤ等で無線 LAN コントローラ等からの意図しない通信による不正トラフィックを検知し、通信の遮断を行うこと。」に変更していただきたい。	無線 LAN コントローラを用いない提案構成もあるため、より幅広い選択肢からの機種選定を促し、コストを含めより最適な提案を可能とするため。		有	意見のとおり修正する。
183	2_要件定義書	26	3.11 情報システム稼働環境に関する事項 (3) ネットワーク ④ LAN 要件 (ウ) 無線 LAN	「不正なアクセスポイントを検知可能であり、切断すべき対象アクセスポイントの情報が取得可能で、切断できること」の仕様について、削除をお願いします。	コスト増につながる要件のため削除をお願い致します。		有	意見のとおり修正する。
184	2_要件定義書	27	3.非機能要件の定義 3.11 情報システム稼働環境に関する事項 (4)ネットワーク ④LAN 要件 (ウ)無線 LAN	「不正なアクセスポイントを検知可能であり、切断すべき対象アクセスポイントの情報が取得可能で、切断できること。」について、「不正なアクセスポイントを検知可能であり、切断すべき対象アクセスポイントの情報が取得可能で、適切な対処ができること。」に変更いただきたい。	当該機能を有する機器メーカーが限定されているため、より幅広い選択肢からの機種選定を促し、コストを含めより最適な提案を可能とするため。		有	意見 No.183 を参照すること。
185	2_要件定義書	27	3.非機能要件の定義 3.11 情報システム稼働環境に関する事項 (5)ネットワーク ④LAN 要件 (ウ)無線 LAN	「無線特有の DoS 攻撃(RF Jamming、認証失敗等の攻撃)、ブロードキャストを利用した無線アクセスポイントの偵察行為等を検知する機能を有していること。」について、「無線特有の DoS 攻撃(RF Jamming、認証失敗等の攻撃)などを検知する機能を有していること。」に変更いただきたい。	当該機能を有する機器メーカーが限定されているため、より幅広い選択肢からの機種選定を促し、コストを含めより最適な提案を可能とするため。		有	意見 No.181 を参照すること。

186	2.要件定義書	26	3.非機能要件の定義 3.11 情報システム稼働環境に関する事項 (4)ネットワーク ④LAN 要件 (ウ)無線LAN	「サポートしている周波数内で、Wi-Fi 以外の電波を出す干渉デバイスを検知し、デバイスの種類を識別できること。」を削除いただきたい。	当該機能を有する機器メーカーが限定されているため、より幅広い選択肢からの機種選定を促し、コストを含めより最適な提案を可能とするため。		有	意見のとおり修正する。
187	2.要件定義書	64	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件	データセンタ要件として「業務系ネットワークにおいてパブリッククラウドを活用する場合・・・」の記載がありますが、この場合におけるデータセンタ利用イメージを、図等で具体的にご教示いただけますでしょうか。	当文面のみだと、利用イメージの理解が困難であるため、図等でご教示いただき、理解度を向上させたいと考えております。		無	別添資料「情報・研修館情報基盤システム概要図」は、業務系ネットワークにクラウドサービス・データセンターを活用したシステム構成図である。ただし、情報基盤システムが提供するサービス・機能の実現手段として、どのサービス・機能をクラウドサービス・データセンターで実現するかについては提案を妨げない。
188	2.要件定義書	27	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件	以下の要件を変更いただきたい。  現在:独立行政法人工業所有権情報・研修館 情報セキュリティポリシー」で定める要保護情報を保管するパブリッククラウドサービスについては、ISO/IEC 27017 及び ISO/IEC 27018 に準拠し ISMS 審査機関による認証を証明できること、または CS ゴールドマーク(クラウドセキュリティ推進協議会が提供するクラウド情報セキュリティ監査制度)を取得していること。  変更案:独立行政法人工業所有権情報・研修館 情報セキュリティポリシー」で定める要保護情報を保管するパブリッククラウドサービスについては、ISO/IEC 27017 及び ISO/IEC 27018 に準拠し ISMS 審査機関による認証を証明できること、または CS ゴールドマーク(クラウドセキュリティ推進協議会が提供するクラウド情報セキュリティ監査制度)を取得していることが望ましいが、難しい場合は、CS シルバーマーク以上を取得している証明と共に、中央省庁または独立行政法人における同等以上の規模の導入実績を 2 件以上提示すること。	本要件は特定のサービスに限定する要件のため、公平性の観点から要件を緩和いただきたい。  CS シルバーマーク以上を有していると共に、中央省庁や独立行政法人における同等以上の規模の導入実績を複数有していれば、求められるセキュリティレベルとしては必要十分であると言えます。  通信回線が、インターネット上の暗号化通信で許容されるレベルのクラウドサービスに対し、当該認証要件を求めるのは要求レベルが高すぎるうえ、提案できるサービスも限られるため、左記の要件変更をお願いします。  本意見を適用頂けないようであれば、クラウドサービスと接続する回線については閉域網とすることを必須条件にすべきと考えます。		有	意見を踏まえ、以下のとおり修正する。 ----- 独立行政法人工業所有権情報・研修館 情報セキュリティポリシー」で定める要保護情報を保管するパブリッククラウドサービスについては、ISO/IEC 27017 及び ISO/IEC 27018 に準拠し ISMS 審査機関による認証を証明できること、または CS ゴールドマークまたはシルバーマーク(クラウドセキュリティ推進協議会が提供するクラウド情報セキュリティ監査制度)を取得していること。 -----
189	2.要件定義書	27	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件	「ISO/IEC27001 に準拠し、ISMS 審査機関による認証を証明できること」とありますが、ISO27001 認証はデータセンター運用部門にて取得していれば問題ないでしょうか。	要件の理解のため。		無	認識のとおりである。
190	2.要件定義書	28	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件	「データセンタ所在地は日本国内であること。また、バックアップのデータセンタについても日本国内であること」と要件にありますが、「バックアップのデータセンタ」	要件定義書にて具体的に示されていないため確認させてください。 バックアップデータを保管するセン		有	意見を踏まえ、以下のとおり修正する。 なお、本要件はパブリッククラウドサービス利用時におけるデータレジデンシーに係る要件

				とは何を示しますか。バックアップデータを保管するセンターのことでしょうか。	ターとするのであれば、データセンターであることは必須かでしょうか。バックアップ媒体保管サービスを提供している企業のサービスを流用することで、提案の幅がひろがると考えます。			であることに留意すること。 ----- データセンターの所在地は日本国内であること。また、バックアップのデータを保管する場所についても日本国内であること -----
191	2_要件定義書	28	3. 11 情報システム稼働環境に関する事項 (4) 施設・設備要件	「データセンタに保存された情報・研修館のデータが日本国外に移動する事がないこと。また、日本国外からアクセスできないこと」と記載がありますが、例えば「公開用 DNS のレコード情報」など、国内外からのアクセスを前提としている「データ」もあることから、『公開を前提としないデータを INPIT 外部からアクセスできないこと』といった記載をご検討ください。	「データ」に関する解釈を明確化したいため。		有	意見のとおり修正する。
192	2_要件定義書	28	3. 11 情報システム稼働環境に関する事項 (4) 施設・設備要件	「データセンタに保存された情報・研修館のデータが日本国外に移動することがないこと。または、日本国外からアクセスできないこと。」とあるが、セキュリティアプライアンス製品のセキュリティ分析のために、最低限の情報(ログ等)を参照することは対象外となる理解でよいか。  上記認識に相違がなければ、「セキュリティアプライアンス製品のセキュリティ分析のために、最低限の情報(ログ等)は対象外とする」旨を追記いただきたい。	要件確認のため。		有	意見を踏まえ、以下のとおり修正する。 ----- データセンタに保存された情報・研修館のデータが日本国外に移動することがないこと。または、日本国外からアクセスできないこと。ただし、事前に情報・研修館職員と協議・了承を得た場合を除く。 -----
193	2_要件定義書	28	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件 ア 立地条件	「東京の液状化予測」において「液状化の発生が少ない地域」または「液状化がほとんど発生しない地域」であること。とあるが、「液状化の可能性がある地域」または「液状化の可能性が低い地域」に変更していただきたい。	現在東京の液状化予測図 平成24年度改訂版にて評価表現が異なっていたため確認となります は「東京の液状化予測」において、「液状化の可能性が高い地域」「液状化の可能性がある地域」「液状化の可能性が低い地域」とされています。		有	意見のとおり修正する。
194	2_要件定義書	28	3.11 (4)施設・設備要件 ケ保管庫	3.11(4)アおよびイについては、ケ保管庫の要件に掛からないという認識でよろしいでしょうか。	受注業者の利便性の高い都市型の保管庫は、データセンタの立地条件・建物条件を満たさない場合が多いと想定され、コストと利便性の面から保管庫の要件は、あくまでケに記載の内容のみと確認したため。		無	認識のとおりである。
195	2_要件定義書	28	ア 立地条件	活断層条件追加  <変更案> 活断層が3km以内に存在しない事、又は存在する活断層における想定震度に対して充分耐えうる設備であること	存在した場合においても対策がなされていれば問題無いと考えます。		有	意見のとおり修正する。ただし、想定震度に充分耐えうる施設・設備であることを証明すること。

196	2_要件定義書	29	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件 オ 空調設備	高効率空調(キャッピング、温・冷気分離、スポット冷却等)を実施していること。とありますが、ホットアイル・コールドアイルの分離という認識でよろしいでしょうか。	要件の理解のため。		無	認識のとおりである。なお、それ以外の方法で高効率空調を実現する提案を妨げるものではない。
197	2_要件定義書	29	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件 オ 電源設備	「非常用発電設備を備えていること。また、非常用発電設備自体の冗長化構成がなされていること」とあるが「非常用発電設備を備えていること。また、非常用発電設備自体の冗長化構成がなされていること、もしくは、データセンタにたいして3経路以上の電源受電経路を有すること」と表現を変更いただけませんか。	3系統以上の電源受電経路を有することは、非常用発電設備の冗長化構成に相当するが、そのように仕様変更いただければご提案の幅が広がると考えるため。		有	意見のとおり修正する。なお、非常用発電設備の冗長化は必須としない。
198	2_要件定義書	29	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件 オ 空調設備	「空調設備への給電は、機器への給電とは別系統であること。また停電時の無停止冷却が可能であることが望ましい。」について「また停電時の無停止冷却が可能であることが望ましい。」を削除いただきたい。	停電時における空調設備の無停止冷却のためにはUPS及び非常用発電機を設けなければならないが、商用電源の停電が発生し、非常用発電機からの給電が始まるまで1分程度であり、1分の空調設備停止により、機器室温度の過度な上昇は発生しないため。		有	意見のとおり修正する。
199	2_要件定義書	30	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件 キ 機器設置区域	「サーバや搬入設備を設置するために必要な床の耐荷重性能は、フリーアクセス部で500kg/m <sup>2</sup> 以上とすること。また、スラブ部では1000kg/m <sup>2</sup> 以上であることが望ましい。」について「サーバや搬入設備を設置するために必要な床の耐荷重性能は、スラブ部では1000kg/m <sup>2</sup> 以上であること。」へ変更いただけますでしょうか。	サーバや搬入設備を設置するサーバラックは、スラブ床へ固定するので、フリーアクセス部の耐荷重を規定する必要がないため。		有	意見のとおり修正する。
200	2_要件定義書	31	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件 ク 機器収納ラック	本要件とは別に別途用意するラックの電源要件について「AC100V 20A」に対応を「AC100V 20A 以上で準備」と変更できないか	本要件とは別に別途用意するラックの電源要件について AC100V 20A に対応とあるが AC100V 20A 以上で準備、たとえば、30A の提供でもよいという認識でよろしいでしょうか。		無	同じ認識である。
201	2_要件定義書	31	3.11 (4) ケ 保管庫	クライアント端末予備機を出荷する際、セットアップは貴館にて行うという認識でよろしいでしょうか。	要件の理解のため。		有	意見を踏まえ、セットアップ作業はマニュアルベースで情報・研修館職員が行うこととする。ただし、受注者は、職員がセットアップを行う際に必要な資材(セットアップツール、マニュアル等)を準備し、提供すること。なお、ネットワーク設定等、職員にて実施することが困難である想定する作業は受注者にて実施すること。
202	2_要件定義書	31	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件 ケ 保管庫	「運用上必要な時又は情報・研修館職員の指示に基づいて受注者にて自由に出し入れできる環境を確保すること。」と記載がありますが、クライアント端末予備機出荷について、特許庁庁舎の情報基盤システムご担当者様にお渡しすればよいという認識でよろしいで	費用試算のため。(チャーター便等の特定の指定制の有無の確認)		有	意見踏まえ、クライアント端末予備機は特許庁庁舎に保管することとする。出荷時の郵送については、端末内に業務データが無いものは一般の宅配便(パソコン梱包用)で問題ないが、端末内に業務データが存在する場合は

				しょうか。 また、外部施設に保管庫を有する場合、一般の宅配便を利用してお渡しするという想定でよろしいでしょうか。				セキュリティ便等のセキュアな郵送方法を採用すること。
203	2_要件定義書	31	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件 ケ.保管庫	クライアント端末予備機を出荷する想定頻度をご教示いただけますでしょうか。例：一ヶ月当たり 40 台等	費用試算のため。		無	出荷頻度については、提案するクライアント端末の故障率を基に想定すること。
204	2_要件定義書	31	3.11 情報システム稼働環境に関する事項 (4) 施設・設備要件 ケ 保管庫 1 ポツ目 2 ポツ目 3 ポツ目	クライアント端末等の物品保管庫についてですが、貴館館内に施設ができる棚等を設置させていただくことは可能でしょうか。	対応の迅速性を考慮し、貴館館内に保管する運用が適していると考えられるため。		無	クライアント端末の予備機は情報・研修館にて保管可能である。それ以外の機器の保管については、情報・研修館と協議・相談の上、決定すること。
205	2_要件定義書	31	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件 ケ.保管庫	文中の「クライアント端末予備機」：別紙1「拠点一覧及び拠点ごとの PC 台数等の情報」に記載の台数の 1 割について 調達するクライアント予備機は業務系 NW、機密性情報系 NW、持込媒体サンドボックス PC の総合計台数の 1 割でしょうか、それとも各システム用で分けた端末ごとの 1 割という解釈でしょうか。 また、クライアント端末の総合計の 1 割という解釈である場合、予備機のスペックはどのシステム用端末のスペックにあわせればよろしいでしょうか。	環境や用途に応じて、数種類の端末が必要になると予想しております。従いまして、端末の種類それぞれに 1 割程度の予備端末を用意する、という認識でよろしいでしょうか。 要件の理解のため確認させていただきたく存じます。		有	予備機の台数は業務系 NW クライアント PC 合計台数の 5%である。予備機のスペックは、業務系 NW クライアント PC と同一とする。 なお、調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、機密性情報系 NW における端末の手配は本調達の範囲外である。
206	2_要件定義書	31	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件 ケ. 保管庫	クライアント端末予備機についてですが、別紙1「拠点一覧及び拠点ごとの PC 台数等の情報」に記載数の総数に対して 1 割を準備する必要があるという理解でよろしいでしょうか？(約 48 台)	予備機の台数が多いように見受けられましたので、障害対応以外に予備機の利用想定があればご教示ください。		有	意見を踏まえ、以下のとおり修正する。 ----- 保管する対象物品は以下のとおりである。 0 クライアント端末予備機： 別紙1「拠点一覧及び拠点ごとの PC 台数等の情報」に記載の台数の 5% -----
207	2_要件定義書	32	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件 ケ.保管庫	「保管対象の空き箱以外は積み上げができないものとする」とありますが、 空き箱の保管は必要でしょうか。 送付の際に利用するのであれば、別手段を講じることは可能としていただけますでしょうか。	要件の確認、提案の幅を広げるため。		有	意見を踏まえ、以下のとおり修正する。 ----- 端末等の送付の際に利用する等、保管対象の空き箱以外は積み上げができないものとする。なお、空き箱を保管することは必須要件ではない。 -----
208	2_要件定義書	31	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件 ケ.保管庫	「安定的な運用に必要な補充等の管理を保管場所と情報・研修館拠点内執務室の間で実施すること」と記載がありますが、こちらは、クライアント予備機端末ではなく、インク、用紙等の消耗品を示しておりますでしょうか。	「運用に必要な補充」は何を想定されているのか不明なため。		無	プリンタ・複合機に使用するインク・トナーを示している。なお、用紙は本調達範囲の対象外である。

209	2_要件定義書	31	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件 ケ 保管庫	予備機クライアント端末の運用方式は、センドバック方式、玉突き方式のどちらを想定されておりますでしょうか。  【センドバック方式】: 予備機クライアント端末を指定の場所へ送付し、故障機を返送いただき修理します。修理完了後、元の設置場所へ送付し、予備機クライアントと入替、予備機クライアント端末を返送していただく方式。  【玉突き方式】: 予備機クライアント端末を指定の場所へ送付し、故障機を返送いただき修理します。修理完了後、予備機の在庫として追加する方式。	予備機クライアント端末の運用方式を確定させるため		無	どちらの方式を採用しても可能とする。ただし、郵送やセットアップ等の作業効率及び費用を考慮し、優れた方式を提案することを期待する。
210	2_要件定義書	31	ケ 保管庫	バックアップテープ保管も記載があるが、同エリア内で問題ないでしょうか	同時被災時にバックアップテープなども被災してしまうため別エリアが望ましい		無	保管庫におけるバックアップテープは未使用(過去のバックアップデータを記録したテープでも、バックアップのために保管する世代を過ぎたものであれば、それは未使用とする)のものを保管すること。バックアップを取得したテープの保管要件については、「要件定義書 2.9 継続性に関する事項」を参照すること。
211	2_要件定義書	32	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件 コ セキュリティ	「一時的な訪問者と継続的に立ち入りを許可されたものを外見上判断できるよう処置を講じること」とあるが、 「一時的な訪問者と継続的に立ち入りを許可された訪問者を外見上判断できるよう処置を講じること」と要件を変更願います。	「許可されたもの」になると、現地職員(オペレータ等の常駐員)もふくまれるため、明示的に訪問者を表現いただくことで、現地職員(常勤者)を対象外としていただきたいため。		無	一時的な訪問者と現地職員(オペレータ等の常駐員)は外見上区別する必要があるため、意見は採用しない。
212	2_要件定義書	32	3.11 情報システム稼働環境に関する事項 (4)施設・設備要件 コ セキュリティ	「マシン室前室に入室する際は伴連れ防止設備により不正侵入を防止する策をとっていること」とあるが、「マシン室前室に入室する際は伴連れ防止対策を講じて不正侵入を防止する策をとっていること」に変更願います。	機械にて伴連れ防止対策を講じているデータセンタはすくなく提供できるデータセンタが限定されます。マシン室への入室はデータセンタオペレータの帯同をもって可能とし入室を管理する等、人為的に対応することで提案の幅を広げていただけないでしょうか。		有	意見のとおり修正する。
213	2_要件定義書	32	3.11 情報システム稼働環境に関する事項 (4)設備要件 コ セキュリティ	「利用するラックが設置される機器設置区域は、物理的に他のラックと隔離(ラック単体で隔離されたことを保証する方式を含む。)」とありますが、ラックキーをラック単位で個別専用キーとすることで無関係な者の開錠、施錠はできない仕組みとし、さらに開錠施錠は当社にて実施するようにしていますが、本処置は「(ラック単体で隔離されたことを保証する方式を含む。)」に該当するという認識でよろしいでしょうか。	要件確認のため。		無	認識のとおりである。
214	2_要件定義書	32	3.11 情報システム稼働環境に関する事項	「情報システム安全対策基準」(平成9年9月24日 通商産業省告示第536号最終改正)に準拠した設備	一般テナントへの設置を対象に情報システムの安全性基準を策定し		無	認識のとおりである。

			(4)施設・設備要件 コ セキュリティ	であることとあるが、情報システム安全対策基準に記載される要件は一般テナントビルを対象としている記述もあります。データセンタ専用建物であれば問題ないでしょうか。	ているものと考えられますが、データセンタ設備であれば全項目を満足させる必要は無いと考えられます。データセンタ専用建物場合は本要件を満たせると考えてよろしいでしょうか。		
215	2_要件定義書	32	3. 11 情報システム稼働環境に関する事項 (4)施設・設備要件 コ セキュリティ	「情報システム安全対策基準(平成9年9月24日通商産業省告示第536号最終改正)に準拠した設備であること。なお、本システムの重要度はAのグループに該当する。」を削除いただけますでしょうか。	20年近く前の基準であり、陳腐化しているため。		無 必須の要件としての変更の必要はないと判断し、意見は採用しない。
216	2_要件定義書	32	3. 12 テストに関する事項	設計、構築・テスト、受入テストの範囲や作業内容を仕様書中に明記するか、具体的なテストシナリオやテストの方法、テストスケジュールを提案に含むよう明記し、提案時の評価で考慮すべきと考えます。	サービスインまでのスケジュールがタイトであり効率的なプロジェクト運営を行う必要があるため。特にテスト作業の進め方において認識齟齬があるまま進めた場合、遅延リスクが高まるため。		無 意見のとおり、作業内容やスケジュールは評価対象とする。
217	2_要件定義書	38	3.13 移行に関する事項 (2)データ移行・システム切替え要件 イ 個別要件 1 端末に関する要件	各拠点、各執務室、各担当様デスクへの端末の設置は、受注者にて実施することでよろしいでしょうか。また、既存クライアントの撤去及び同拠点内での指定の保管場所への運搬も受注者にて実施する認識でよろしいでしょうか。	要件確認のため。		無 特許庁庁舎・三井ビル拠点は、稼働前にPCを受注者から情報・研修館職員の代表に渡し、代表者から利用者個人に配布する想定である。それ以外の拠点は、受注者が現地で拠点構築作業を行う際、利用者個人(または代表者)に渡すことを想定している。
218	2_要件定義書	38	3.13 移行に関する事項 (2)データ移行・システム切替え要件 イ 個別要件 1 端末に関する要件	PCはデータ移行のため、並行稼働を想定していると思われませんが、拠点作業は設置・撤去と最低2回は必要となりますでしょうか。	展開作業計画の立案・ご提案・試算に係わるため。		無 本調達で手配するPCの設置は受注者で行うが、既存PCの回収は発注者側で行う。なお、既存PCは平成30年1月中は並行稼働予定である。
219	2_要件定義書	41	3. 14 引継ぎに関する事項	次期情報基盤システム検討時の引継ぎ先に次期情報基盤システム構築事業者が含まれているが、支援事業者のみの理解でよいか。	検討時は構築事業者が未決定である認識のため。		有 意見のとおり、検討時は構築事業者が未決定である。ただし、構築期間中においては、情報・研修館の依頼に基づき、受注者は情報提供等を行うこと。
220	2_要件定義書	41	3. 14 引継ぎに関する事項	次期情報基盤システム検討時に発生する「費用の発生状況、契約内訳」については、除外いただきたい。	費用については、発注者と受注者間の金銭契約に基づく事柄のため、第三者である次期構築事業者の開示できかねる情報も含むため。		有 意見のとおり修正する。
221	2_要件定義書	42	3.16(1)運転管理・監視等要件	運用業務の受付時間及び作業時間を下記の通り修正願います。  現在:開館日の8時30分~18時15分 変更案:平日の9時~17時30分	お問い合わせ対応窓口(障害対応等は除く)は、一般企業の勤務時間帯と同じ時間帯での対応(平日9時~17時30分)であることが多く、その時間帯から外れる場合は特別対		無 必須の要件としての変更の必要はないと判断し、意見は採用しない。

					応となりコストに大きく影響するため。			
222	2_要件定義書	43	3. 16運用・保守に関する事項 (4)運用・保守実績の評価と改善 ア報告の実施	「運用・保守作業の工数実績」を報告の項目として追加するべきと考えます。	調達仕様書(案)P.13 イ定常時対応の項に記載されているため。		有	意見のとおり修正する。
223	2_要件定義書	43	3. 16運用・保守に関する事項 (4)運用・保守実績の評価と改善 ア報告の実施	「システムの稼働状況」については、削除しても良い項目であると考えます。	SLA の報告の中で各サービスの稼働率の報告が含まれると思われる、計画停止や障害による停止時間の報告は、サービスの稼働率における備考として必然的に報告されるべきものであるため。		有	意見のとおり修正する。
224	2_要件定義書	43	3.16 運用・保守に関する事項 (4)運用・保守実績の評価と改善 イ サービスレベルの管理	受注者は、情報基盤システムの運用・保守を実施するにあたり、受注後に情報・研修館職員と以下に示す項目を母数として具体的内容を検討し SLA を締結すること。  ・3.3-(2) データ量:本書 P7 ・3.3-(3) 処理件数:本書 P7-8 ・3.4 性能に関する事項:本書 P8-9 ・3.5 信頼性に関する事項:本書 P10-11 ・3.9-(1) 継続性に係る目標値:P13 ・3.10 情報セキュリティに関する事項:P14-21 ・別紙6:サービスレベル項目一覧	SLA にて締結される内容、条件及び数値については、コストに影響があるため、明確に条件を提示していただきたい。	無し	無	SLA は要件定義書の別紙 6「サービスレベル項目一覧」に記載された内容が該当する。
225	2_要件定義書	43	3. 16運用・保守に関する事項 (4)運用・保守実績の評価と改善 イ サービスレベルの管理 2 サービスレベルの報告・評価・改善	9 項目目については、「対応に必要な人的リソースの追加、体制の変更、対応のために必要なシステムの導入等に費用が係る場合、必要に応じて情報・研修館職員と協議を行うこと。」に変更する必要があると考えます。	新たな施策等によるシステムの追加が発生した場合など、SLA の目標値の達成に向け、適正な形で運用・保守作業を実施するため。		無	サービスレベルを遵守できなかった場合に実施する対応に係る費用は受注者にて負担するものとするため、意見は採用しない。なお、新たな施策等によるシステムの追加が発生した場合については、SLA に限らず別途協議することとする。
226	3_別紙 1_拠点一覧及び拠点ごとの PC 台数等の情報	-		PC の導入拠点多く、導入業者の提案ベースで PC の据付スケジュールをご提示した場合、貴館の想定スケジュールと大幅な乖離があった際、スムーズなご対応が難しくなる可能性があるため、現在想定されている PC の据付および回収スケジュールをご提示いただけますでしょうか。	展開作業計画の立案・ご提案・試算に係わるため。		無	特許庁庁舎・三井ビル拠点は、稼働前に PC を受注者から情報・研修館職員の代表に渡し、代表者から利用者個人に配布する想定である。受注者から情報・研修館職員の代表に渡すタイミングは、稼働前の1ヶ月前後を想定しているが、受注後に協議可能である。それ以外の拠点は、受注者が現地で拠点構築作業を行う際、利用者個人(または代表者)に渡すことを想定している。タイミングは、各拠点の構築タイミングにより様々であるため、



								受注後に検討予定である。 なお、現行システムで利用している PC の回収は、発注者側で行う。回収スケジュールは現時点で未決定である。
227	4_別紙 2 提供サービス・機能 一覧	2	1. 認証基盤サービス 業務系 NW	シングルサインオン技術を活用して～(3)にて認証情報は拠点内またはデータセンターに設置したサーバーに格納・管理との指定がありますが、クラウドサービスとして、シングルサインオン基盤を提供しているソリューションもございます。そのため、クラウドサービスも認証情報の格納・管理先として追記いただけませんかでしょうか。	Office 365 に対する認証基盤をクラウド化することにより、ActiveDirectory(認証基盤)が障害が発生しても、Office 365 の継続利用ができるような構成も組むことができ、障害対策及び BCP 対策に繋がると考えます。	資料名:HDE One 紹介資料 該当ページ:19 ページ ※赤字箇所	有	意見を踏まえ、拠点内またはデータセンター設置と同等以上のセキュリティおよびコストメリットを担保する場合は、クラウドサービスの活用も許容することとする。
228	4_別紙 2 提供サービス・機能 一覧	3	1.認証基盤サービス ・統合 ID 管理機能 を提供すること。 (1)	ディレクトリ以外にも情報連携する必要があるシステムがあれば情報をいただきたく存じます。	費用試算のため。		無	認証基盤サービスは、情報基盤システムのディレクトリに関連する以下のサービスと情報連携することを想定している。 ・クライアント PC サービス ・クライアントソフトウェアサービス ・共有ストレージサービス ・グループウェアサービス ・コミュニケーションサービス ・イントラサービス ・複合機サービス ・業務用サーバ提供サービス ・セキュリティ対策サービス ・活用するクラウドサービス なお、情報基盤システム、情報基盤システムが接続するクラウドサービス外のシステムと情報連携する予定はない。
229	4_別紙 2 提供サービス・機能 一覧	3	1.認証基盤サービス ・統合 ID 管理機能 を提供すること。 (2)	生体による主体認証データの管理方法について、クライアント PC のみで管理するものか、別途管理サーバで管理するものか明確にしていただければと思います。	セキュリティ上、生体データはサーバ上に一元管理するほうが良いものと考えます。		無	クライアント PC のみで管理し、OS が持つ機能を最大限に活用することを想定している。
230	4_別紙 2 提供サービス・機能 一覧	3	1.認証基盤サービス ・統合 ID 管理機能 を提供すること。 (3)	3 種類のデータは全て別ファイルで別フォーマットのファイルかを明確にいただきたく存じます。	費用試算のため。		無	全て CSV ファイルの別ファイルで提供する予定である。
231	4_別紙 2 提供サービス・機能 一覧	3	1.認証基盤サービス ・統合 ID 管理機能 を提供すること。 (3)	3 種類のデータを出力する源泉となるシステムを明確にしていいただきたく存じます。	要件の理解のため。		無	情報・研修館にて作成し、提供する予定である。
232	4_別紙 2 提供サービス・機能 一覧	3	1. 認証基盤サービス (5)組織データには	(iii)適用会議年月日、適用終了年月日とあるが、適用開始年月日、適用終了年月日が正しい記載ではないでしょうか。	誤字と思われるため。		有	意見のとおり修正する。

233	4.別紙2 提供サービス・機能 一覧	4	1.認証基盤サービス 機密性情報系 NW 3 ポツ目 (5)	文面から「適用開始年月日」の誤記と思われます。	要件確認のため。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
234	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW	下線の追加をお願いいたします 『ID/Password、証明書ベース等』	セキュリティ確保の提案ソリューションを広げられるため。 証明書ベースとすることで ID/Password 以上のセキュリティ強度を確保できるため。	補足資料 ③ Windows Hello for Business	有	意見を踏まえ、要件定義書の別紙2「提供サービス・機能一覧」の「2. クライアント PC サービス 業務系 NW」の一部記載を以下に修正する。 ----- 情報基盤システムのドメインへログインする際に生体認証と ID/Password、証明書ベース等の生体認証とは異なる認証を併せた多要素認証を行うこと。 -----
235	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW	下線の追加をお願いいたします 『オンライン・オフラインの動作切替はネットワークへの接続状況等から自動で判別し切替が行われるようにすることが望ましい。』	ネットワークの状態からオンライン・オフラインの判定を 100%確実に実行することが難しいと考えられるため、要件の緩和をお願いいたします。		有	意見を踏まえ、要件定義書の別紙2「提供サービス・機能一覧」の「2. クライアント PC サービス 業務系 NW」の一部記載を以下に修正する。 ----- オンライン・オフラインの動作切替はネットワークへの接続状況等から自動で判別し切替が行われるようにすることが望ましい。 -----
236	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW 5 ポツ目	「オフライン利用時には処理は端末を利用し、データは一時的に PC のメモリ上に保存し、ネットワーク接続時にクラウドサービス上またはデータセンターのサーバに保存可能なこと」とありますが、ネットワーク接続時のデータの保存は自動・手動を問わず適切な手段でクラウドサービス上またはデータセンターのサーバに保存できればよいという認識でよろしいでしょうか。	要件確認のため。		有	意見 No.235 を参照すること。
237	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW 6 ポツ目	クライアント PC にて、ネットワークの状況からオンライン／オフラインを自動判別は難しいと考えるため、『自動判別が望ましい』という文言の追加をお願いいたします。	標準機能での実現が難しく、コスト増につながる恐れがあるため、提案の幅を広げるためにも条件の緩和をお願いいたします。		有	意見 No.235 を参照すること。
238	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW	「オンライン・オフラインの動作切替はネットワークへの接続状況等から自動で判別し切替が行われるようにすること。」と記載がございますが、自動切り替えは「オンラインからオフライン」が実装必須と考えます。一方、「オフラインからオンライン」も実装することでネットワーク不安定時に切替が頻発してしまう可能性があることから、「オンラインからオフライン」への動作切替を自動判別し切り替わること』といった記載をご検討ください。	ネットワークが不安定な際に切替え頻発になる事象を避けるため		有	意見 No.235 を参照すること。

239	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス	クライアント PC サービスの要件全般について、知財総合支援窓口拠点以外の拠点についても、仮想デスクトップ型環境の採用をご検討されてはいかがでしょうか。 なお、以下弊社提出意見の No.240~243、250~253 については、上記前提とした場合の仕様要件の修正案を記載いたします。	仮想デスクトップ型環境は、クライアント環境のセキュリティ対策の維持等に優位性があり、提案者の選択肢に物理 PC のみではなく、仮想デスクトップ環境を含めることで、コストを含めより最適な提案を可能とするため。		有	意見を踏まえ、以下のとおり修正する。 ----- セキュア PC と同等の要件を満たし、コストメリットを担保できるのであれば、仮想デスクトップ環境によるクライアント PC サービスの提供の提案も可とする。 -----
240	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW	「業務系 NW 接続時は CPU、メモリ等のリソースは端末のものを利用して処理し、データの格納先はクラウドサービス上またはデータセンターに保存すること。」について、「ただし、仮想デスクトップ型環境を採用する場合を除く。」を追記いただきたい。	仮想デスクトップ型環境の採用を考慮した場合、CPU、メモリ等はシンクライアントサーバのリソースを利用するため。		有	意見 No.239 を参照すること。
241	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW	「オフライン利用時には処理は端末を利用し、データは一時的に PC のメモリ上に保存し、ネットワーク接続時にクラウドサービス上またはデータセンターのサーバに保存可能なこと(メモリに保存されたデータは PC 電源 OFF により消去されること)。」の後に「ただし、仮想デスクトップ型環境を採用する場合を除く。」を追記いただきたい。	仮想デスクトップ型環境を採用する場合は、オフラインの利用を想定しないため。		有	意見 No.239 を参照すること。
242	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW	「オンライン・オフラインの動作切替はネットワークへの接続状況等から自動で判別し切替が行われるようにすること。」の後に「ただし、仮想デスクトップ型環境を採用する場合を除く。」を追記いただきたい。	仮想デスクトップ型環境を採用する場合は、オフラインの利用を想定しないため。		有	意見 No.239 を参照すること。
243	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス 業務系 NW	「Windows 10 Enterprise が提供する仮想化ベースのセキュリティ対策機能を利用できるハードウェア端末であること。」の後に「ただし、仮想デスクトップ型環境を採用する場合を除く。」を追記いただきたい。	該当箇所が、仮想デスクトップ型環境を採用しない場合のセキュリティ対策を想定した要件であるため。		有	意見 No.239 を参照すること。
244	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス	オフライン利用時には処理は端末を利用し、データは一時的に PC のメモリ上に保存し、とありますが、オンライン時でもメモリ上のデータ保存領域は作成され、利用するしないはユーザの判断、という認識でよろしいでしょうか。	メモリ上の一次保存領域の性質と使用方法をユーザへ周知することで違和感なく利用できると考えます。		有	意見 No.235 を参照すること。オンライン時はデータの保存領域はファイルサーバ上となる。ユーザがデータの保存領域を選択するのではなく、端末が自動でネットワークの状態を判別することが望ましい。
245	4.別紙2 提供サービス・機能 一覧	4	2. クライアント PC サービス	クライアント PC サービスのオフライン利用時には PC が保有するメモリ上に情報を一時保管し、ネットワーク接続時にサーバに通常通り保管されるが、ネットワークが接続状態にならず作業中のデータは、PC サービス自体が保有するバッテリー持続する間は保有するが、消耗による稼働できなくなった場合の想定処理をご教授頂きたい。	仕様を明確にするため		無	ネットワーク接続前に、バッテリー消耗により稼働できなくなった場合には、サーバへの保管対象外(保管不可能)となる想定である。
246	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス業務系 NW 端末仕様	CPU につきまして、「Intel Core i5-4200M プロセッサ(2.50GHz)相当以上を有すること。」とございますが、「Core i5-6200U プロセッサ(2.30GHz)相当以上を有すること。」へ記載の変更をご提案申し上げます。	本件、OS を Enterprise にて使用されると理解しました。 その場合、Core i5-6200U プロセッサ(2.30GHz)(第 6 世代以降)以上が搭載された PC でないと、正常起	—	有	意見のとおり修正する。

					動に起因するドライバが対応できていない為、変更のご提案を申し上げます。			
247	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス 業務系 NW	「Intel Core i5-4200M Processor (2.50GHz)相当以上を有すること」と記載がありますが、製品による必須要件でなければ Intel Core(TM) i5-6200U プロセッサ(2.3-2.8GHz/3MB)でのご提案を許容頂けないでしょうか。	インストールアプリケーション等による必須要件で無ければ、PC スペックについては詳細な記載は避けてご提案機種の選択肢を増やして頂けるようご検討をお願い致します。		有	意見 No.246 を参照すること。
248	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス	内蔵型補助記憶装置ドライブの容量は、最低要件ですと OS のほかに必要なアプリケーションを導入した後で、業務上の操作で必要な空き容量が確保できますでしょうか。	・業務系 NW 用の場合、OS:20GB、仮想メモリ:12GB の合計約 32GB を消費します。残り 32GB で必要なアプリケーションを導入した後、ワークスペースで数 GB の容量が確保できなければ、パフォーマンスに影響が出る恐れがあります。 ・機密性情報系 NW 用では同様に、OS と仮想メモリの合計で約 26GB となり、空き容量は 6GB しかありません。 ※仮想メモリのサイズの目安は、物理メモリ x 1.5 倍としています。		無	クライアント PC サービスに係る要件を満たす方式を踏まえ、内蔵型補助記憶装置ドライブの容量を提案すること。ただし、クライアント端末内には最小限のデータしか保存しないこととし、システム領域を除く業務データは原則ファイルサーバ上に格納するように留意すること。なお、機密性情報系 NW 端末については、調達範囲に関する意見を踏まえ、今回の調達範囲外とすることにした。
249	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス 機密性情報系 NW	下線の追加をお願いいたします 『ID/Password、証明書ベース等』	セキュリティ確保の提案ソリューションを広げられるため。証明書ベースとすることで ID/Password 以上のセキュリティ強度を確保できるため。	補足資料 ③ Windows Hello for Business	無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
250	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス 機密情報系 NW	「 機密系情報 NW 接続時は CPU、メモリ等のリソースは端末のものを利用して処理し、データの格納先はクラウドサービス上またはデータセンターに保存すること。」について、「ただし、仮想デスクトップ型環境を採用する場合を除く。」を追記いただきたい。	仮想デスクトップ型環境の採用を考慮した場合、CPU、メモリ等はシンクライアントサーバのリソースを利用するため。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
251	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス 機密情報系 NW	「 オフライン利用時には処理は端末を利用し、データは一時的に PC のメモリ上に保存し、ネットワーク接続時にデータセンターのサーバに保存可能なこと(メモリに保存されたデータは PC 電源 OFF により消去されること)。」の後に「ただし、仮想デスクトップ型環境を採用する場合を除く。」を追記いただきたい。	仮想デスクトップ型環境を採用する場合は、オフラインの利用を想定しないため。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
252	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス 機密情報系 NW	「 オンライン・オフラインの動作切替はネットワークへの接続状況等から自動で判別し切替が行われるようにすること。」の後に「ただし、仮想デスクトップ型環境を採用する場合を除く。」を追記いただきたい。	仮想デスクトップ型環境を採用する場合は、オフラインの利用を想定しないため。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。

253	4.別紙2 提供サービス・機能 一覧	5	2. クライアント PC サービス 機密情報系 NW	「 Windows 10 Enterprise が提供する仮想化ベースのセキュリティ対策機能を利用できるハードウェア端末であること。」の後に「ただし、仮想デスクトップ型環境を採用する場合を除く。」を追記いただきたい。	該当箇所が、仮想デスクトップ型環境を採用しない場合のセキュリティ対策を想定した要件であるため。		無	調達範囲に関する意見を踏まえ、機密情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
254	4.別紙2 提供サービス・機能 一覧	5	機密情報系 NW 5 ポツ目	「オフライン利用時には処理は端末を利用し、データは一時的に PC のメモリ上に保存し、ネットワーク接続時にデータセンターのサーバに保存可能なこと」とありますが、ネットワーク接続時のデータの保存は自動・手動を問わず適切な手段でデータセンターのサーバに保存できればよいという認識でよろしいでしょうか。	要件確認のため。		無	調達範囲に関する意見を踏まえ、機密情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
255	4.別紙2 提供サービス・機能 一覧	6	2 クライアント PC サービス 仮想デスクトップ 要求一覧 No1 接続形態等	CPU の要求仕様において、仮想デスクトップを想定した仕様への変更をお願いします。 (修正案)CPU:2.1GHz 2vCPU 以上	仮想デスクトップであるため、ここで 2core と記載すると物理サーバの CPU 物理コア数と混同し誤解を招く恐れがあります。		無	調達範囲に関する意見を踏まえ、機密情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
256	4.別紙2 提供サービス・機能 一覧	6	2. クライアント PC サービス 機密情報系 NW 6 ポツ目	クライアント PC にて、ネットワークの状況からオンライン/オフラインを自動判別は難しいと考えるため、『自動判別が望ましい』という文言の追加をお願いいたします。	標準機能での実現が難しく、コスト増につながる恐れがあるため、提案の幅を広げるためにも条件の緩和をお願いいたします。		無	調達範囲に関する意見を踏まえ、機密情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
257	4.別紙2 提供サービス・機能 一覧	6	2. クライアント PC サービス 機密情報系 NW	「Intel Core i3-4000M Processor (2.40GHz) 相当以上を有すること。」と記載がありますが、製品による必須要件でなければインテル Core™ i3-6100U プロセッサ (3MB キャッシュ、2.3GHz) でのご提案を許容頂けないでしょうか。	インストールアプリケーション等による必須要件で無ければ、PC スペックについては詳細な記載は避けてご提案機種の選択肢を増やして頂けるようご検討をお願い致します。		有	意見 No.258 を参照すること。
258	4.別紙2 提供サービス・機能 一覧	6	2. クライアント PC サービス機密情報系 NW 端末仕様	CPU につきまして、「Intel Core i3-4000M プロセッサ (2.40GHz)相当以上を有すること。」とございますが、「Core i3-6100U プロセッサ(2.30GHz)相当以上を有すること。」へ記載の変更をご提案申し上げます。	本件、OS を Enterprise にて使用されると理解しました。 その場合、Core i3-6100U プロセッサ (2.30GHz) (第 6 世代以降)以上が搭載された PC でないと、正常起動に起因するドライバが対応できていない為、変更のご提案を申し上げます。	—	有	調達範囲に関する意見を踏まえ、機密情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。 なお機密情報系 NW クライアント PC と同等のスペックを想定していた持ち込み媒体サンドボックス PC については、意見を踏まえ Core™ i3-6100U プロセッサ (3MB キャッシュ、2.3GHz) 相当以上に修正する。
259	4.別紙2 提供サービス・機能 一覧	7	2 クライアント PC サービス 仮想デスクトップ 要求一覧 No1 接続形態等	仮想デスクトップでの OA 業務を前提に置いた場合、IOPS は 30~40 もあれば十分と考えます。現在の「IOPS 200 以上」については、OA 用途では過剰な要求仕様と考えます。	過剰な要求仕様となっており、入札価格の高騰につながります。		無	調達範囲に関する意見を踏まえ、機密情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
260	4.別紙2 提供サービス・機能 一覧	7	2. クライアント PC サービス	表の記載内容は、仮想デスクトップのものではなく、物理 PC のものを思われますが、仮想デスクトップ環境側(サーバ側)の要件があれば明記をお願いしたい。	要件確認のため。		有	意見 No.239 を参照すること。

261	4_別紙2 提供サービス・機能 一覧	10	3.10 ファイル圧縮、解凍機能 機密性情報系 NW	「多様な形式のファイル圧縮、解凍ができ、パスワードにも対応できる機能(「ALZip」相当の機能)を提供すること。「ALZip」相当の機能を提供すること。」  文末の「「ALZip」相当の機能を提供すること。」は文章が重複しているため、誤記と思われるので削除をお願いいたします。	誤記のため		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
262	4_別紙2 提供サービス・機能 一覧	10	3.13 個別業務処理機能	個別の業務処理システムへの接続方式について、指定はございますでしょうか。	要件確認のため。		無	個別の業務処理システムへの接続方式についての指定はない。
263	4_別紙2 提供サービス・機能 一覧	11	4. 共有ストレージサービス	以下の要件を削除いただきたい。 「フォルダごと、利用者及びグループに対して使用量制限を設定できること」	本要件は特定のクラウドサービスに限定する内容であると思われます。 実現する場合はコストに大きく影響するうえ、本要件の削除によるセキュリティレベルへの影響は無いため、公平性の観点から削除をお願いいたします。		有	意見を踏まえ、以下のとおり修正する。  ----- フォルダごと、利用者及びグループに対して使用量制限を設定できることが望ましい。  -----
264	4_別紙2 提供サービス・機能 一覧	11	4. 共有ストレージサービス 機密性情報系 NW 1 ポツ目	「利用者のデータを利用者専用の領域、…」とありますが、機密性情報系 NW に利用者専用の領域(個人用領域)は不要という認識です。	右記要件定義書内において、機密性情報系 NW に個人用のストレージは対象外となっており、要件確認のため。	要件定義書 P7 3.3 規模に関する事項 (2) データ量 図表3-3-1 データ量 No.3 個人ストレージ	無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
265	4_別紙2 提供サービス・機能 一覧	11	4. 共有ストレージサービス 機密性情報系 NW 7 ポツ目	業務系 NW とは異なる共有方式を定義しておりますでしょうか。	「機密性の高いデータ」として特記されておりますが、機密性情報系 NW はインターネットと接続しないことが前提ですので、特に「機密性の高いデータ」と明記されていることより、業務系 NW とは異なる共有方式を必要とされていると捉えることができます。 要件の確認をさせていただきます。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにした。
266	4_別紙2 提供サービス・機能 一覧	11	4. 共有ストレージサービス 機密性情報系 NW	・機密性の高いデータについては、物理的にインターネットと接続しないネットワーク状態で、組織、拠点内及び任意のグループで共有、保存するための機能を提供すること。  ネットワーク仮想化技術を利用した論理的なネットワーク分離においても、十分にセキュリティを確保した上でコストメリットのあるネットワークの構築が可能となりま	コスト最適化のため		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。

				すので、ネットワークについては論理的な分離での提案を許容頂けますようお願いいたします。				
267	4_別紙2 提供サービス・機能 一覧	13	5.5 全文検索機能	次の文言の削除をお願いいたします。 『一太郎7以上』	製品選定の幅を広げるため。		有	意見を踏まえ、一太郎は全文検索の対象から除外することとする。
268	4_別紙2 提供サービス・機能 一覧	13	5. グループウェアサービス 業務系 NW 5.5 全文検索機能 4 ポツ目	別添資料 1 に例示されている Office365(Sharepoint Online)の全文検索にて、ファイル名のみで『一太郎 7 以上』の中身がクローリングできないため、『一太郎 7 以上』の文言削除をお願いいたします。	標準機能での実現が難しく、コスト増につながる恐れがあるため、提案の幅を広げるためにも条件の緩和をお願いいたします。		有	意見 No.267 を参照すること。
269	4_別紙2 提供サービス・機能 一覧	13	5. 5 全文検索機能	検索対象として一部の文書形式は全文検索できるソフトウェアが限られておりますので、対象除外の文書形式について検討いただきますようお願いいたします。	ご提案機器構成に関連するため。		有	意見 No.267 を参照すること。
270	4_別紙2 提供サービス・機能 一覧	13	5.5 全文検索機能	要件定義書 P9 では機密性情報系 NW にも必要の○が付いているが、このページでは不要となっております。 どちらの記載が正でしょうか。	要件の理解のため。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
271	4_別紙2 提供サービス・機能 一覧	14	6.1 メール機能	下線の文言へ変更をお願いいたします 『証跡確保のためメールを複製または原本保証の上』	製品選定の幅を広げるため。 『複製』せずにメール原本を保証する仕組みがあり、複製タイプ、別の方法による原本保証タイプのどちらの製品も提案できるようにするため。		有	意見を踏まえ、要件定義書の別紙 2「提供サービス・機能一覧」の「6.1. メール機能」の一部記載を以下に修正する。 ----- 館内・館外間のメール送受信時において、証跡確保のためメールを複製または原本保証の上、2 年間以上保管できること。メールの容量については、「3. 5 信頼性に関する事項」を参照すること。また、保管されたメールを必要に応じて検索・参照できること。 -----
272	4_別紙2 提供サービス・機能 一覧	14	5. コミュニケーションサービス 6.1 メール機能 業務系 NW 14 ポツ目	「館外から受け取るメールは全てプレーンテキストに変換すること」につきまして、クライアントにて受け取るメールを、全てプレーンテキストで表示することで仕様を満たすという認識でよろしいでしょうか。	要件確認のため。		無	館外同様に、情報・研修館内での送受信時のメールも全てプレーンテキストになっても構わない。
273	4_別紙2 提供サービス・機能 一覧	14	6.1 メール機能	下線の追加をお願いいたします 『館外からのメールは全てプレーンテキストに変換することが望ましい。』	製品選定の幅を広げるため プレーンテキストにすることで、悪意のある URL を発見させることを目的と推測しておりますが、人間に任せずシステム側で URL を確認する方法を利用することで安全性が向上します。 プレーンテキストを人間が確認する場合、紛らわしく、判別しにくい URL を人間が正確に判断すること	補足資料 ④ Office 365 Advanced Threat Protection 概要	有	意見を踏まえ、要件定義書の別紙 2「提供サービス・機能一覧」の「6.1. メール機能」の一部記載を以下に修正する。 ----- 館外からのメールは全てプレーンテキストに変換することが望ましい。 -----

					はユーザーに負荷を与えるため、システムの活用を推奨いたします。			
274	4.別紙2 提供サービス・機能 一覧	14	6.1 メール機能	下記の要件の追加をお願いします。  ・メール送受信時に、サーバ側で複数のメーカーのエンジンによるアンチウイルスチェックを行うこと	メール送受信に関しては、クライアントPCと異なるウイルスチェックは当然のこと、サーバ側でも多段で実施することで、ウイルスメールのすり抜けを未然に防止できます。  一般的なメールセキュリティサービスにおいて標準で対応している機能だと存じますので、コスト増にならずセキュリティレベルを向上できる内容として、本要件の追加をお願いします。		無	必須の要件とする必要はないと判断し、意見は採用しない。
275	4.別紙2 提供サービス・機能 一覧	14	6.1 メール機能	下記の要件の追加をお願いします。  ・スパムメールについては、該当のメールを隔離し、隔離レポートとして定期的に利用者へ通知すること。隔離レポートは、本文も含めてメールボックスとは別のセキュアな環境で確認できること。	スパムメール対策については、日々精度の向上は行われていても、誤判定を完全になくすことは難しいです。 一方、業務でやり取りされるメールの場合、誤って迷惑メールと判定されてしまい、気づかず受信できないと、業務に影響が出てしまいます。そのため、迷惑メールと判定されたものは隔離メールとして保存し、その内容を定期的に利用者へ通知することで、誤判定による業務影響を格段に少なくすることが可能です。また、隔離メールの確認の際に大事なポイントは、メールボックスへリリースすることなく、隔離されたメールの内容が確認できることとなります。  一般的なメールセキュリティサービスにおいて標準で対応している機能だと存じますので、コスト増にならずセキュリティレベルを向上できる内容として、本要件の追加をお願いします。		無	必須の要件とする必要はないと判断し、意見は採用しない。
276	4.別紙2 提供サービス・機能 一覧	14	6.1 メール機能	下記の要件の追加をお願いします。  送信メールに対し、Content-Type および拡張子による検査を行い、外部への送信がふさわしくないファイルあった場合、送信を保留できること。	送信メールは、セキュリティ対策を怠りがちですが、拡張子やキーワードに不適切なものが含まれていないかのチェックは非常に重要です。		無	必須の要件とする必要はないと判断し、意見は採用しない。



				<p>また、送信メール本文と添付ファイルに含まれる文字列に対して、キーワードで検査を行い、個人情報など外部への送信がふさわしくない単語が含まれていた場合、送信を保留できること。</p>	<p>特にメールからの個人情報漏えい事件は日増しに増えており、対策強化が必須です。</p> <p>昨今では、メール監査の機能は一般的なメールセキュリティ製品にて提供されており、費用についても情報漏えいリスクによる影響と比較すれば大きな影響があるものではないため、要件への追加をお願いします。</p>		
277	4_別紙2 提供サービス・機能 一覧	14	6.1 メール機能	<p>下記の要件の追加をお願いします。</p> <p>「なりすましメールを防ぐための送信ドメイン認証として SPF (Sender Policy Framework : RFC4408) 及び DKIM (DomainKeys Identified Mail : RFC4871) に送受信とも対応していること。」</p>	<p>マルウェアを含むメールの大半はなりすましメールであることから、なりすまし対策をおこなうことが、セキュリティ強化にとって SPF, DKIM は最も重要な方法の一つであるためです。</p> <p>中央省庁や独立行政法人においてはほぼ全ての組織で導入されております。</p> <p>一般的なメールセキュリティサービスにおいて標準で対応している機能だと存じますが、仮に現時点で要件に記載がなく対応していない製品が導入された場合、後にコスト増の要因になります。</p> <p>最低限のセキュリティレベル遵守のため、本要件の追加をすべきと考えます。</p>		<p>有</p> <p>意見を踏まえ、以下のとおり修正する。</p> <p>-----</p> <p>なりすましメールを防ぐためのドメイン認証として SPF (Sender Policy Framework : RFC4408) に対応していること。DKIM (DomainKeys Identified Mail : RFC4871) は対応していることが望ましい。</p> <p>-----</p>
278	4_別紙2 提供サービス・機能 一覧	14	6.1 メール機能	<p>下記の要件の追加をお願いします。</p> <p>「任意のドメインに対し、SPF の認証結果が成功以外の場合に受信拒否する設定がおこなえること。」</p>	<p>上記のとおり、SPF の認証結果をもとに受信拒否する機能はセキュリティ上極めて重要です。</p> <p>ただし、全てのドメインが SPF に対応しているとは限らないため、単に SPF の結果に基づくフィルタではなく、ドメインごとに SPF の結果に基づくフィルタが必要です。(本機能を有しないと、事実上 SPF に基づくフィルタをおこなうことができないと考えます)</p>		<p>有</p> <p>意見を踏まえ、別紙 2「提供サービス・機能一覧」の「6.1 メール機能」に以下を追記する。</p> <p>-----</p> <p>任意のドメインに対し、SPF の認証結果が成功以外の場合に、受信拒否や注意喚起等の設定がおこなえること。</p> <p>-----</p>

					一般的なメールセキュリティサービスにおいて標準で対応している機能だと存じますので、コスト増にならずセキュリティレベルを向上できる内容として、本要件の追加をお願いします。			
279	4_別紙2 提供サービス・機能 一覧	14	6.1 メール機能	下記の要件の追加をお願いします。  「添付ファイルに対してサンドボックス機能による振る舞い検知をおこない、マルウェアの可能性があると判断された場合は、対象のファイルをブロックすること。また、振る舞い検知をおこなう仮想環境は日本語 OS とすることとし、仮想環境では動作しないマルウェアへの対策として、リバースエンジニアリング機能も提供すること。また、タイムアウト時間の設定や検査対象、対象外の送受信者設定が可能であること」	サンドボックス機能については、要件定義書 P16 にも記載はあるものの、詳細に関する記載がないため、提供サービス・機能一覧に記載をお願いいたします。  また、振る舞い検知については英語 OS や仮想環境では動作しないマルウェアも存在するため、それらへの対策が必須であると考えます。  メールセキュリティサービスにおいて、サンドボックス機能としては一般的に標準で対応している機能であるうえ、個別にアプライアンス機器を構築・運用するのに比べ、コストを格段に下げることが可能です。セキュリティレベル向上のため、本要件の追加をお願いします。		無	必須の要件とする必要はないと判断し、意見は採用しない。
280	4_別紙2 提供サービス・機能 一覧	14	6.1メール機能 業務系 NW	アーカイブに関して、管理者にて検索したログを取得することが明記されていないため、監査上必要ではないでしょうか。	メール検索者がどのような内容を検索・閲覧したのかといった特権監査の仕組みが必要と考えます。メール検索者のログがないと不必要な検索や閲覧が発生していたかを追うことができません。		無	必須の要件とする必要はないと判断し、意見は採用しない。
281	4_別紙2 提供サービス・機能 一覧	14	6.1メール機能 業務系 NW	メールの宛先、件名、本文、添付ファイル等の指定した条件に基づき送信を制限できること。とございますが、添付ファイル(添付ファイル内のキーワード含む)とされた方が良いでしょう。	添付ファイルのみの記載ですと、添付ファイルが付いているかどうかだけでは判断できないソリューションもございますので、機密ファイルの流出を防ぐには、添付ファイル内のキーワードも送信制御できることが必要と考えます。		無	必須の要件とする必要はないと判断し、意見は採用しない。
282	4_別紙2 提供サービス・機能 一覧	14	6.1メール機能 業務系 NW	コミュニケーションサービスをクラウドサービスで提案する場合は、誤送信防止機能・添付ファイルのパスワード暗号化機能もクラウドサービスとすること。を追記されてははいかがでしょうか。	メールをクラウドサービスでご利用される場合、誤送信防止機能及び添付ファイルのパスワード暗号化機能もクラウドサービスをご利用されることで、データセンターから	資料名:HDE One 紹介資料 該当ページ:35 ページ ※構成イメージ	無	必須の要件とする必要はないと判断し、意見は採用しない。

					のネットワーク負荷の低減効果も ございます。			
283	4_別紙2 提供サービス・機能 一覧	14	6. 1メール機能 業務 系 NW	誤送信防止機能・添付ファイル及び、パスワード暗号 化機能の運用中の設定変更も提供サービスに含むこ と。 を明記された方が良いと考えます。	運用・保守業務にも明記がなく、提 供サービスによっては、お客様側 での設定変更ができず、別途有償 のものもございますので、明記され た方が安全かと思えます。		無	必須の要件としての変更の必要はないと判断 し、意見は採用しない。
284	4_別紙2 提供サービス・機能 一覧	16	8. 複合機サービス	印刷サービスの管理に関する要件が記載されてお りませんが、プリントサーバによる印刷サービスは必要 でしょうか。 必要な場合、ActiveDirectory での管理という理解で よろしいでしょうか。	印刷管理の要件が記載されていま せんでした。 スキャナー機能の要件が記載され ていませんでした。 印刷管理が必要な場合、プリントサ ーバが必要になるので、システム 構成に影響がございました。		有	認証機能を持つプリンタについては、プリント サーバによる ActiveDirectory と連携した印 刷サービスが必要である。利用者は任意のプ リンタで IC カード認証を行うことで、利用者の 印刷ジョブを認証したフロアプリンタから出力 する。意見を踏まえ、以下のとおり修正する。 ----- 認証機能を持つプリンタについて、利用者が 任意のプリンタで IC カード認証を行うことで、 利用者の印刷ジョブを認証したフロアプリンタ から出力できること。 -----
285	4_別紙2 提供サービス・機能 一覧	19	9. 業務用サーバ提供 サービス 機密性情報系 NW	仮想サーバの想定スペックを教えてくださいませ か。また、台数は5台想定のほか、仮想化予定の「窓ロ イントラ DB」を含めて合計6台という認識で良いで すか。	仮想ホストをサイジングするため には必要な情報です。確定情報で はなく目安でも結構です。		無	調達範囲に関する意見を踏まえ、機密性情報 系 NW の設計・構築及び運用・保守は今回の 調達範囲外とすることにしたため、本意見は 採用しない。
286	4_別紙2 提供サービス・機能 一覧	19	9. 業務用サーバ提供 サービス	運用開始後に仮想サーバが増えることはありませ か。また、リソース配分は基本スペックを基にしてどの程度 の幅を持たせることを想定されていますでしょうか。	仮想ホストをサイジングするにあ たり参考となる情報です。		無	運用期間中に仮想サーバが増える可能性が あるが、現時点では明確な想定がない。その ため、リソース増強の容易な構成の提案を期 待する。
287	4_別紙2 提供サービス・機能 一覧	19	9. 業務用サーバ提供 サービス	機密性情報系 NW につきましては物理サーバ換算で 5台程度、また「窓ロイントラ DB」用に必要リソースの 記載がございますが、業務系 NW につきましても必要 リソースの記載を仕様書にてご提示願います。	ご提案機器構成に関連するため。		無	現時点で業務系 NW で提供する業務用サー バはない。ただし、今後業務用サーバを提供 することに備えて、拡張性を考慮したシステム とすること。なお、業務用サーバ提供により、 CPU、メモリやハードディスク等のリソースが 必要になった場合には、情報・研修館と協議の 上、対応を決定することとする。
288	4_別紙2 提供サービス・機能 一覧	20	10. 内部 DNS サービ ス 機密性情報系 NW 6 ポツ目	不要な項目だと思われるので、削除をお願いいた します。	機密性情報系 NW には外部向け DNS コンテンツサーバは存在しな いとの認識です。		無	調達範囲に関する意見を踏まえ、機密性情報 系 NW の設計・構築及び運用・保守は今回の 調達範囲外とすることにしたため、本意見は 採用しない。
289	4_別紙2 提供サービス・機能 一覧	20	10.内部 DNS サービス	業務系と機密性情報系 NW とで、同一ドメインを利用 されるようですが、相互の NW の内部 DNS は別ホス トを立てて NW を分けつつ、同一のドメインをそれぞれ 独立して別管理する理解でよろしいでしょうか。	設計方針を明確にするため		無	調達範囲に関する意見を踏まえ、機密性情報 系 NW の設計・構築及び運用・保守は今回の 調達範囲外とすることにしたため、本意見は 採用しない。

290	4.別紙2 提供サービス・機能 一覧	20	11.外部公開用 DNS サービス	業務系 NW 「・外部との通信における名前解決を行う。プライマリの DNS サーバはデータセンターに設置し、セカンダリを通信キャリアが提供する DNS サービスで実現することとする。」と記載がございますが、ホスティング等の外部サービスも利用可能として頂くことを希望いたします。	外部 DNS サーバは攻撃に晒され易い為、回線等に影響を及ぼしうるデータセンター内に設置するよりも、ホスティング等の外部サービスを利用した方がセキュリティ面や運用面で優位と考えられる為。		有	意見のとおり修正する。
291	4.別紙2 提供サービス・機能 一覧	20	11. 外部公開用 DNS サービス ・GUI を用いて設定できること	セカンダリ DNS に対する要件でしょうか。それともプライマリ DNS とセカンダリ DNS 両方に適用する要件でしょうか。	提案構成が異なるため、要件確認させていただきたく存じます。		無	プライマリ DNS に係る要件であるが、セカンダリ DNS についても GUI を用いて設定できるほうが望ましい。
292	4.別紙2 提供サービス・機能 一覧	20	11.外部公開用 DNS サービス	業務系 NW に関して、逆引きの提供必要可否及び、正逆それぞれの IPv6 の名前解決の必要可否についてご記載頂くことを希望いたします。	逆引きおよび IPv6 の利用有無により、サービス構成が変更となる為。		無	必須要件とはしない。
293	4.別紙2 提供サービス・機能 一覧	21	12. LAN サービス	「また、外部 Security Operation Center 等の接続について、今後その必要性が発生した場合に、柔軟に対応できるネットワーク設計とすること。」とあるが、LAN サービスの提供範囲にて外部 SOC が接続される場合とはどうな状況を想定すればよいか。	要件確認のため。		無	データセンタ内の情報・研修館が指定した機器に接続することを想定している。
294	4.別紙2 提供サービス・機能 一覧	21	12.LAN サービス 業務系 NW 機密性情報系 NW	以下の要件を変更願います。(業務系、機密性それぞれ)  現:ネットワーク仮想化技術を利用し 変更案:ネットワーク仮想化技術等を利用し	他の項目においては「ネットワーク仮想化技術”等”を利用し」の記述となっており、相互に接続するネットワークであるため、記述も同様とする必要があると考えます。		有	意見のとおり修正する。なお、調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、機密性情報系 NW に関する意見は採用しない。
295	4.別紙2 提供サービス・機能 一覧	22	15.セキュリティ対策サービス 15.1 持込媒体サンド ボックス PC 業務系 NW	以下について、具体的にご教示ください。  持込媒体サンドボックスとは、端末内のファイルにおける不審な振る舞いを検知する機能との理解で正しいでしょうか。それとも、不審なファイルがウイルスかどうかの判定まで必要になりますでしょうか。	サンドボックス機能と振る舞い検知機能の言葉の定義を明確にする為です。		無	「持込媒体サンドボックス PC」は、持込媒体にあるデータをその PC 上で振る舞いをチェックし、検知する機能を行うための端末を指す。
296	4.別紙2 提供サービス・機能 一覧	23	16 プロキシサービス	2 つ目について、下記の通り修正をお願いいたします。  ・現在:頻繁にアクセスされるコンテンツをディスク上に蓄積し、アクセスリクエストに対し、素早くコンテンツの配信を行える機能を有すること。  ・変更案:頻繁にアクセスされるコンテンツへのアクセスリクエストに対し、素早くコンテンツの配信を行えるよう、十分な Web アクセス性能を維持できる設計を行うこと。	Web アクセス性能の維持のためには、キャッシュも一つの方法ですが、プロキシ自体の性能を向上させる方法もあります。 また、頻繁にアクセスされるコンテンツは更新頻度の高いサイトであるケースが多く、内部キャッシュにより古いコンテンツが参照されてしまう可能性も高いです。  そのため、仕様をキャッシュ機能に限定せず、手段については応札者に提案させるのが、良いと考えます。		有	意見のとおり修正する。

297	4_別紙2 提供サービス・機能 一覧	23	16 プロキシサービス	<p>下記の要件の追加をお願いします。</p> <p>「Web 経由でダウンロードを試みたファイルに対してサンドボックス機能による振る舞い検知をおこない、マルウェアの可能性があると判断された場合は、対象のファイルをブロックすること。また、振る舞い検知をおこなう仮想環境は日本語 OS とすることとし、仮想環境では動作しないマルウェアへの対策として、リバースエンジニアリング機能も提供すること」</p>	<p>未知のマルウェアの最も多い侵入経路の一つが Web 経由によるものです。</p> <p>未知のマルウェアを防ぐための現時点で最も有効な手段の一つが振る舞い検知です。</p> <p>また、英語 OS や仮想環境では動作しないマルウェアも存在するため、それらへの対策が必要と考えます。</p> <p>一般的な Web セキュリティサービスにおいて、サンドボックス機能としては標準で対応している機能だと存じますので、コスト増にならずセキュリティレベルを向上できる内容として、本要件の追加をお願いします。</p>		無	必須の要件とする必要はないと判断し、意見は採用しない。
298	4_別紙2 提供サービス・機能 一覧	23	16 プロキシサービス	<p>下記の要件の追加をお願いします。</p> <p>「クライアント PC からの Web 接続時、Web コンテンツを分離された環境で実行し、マルウェアのリスクを低減する機能を有すること。また、ファイルをローカル PC にダウンロードする際には、Web 通信に対してアンチウイルス、URL フィルタリング、サンドボックス機能を提供すること。」</p>	<p>クライアント PC からの Web セキュリティ対策に、URL フィルタリングは欠かせませんが、それで十分ではなく、NISC やセキュリティベンダ、ISP による情報を適用しても、いたちごっこであるため、当然セキュリティリスクは残ります。</p> <p>そういった対策として、Web コンテンツをダウンロードすることなく、描画情報だけを見る、仮想環境でのブラウジングが効果を発揮します。</p> <p>ただし、実際にダウンロードが必要な場合も当然ありますので、その際には、アンチウイルス、URL フィルタリング、サンドボックス機能による対策が必須であると考えます。</p>		無	必須の要件とする必要はないと判断し、意見は採用しない。
299	4_別紙2 提供サービス・機能 一覧	23	16 プロキシサービス	<p>Web フィルタに関する下記要件の追記をお願いします。</p> <ul style="list-style-type: none"> <li>・フィルタリング URL データベースがユーザー定義カテゴリ 10 を含む 110 カテゴリ以上に分類されており、適用カテゴリはユーザーが任意に設定することができること</li> <li>・フィルタリング URL データベースの閲覧規制時の挙動として、カテゴリごとに「ブロック」「許可」「パスワード</li> </ul>	<p>Web フィルタ機能については、要件定義書 P16 にも記載はあるものの、詳細に関する記載がないため、提供サービス・機能一覧に記載をお願いいたします。</p> <p>Web フィルタは既製品としては、登録した URL をフィルタするのみの簡易的なものから、用途に応じてさまざまな機能を有した製品まで多</p>		無	必須の要件とする必要はないと判断し、意見は採用しない。

				<p>解除「警告」「監視」の設定が可能であること</p> <p>・管理者画面上から、Web サイトへの投稿について、添付ファイル復元を含む HTTP/HTTPS データの内容確認が可能であること</p>	<p>数存在します。</p> <p>左記の要件を追加いただくことで、INPIT 様の業務上の Web サイト閲覧、使用要件に合わせた適切なポリシーの適用が可能となります。</p> <p>一般的な Web セキュリティサービスとしては標準で対応している機能だと存じますので、コスト増にならずセキュリティレベルを向上できる内容として、本要件の追加をお願いします。</p>			
300	別紙 2 提供サービス・機能一覧 (または別紙 5 運用保守作業項目一覧)	23 (4/5)	16 プロキシサービス (URL フィルタリング設定)	<p>Web フィルタに関する下記要件の追記をお願いします。</p> <p>・インターネットサービスプロバイダのバックボーン上で収集した悪性 URL サイト情報をフィルタリングのデータベースとして提供し、該当のウェブサイトへのアクセスを制限できること。</p>	<p>URL フィルタのブラックリスト情報追加作業は、いちごっこであり、NISC やセキュリティベンダのみの情報を適用しても、当然リスクは残ります。</p> <p>これに加え、ISP が個別に収集している情報を適用することで、よりリスクを低減させることが可能であると考えます。</p> <p>一般的な Web セキュリティサービスとしては標準で対応している機能だと存じますので、コスト増にならずセキュリティレベルを向上できる内容として、本要件の追加をお願いします。</p>		無	必須の要件とする必要はないと判断し、意見は採用しない。
301	4 別紙 2 提供サービス・機能一覧	23	17 セキュア USB メモリ	<p>容量要件の拡大</p> <p>&lt;変更案&gt; 容量は 4GB 以上とすること</p>	<p>大容量のデータを使用にも対応できるようにするため</p>		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
302	4 別紙 2 提供サービス・機能一覧	23	17. セキュア USB メモリ (3)管理用サーバ	<p>P1 の表中に利用者数が業務系 NW で 5 名とありますが、セキュア USB メモリの必要個数は、何個でしょうか。集中管理するためのサーバを構築する必要がありますでしょうか。</p>	<p>サーバによる集中管理が可能な製品は、メーカーが限定されております。</p> <p>また、使用個数が少ないのであれば、費用対効果を考慮し、要件の緩和をご検討いただきたく存じます。</p>		有	セキュア USB メモリの必要個数は、50 個である。集中管理は必要である。
303	4 別紙 2 提供サービス・機能一覧	23	17. セキュア USB メモリ	<p>セキュア USB メモリについて、想定される数量の記載を仕様書にてご提示願います。</p>	<p>調達台数確認のため。</p>		有	セキュア USB メモリの数量は、50 である。意見を踏まえ、要件定義書の別紙 2「提供サービス・機能一覧」に記載した数量を修正する。

304	4.別紙2 提供サービス・機能 一覧	25	17.セキュア USB メモリ (2)管理用端末機能	セキュア USB メモリの管理用端末について、想定される数量をご教示願います。また、機能を導入する端末は別紙1に記載の業務系 PC の台数に包括されている想定でしょうか。	調達台数確認のため。		有	セキュア USB メモリの管理用端末の数量は、1 である。この 1 台は特許庁庁舎に設置し共用する。意見を踏まえ、要件定義書の別紙2「提供サービス・機能一覧」に記載した数量を修正する。
305	5.別紙3 情報基盤 システムの全体概要	11 6	クラウドサービスについて	クラウドサービスにおける、IaaS 系、SaaS 系と記載のあるものについて、本調達とは切り分けた方が良くかと考えます。	たとえば SaaS 型のサービスを提供できる業者は多数いるので、価格競争が生じやすいと考えます。よってトータルコスト削減につながるのではないかと考えます。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
306	5.別紙3 情報基盤 システムの全体概要	11 6	クラウドサービスについて	上記同様	直近、貴機構の業務において利用していない新たなサービスについては、導入時期を改めてもよいのではないのでしょうか。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
307	5.別紙3 情報基盤 システムの全体概要	-	-	データセンター(業務系 NW)、データセンター(機密性情報系 NW)間の「データ授受専用機器」の機能要件が別紙2に記載ないため、定義が必要であれば記載いただきたい。自由提案であれば不要です。	-		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
308	5.別紙3 情報基盤 システムの全体概要	-	クラウドサービスとの 接続について	IaaS 系に構築されるシステムは Internet に晒す必要の無いシステムと考えられるため、IaaS との接続は各クラウドベンダーがサービスする専用線接続サービスにすべきと考えます。	Microsoft Azure、AWS などの主要クラウドベンダーは、組織とのセキュアな接続を実現するために専用線接続サービス(express Route や DirectConnect など)のサービスを提供しているため、これを利用した方がセキュリティを担保する事が可能であるため。		有	意見を踏まえ、閉域網での接続が望ましい旨を別紙3「情報基盤システムの全体概要」に補記する。
309	6.別紙4 ネットワーク構成図	-	構成図	パブリッククラウドへの接続回線について、下記に変更をお願いします。  ・現在:SSL/TLS or 閉域接続 ・変更案:閉域接続	ベストエフォートタイプのインターネット回線を利用してクラウドを利用した場合、トラフィックの逼迫による通信断が発生する可能性があります。(特に、WindowsUpdate 等セキュリティ対策のためのデータを外部からダウンロードする場合等)その際には、パブリッククラウドサービスに構築されている業務系サーバやファイルサーバ、Office365 が利用不可となり、すべてのユーザに対する業務への影響が著しく大きくなります。  また、メールデータ及びファイルサーバの格納データは各職員の端末から移行する要件となっていますが、ベストエフォート回線では帯域		有	意見 No.308 を参照すること。

					が安定せず、移行計画及びリハーサル通りに実施することが困難と考えます。			
					以上の理由より、左記の要件への変更をお願いします。			
310	7_別紙 5 運用保守作業項目 一覧	1	No2、問題管理	「システム運用中に発生したセキュリティイベントについては・・・」の内容はイベント管理であるため、作業項目にイベント管理を追加したうえで、移動した方がよいと考えます	作業項目には、運用保守作業に必要な各種管理項目が記載されているが、サービスマネジメントの起点となるイベント管理が、作業項目に記載されていないため		有	意見のとおり修正する。
311	7_別紙 5 運用保守作業項目 一覧	1	4 構成管理	「端末の払い出し等、試験端末の管理を行うこと」と記載がありますが、試験端末の用途及び数量をご教示頂けますでしょうか。また試験端末の準備は本調達の範囲内でしょうか。	調達台数確認のため。		無	試験端末の用途は、OS マイナーバージョンアップ等、利用者の端末環境に影響が発生する可能性があるものについて、受注者が試験端末で検証するために利用する。数量は数台程度を想定し、本調達に含む。
312	7_別紙 5 運用保守作業項目 一覧	1	7 セキュリティ管理	「製品・プロダクトに対する脆弱性情報収集・提供に加え、採用している技術や方式、アルゴリズム等も対象とした新たな脅威や脆弱性に関する情報を収集・提供すること。」と記載があり、実施頻度が「毎日」となっていますが、情報収集は毎日、報告につきましては緊急性の高いものは即時、緊急性の低いものは月次定例会にて報告とさせて頂けないでしょうか。	提示価格低減のため。		有	意見を踏まえ、以下のとおり修正する。 (項番 7 の実施頻度) ----- 情報収集は毎日 報告は緊急性の高いものは即時、低いものは月次定例会にて実施 -----
313	7_別紙 5 運用保守作業項目 一覧	1	13 会議体	「システム上の課題に対する対応状況について週次報告を行うこと。」と記載がありますが、週次報告については状況に応じてメールでの報告も可とする旨の記載をご検討願います。	提示価格低減のため。		有	意見を踏まえ、月次報告は対面必須で行い、週次は原則メールとし必要に応じて対面で実施するものとする。
314	7_別紙 5 運用保守作業項目 一覧	1	13 会議体	「改善策検討会議に参加すること。」と記載がありますが、改善策検討会議について、概要、開催頻度等を記載いただけますようご検討願います。	実施内容、開催頻度により、提示価格に差異が発生するため。		有	意見を踏まえ、項番 15 の改善策検討会議への参加要件は削除し、項番 12 の月次報告にて、発生した問題に対する改善策を検討・報告するものとする。
315	7_別紙 5 運用保守作業項目 一覧	1	項番 16 ヘルプデスク 利用者要求対応 受付	ヘルプデスクへ問い合わせる申告元に関する表記を「利用者」ではなく、より厳密に情報・研修館職員もしくは情報基盤システム利用者(「【新基盤】03_別添資料 2_要件定義書(案)の図表3-1-1 情報システムの利用者の種類、特性」を参照)に記載を変更いただきたい。	本調達においては問い合わせを受付ける対象は一般利用者(国民等)からの直接的な受付はしないものと認識しているため。		有	意見を踏まえ、以下のとおり修正する。 ----- 情報基盤システム利用者(一般利用者(国民等)は除く。) -----
316	7_別紙 5 運用保守作業項目 一覧	2	項番 18~29 ヘルプ デスク 利用者要求対応 依頼申請対応	依頼者申請対応として実施する項番 19~29 の作業に対してヘルプデスクで受付してから対応完了するまでの対応期日を明確にしていきたい。	各社の見積もり条件を均質化するため。		無	対応期日については、運用計画の作成時に協議の上、決定することとする。



317	7.別紙 5 運用保守作業項目 一覧	2 3 5	19 認証基盤サービス 24 IC カード再発行手 続き 25 アカウント無効化 27 IC カード忘れ対応 28 パスワード初期化 29 アカウントロック解 除 34 盗難・紛失対応 47 セキュア USB メモ リ運用 110 セキュリティ保持 対応	以下の運用業務については即時的な対応が求められる業務であり、受注者による非常駐での対応は困難と考えております。受注者による手順の提示・電話等による支援のもと、貴館によるご対応をご検討頂けないでしょうか。 ・パスワード初期化 ・アカウントロック解除 ・毀損・紛失した IC カード情報を本システムから削除すること。 ・利用者が IC カードを紛失した場合、不正利用されないよう IC カードアカウントを無効化すること。 ・利用者が IC カードを忘れた場合、1 日限定パスワードを発行すること。 ・利用者が IC カードパスワード又はシングルサインオンパスワードを忘れた場合、これらパスワードを初期化すること ・利用者が一定回数以上パスワードを間違えてアカウントがロックされた場合、アカウントロックを解除すること ・盗難又は紛失の報告を受けた端末及びモバイル端末に対して、ネットワーク接続を遮断すること。 ・セキュア USB メモリを紛失した場合、紛失 USB メモリを利用不可能にし、新たに USB メモリを払い出すこと。 ・セキュリティ侵害の拡散を防止する対応(障害対象機器のネットワーク切り離し、ウイルス駆除等)を行うこと。	即時的な対応が必要となる業務であり、非常駐の運用体制では迅速な対応が困難であるため。また提示価格の低減が見込めるため。		有	意見 No.322、201 を踏まえて、以下の作業はマニュアルベースで情報・研修館職員が行うこととする。ただし、受注者は、職員が初期化を行う際に必要な資材(初期化ツール、マニュアル等)を準備し、提供すること。なお、職員にて実施することが困難であると想定する作業は受注者にて実施すること。  ・毀損・紛失した IC カード情報を本システムから削除すること。 ・利用者が IC カードを紛失した場合、不正利用されないよう IC カードアカウントを無効化すること。 ・利用者が IC カードを忘れた場合、1 日限定パスワードを発行すること。 ・利用者が IC カードパスワード又はシングルサインオンパスワードを忘れた場合、これらパスワードを初期化すること ・利用者が一定回数以上パスワードを間違えてアカウントがロックされた場合、アカウントロックを解除すること ・セキュア USB メモリを紛失した場合、紛失 USB メモリを利用不可能にし、新たに USB メモリを払い出すこと。
318	7.別紙 5 運用保守作業項目 一覧	2	20 クライアントソフト ウェアサービス	申請依頼対応の項目として「ソフトウェア利用申請」との記載がありますが、利用可能なソフトウェア一覧にないソフトウェアの利用可否については、受注者の支援のもと、貴館にて判断いただけるという想定でよろしいでしょうか。	ソフトウェアの利用可否の最終判断については、貴館にて決定いただく必要があると考えるため。		無	認識のとおりである。
319	7.別紙 5 運用保守作業項目 一覧	2	22 グループウェアサ ービス	申請依頼対応の項目として「電子掲示板設定変更」と記載がございますが、電子掲示板の設定変更については、掲示板全体に係る設定変更等は受注者が実施し、掲載されるコンテンツについては貴館が実施するという理解でよろしいでしょうか。	電子掲示板内のコンテンツについては、受注者が閲覧することが好ましくない内容も含まれることが想定されるため。		無	認識のとおりである。
320	7.別紙 5 運用保守作業項目 一覧	2	項番 34 ヘルプデスク 端末運用 盗難・紛失対応	項番 34 の作業に対してヘルプデスクで受付してから対応完了するまでの対応期日を明確にさせていただきたい。	各社の見積もり条件を均質化するため。		無	意見 No.316 を参照すること。
321	7.別紙 5 運用保守作業項目 一覧	2	34 盗難・紛失対応	「盗難又は紛失の報告を受けた端末及びモバイル端末に対して、ネットワーク接続を遮断すること。」と記載	仕様書、要件定義書の他の項目にも表記がない機器であるため。		有	意見を踏まえ、モバイル端末の記載を削除する。

				がありますが、ここでの「モバイル端末」とは何を指すものかの記載を仕様書にてご提示願います。			
322	7.別紙 5 運用保守作業項目 一覧	2	36 端末回収	端末回収における初期化については、手順書をもとに職員様が現地で実施し、送付頂いた後に受注者が初期化を再確認する運用はいかがでしょうか。	端末上に個別データを残さない設計と考えますが、一部設定情報等が残っている状態の端末をそのまま輸送することは好ましくないため。		有 意見を踏まえ、初期化作業はマニュアルベースで情報・研修館職員が行うこととする。ただし、受注者は、職員が初期化を行う際に必要な資材(初期化ツール、マニュアル等)を準備し、提供すること。なお、ネットワーク設定等、職員にて実施することが困難であると想定する作業は受注者にて実施すること。
323	7.別紙 5 運用保守作業項目 一覧	2/ 5	作業項目: 端末障害 対応 7 ポツ目	・端末の付属品(ヘッドセット等)についても同様の対応を行うこと。 について、3 ポツ目に ・復旧が不可能な場合は、端末供給元に対して修理依頼を行い、端末を引き渡すこと。  との記載がありますが、付属品については修理対応に加え、予備の正常品または互換性のある他製品との交換対応でも可との認識でよろしいでしょうか。	クライアント端末本体は契約期間内の保守対応が可能ですが、付属品は基本的には修理ではなく予備の正常品または同等の互換品との交換対応となるため。		無 認識のとおりである。
324	7.別紙 5 運用保守作業項目 一覧	2/ 5	作業項目: 持込媒体 サンドボックス管理、 緊急避難用サンドボ ックス検知対応	「緊急避難用端末」はどのような端末でしょうか。運用中のサンドボックス PC とは別に、同じ構成の予備端末をあらかじめ常備しておくということでしょうか。それとも、一般のクライアント PC を応急的にサンドボックス PC へ転用するための手段を用意しておくということでしょうか。	「緊急避難用端末」とは何かを正確に知りたいと考えます。		有 意見 No.325 を参照すること。
325	7.別紙 5 運用保守作業項目 一覧	2	42 緊急避難用サンド ボックス検知対応	「障害に伴い持込媒体サンドボックス PC が利用不可能な状態になった場合、利用者が持ち込み媒体のサンドボックス検知を行えるよう緊急避難用端末を準備すること。」と記載がありますが、緊急避難用端末の要件について明確化することをご検討願います。「持込媒体サンドボックス PC」と同等の機能を持つ端末という理解でよろしいでしょうか。	「緊急避難用端末」について明確化するため。		有 緊急避難用端末は、持込媒体サンドボックス PC が故障した時に直ちに利用する端末を想定していたが、意見を踏まえ、故障時は予備機と交換することとする。そのため、緊急避難用端末の手配は要件から削除する。
326	7.別紙 5 運用保守作業項目 一覧	2	42 緊急避難用サンド ボックス検知対応	緊急避難用端末は「持込媒体サンドボックス PC」設置拠点に各 1 台ずつ配備する想定でよろしいでしょうか。また、別紙 1 には当該端末の数量は含まれていないという理解でよろしいでしょうか。	端末の数量により提示価格に差異が発生するため。		有 意見 No.325 を参照すること。
327	7.別紙 5 運用保守作業項目 一覧	2	43 持込媒体サンドボ ックス PC マスタ更新	持込媒体サンドボックス PC のマスタイメージ取得について、実施頻度が「月次」となっていますが、年次での実施に仕様緩和いただきますようご検討願います。	提示価格低減のため。		有 意見を踏まえ、別紙 5「運用保守作業項目一覧」の項番 43 の頻度を以下のとおり修正する。 ----- OS のマイナーバージョンアップ等、サンドボックス端末に大型アップデートが発生するタイミングで実施。半年に一回程度を想定。 -----

328	7_別紙 5 運用保守作業項目 一覧	2	44 持込媒体サンドボックス PC 交換用 PC 最新化	「常時交換が可能なように、持込媒体サンドボックス PC(交換用)の状態を最新化すること。」と記載がありますが、持込媒体サンドボックス PC(交換用)とは、受注者が保管庫にて管理する予備機という理解でよろしいでしょうか。	「持込媒体サンドボックス PC(交換用)」について、明確化するため。		有	意見 No.325 を踏まえて、持込媒体サンドボックス PC(交換用)は、発注者側で保管する予備機から交換することとする。
329	7_別紙 5 運用保守作業項目 一覧	3	48 登録外媒体ホワイトリスト登録	「本調達に含まれない媒体(館内で既に利用している USB メモリや USB ハードディスク等)について、新たにホワイトリストへ登録すること。」と記載がありますが、登録の必要がある機器の具体的な数量をご教示いただけますでしょうか。	数量規模によっては提示価格に差異が発生するため。		無	初期登録は 10 程度、年間 5 程度の登録対象が増加する見込みである。
330	7_別紙 5 運用保守作業項目 一覧	3	63 バックアップ媒体管理・交換	バックアップ媒体の保管・搬出における実施頻度が「日次」となっていますが、バックアップ媒体の交換等のタイミングはバックアップ設計等に依存しますので、頻度については「適宜」としてはいかがでしょうか。	バックアップ方式により最適な実施頻度が異なることが想定されるため。		有	意見のとおり修正する。
331	7_別紙 5 運用保守作業項目 一覧	3	66 ウイルスパターンファイルの取得及び配布、試験	機密性情報系 PC については非インターネット環境につき、手動でウイルスパターンファイルを更新する必要があるものと考えております。本作業については貴館にて実施いただくことは可能でしょうか。	非常駐での運用業務を想定しており、週次でのウイルスパターンファイル更新・試験の実施により提示価格が高騰することが想定されるため。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
332	7_別紙 5 運用保守作業項目 一覧	3	No.66 ウイルスパターンファイルの取得および配布、試験	作業項目「ウイルスパターンファイルの取得及び配布、試験」の内容を、試験端末にてウイルスパターンファイルの配布状況や、業務上必要なサービス利用影響を常に確認できる環境を維持管理することのように変更した方がよいと考えます。	ウイルスパターンファイルは日々更新されるものであるため、パターンファイルの配布状況についてはウイルス対策ソフトの管理ツールで確認することが確実な方法である。ただし、パターンファイルの更新により業務上必要なサービスの利用に影響を与える可能性は排除できないため、このような状況が発生した際に受注者が即座に原因調査を行える環境を常に維持することで、業務影響を最小限にとどめることができるため。		有	意見を踏まえ、ウイルスパターンファイル(ウイルス定義ファイル)は即時の適用が必要なため、自動で更新する設計に変更する。また意見 No.346 記載のとおり、ウイルスパターンファイル(ウイルス定義ファイル)の更新状況等を監視することとする。
333	7_別紙 5 運用保守作業項目 一覧	3	No.66 ウイルスパターンファイルの取得および配布、試験  No.67 ウイルスパターンファイルの配布	ウイルスパターンファイルをウイルス定義ファイルに変更すべきと考えます	ウイルスパターンファイルは特定メーカーにおける定義ファイルの呼称であるため、特定メーカーの製品を連想させるため。		有	意見を踏まえ、ウイルスパターンファイル(ウイルス定義ファイル)と修正する。
334	7_別紙 5 運用保守作業項目 一覧	3	70 セキュリティパッチ適用	「セキュリティ情報を収集し、脆弱性が発見された場合セキュリティパッチを適用すること」と記載がありますが、以下のとおり記載内容を変更することをご検討願います。 ・セキュリティ情報を収集し、脆弱性が発見された場合	セキュリティパッチの適用がシステムの安定稼働に影響を与える場合もあるため、お客様と協議のうえで必要に応じて適用する運用が望ましいと考えます。		有	意見のとおり修正する。

				は、当館職員と協議のうえ、必要に応じてセキュリティパッチを適用すること。				
335	7_別紙 5 運用保守作業項目 一覧	3	72 セキュリティワイヤ ーの鍵管理(業務系 NWPC)	「業務系 NWPC のセキュリティワイヤーを施錠する鍵について管理を行うこと。」と記載がありますが、常駐を想定していないため、ワイヤーの保管につきましては特許庁庁舎内にて保管とさせていただきます。またワイヤーや鍵と言った物理的なセキュリティ器具の管理は万全を期す意味でも貴館での管理が望ましいと考えます。	ご提案する運用内容に関連するため。		有	意見を踏まえ、セキュリティワイヤー及びその鍵の保管は、受注者ではなく、情報・研修館で実施することとする。以下の項番の運用保守作業項目は要件から削除する。 要件定義書の別紙 5「運用保守作業項目一覧」の項番 45,46,47,72,73,84,85,86
336	7_別紙 5 運用保守作業項目 一覧	3	73 セキュリティワイヤ ーの鍵管理(機密性 情報系 NWPC)	「機密性情報系 NWPC のセキュリティワイヤーを施錠する鍵について管理を行うこと。」と記載がありますが、「管理」の定義について確認させてください。また常駐を想定していないため、ワイヤーや鍵の保管につきましては特許庁庁舎内にて保管とさせていただきます。	ご提案する運用内容に関連するため。		無	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにしたため、本意見は採用しない。
337	7_別紙 5 運用保守作業項目 一覧	4	79 ユーザパスワード 変更	「定期的にパスワード変更する必要があるユーザについて、パスワード変更作業を実施すること」と記載がありますが、受注者が運用業務実施にあたり利用するユーザが対象であり、職員様が利用するユーザではないという理解でよろしいでしょうか。	職員様のユーザパスワード変更は、受注者から提示された手順のもとに、ご本人様にて実施頂いたほうが良いと考えるため。		無	認識のとおりである。
338	7_別紙 5 運用保守作業項目 一覧	4	80 検疫検査判定ポリ シー更新	「ウイルス対策ソフトの定義ファイル情報、ソフトウェアのセキュリティパッチ情報を確認し、最新の検疫検査判定ポリシーへ更新すること」と記載がありますが、「検疫検査判定ポリシー」の内容について、可能な範囲で開示願います。	「検疫検査判定ポリシー」について明確化するため。		有	意見を踏まえ、以下のとおり修正する。 ----- ウイルス対策ソフトの定義ファイル情報、ソフトウェアのセキュリティパッチ情報を確認し、パッチ等が適用されていない端末があれば、必要な対応策を検討すること。 -----
339	7_別紙 5 運用保守作業項目 一覧	4	No.81 電子証明書の 管理	24 時間 365 日の対応時間が必要だと考えらる、明確な理由に作業内容を変更すべきだと考えます。	証明書の有効期限管理をは計画的に実施できるため 24 時間 365 日は必要ないと考えます。 検疫の機器認証の証明書管理において、24 時間 365 日の対応が必要となるのは、機器の紛失、盗難時に証明書を失効させるようなケースだと考えられるため、もしも、このような目的であるならば明確に記載すべきであると考えため。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
340	7_別紙 5 運用保守作業項目 一覧	4	項番 82 オペレーシ ョン 定常時運用 定常及び定形作業 URL フィルタリング設 定	項番 82 の作業について受付してから対応完了するまでの対応期日を明確にしていきたい。	要求内容を明確化するため。		無	意見 No.316 を参照すること。

341	7.別紙 5 運用保守作業項目 一覧	4	83 セキュリティ監査 対応	「情報・研修館が定期的に行っているセキュリティ監査で問題点を指摘された場合は、情報・研修館の指示に従って、適切な対処を行うこと。」と記載がありますが、調達期間において想定されるセキュリティ監査の実施回数(頻度)について明記するようご検討願います。	実施回数によって提示価格に差異が発生するため。		有	頻度は契約期間中に1、2回である。
342	7.別紙 5 運用保守作業項目 一覧	4	84 セキュリティワイヤ ー払出	「職員の入館等で新たなセキュリティワイヤーが必要となった場合、郵送にてセキュリティワイヤーを利用者に払い出す。」と記載がありますが、ワイヤーや鍵と言った物理的なセキュリティ器具の管理は万全を期す意味でも貴館での管理が望ましいと考えます。	ご提案する運用内容に関連するため。		有	意見 No.335 を参照すること。
343	7.別紙 5 運用保守作業項目 一覧	4	85 セキュリティワイヤ ー返却	「職員の退職等で PC が不要となった場合、郵送にて利用者からセキュリティワイヤーを受け取る。」と記載がありますが、ワイヤーや鍵と言った物理的なセキュリティ器具の管理は万全を期す意味でも貴館での管理が望ましいと考えます。	ご提案する運用内容に関連するため。		有	意見 No.335 を参照すること。
344	7.別紙 5 運用保守作業項目 一覧	4	86 セキュリティワイヤ ー交換	「セキュリティワイヤーを破損・紛失した場合、郵送にて利用者から当該セキュリティワイヤーを受け取り、新たにセキュリティワイヤーを引き渡す。」と記載がありますが、ワイヤーや鍵と言った物理的なセキュリティ器具の管理は貴館での管理が望ましいと考えます。	ご提案する運用内容に関連するため。		有	意見 No.335 を参照すること。
345	7.別紙 5 運用保守作業項目 一覧	3/ 5	オペレーション 定常時運用 セキュリティ監視・ウィ ルス検知監視	内部対策の監視として、内部における不正な通信の監視も要件として、追加いただいたほうがよいと考えます。	標的型攻撃の内部に侵入してから取る行動として、より攻撃に有益な情報を搾取するためのクライアント間の横展開(探索)があります。この行動を察知するためにも、攻撃の起点となる、クライアント間、クライアントとサーバ間の通信の監視は必要と考えます。		無	必須の要件とする必要はないと判断し、意見は採用しない。
346	7.別紙 5 運用保守作業項目 一覧	3/ 5	オペレーション 定常時運用 セキュリティ監視・ウィ ルス検知監視	不正プログラム対策ソフトウェアのスキャン結果のみでなく、不正プログラム対策ソフトウェアの稼動状況、定義ファイル更新状況、などの状態の監視も追加願います。	必須要件に不足があると考えます。 状態を踏まえて、スキャン結果の正当性までを見ることを監視作業の範囲とすべきと考えます。		有	意見を踏まえ、「要件定義書(案)」の別紙 5「運用保守作業項目一覧」の項番 57 に以下の要件を追加する。 ----- 不正プログラム対策ソフトウェアが適切に動作していることを確認するため、定義ファイルの更新状況等を監視すること。 -----
347	7.別紙 5 運用保守作業項目 一覧	3/ 5	オペレーション 定常時運用 セキュリティ監視・ウィ ルス検知監視	貴館への報告内容の確からしさ・精度の向上のため、セキュリティ対策・セキュリティ監視を担うハードウェア・ソフトウェアの連携を進んで取り入れることを要件追加願います。	連携のないハード・ソフトばかりのセキュリティ対策・セキュリティ監視の仕組みである場合、“人”による判断が入ります。“人”による判断では、判断できるレベル・正確性について、“人”によって差が発生することは明らかです。 できる限り、システムティックに行っ		無	必須の要件とする必要はないと判断し、意見は採用しない。

					た分析結果や脅威情報の報告を業者に要求することで、貴館に正確な情報が提供される確立を上げることが可能と考えます。			
348	7_別紙 5 運用保守作業項目 一覧	3/ 5	オペレーション 定常時運用 セキュリティ監視・ウイルス検知監視	以下の文言を追加することをご提案いたします。  管理部門より遠隔地にある拠点端末におけるワクチンソフトのインストール状況、定義ファイルのバージョン管理等、基本的な端末への対策が保持できていることが適宜、確認可能であること。	昨今の標的型攻撃の侵入傾向として、遠隔地にある拠点端末が狙われて、組織内部へと侵入される傾向があります。端末におけるセキュリティ対策の基本となるワクチンソフトによる対策は、持続性が担保される必要があります。		無	要件定義書「3. 10 情報セキュリティに関する事項」の「不正プログラム対策の管理」に同様の意図の要件を記載済であるため、意見は採用しない。
349	7_別紙 5 運用保守作業項目 一覧	3/ 5	オペレーション 定常時運用 セキュリティ監視・ウイルス検知監視	以下の文言を追加することをご提案いたします。  セキュリティの専門的な知見を提供するベンダを含めた体制を提供すること。	NISC が公開している「日本年金機構における個人情報流出事案に関する原因究明調査結果」にも記載があるようにシステムの構築・運用事業者とは独立した第三者の事業者と平常時から連携する体制を保有することが望ましいと考えます。		無	調達仕様書の「4. 2 作業要員に求める資格等の要件」に同様の意図の要件を記載済であるため、意見は採用しない。
350	7_別紙 5 運用保守作業項目 一覧	3/ 5	オペレーション 定常時運用 セキュリティ監視・ウイルス検知監視	以下の文言を追加することをご提案いたします。  組織内部において、端末間及び端末からサーバへの通信を検知する機能を提供すること。	今日までに公表されているインシデント事例を鑑みますと、万が一、組織内部においてウイルスが拡散した場合、感染端末から権限昇格を許可されている端末や重要サーバへと垂直水平に展開することが確認されている為、対策が重要であると考えます。		有	意見を踏まえ、要件定義書の図表 3-10-1「情報セキュリティ対策要件」の「侵入検知」に要件として記載する。
351	7_別紙 5 運用保守作業項目 一覧	3/ 5	オペレーション 定常時運用 セキュリティ監視・ウイルス検知監視	以下の文言を追加することをご提案いたします。  導入するセキュリティ製品については、単一的に動作するものではなく、製品または機能同士が連携するものを積極的に採用すること。	製品が保有する脅威情報は、なるべく製品間、機能間で複合的に作用することが望ましいと考えます。また、管理負荷の軽減やコストの低減についても効果的であると考えます。		有	意見を踏まえ、図表 3-10-1「情報セキュリティ対策要件」の「不正プログラム対策」に以下を追記する。 ----- 導入するセキュリティ製品については、コストメリットが担保される場合は、製品または機能同士が連携するものを採用することが望ましい。 -----
352	7_別紙 5 運用保守作業項目 一覧	4	98 インストーラの作成	「PC の環境変更資材の配布用インストーラ(MSI 形式)を作成すること。」と記載がありますが、インストーラの作成について、想定される作業内容、実施回数(頻度)についての記載を仕様書にてご提示願います。また、MSI 形式に限定する必要は無いと思われるので、「(MSI 形式)」の表記を削除する等、仕様の緩和についてご検討願います。	作業内容と実施回数によって提示価格に差異が発生するため。		有	マイクロソフト社の製品については、原則月 1 回インストーラを作成し、配布すること。また緊急性の高いものについては、INPIT と調整の上で対応すること(年 2 回程度を想定)。その他 PC の環境変更については、受注者が提供するサービス・機能を構成するソフトウェアに依存するため、現時点で頻度は未定である。

								インストーラの形式については、意見を踏まえ、「(MSI形式)」の表記を削除する。
353	7_別紙5 運用保守作業項目 一覧	5	No.109 バックアップ からのリストア	対象となるシステムに関する情報を記載すべきである と考えます	障害発生に伴いリストアが必要となったシステムが職員が利用する端末であった場合、24時間365日は必ずしも必要ないと考えます。したがって、対象となるシステムに関する情報(業務に重大な影響を与えるシステム等)を記載すべきと考えます。 なお、このような文言がない場合、提案者は職員が利用する端末を24時間365日対応の対象とする可能性があり、これにより運用者の体制が肥大化しコストが増加されることを排除するため。		無	リストアが必要となった場合の対象サービス機能は、要件定義書の図表3-9-1「目標復旧時間の設定対象と設定値」を参照すること。
354	7_別紙5 運用保守作業項目 一覧	5	No.112 セキュリティ 保持対応 箇条書き 2つめ (地方拠点にある障害 対応・・・)	地方拠点にある障害対象機器のネットワークが切り離された際には、情報・研修館職員に切り離された旨を報告し、再接続については情報・研修館職員の承認を得たうえで行うことに変更すべきと考えます。	被害を最小限にとどめる場合、即座にネットワークを切り離す必要があるため、SIEMと連携した自動遮断の導入を検討すべきである。自動遮断された場合は、その旨を情報・研修館職員に報告し、調査・対策を施したうえで当該ネットワークの再接続に関するリスクを含めた報告を提出し、情報・研修館の承認を得たうえで再接続するべきと考えるため。		無	詳細な運用フローについては運用・保守実施要領において協議するため、意見は採用しない。
355	7_別紙5 運用保守作業項目 一覧	5	No.112 セキュリティ 保持対応 箇条書き 3つめ	フォレンジック対応は受注者が主体的に実施するのではなく、情報・研修館が発注したフォレンジック業者に対し支援を行うことに変更すべきと考えます。	受注者(運用者)の不正によるインシデントの場合、運用者は、フォレンジックに必要な各種ログ情報等を容易に削除(隠滅)できるため、フォレンジックの正当性が確実に保証されているとはいいがたい。したがって、受注者(運用者)は情報・研修館が契約する第三者のフォレンジック事業者の調査が円滑に行われるように支援する内容に変更するべきと考えるため。		有	意見のとおり修正する。
356	7_別紙5 運用保守作業項目 一覧	5/ 5	障害時運用(セキュリ ティ障害対策) セキュリティ保持対応	以下の文言を修正することをご提案いたします。  検体がウイルスであるか解析を行い、ウイルスであれば、ワクチンベンダと連携し、対応するパターンファイルによる駆除まで行うこと。	イベントやインシデントに該当する事案の最終的な対処方法である、ワクチンベンダが作成する、対ウイルス用ワクチンによる駆除を明記する必要があると考えます。		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。

357	7.別紙 5 運用保守作業項目 一覧	5/ 5	障害時運用(セキュリティ障害対策) セキュリティ保持対応	以下の文言を追加することをご提案いたします。  情報・研修館で確認できている脅威情報以外に他組織や日本国内をとりまく脅威情報等についても広く情報提供を行うこと。	サイバー攻撃の流行や傾向について、幅広く情報収集を行うことで、早期の段階で予防策を講じることが出来る為、重要事項であると考えます。		無	別紙 5「運用保守作業項目一覧」の No.12 に同様の意図の要件を記載済であるため、意見は採用しない。
358	7.別紙 5 運用保守作業項目 一覧	-	-	想定インシデント数、コール数など数量などがわかるものは 記載できますでしょうか  <変更案> 随時 ⇒ 10 件/月(想定)など	見積もりブレを無くするため		有	意見を踏まえ、要件定義書の別紙 5「運用保守作業項目一覧」に、現行システムにおけるコール数の件数を追記する。
359	7.別紙 5 運用保守作業項目 一覧		-	下記要件を追記願います。  各接続拠点に設置するハードウェア(WAN ルータ、L2SW、AP 等)および回線(モバイル回線・端末含む)の障害時、故障箇所特定後、オンサイト保守を行うこと。	障害時の現地保守対応に関する記載が無かったため、見積範囲を明確にするため、現地保守に関する要件の明記をお願いします。		有	意見を踏まえ、要件定義書の別紙 5「運用保守作業項目一覧」の「保守対応」に以下を追記する。 ----- 作業項目: 機器保守 作業内容: 各拠点に設置するネットワーク機器(WAN ルータ、L2 スイッチ、アクセスポイント等)および通信回線装置に障害が発生した場合には、オンサイト保守を行うこと。ただし、クライアント PC はオンサイト保守の対象外とする。 -----
360	8.別紙 6_サービス レベル項目一覧	1	-	項番 1~9 の内容と項番 10~15 に記載された内容は、分けて記載するべきと考えます。	項番 1~9 はサービスに対して求められているサービスレベルであり、項番 10~15 は各サービスに対して設定された SLA の目標値を達成するため設定された OLA の位置付にあると考えます。運用・保守で達成すべきは OLA として設定された目標値であり、報酬額の評価対象に関しても OLA の達成状況に対する評価が妥当であるため。		無	SLA 及び OLA は両方とも発注者として受注者に遵守していただきたい項目であるため、記載はこのままとし、意見は採用しない。
361	8.別紙 6_サービス レベル項目一覧	1	サービスレベル項目 一覧	稼働率の算出方法について、稼働単位が複数に分かれるもの(回線や各種サービス)については当該対象が全面的に利用不可になった場合を停止をして算出する想定で良いかご教示頂きたい	仕様を明確にするため		有	稼働率は以下の内容で算出する。 稼働率 = (月間の総[稼働保証時間] - 月間の総[稼働保証時間]内のサービス停止時間) ÷ 月間の総[稼働保証時間] ただし、計画停止(担当職員からの依頼によるサービス停止又は担当職員と協議し承認されたサービス提供停止が不可欠な保守メンテナンスによる停止)は除く。 なお、ベストエフォート型回線等、回線の種



								別・特性により稼働率を保証できないものは、情報・研修館と協議の上、稼働率の設定について決定することとする。
362	8_別紙 6_サービスレベル項目一覧	1	10 運用保守 インシデント管理 一時窓口解決率	「一次窓口(問い合わせを受けた担当者)で解決した割合」については評価対象とする範囲を明確に定義していただきたい。また、本 SLA については経験やノウハウの蓄積が必要と認識しているため、実績に基づいて基準値を設定し、運用開始 1 年後より評価開始とするなど条件を緩和していただきたい。	・要求内容を明確化するため。 ・SLA 要件を満たすために体制の過剰確保など各社ともコスト高になることが予想されるため。		無	SLA について、稼働開始後 3 ヶ月は調整期間とし、4 ヶ月目から遵守の対象としている。稼働開始後 1 年より評価開始とすることは許容できないため、意見は採用しない。
363	8_別紙 6_サービスレベル項目一覧	1	11 運用保守 インシデント管理 サービスデスク対応時間	「利用者からのサービス要求」の内容と対応時間を具体的に記載していただきたい。 (例: 内容は「別紙 5 運用保守作業項目一覧」-「項番〇〇」、対応時間は「対応時間」の記載とする等)	要求内容を明確化するため。		無	意見 No.316 を参照すること。
364	8_別紙 6_サービスレベル項目一覧	1	11 運用保守 インシデント管理 サービスデスク対応時間	「受付けてから対応完了するまでの平均時間」を「受付けてから一次回答を実施するまでの平均時間」としていただけますでしょうか。	・利用者の問い合わせ内容によってはヒアリングに時間を要す場合もあるため。 ・SLA 要件を満たすために体制の過剰確保など各社ともコスト高になることが予想されるため。		無	対応完了とするか一次回答とするかは、運用計画の作成時に協議の上、決定することとする。
365	8_別紙 6_サービスレベル項目一覧	1	12 運用保守 コール対応 電話呼放棄率	「着信電話に出られなかった確率」を算出するための、前提とするコール頻度やコール数の条件を提示いただけますでしょうか。	各社の見積もり条件を均質化するため。		有	意見 No.358 を参照すること。
366	8_別紙 6_サービスレベル項目一覧	1/ 1	No14 マルウェア等対策 No15 不正アクセス対策	「マルウェア等の侵入」や「不正アクセス」は、PC 端末や各システムに対して起こった際の検知という理解でよろしいでしょうか？	インターネット側からは各ゲートウェイサービスでマルウェアや不正アクセスを検知し、遮断するため、遮断したものについては SLA 値に従った連絡対応は不要という理解で良いかの確認をさせていただきました。		無	認識のとおりである。
367	8_別紙 6_サービスレベル項目一覧	-	-	データセンター カテゴリの追加  <変更案> ・無停電電源装置(UPS)の電力供給時間 : 停電時より 10 分以上 ・非常用発電設備(発電機)の起動時間 : 停電時より 5 分以内 ・非常用発電設備(発電機)の連続稼働時間: 連続稼働時間 96 時間以上 ・入退室記録の保存期間 : 3 年間 ・監視カメラ(24 時間 365 日稼働)の監視映像保存期間 : 3 年間	データセンターの SLA 記載が無い		無	必須の要件としての変更の必要はないと判断し、意見は採用しない。
368	8_別紙 6_サービスレベル項目一覧	-	-	免責範囲についても記載が必要  <変更案>	どこまでの範囲で免責になるか不明確なため		無	免責事項については、要件定義書「3.16 運用・保守に関する事項」に記載済であるため、意見は採用しない。

				<p>免責範囲</p> <ul style="list-style-type: none"> <li>・委託者側理由により障害復旧できない場合</li> <li>・委託者側理由により障害検知出来なかった場合</li> <li>・委託者側理由によりシステムが利用できなかった場合</li> </ul> <p>など</p>				
369	99_文書名なし	-	-	本調達においては、総合評価方式で公示されると考えていますが、その場合の評価項目の内訳をご教示いただけますでしょうか。(例: 価格点 100/技術点 300)	本件参加に向けて、事前に確認したいため。		無	評価項目については、入札公告時の公示資料で公開する。
370	99_文書名なし	-	-	上記と関連し、総合評価方式の場合、入札公示後「提案書評価項目表」をご教示いただけると考えて宜しいでしょうか。	提案書による総合評価方式の場合、一般的に「提案書評価項目表」をご教示いただけるケースが多いため。		無	評価項目については、入札公告時の公示資料で公開する。
371	99_文書名なし	-	-	本件に係る調達公示から業者決定までの具体的スケジュールをご教示いただけますでしょうか。	当社における、本件設計以降の工程に係る要員確保に関わるため、本件公示前にご教示いただきたいと考えております。		無	公示から落札業者決定までのスケジュールは、入札公告時の公示資料で公開する。
372	99_文書名なし	-	-	本件調達に係る、貴機構予算をご教示いただけますでしょうか。	貴機構のご予算を考慮し、提案内容を決定する必要があると考えたため。		無	本調達の予算に関する情報は公開していない。
373	99_文書名なし	-	-	本件の契約書(案)について、ご提供いただけますでしょうか。	本件参加に向けて、想定されている契約内容を確認したいため。		無	契約書は入札公告時の公示資料で公開する。
374	99_文書名なし	-	-	本件調達に係る、貴機構から落札業者への費用の支払い方法について、御相談は可能でしょうか。 ※12月に初期構築費、それ以降は月額請求になると考えております。	本件落札後の貴機構の支払い方法を事前に理解したいため。		無	設計・構築業務、稼働後4年間分の運用・保守業務費用を合計したものを契約期間内で月次で按分し、その費用を落札業者へ支払う。ただし、当該契約期間に利用者増減や拠点数変更等が発生した場合には、そのタイミングで、利用者数や拠点数等の利用量・規模に応じて、変更契約を行うことを想定している。
375	99_文書名なし	-	-	装置に添付されている保管品の保証書及び、不要な添付品は廃棄で問題ないでしょうか。	保証書、添付品は保管しておく必要があるか確認させていただくため		無	情報・研修館としては必要なサービスが受注者から提供されるのであれば、廃棄でも保管でもどちらでもかまわないため、保管要否は受注者にて判断するものとする。
376	99_文書名なし	-	-	ノートPC本体以外の機器の保管はありますか。	保管機器の種類を確認させていただくため。		無	ノートPCの付属品や消耗品、及びネットワーク機器等、運用保守作業の実施において効率的且つ費用の低減に資するものであれば、保管の対象として提案することを妨げない。
377	99_文書名なし	-	-	契約書に提案書を添付し、契約前提とさせていただくことは可能でしょうか。	提案内容を貴館にて採用いただき受注できた場合、提案内容と設計・構築時の対応内容が異なることを防止するため。納期・コストに影響します。		無	提案書は契約書類の一部であると認識している。

378	99_文書名なし	-	-	機密系ネットワークと業務系ネットワークを一括で調達される要件となっておりますが、分離調達としていただけないでしょうか。	昨今高度化している標的型攻撃への対策を十分に考慮した構成でご提案する場合、機密系・業務系の両方のシステム構築はスケジュール上実現が難しいと考えるため。		有	調達範囲に関する意見を踏まえ、機密性情報系 NW の設計・構築及び運用・保守は今回の調達範囲外とすることにした。
379	本調達全般について	-	-	調達の範囲を、設計・構築と運用・保守に分割すべきと考えます。	2016年10月にNISCより「高度サイバー攻撃対処のためのリスク評価等のガイドライン」が示されました。ガイドラインではシステムの監視やネットワークの遮断について具体的な対策を導入し、運用することを求めています。 ネットワーク等基盤構築を行う本調達は当該ガイドラインに大きく影響を受けるもので、ガイドラインを遵守したセキュリティ設計としその環境を踏まえて、適切な運用設計をすべきであり、貴法人とシステム及びセキュリティ設計について合意してから、改めてその環境を適切に運用するための要件を整え、運用・保守の調達を行うべきであるため。以上により、設計・構築と運用・保守は調達を分割すべきと考えます。 また、運用に特化し低コストでサービス提供を行っている運用事業者も市場には存在するため、専門の業者へ委託することでコスト低減の可能性もあるため。		無	本調達範囲を分割することは行わないため、意見は採用しない。
380	本調達全般について	-	-	ネットワーク回線について、その種別により分割して調達すべきと考えます。(無線LANと一般回線等)	ネットワークはその種別により設計者や実作業担当者のスキルも大きく異なるため、一括調達では受発注者ともに管理等負荷が高まり、十分な品質が確保できないなどリスクが高いため。		無	回線種別により調達範囲を分割することは行わないため、意見は採用しない。