LAN調達仕様書意見に対する対応

注） 1.種目欄には、意見の種類を以下から選択して、その番号を記載すること。

［1. 要求水準を下げる。 2. 要求水準を上げる。 3. 文章だけを修正する。 4. その他 ］

No.	資料名	頁番号	項 目	種別	意　　見	理　　由	回　　答
1	調達仕様書	1	第1章 概要 2 調達の背景	4	「現行システムは、平成30年12月末の運用終了を予定している。」という記載、並びに、要件定義書のP118 13.1.3 (3)仮運用（並行運用）「・大規模なトラブル等により次期システムを用いた業務遂行が困難である場合には、現行システムへの切り戻しを行うこと。」との記載がありますが、大規模なトラブル等による、現行システムへの切り戻し作業については、平成31年1月以降の調整は一切できないという事でしょうか。 次期システムへの移行にあたり、既存の内閣府LAN上の個別システムの更改も同時期に実施され、各々の個別システム更改の作業スケジュールにも大きく影響するため、平成31年1月以降も調整により、現行システムの利用が可能となるよう、予め調整いただいた方がよろしいのではないかと存じます。	システムの運用継続性を確保するため	御意見として承りましたが、調達仕様書（案）の通りとします。 なお、現行システムへの切り戻しは、仮運用（並行運用）時を想定した要件となります。また、現行システム契約終了が平成30年12月31日となっており、その時点をもって現行システムは撤去される為、平成31年1月以降に現行システムへの切り戻しは出来ません。
2	調達仕様書	31	第5章 作業の実施体制・方法 1 作業の実施体制 1.2 移行時体制	1	【要件】 ・現行システム運用体制と調整にあたり発生する費用及び現行システムの設定変更等の作業に必要となる費用は本調達に含むこと。 上記の要件について、削除、もしくは受注後に別途協議とする旨への緩和を検討願います。	調整次第で費用が変動する可能性があり、見積りの精度を向上させるため。	御意見として承りましたが、現行システム運用体制との調整費用は本調達に含まれることから、調達仕様書（案）の通りとします。
3	要件定義書	10	第2章 機能要件 1 機能に関する事項 1.1 LAN要件 1.1.11 ウイルスゲートウェイ要件	2	以下のように修正することを推奨いたします。 変更前 「10/100BASE-TX のポートを 2 ポート以上、10/100/1000BASE-T のポートを 2 ポート以上有 すること。」 変更後 「10/100/1000BASE-T のポートを 4 ポート以上有 すること。」	"10/100BASE-TX" は古い規格であり、入手性も悪く製品が限定されます。 そのため、上位互換でありかつ現在の標準である "10/100/1000BASE-T"に統一したほうが良いと考えます。	御意見を参考に、要件定義書（案）の一部を変更いたします。
4	要件定義書	11	第2章 機能要件 1 機能に関する事項 1.1 LAN要件 1.1.12　負荷分散装置要件	1	下記文面の修正を提案いたします。 ・10/100/1000BASE-Tを8ポート以上有すること。 →　1000BASE-Tを8ポート以上有すること	近年の技術革新により安価で広帯域な製品が増え、10/100Base-Tを除いた1000Base-Tを主流とした従来より安価な製品が増えております。 そのため、対象となる製品の選択肢を広げより優れた製品選定を実施するため	御意見を参考に、要件定義書（案）の一部を変更いたします。
5	要件定義書	13	第2章 機能要件 1 機能に関する事項 1.1 LAN要件 1.1.17 WAN ルータ要件（WAN 調達）	1	【要件】 仕様全般 WANルータ（WAN調達）との接続が発生する為、WANルータの詳細な機器仕様等に係る要件を記載すべきものと考えます。	調達範囲及び仕様明確化のため。	御意見を参考に、要件定義書（案）の一部を変更いたします。
6	要件定義書	21	第2章 機能要件 1 機能に関する事項 1.2 サービス要件 1.2.5 Proxy 要件	2	以下のように修正することを推奨いたします。 変更前 「HTTPS に対応すること。」 変更後 「HTTPS に対応し、<u>復号化してウィスルスキャンが可能なこと。</u>」	多くのサイトが常時SSL化されるようになり、またマルウェア自身もSSL通信を利用するようになっています。 そのため、ProxyにおいてSSLを復号化して内容を検査することは、セキュリティを確保するうえで必須の要件であると考えます。	御意見を参考に、要件定義書（案）の一部を変更いたします。
7	要件定義書	30	第2章 機能要件 1 機能に関する事項 1.2 サービス要件 1.2.10 プリンタサーバ要件	4	年末の複合機入替時の支援作業について過去の実績を示した方が良いのではないでしょうか。	要件明確化のため。	年度末の複合機入替時の支援作業について、実績等の情報については、資料閲覧の際に開示します。
8	要件定義書	40	第2章 機能要件 1 機能に関する事項 1.3 運用管理機能要件 1.3.3 行政端末管理機能要件	3	構成情報を「ユーザ単位」で収集出来ることとなっておりますが、収集する構成譲情報の内容が端末に関する情報になっており、構成情報の収集を「端末単位」に変更して頂けないでしょうか。	要件明確化のため。	御意見を参考に、要件定義書（案）の一部を変更いたします。

LAN調達仕様書意見に対する対応

注） 1.種目欄には、意見の種類を以下から選択して、その番号を記載すること。

［1. 要求水準を下げる。 2. 要求水準を上げる。 3. 文章だけを修正する。 4. その他 ］

No.	資料名	頁番号	項 目	種別	意　　見	理　　由	回　　答
9	要件定義書	83	第3章 非機能要件 10 情報セキュリティに関する事項 10.3 証跡管理	2	以下のように修正することを推奨いたします。 変更前 「収集する証跡ログは以下に示すものを想定している。具体的な収集情報・保管期間については契約締結後、内閣府 PJMO と協議の上、決定すること。」 変更後 「収集する証跡ログは以下に示すものを想定している。具体的な収集情報・保管期間については契約締結後、内閣府 PJMO と協議の上、決定すること。また、対象ログの検討および決定に際しては、最新の脅威動向およびマルウェア解析、インシデント対応等の知識を有する専門家が参加すること。」	セキュリティの観点でログの収集や分析を行う場合、どのログを収集するか、また各ログの中のどの項目を、どのレベルで出力するかは非常に重要となります。 また、システムの構築後に収集対象ログを追加、またはログの出力レベルを変えることは困難な場合があります。 そのため、対象ログの検討・決定については設計時点で実際のログ分析やインシデント対応を経験した専門家を含めて行うことが望ましいと考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 運用の体制は、どのような専門家を含めるかについても、御提案頂きます。
10	要件定義書	84	第3章 非機能要件 10 情報セキュリティに関する事項 10.3 証跡管理	2	以下のように修正することを推奨いたします。 変更前 「取得した証跡を用いて、必要に応じて点検及び分析を行い、その結果に応じて必要な対策を行うこと。また、取得した証跡において、情報セキュリティ上の脅威となる兆候を発見した場合についても同様の対策を行うこと。」 「取得した証跡を用いて、分析を行い対策の要否とリスクの有無を判断し、報告すること。また、リスクのある事象については、他の環境においても同様の事象が認められないか全体の点検を行い、必要に応じて対策を行うこと。」	標的型攻撃の場合、同時に複数の人にメールを送り攻撃を行う場合があります。特に今回は複数の拠点にシステムがあるため、同時に複数拠点が狙われる可能性も考えられます。 そのため、例えば8号館庁舎のシステムである事象があった場合、同様の事象が特定部局においても発生していないか確認する必要があると考えます。	御意見を参考に、要件定義書（案）の一部を変更いたします。
11	要件定義書	89	第3章 非機能要件 10 情報セキュリティに関する事項 10.10 コンテンツフィルタリング要件	2	以下のように修正することを推奨いたします。 変更前 「禁止 URL 及び許可 URL をカテゴリ別に詳細に設定出来ること。」 変更後 「禁止 URL 及び許可 URL をカテゴリ別に詳細に設定出来ること、また許可URLであってもレピュテーション情報をもとに通信をブロックできること」	標的型攻撃では、許可されている正規のサイトが改ざんされ、その結果マルウェアに感染するいわゆる「水飲み場型攻撃」も利用されます。 そのため、単純なカテゴリフィルタだけでは、十分なセキュリティが確保するのは困難です。許可されているURLであっても、アクセス時のレピュテーション情報をもとにブロックする仕組みが必要であると考えます。	御意見として承りましたが、標的型攻撃対策やその他のセキュリティ対策との組み合わせによって対応可能な要件となっている為、要件定義書（案）の通りとします。
12	要件定義書	90	第3章 非機能要件 10 情報セキュリティに関する事項 10.11 標的型攻撃対策	4	「対策の詳細内容については、設計段階において、内閣府 PJMO 及び各設計・構築事業者間との調整や協議の上、決定すること。」 と標的型攻撃対策の要件に記載がありますが、システムの特性、昨今の脅威状況等を踏まえ、詳細な設計に入る前の段階で、必要となるセキュリティ要件をより明確にすることを推奨いたします。	運用開始後の「セキュリティ事故」を招かないよう、過不足なくセキュリティ機能、及びセキュリティ運用の要件を仕様書に記載する必要があると考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 設計フェーズにおける「詳細設計の前に何を決定すべきか」は応札事業者の提案に応じて契約締結後に協議する為、仕様としての定義はいたしません。
13	要件定義書	90	第3章 非機能要件 10 情報セキュリティに関する事項 10.11 標的型攻撃対策	4	現状、標的型攻撃対策の要件としての記載はありませんが、以下のような対策を盛り込むことを推奨いたします。 追加 「セキュリティベンダや、政府機関から提供された脅威情報、及び組織内で検知したマルウェア等の情報をサーバ上で集中管理し、独自の脅威データベースを構築する。」	セキュリティベンダから提供される脅威情報や、NISC等の政府機関から提供される脅威情報を有効に活用することで防御力を向上させることが期待できます。 一方で、マルウェアは標的となる組織毎にカスタマイズされて使用される傾向があることから、組織独自の脅威データベースを整備することが望ましいと考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、セキュリティに関する情報収集等は、「第3章 非機能要件 16.1.7 情報セキュリティ対策業務」に記載しております。
14	要件定義書	90	第3章 非機能要件 10 情報セキュリティに関する事項 10.11 標的型攻撃対策	4	現状、標的型攻撃対策の要件としての記載はありませんが、以下のような対策を盛り込むことを推奨いたします。 追加 「集中管理している独自の脅威情報を、各セキュリティ機器(proxy装置、ネットワークセキュリティ監視装置等）と自動的に情報共有し、不正な通信やマルウェアの実行等を防御できること。」	脅威情報を各機器で維持・管理するのは運用上負荷がかかります。 そのため、サーバ上で集中的に管理している脅威情報を各セキュリティ機器と自動的に情報共有し、防御する仕組みを導入することが望ましいと考えます。 これにより、コストを削減しつつ防御力を向上させることが可能です。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、標的型攻撃の事象を検知した場合においては「第3章 非機能要件 16.1.9 標的型攻撃対応業務 (2) 対応」に記載しております。

LAN調達仕様書意見に対する対応

注） 1.種目欄には、意見の種類を以下から選択して、その番号を記載すること。

［1. 要求水準を下げる。 2. 要求水準を上げる。 3. 文章だけを修正する。 4. その他 ］

No.	資料名	頁番号	項 目	種別	意 見	理 由	回 答
15	要件定義書	90	第3章 非機能要件 10 情報セキュリティに関する事項 10.11 標的型攻撃対策	4	現状、標的型攻撃対策の要件としての記載はありませんが、以下のような対策を盛り込むことを推奨いたします。 追加 「セキュリティに関するログを一元的に収集、正規化、管理し相関分析機能等により、脅威の可視化ができること。また分析した結果は管理者向け、CSIRTチーム向け、インシデント対応者向けなど、役割に応じて適切な画面を任意に作成できること」	現象の要件定義書には、明示的にログを総合的に分析する機器の記載がありません。セキュリティ状況の把握や調査をするためにこのような機器は必須であると考えます。(現状SIEMとコンサルタントによる監視を実施) また、各担当者が役割に応じて、即座に状況の把握や調査ができるよう、状況可視化の際に画面等は任意に作成できるほうが望ましいと考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、セキュリティに関する情報収集等は「第3章 非機能要件 16.1.7 情報セキュリティ対策業務」に記載しております。
16	要件定義書	90	第3章 非機能要件 10 情報セキュリティに関する事項 10.11 標的型攻撃対策 10.11.1 ネットワークセキュリティ監視装置による対策	2	以下のように修正することを推奨いたします。 変更前 「ネットワークセキュリティ監視装置によって、次期システムと外部（インターネット、政府共通ネットワーク等）との通信及び次期システム内部の通信（次期システム内の主要な拠点間）をモニタリングし、標的型攻撃等を検知すること。」 変更後 「ネットワークセキュリティ監視装置によって、次期システムと外部（インターネット、政府共通ネットワーク等）との通信及び次期システム内部の通信（次期システム内の主要な拠点間）をモニタリングし、標的型攻撃等を検知すること。<u>また、検知した際の攻撃パケットをキャプチャーできること</u>」	検知した際の攻撃パケットは、攻撃の調査・解析をする上で重要な情報の一つとなりますので、保存できるほうが良いと考えます。	御意見として承りましたが、証跡情報を基にした相関分析により、不審な動作の検出を可能とする要件が別途記載されている為、要件定義書（案）の通りとします。
17	要件定義書	90	第3章 非機能要件 10 情報セキュリティに関する事項 10.11 標的型攻撃対策 10.11.1 ネットワークセキュリティ監視装置による対策	2	以下のように修正することを推奨いたします。 変更前 「サンドボックス技術（仮想解析）によって、未知のマルウェアを検知する機能を有すること。サンドボックスによる仮想解析は次期システム環境に適したカスタマイズが可能であること。」 変更後 「サンドボックス技術（仮想解析）によって、未知のマルウェアを検知する機能を有すること。サンドボックスによる仮想解析は次期システム環境に適したカスタマイズが可能であること。<u>サンドボックスは自動解析、及び解析対象ファイルを手動で実行し、ライセンスへの同意やクリックといったユーザ動作を行いながら解析をする機能を有すること。</u>」	昨今のマルウェアはサンドボックスによる解析を回避する機能があります。この中には、パスワード付きでファイルを暗号化するなど、ユーザ入力が必要になるものが含まれます。 そのため、自動だけでなく手動で実際のユーザが操作する際と同じ条件で解析をする機能があると、マルウェアの調査をする際に非常に有用であると考えます。	御意見として承りましたが、次期システム環境に適したカスタマイズが可能という要件として記載されている為、要件定義書（案）の通りとします。
18	要件定義書	91	第3章 非機能要件 10 情報セキュリティに関する事項 10.11 標的型攻撃対策 10.11.2 コンテンツフィルタリング機能による対策	2	以下のように修正することを推奨いたします。 変更前 「コンテンツフィルタリング機能による標的型攻撃等の対策については、「第 3 章 10.11.1ネットワークセキュリティ監視装置による対策」と連携すること。」 変更後 「コンテンツフィルタリング機能による標的型攻撃等の対策については、「第 3 章 10.11.1ネットワークセキュリティ監視装置による対策」と連携して<u>マルウェアのダウンロードを初回から防御できること。</u>」	現状”連携すること”としか記載がありませんが、要件を明確にするため、またマルウェア感染を防ぎセキュリティレベルを向上させるため、防御できることを明確に記載したほうが良いと考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、「第2章 機能要件 1.2.5 Proxy要件」においてマルウェアの監視を実施する要件、「第3章 非機能要件 10.11.3 ウイルスゲートウェイによる対策」の中でマルウェアの侵入を防御する要件を記載しております。
19	要件定義書	91	第3章 非機能要件 10 情報セキュリティに関する事項 10.11 標的型攻撃対策 10.11.3 ウイルスゲートウェイによる対策	3	以下のように修正することを推奨いたします。 変更前 「ウイルスゲートウェイによって、メール及びウェブアクセスによるマルウェアの侵入を検知・駆除し、標的型攻撃等を防御すること。」 変更後 「ウイルスゲートウェイによって、メール及びウェブアクセスによるマルウェアの侵入を検知・駆除、<u>または遮断し</u>、標的型攻撃等を防御すること。」	ウィルスゲートウェイは、「第 3 章 11.1.8 標準ウイルスゲートウェイ」の要件から、ブリッジでの接続となります。 そのため、本GWではメールやWebの通信を終端しない構成となり、マルウェアだけ駆除するのは技術的に困難だと考えます。	御意見として承りましたが、標的型攻撃等を防御するという要件には遮断も含まれている為、要件定義書（案）の通りとします。

LAN調達仕様書意見に対する対応

注） 1.種目欄には、意見の種類を以下から選択して、その番号を記載すること。

［1. 要求水準を下げる。 2. 要求水準を上げる。 3. 文章だけを修正する。 4. その他 ］

No.	資料名	頁番号	項 目	種別	意 見	理 由	回 答
20	要件定義書	92	第3章 非機能要件 10 情報セキュリティに関する事項 10.13 セキュリティ対策における定期的な改善の施策	4	インターネットセキュリティゲートウェイ、侵入検知による、セキュリティ処理の自動的な最適化となっておりますが、削除して頂けないでしょうか。	インターネットセキュリティゲートウェイに関する要件が本文中に記載されていないため。	御意見を参考に、要件定義書（案）の一部を変更いたします。
21	要件定義書	97	第3章 非機能要件 11 情報システム稼動環境に関する事項 11.1 ハードウェア構成 11.1.8 標準ウイルスゲートウェイ	1	以下のように修正することを推奨いたします。 変更前 「ネットワークパフォーマンスを低下させること無く、電子メール（SMTP、POP3、IMAP）、転送ファイル（FTP）、ウェブ（HTTP）トラフィックからのマルウェアに対して防御可能なこと。また添付ファイルに対してもスキャンを行うこと。 」 変更後 「ネットワークパフォーマンスを低下させること無く、電子メール（SMTP）、転送ファイル（FTP）、ウェブ（HTTP）トラフィックからのマルウェアに対して防御可能なこと。また添付ファイルに対してもスキャンを行うこと。」	電子メールは、SMTPプロトコル経由でメールサーバに配送され、その後メールサーバからPOP3/IMAP等でクライアントに配送されます。 そのため、まずSMTPでスキャンされ、その後にPOP3,IMAP等でスキャンしても、同じエンジンで同じファイルを二重にチェックすることになり、負荷が上がるだけでセキュリティ向上に繋がらないと考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 「電子メール（SMTP、POP3、IMAP）」の記載は、二重にチェックするという意図では無く、各プロトコルに対して、マルウェアの防御が可能なことを機能要件として示しています。
22	要件定義書	98	第3章 非機能要件 11 情報システム稼動環境に関する事項 11.1 ハードウェア構成 11.1.8 標準ウイルスゲートウェイ	2	「クライアントライセンスは、無制限ライセンスとする。」という仕様要件を削除して頂く、もしくは要件の緩和として「有限ライセンスでの提案も可とする」といった要件の追加をご検討頂けないでしょうか？	理由は、無制限ライセンスを保持する製造業者は、特定の業者しか存在しないためです。有限ライセンスしか保持しない製造業者にも提案の機会を頂くことでご提案できるソリューションを広げることにつながります。	御意見を参考に、要件定義書（案）の一部を変更いたします。
23	要件定義書	100	第3章 非機能要件 11 情報システム稼動環境に関する事項 11.1 ハードウェア構成 11.1.11 プリンタ (1) 幹部用プリンタ	1	D(奥行) 570mmまで緩和願いたい	当該仕様の緩和により、低価格・低ランニングコストの機種が提案可能となるため	御意見を参考に、要件定義書（案）の一部を変更いたします。
24	要件定義書	100	第3章 非機能要件 11 情報システム稼動環境に関する事項 11.1 ハードウェア構成 11.1.11 プリンタ (2) 貸出用プリンタ	1	20枚以上に緩和願いたい	当該仕様の緩和により、低価格・低ランニングコストの機種が提案可能となるため	御意見を参考に、要件定義書（案）の一部を変更いたします。
25	要件定義書	119	第3章 非機能要件 13 移行に関する事項 13.2 移行要件 13.2.2 移行作業	1	【要件】 ・ 移行作業にあたっては、現行システム運用・保守業者との調整を行った上で実施すること。調整に対し発生する費用及び現行システムの変更作業に必要となる費用は本調達に含むこと。 上記の要件について、削除、もしくは受注後に別途協議とする旨への緩和を検討願います。	調整次第で費用が変動する可能性があり、見積りの精度を向上させるため。	御意見として承りましたが、現行システム運用体制との調整費用は本調達に含まれることから、要件定義書（案）の通りとします。
26	要件定義書	121	第3章 非機能要件 13 移行に関する事項 13.2 移行要件 13.2.6 移行期間中における運用・保守・監視	1	【要件】 ・現行システム運用体制と調整にあたり発生する費用及び現行システムの設定変更等の作業に必要となる費用は本調達に含むこと。 上記の要件について、削除、もしくは受注後に別途協議とする旨への緩和を検討願います。	調整次第で費用が変動する可能性があり、見積りの精度を向上させるため。	御意見として承りましたが、現行システム運用体制との調整費用は本調達に含まれることから、要件定義書（案）の通りとします。
27	要件定義書	124	第3章 非機能要件 15 教育に関する事項 15.1 教育対象者の範囲、教育の方法 15.1.1 移行時の教育	4	(3) 部局のシステム担当者に対する教育において、 現地での集合研修が必要な個所について、明示いただいた方が良いのではないでしょうか。	要件明確化のため。	移行時教育の実績等の情報については、資料閲覧の際に開示します。

LAN調達仕様書意見に対する対応

注） 1.種目欄には、意見の種類を以下から選択して、その番号を記載すること。

［1. 要求水準を下げる。 2. 要求水準を上げる。 3. 文章だけを修正する。 4. その他 ］

No.	資料名	頁番号	項 目	種別	意　　見	理　　由	回　　答
28	要件定義書	137	第3章 非機能要件 16 運用に関する事項 16.1 運転管理・監視等要件 16.1.7 情報セキュリティ対策業務	2	情報セキュリティ対策業務として、記載のもの以外に下記2つを追加することを推奨いたします。 ・脅威動向に応じた対応の検討および実施 ・未知のマルウェア感染検知を想定したログ分析	セキュリティ運用の中で、最新の脆弱性や流行りの攻撃手法など脅威動向を常に把握しておくことが重要です。 また、これら最新の脅威動向を把握した上で、ログ分析を行うことが重要と考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、情報セキュリティの対策業務については、「第3章 非機能要件 16.1.9 標的型攻撃対応業務 (2) 対応」に記載しております。
29	要件定義書	137	第3章 非機能要件 16 運用に関する事項 16.1 運転管理・監視等要件 16.1.7 情報セキュリティ対策業務	2	以下のように修正することを推奨いたします。 変更前 「セキュリティを維持確保する為に必要とされる作業を適切に行い、最新の状態を保つこと。作業周期については、内閣府 PJMO と協議の上、決定すること」 変更後 「セキュリティを維持確保する為に必要とされる作業を適切に行い、最新の状態を保つこと。作業周期については、内閣府 PJMO と協議の上、決定すること。また、リスクの高い脅威に対してセキュリティを確保できていない環境が存在している事が判明した場合は、平日3日以内に想定されるリスクと現状を報告の上でリスク低減策を検討し、内閣府 PJMO と協議の上で対応すること。」	リスクの高い脅威に対しては、その影響と対策について早急にPJMOに報告し、対応する必要があると考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、作業周期等は、内閣府PJMOと協議の上、決定します。
30	要件定義書	139	第3章 非機能要件 16 運用に関する事項 16.1 運転管理・監視等要件 16.1.9 標的型攻撃対応業務 (1) 監視	2	以下のように修正することを推奨いたします。 変更前 「マルウェア（未知のものを含む）の次期システムへの感染・侵入に関して、セキュリティ監視装置等による検知アラート、警告ログ等を常時監視すること。」 変更後 「マルウェア（未知のものを含む）の次期システムへの感染・侵入に関して、セキュリティ監視装置等による検知アラート、警告ログ等を常時監視すること。また、定期的なログ分析等を実施し能動的にマルウェア感染等の検知と調査（Threat Hunting)に努めること。」	様々なセキュリティ対策を実施したとしても、未知のマルウェアを使用した攻撃を100%事前に検知・防御することは非常に困難です。 そのため、セキュリティ機器が出すアラートの単純な監視だけではなく、定期的にログ分析等を行って不審な活動などを能動的に見つけ出す運用が必要と考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、具体的な対応については、「第3章 非機能要件 16.1.9 標的型攻撃対応業務 (2) 対応」に記載しております。
31	要件定義書	139	第3章 非機能要件 16 運用に関する事項 16.1 運転管理・監視等要件 16.1.9 標的型攻撃対応業務 (1)監視	2	以下のように修正することを推奨いたします。 変更前 「 標的型攻撃等に対する監視業務の詳細（監視体制、監視業務フロー等）に関しては、設計段階において、内閣府 PJMO 及び各設計・構築事業者間との調整や協議の上、決定するものとする。」 変更後 「標的型攻撃等の対応業務の詳細（通知方法、対応内容、対応フロー等）に関しては、設計段階において、セキュリティ運用の効率化および検知精度向上に繋がる仕組みや監視対象ログを整理し、内閣府 PJMO 及び各設計・構築事業者間との調整や協議の上、決定するものとする。また、本業務について、Web 事業者及び WAN 事業者と連携して業務の実施にあたること。」	セキュリティの観点でログの収集や分析を行う場合、どのログを収集するか、また各ログの中のどの項目を、どのレベルで出力するかは非常に重要となります。 また、システムの構築後に収集対象ログを追加、またはログの出力レベルを変えることは困難な場合があります。 そのため、対象ログの検討・決定については設計時点で実際のログ分析やインシデント対応を経験した専門家を含めて行うことが望ましいと考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、標的型攻撃への対応業務として、「第3章 非機能要件 16.1.9 標的型攻撃対応業務 (2) 対応」に記載しております。
32	要件定義書	139	第3章 非機能要件 16 運用に関する事項 16.1 運転管理・監視等要件 16.1.9 標的型攻撃対応業務 (2) 対応	2	以下のように修正することを推奨いたします。 変更前 「検知ログ・警告ログ等を利用し、未知のマルウェアに感染した機器を特定し速やかに報告すること。」 変更後 「検知ログ・警告ログ等を利用し、未知のマルウェアに感染した機器を特定し速やかに、影響範囲とその対応策を検討し報告すること。」	昨今のマルウェアは1台のクライアント機器に感染した後、他のクライアント機器や、サーバ機器に対して感染活動を広げます。 そのため、対応が遅くなればなるほど被害範囲が広がり、対応や復旧に時間がかかるため、速やかに影響範囲と対応策を検討する仕組みが必要と考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、セキュリティに関する情報収集等は「第3章 非機能要件 16.1.7 情報セキュリティ対策業務」に記載しております。

LAN調達仕様書意見に対する対応

注） 1.種目欄には、意見の種類を以下から選択して、その番号を記載すること。

[1. 要求水準を下げる。 2. 要求水準を上げる。 3. 文章だけを修正する。 4. その他]

No.	資料名	頁番号	項 目	種別	意　　見	理　　由	回　　答
33	要件定義書	140	第3章 非機能要件 16 運用に関する事項 16.1 運転管理・監視等要件 16.1.9 標的型攻撃対応業務 (2) 対応	2	以下のように修正することを推奨いたします。 変更前 「四半期毎に、セキュリティ対策の専門家等による分析結果の報告やアドバイスを提供すること。」 変更後 「セキュリティ対策の専門家等による分析の実施と分析結果の報告やアドバイスを週3日程度（8号館庁舎分の分析作業1日、特定部局の分析作業1日、アドバイス全般1日）提供すること。また改善に向けた提案を月に1回実施すること。なお分析および報告には、最新の脅威動向およびCyber Threat Intelligenceに精通する専門家が参加すること。」	標的型攻撃は非常に巧妙になっており、ログの分析作業には高度なセキュリティの知識と経験が必要となります。 そのため分析作業の実施も含め、セキュリティに精通した人物によるアドバイスが常に得られる体制が必要と考えます。	御意見として承りましたが、要件定義書（案）の通りとします。 なお、標的型攻撃への対応業務において、「第3章 非機能要件 16.1.9 標的型攻撃対応業務（2）対応」に事象の内容や原因追究、影響範囲の見極めや対応策の検討を要件として記載しております。

LAN調達仕様書質問に対する回答

注）１．種別欄には、質問の種類を以下から選択して、その番号を記載すること。
［１．仕様書（案）に対する質問。　２．要件定義書（案）に対する質問。　3. その他］

No.	資料名	頁番号	項 目	種別	質　　問	理　　由	回　　答
1	調達仕様書	18	第3章 作業の実施内容 1 作業内容 1.1 設計・構築業務 1.1.7 現地調査	1	【要件】 ・本調達で導入する無線LAN アクセスポイントの全ての箇所において、事前・事後サイトサーベイを実施し、既設電波測定結果資料等（図面プロット・電波測定値等）を図面及び報告書にまとめて提出すること。また、機器設置完了時の電波測定資料も図面及び報告書にまとめて提出すること。 上記の要件について、事前、事後、機器設置完了時の3回サイトサーベイを実施するという認識でよろしいでしょうか。 事後サイトサーベイと機器設置完了時は同義と考えられますが、事後サイトサーベイとはシステムリリース直前に実施するという意味でしょうか。	事後サイトサーベイと機器設置完了時の違いを明確化し、業者毎での回数見積りの相違をなくすため。	サイトサーベイの回数は、事前と機器設置完了時の2回となります。 御質問を参考に、調達仕様書（案）の一部を変更いたします。
2	要件定義書	21	第2章 機能要件 1 機能に関する事項 1.2 サービス要件 1.2.5 Proxy要件	2	HTTP1.1及び2.0に対応したHTTPリクエストの中継機能を有すること、との記載がございますが、下記の様に変更は可能でしょうか。 「HTTP1.1（2.0に対応していれば尚、良い）に対応したHTTPリクエストの中継機能を有すること」	HTTP2.0の記載により、現状、製品の選択肢が限定されるため。	現状において製品の選択肢が限定される為、御質問を参考に、要件定義書（案）の一部を変更いたします。
3	要件定義書	30	第2章 機能要件 1 機能に関する事項 1.2 サービス要件 1.2.11 バックアップ要件	2	バックアップメディアについては、4年分を本調達に含めるのでしょうか。	要件明確化のため。	「別紙12 内閣府LAN（共通システム）データバックアップ管理及びログ管理一覧」に示す通りとなります。 バックアップメディアの必要数を算出するにあたり、サーバ毎のバックアップ方式及びバックアップ取得頻度の案を示しております。
4	要件定義書	32	第2章 機能要件 1 機能に関する事項 1.2 サービス要件 1.2.15 仮想デスクトップ要件	2	【要件】 ・仮想デスクトップは最大5,700台（仮想デバイス数）とすること。また、最大同時アクセス数5,700を想定すること。なお、人事異動（最大800人程度）を考慮すること。 上記の要件について、「人事異動（最大800人程度）を考慮」は、具体的にはどのような考慮が必要となりますでしょうか。	要件明確化のため	現行システムの実績として、大規模な定期人事異動時には最大800人程度の異動が発生、一時的にアカウントが重複しており、解消するまでに申請から異動完了まで2週間程度の期間を要しておりますので、当該実績を考慮したライセンス契約、システム構成等を御提案ください。
5	要件定義書	33	第2章 機能要件 1 機能に関する事項 1.2 サービス要件 1.2.16 共有ストレージ要件 (1) 基本要件	2	【要件】 ・府外関係者のアカウントを作成し、利用することが出来ること。 上記の要件について、「府外関係者のアカウント」の数量は、どの程度を想定すればよろしいでしょうか。	要件明確化のため	現行における府外関係者のアカウント数の実績等の情報については、資料閲覧の際に開示します。
6	要件定義書	43	第2章 機能要件 1 機能に関する事項 1.4 行政端末要件	2	運用者が利用する端末が、ここで示されている端末に含まれるか読み取れないため、明確にする必要があると考えます。	運用者の端末数量を明確にするため。	「第2章 機能要件 1.4 行政端末要件」の「表 2-1-1　行政端末の機能要件一覧」に示す共用端末の150台の内、運用者用端末として20台程度を想定しております。なお、障害時や非常時においては災害用端末として使用する為、運用者が利用する端末は必要に応じて別途御用意頂きます。 また、運用の効率性等を考慮した上で、20台以上必要と判断される場合には本調達の範囲で御用意ください。ただし、御提案頂く端末については、「第3章 非機能要件 10.12 行政端末に関するセキュリティ対策」「第3章 非機能要件 16.1.4 行政端末管理業務」の要件を満たしている必要があります。
7	要件定義書	46	第2章 機能要件 1 機能に関する事項 1.4 行政端末要件 1.4.3 ソフトウェア要件	2	OASYSが枠外になってますが、これが表のなかの数量に含まれるか明確にしたほうが良いのではないでしょうか。	要件明確化のため。	「第3章 非機能要件 11.2 ソフトウェア構成 ④ ワープロ閲覧・編集」に示す要件を満たすソフトウェアを数量5,700御用意頂き、別途、富士通OASYSを数量5御用意頂きます。 御質問を参考に、要件定義書（案）の一部を変更いたします。
8	要件定義書	60	第2章 機能要件 1 機能に関する事項 1.7 Web申請システム要件 1.7.2 各種申請	2	データバックアップ機能は持たせるのでしょうか。	要件明確化のため。	現行システムにおいてもデータバックアップ機能を備えている為、必要な機能となります。 御質問を参考に、要件定義書（案）の一部を変更いたします。

注）１．種別欄には、質問の種類を以下から選択して、その番号を記載すること。
［１．仕様書（案）に対する質問。　２．要件定義書（案）に対する質問。　3．その他］

No.	資料名	頁番号	項 目	種別	質　　問	理　　由	回　　答
9	要件定義書	65	第2章 機能要件 1 機能に関する事項 1.11 復興庁要件	2	撤去については組織が廃止となるタイミングで実施するのでしょうか。	要件明確化のため。	御認識の通りとなります。 復興庁については平成33年3月31日の組織廃止、その他組織については平成34年12月31日の運用終了を持って撤去作業を実施ください。
10	要件定義書	119	第3章 非機能要件 13 移行に関する事項 13.2 移行要件 13.2.1 移行体制	2	【要件】 ・ 移行期間中における次期システムに関する職員からの問合せを受け付ける移行ヘルプデスク等を設置すること。 上記の要件について、対応時間は、平日9:30～18:15（内閣府の閉庁日（土・日曜、祝祭日、振替休日、国民の休日、年末年始（12月29 日～1 月3 日））を除く）の認識で問題ありませんでしょうか。	対応時間を明確化するため。	御認識の通りとなります。 ただし、応札事業者が策定する移行計画・スケジュールに応じて、内閣府PJMOと協議の上、決定されます。
11	要件定義書	136	第3章 非機能要件 16 運用に関する事項 16.1 運転管理・監視等要件 16.1.6 システム更新業務 (4) 行政端末 ③ 内閣府LAN接続支援	2	過去の接続支援の実績はどの程度であったのでしょうか。	要件明確化のため。	現行における内閣府LAN接続支援の実績等の情報については、資料閲覧の際に開示します。
12	別紙13運用工数一覧	－	－	3	作業時間月平均合計5,328時間は、常駐しているLAN事業者の作業者の月当たりの平均作業時間と考えてよろしいでしょうか。	運用工数積算の参考にするため。	御認識の通りとなります（一部、現行システムにおける運用管理事業者の工数も含まれます）。
13	別紙27別途保守機器一覧	－	17	3	次期LANシステム調達以外に下記無線LAN用機器の保守が必要になる理解でよいでしょうか。　（SW×43台、AP×271台）	調達範囲の確認のため。	御認識の通りとなります。 なお、次期システム調達以外の保守対象機器は「別紙27 内閣府LAN（共通システム）別途保守機器一覧」に示しております。