調達件名：令和４年度ガバメントソリューションサービスにおけるセキュリティ脅威の検知・分析・遮断サービスの提供

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
1	意見	調達仕様書　２ 実施作業内容	8	2	1	①	2	① セキュリティ監視（SOC）・インシデント対応は、24 時間 365 日対応セキュリティ 監視と対応を行うマネージドセキュリティサービスであること	Microsoft365E5・行政・軍事・インフラ他も共通でAI監視とPowerAPPｓ（データバース）の設定も追加、弊社の最新版でスパムは99.9%で破壊と分析が可能です。国際標準のMicrosoft365運用企業は通常仕様になっています。3年間インシデントなし＝スパムはすべて破壊+分析システム保護停止は1件のみ、原因はSHA384の事案のみ。	御意見ありがとうございます。 審査等の際に参考とさせていただきます。
2	意見	調達仕様書　２ 実施作業内容	8	2	1	⑧	2	⑧ 情報セキュリティインシデント発生又はそのおそれがある時、次の対応を行えること。 ・ デジタル庁の担当者の求めに応じ、ダークウェブ等の特殊な環境を用いたアクセスが必要なネットワーク等で公開されている情報について、年２回までの調査を実施し、ガバメントソリューションサービスの影響有無等の結果を報告すること。 ・ デジタル庁の担当者の求めに応じ、端末、Windows サーバの調・報告ができる簡易的なフォレンジックを提供すること。	サーバーとクラウドのIP通過履歴で、定期解析も追加する。 サーバーは管理ファイルの脆弱性が発生しやすい。信用性で疑問有り、重要ファイルはOneDriveの並行利用を推奨します。 原則としてアプリケーションシステム管理へ移行しないと採用の意味がない。	御意見ありがとうございます。 審査等の際に参考とさせていただきます。
3	意見	調達仕様書　２ 実施作業内容	10	2	2	④	2	2.3 技術的要件	PowerAPPｓ・OneDriveの採用と設定、SNSのタブレット管理と接続可能端末を各部署で2台予算化する。同じユーザー使用料金でパフォーマンスを上げる。	御意見ありがとうございます。 審査等の際に参考とさせていただきます。
4	意見	調達仕様書　３ その他遵守事項	15	3	1	1	4	受注者に求める資格等 受注者は、ISMAP またはこれに準ずる認証（ISO27001/ISMS 認定等）を受けている こと。	追加でMicrosoft365E5以上の運用実績や研究開発がある事業所、NATO圏内IT開発ベンチャーなど経験重視の審査へ移行する。ISMSは古い。	御意見の資格等は「等」に含まれるものと考えております。
5	意見	1 情報取扱者名簿及び情報管理体制図　別添資料2【追加支援】	1	1	1	図1	2	運用実績の事業者が実施する、作業管理を内容で追加する。国内・国際標準を偽装などして受注した事例から確認の強化。図1の表に運用実績企業チェック	二重・三重の確認があれば防げることは事前に実施できる計画にする。	御意見ありがとうございます。 審査等の際に参考とさせていただきます。
6	意見	調達仕様書	9	2	3	（1）	4	「②リスクやインシデントを検知した際は、チケットを作成し、デジタル庁が設定する担当者に対して指定された方法によりエスカレーションすること」との記載がありますが、「指定された方法」とは具体的にどのような方法を想定しているか、ご教示お願いします。	サービス・製品選定のため	2.3（５）①に記載する方法です。 この旨仕様書に明記いたします。
7	意見	調達仕様書	9	2	3	（1）	4	「⑧デジタル庁の担当者の求めに応じ、ダークウェブ等の特殊な環境を用いたアク セスが必要なネットワーク等で公開されている情報について、年２回までの調査を 実施し、ガバメントソリューションサービスの影響有無等の結果を報告すること。」との記載がありますが、通常のSOCサービス以外の製品を組み合わせて、上記要件に対応するという理解で宜しいでしょうか。	サービス・製品選定のため	御理解のとおりです。 SOCサービス以外の製品を組み合わせる形でも要件に対応いたします。なお、その際、データの送受信など、情報の取扱いを確認させていただく可能性がありますので、あらかじめ御承知置きください。
8	意見	調達仕様書	13	2	4	（1）	3	成果物について、運用計画書の提出時期は「契約締結後40営業日以内」となっています。一方で、調達仕様書p.6 1.4 作業スケジュールを見ると、業務実施がR4年2月以降となっています。一般的に運用計画書策定後から運用業務が開始されるものと思われるため、運用計画書の提出時期前倒しまたは業務実施開始の後ろ倒しをご検討願います。	要件確認・明確化のため	可能な範囲から業務実施いただきたいと考えておりますため、例えば、契約後において小規模で業務実施を開始し、並行で運用計画書を作成し、運用計画書が承認され次第、当該運用計画書に基づく業務を本格開始いただきたいと考えております。 そのため、運用計画書の作成始期と業務実施の始期を同一としております。
9	意見	調達仕様書	18	3	6		3	「3.6 入札参加に関する事項」に記載の 「https://cio.go.jp/sites/default/files/uploads/documents/digital/20210901_procurement_03.pdf」について、「アクセス先のページが見つからない」旨のエラー画面となります。記載URLのご確認をお願いします。	要件確認・明確化のため	以下のとおり修正いたします。 https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c5d7192e-22e0-4810-8afd-ce83c50af6a4/20220309_policies_procurement_doc_01_1.pdf

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
10	意見	調達仕様書	10	2	3	(2) ④	3	「Microsoft 365 E5 に含まれる下記のサービスに関連するログ」について、想定されているデバイス数・ユーザ数を記載をお願いします。	提供するサービスの規模を把握して、費用を算出するために必要です。	契約期間中において想定される最大デバイス数、ユーザー数は約40,000です。 この旨、仕様書にも記載いたします。
11	意見	調達仕様書	11	2	3	(3) ②	3	ログメッセージ受信のために、デジタル庁が契約しているクラウド（Azure）に対してアプリケーションなどのリソースを追加した際に費用が発生する場合がありますので、その場合の費用を本調達に含めるかの記載をお願いします。	提供するサービスの費用を算出するために必要です。	ご記載の費用は本調達に含めないこととしていただいて問題ございません なお、ご記載のアプリケーションなどのリソースの追加については、別途デジタル庁が必要と認める場合において実施することを予定しております。
12	意見	01_調達仕様書_ver1	11	2	3	5	1	「通知に関する要件」として、「①リスクやインシデント(被疑要件)を特定した場合、特定後 1 時間以内にチケットを発行し、デジタル庁担当者によってあらかじめ設定された通知ポリシーに従い通知を行うこと」との記載があるが、具体的な通知ポリシーの内容（連絡先、手段等）を開示して頂きたい。	通知ポリシーにより、通知に関わるシステムの改修要否・体制の構成に影響があり、それらの費用を算出するために必要なため。	①で記載する「あらかじめ設定された通知ポリシー」は、業務開始後において④にて設定する通知ポリシーです。 なお、掲載連絡に係る連絡先及び手段を③へ記載いたしました。
13	意見	01_調達仕様書_ver1	10	2	3	2	3	「⑤ ①から生成されるログは全て相関分析に利用すること。③から生成されるログを相関分析の対象とする場合には加点とする」を「②、③から生成されるログは全て相関分析に利用すること。③から生成されるログを相関分析の対象とする場合には加点とする」に変更いただきたい。	①は「以下の監視対象機器」とあるため、全体についての説明と理解しております。相関分析の対象となるのは、②または③で生成されたログという理解で問題なければ文章の修正をおねがいいたします　。	以下のとおり修正いたします。 「④ ①及び③から生成されるログを相関分析に利用すること。なお、②から生成されるログを相関分析の対象とする場合には加点とする」
14	意見	01_調達仕様書_ver1	9	2	3	(1) ⑥	2	⑥「ポータルを構成するにあたってインフラレベル(サーバとストレージレベル)で分割されている場合には加点とする 」とありますが、インフラレベルの分割を行うのであればポータルだけでなく、システム全体とすべきではないでしょうか？	情報漏えいの防止策としてシステムを分割するのであれば、ポータルのみでは不十分と考えます。	ご意見を踏まえ、以下のとおり修正いたします。 「ポータルを構成するシステムが論理的及び物理的に分割されている場合には加点とする。」
15	意見	01_調達仕様書_ver1	11	2	3	(4) ④	3	④「関連する通信記録を受信してから 2 時間以内に行うこと」は、「関連する通信記録を受信してから、または、分析によってインシデントを認知してから 2 時間以内」に変更頂きたい。	④「関連する通信記録を受信してから 2 時間以内に行うこと」とあるが、巧妙化が進むサイバー攻撃では、事後の詳細調査からインシデントが発見されるケースもあるため、”通信記録の受信”からではなく、分析の結果、”インシデントを認知”してからの時間も併記	インシデントの通報に関しては、おそれがある場合も報告する必要があることから、関連する通信記録を受信した段階で通報することとしております。
16	意見	01_調達仕様書_ver1	11	2	3	(4) ⑤	3	「SOC 業務を 3 年以上行っている経験」は、「SOC 業務を 3 年以上行っている経験、または同等のスキルを有する者」に変更頂きたい。⑥についても同様である。	「SOC 業務を 3 年以上行っている経験」となっているが、経験年数ではなく、業務可能なスキルで判断すべきと考えます。 また、昨今の新入社員は学生時代からサイバーセキュリティの勉学に励み、優秀な人材も多く、これらメンバーの参画企画も踏まえ、「SOC 業務を 3 年以上行っている経験、または同等のスキルを有する」に変更頂きたい。	ご意見ありがとうございます。 業務可能なスキルも重視するところではありますが、セキュリティインシデントにいかに気づけるかという点は、SOC経験者でしか持ちえないことから、当要件を採用しております。。 なお、記載の経験は「インシデント分析に関する技術的要件」として、受注者に求める経験です。
17	意見	01_調達仕様書_ver1	9	2	3	(1) ⑧	2	「デジタル庁の担当者の～フォレンジックを提供すること。」に対し、求める調査範囲を明記することを推奨します。以下、弊社が考える一般的に求められる調査範囲４点を記載します。 ①侵入原因の痕跡調査 　侵害に至った原因について端末および各種ログから調査 ②侵害による影響調査 　侵害を受けたことによる端末への各種影響などを端末および各種ログなどから調査 ③被害範囲の痕跡調査 　侵害端末からの侵害拡大痕跡について端末および各種ログなどから調査 ④情報漏えい痕跡調査 　情報漏えいの痕跡について端末および各種ログなどから調査	フォレンジック調査といってもそのレベルは業者によりピンキリのため、求めるレベルや範囲を最低限明記した方がよいと考えます。	ご意見ありがとうございます。 本件要件は、付加的に求めるものであり、仕様書記載の要件を満たせば足り、これ以上の詳細な要件を求めるものではございません。

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
18	意見	01_調達仕様書_ver1	9	2	3	(1) ⑧	2	「デジタル庁の担当者の～フォレンジックを提供すること。」に対し、調査結果の提出を求める旨、明記することを推奨します。その場合、「結果報告書」等の形で対策案含め取りまとめることを求めることで、Microsoft Defender for Endpoint等監視機器からのアラート内容をそのまま通知する報告は不可とすることを推奨します。	フォレンジック調査といってもそのレベルは業者によりピンキリのため、求めるレベルや範囲を最低限明記した方がよいと考えます。	ご意見ありがとうございます。 本件要件は、付加的に求めるものであり、仕様書記載の要件を満たせば足り、これ以上の詳細な要件を求めるものではございません。
19	意見	01_調達仕様書_ver1	9	2	3	(1) ⑧	2	「デジタル庁の担当者の～フォレンジックを提供すること。」に対し、インシデント対応の専門部隊にて対応する旨明記することを推奨します。	フォレンジック調査といってもそのレベルは業者によりピンキリのため、求めるレベルや範囲を最低限明記した方がよいと考えます。	ご意見ありがとうございます。 本件要件は、付加的に求めるものであり、仕様書記載の要件を満たせば足り、これ以上の詳細な要件を求めるものではございません。
20	意見	令和４年度ガバメントソリューションサービスにおけるセキュリティ脅威の検知・分析・遮断サービスの提供 調達仕様書	6	1	4		3	項目3は「月次報告会議事及び」の文言の続きを確認お願いいたします。	項目3は内容が途中で切れているように見受けられるためです。	ご意見ありがとうございます。 以下のとおり修正いたします。 「月次報告会議事及び」→「月次報告会」
21	意見	同上	10	2	3	(2) ④	2	ご利用のMicrosoftライセンスに「Microsoft Defender for Office 365」が含まれており、当該機能を利用できる環境の場合には、当該機能も監視対象に含めるのがセキュリティ上望ましいと考えます。	「Microsoft Defender for Office 365」は、マルウェアを含むファイル・攻撃目的のURLの配送といった、メール経由での外部からのサイバー攻撃を発見、防止を目的とする機能と理解しているためです。	ご意見ありがとうございます。 「Microsoft Defender for Office 365」を監視対象に含めることといたします。
22	意見	同上	12	2	3	(7) ①	3	なお書きを追記いただくことは可能でしょうか。 「①通知した被疑要件に関する情報と分析状況をリストにまとめ、月次でデジタル庁担当者に提出すること。また、デジタル庁担当者からの要望に応じた統計データを月次レポートに含めること。 なお、当該要望は原則、運用開始前に協議のうえ調整することとする。」	仕様からは、月次レポートに関するお客様からの要望を常時受け入れるように見受けられますが、運用開始前に極力すり合わせを行うことで、開始後の認識齟齬が減らせると考えるためです。	ご意見ありがとうございます。 ご意見を踏まえ、取り入れさせていただきます。
23	意見	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	⑥	1	＜仕様書＞ リスクやインシデントと判定された事象をチケットとして登録、表示することのできるチケッティングシステムをデジタル庁専用ポータルとして提供すること。また、このポータルは本サービスを提供する事業者内でテナントとして分割されており、他社に対して情報が漏えいしないよう厳格に管理されていること。ポータルを構成するにあたってインフラレベル(サーバとストレージレベル)で分割されている場合には加点とする ＜修正案＞ ポータルを構成するにあたっては、原則としてISMAPを取得しているクラウドサービスを用いる場合は加点とする。オンプレミス相当での構築とする場合は、インフラレベル(サーバとストレージレベル)で分割されている場合には加点とするが、『『政府機関等のサイバーセキュリティ対策のための統一基準（令和３年度版）』を遵守の上、OSやミドルウェア等の各種セキュリティパッチが即時に適用されており、設計上セキュリティ的な脆弱性が発生しえないことを、設計書、運用マニュアル等を提示すること。	GSSはMicrosoftなどのSaaSを活用してる中で、本項目のみSaaS利用を選択肢から除外されているように読み取れました。ISMAPなどの条件のもと利用可能にすることが、貴庁の趣旨に適していると考えます。 また、オンプレミスでの実装を前提としたようなサービスは逆にパッチ適用の遅れのリスク、各種設定漏れ、設計上の不備など、逆にセキュリティ的なリスクが高まると考えます。 そのため、左記のように修正することを推奨します。	前段に関しては、ISMAP取得に限定した場合、参入障壁となる可能性があることから、現状のままとさせていただきます。 後段に関しては、設計上、セキュリティ的な脆弱性が発生し得ない環境を構築することは理論上困難と考え、要件を満たすことが困難となり、参入障壁となりかねないことから、現状のままとさせていただきます。 なお、提案時にこのような内容で対応できる、ということをご提案いただくことを妨げるものではありません。
24	意見	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	⑦	2	＜仕様書＞ 上記ポータルにおいては次の要件を満たすこと。 ・ チケット情報に加え、分析結果に関連するログ情報もしくはログ情報に対するリンクを示すことができること ・ 受注社が自社で開発・運用しているサービスであり、受注者がポータルを構成する機器及びソフトウェアの保守を適切に実施し、不具合発生時も受注者で対応するなど、受注者が管理責任を負うこと。 ＜修正案＞ 上記ポータルにおいては次の要件を満たすこと。 ・ チケット情報に加え、分析結果に関連するログ情報もしくはログ情報に対するリンクを示すことができること ・ 受注社が自社で開発・運用しているサービスであり、受注者がポータルを構成する機器及びソフトウェアの保守を適切に実施し、不具合発生時も受注者で対応するなど、受注者が管理責任を負うこと。 ・ポータルにログインする際には多要素認証を必須とすることができること。	『政府機関等のサイバーセキュリティ対策のための統一基準（令和３年度版）』8.1.3　遵守事項においても多要素認証の実装は義務付けられております。また、認証方式に指定がない場合は、IDとPASSだけでアクセスできる方式を容認してしまい、リスクが高まると考えます。 そのため、左記のように修正することを推奨します。	ご指摘ありがとうございます。 本件は加点要素として仕様書に記載することといたします。

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
25	意見	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	⑧	3	＜仕様書＞ デジタル庁の担当者の求めに応じ、ダークウェブ等の特殊な環境を用いたアクセスが必要なネットワーク等で公開されている情報について、年２回までの調査を実施し、ガバメントソリューションサービスの影響有無等の結果を報告すること。 ＜修正案＞ デジタル庁の担当者の求めに応じ、ダークウェブ等の特殊な環境を用いたアクセスが必要なネットワーク等で公開されている情報について、年２回までの調査を実施し、ガバメントソリューションサービスの影響有無等の結果を報告すること。 なお、調査にあたってはRecordedFutureなどのクラウドサービスなどのツールを用いる場合はISMAP取得をしているクラウドサービスを利用すること。	原則ISMAPを取得しているサービスを用いる必要があると理解しており、要件を明確化し、落札後の認識差異によるトラブルを防止するため。	例示されているサービスはISMAPを取得しているサービスではなく、記載することでミスリードになる可能性があるため、原案のままといたします。
26	意見	01_調達仕様書_ver1.0.pdf	11	2.3	(4)	④	1	＜仕様書＞ 被疑通信の特定は、関連する通信記録を受信してから2時間以内に行うこと ＜修正案＞ 被疑通信の特定は、関連する通信記録を受信してから原則2時間以内に行うこと	2時間以内を原則としますが、攻撃によっては遡り分析をすることで関連通信が見つかる場合もあり、2時間以内を要件にしてしまうと遡り分析ができなくなるため。	インシデントの通報に関しては、おそれがある場合も報告する必要があることから、関連する通信記録の受信の段階で通報することとしております。また、あくまで被疑段階であることから、継続して調査するかどうかは、SOC側の能力・知見によるところと考えます。
27	意見	01_調達仕様書_ver1.0.pdf	15	3.1	(1)	-	2	＜仕様書＞ 受注者は、ISMAP またはこれに準ずる認証（ISO27001/ISMS 認定等）を受けていること。 ＜修正案＞ 受注者は、ISMAP またはこれに準ずる認証（ISO27001/ISMS 認定等）を受けていること。 受注者は本調達と同等規模（約4万人）の中央省庁におけるSOC業務を実施した経験を有していること。	SOC事業者の能力の測定は困難であり、最低限同規模の案件の対応の実績を有していない場合は、業務履行途中で要員不足や、能力不足が判明する可能性が非常に高いと推測します。 本調達は国内最有数希望の調達になることが想定され、規模を考慮した場合、同種かつ同程度の規模を有していることで、一定水準の品質を担保させることを推奨します。	参入障壁となる恐れがあるため、原案のままとさせていただきます。
28	意見	01_調達仕様書_ver1.0.pdf	8	2	1	（2）	2	運用計画に関して以下の項目を追記いただくと、SoC基盤の安定稼働やデジタル庁様の運用負荷軽減につながると考えます。 「キ）Managed-SoCの採用の採用を踏まえ、Microsoft 365 E5 の SaaSサービスに関するバージョンアップ、メンテナンス作業等に関し、ポータルおよび電子メールで事前通知する仕組みと体制 ク）バージョンアップやメンテナンス内容に関し、ポータルでの表示及び月次報告会での報告に関する手順」	従来のオンプレミスの運用と異なり、運営主権がクラウド・SaaSベンダーが主体となってバージョンアップ、メンテナンスを行うためコントロールが難しいこと、情報収集も大変なため、なるべくManaged SoCベンダーにオフロードいただくことが負荷軽減、安定稼働につながると考えます。 （SaaSベンダーからメンテナンス、バージョンアップ情報や内容の詳細をポータルにて提供しますが、ポータルに簡易情報を掲載するだけで、お客様に情報通知しないSaaSベンダーがあります。これらを踏まえManaged-SoCベンダーにてバージョンアップ等ののメンテナンス情報をデジタル庁様に通知する仕組みが必要と考えます）	御意見ありがとうございます。 御意見を踏まえ、本文に取り入れさせていただきます。
29	意見	01_調達仕様書_ver1.0.pdf	11	2	3	（3） ⑤	2	世間の動向を鑑みると、不正アクセス発生等から1年以上経過したのちに情報漏えいや攻撃させていたことに気付く事例も多数あるため、 「⑤受信したログメッセージは最低 1年6か月保存し、デジタル庁専用 Web ポータルから閲覧できる」 との、原案より期間を長くすることを提案します。 (設備、費用の観点もあるため、少なくとも保存期間の検討が必要と思料します)	NISCも過去の事例を踏まえ、推奨は1年以上保存としていること。不正アクセス発生等から1年以上経過したのちに気付き1年以上前に遡って調査するケースもあるため。	御意見ありがとうございます。今回の契約がおよそ１年間の契約となることから、契約期間を超えない１年間の保存とさせていただいております。 今後、長期間の契約となる場合は１年以上の保存とすることも検討いたします。
30	質問	調達仕様書	10	2	3	（1）	1	「⑧～デジタル庁が指定する場所に参集を求めることがあるため、確実に参集できる体制を整備すること。」との記載がありますが、デジタル庁が指定する場所とは、原則都内の想定でしょうか。	要件確認のため	原則都内２３区内を想定しております。
31	質問	01_調達仕様書_ver1	9	2	3	1	1	「セキュリティ監視（SOC）及びインシデント対応に関する要件」として、「①セキュリティ監視（SOC）・インシデント対応は、24 時間 365 日対応セキュリティ監視と対応を行うマネージドセキュリティサービスであること 」とあるが、分析システムの定期メンテナンス・収容データセンターのメンテナンス等を要因とする、計画された分析遅延（1～数時間程度）は許容されるか。	作業範囲の確認のため	例えば、法定点検の実施のようなやむを得ない状況があれば、事前にデジタル庁と協議の上許容することも可能です。

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
32	質問	01_調達仕様書_ver1	10	2	3	1	1	「セキュリティ監視（SOC）及びインシデント対応に関する要件」として、「⑧情報セキュリティインシデント発生又はそのおそれがある時、次の対応を行えること」に「デジタル庁の求めに応じて、デジタル庁が指定する場所に参集を求めることがあるため、確実に参集できる体制を整備すること。」とあるが、依頼から参集に許容される時間は何時間か。または依頼に対しWeb会議の開催を要望することは可能か。	作業範囲の確認のため	３時間以内の参集を想定しています。 また、デジタル庁が参集を求める場合は、原則は物理的な参集を想定しておりますが、交通途絶等のようなやむを得ない場合においては、Web会議での参集も可能とする予定です。
33	質問	01_調達仕様書_ver1	11	2	3	4	1	「インシデント分析に関する要件」として、「②監視対象装置から送出されるログメッセージを相関分析し少なくとも次の 4 種類の被疑通信を特定できること-(イ)情報漏えいにつながる通信」との記載があるが、内部者が情報漏洩のために外部へ通信しようとしているといった内部情報漏洩は分析対象のインシデントに含まれるか。	作業範囲の確認のため	ご指摘の情報漏えいのケースも含まれます。
34	質問	01_調達仕様書_ver1	11	2	3	4	1	「インシデント分析に関する要件」として、「③ログメッセージ分析による被疑通信特定サービスは 24 時間 365 日提供すること」との記載があるが、分析システムの定期メンテナンス・収容データセンターのメンテナンス等を要因とする、計画された分析遅延（1～数時間程度）は許容されるか。	作業範囲の確認のため	例えば、法定点検の実施のようなやむを得ない状況があれば、事前にデジタル庁と協議の上許容することも可能です。
35	質問	01_調達仕様書_ver1	15	3	2		1	「本調達の作業場所は、提案においてデジタル庁が提供する場所での作業が必須となる場合を除き、受注者において準備すること」との記載があるが、原則として作業は機材設置・設定投入等現地作業を必須とする場合を除き自社にて作業を行う前提でよいか。	作業範囲の確認のため	ご認識のとおり、各受注者様の作業場所（自社等）で作業を行うことを前提としています。
36	質問	01_調達仕様書_ver1	10	2	3	2	1	「以下の監視対象装置に対して、装置やサービスの死活監視を行うこと～それぞれの機器やサービスの詳細については閲覧資料において示す。」とありますが、当該ページの②、③のサービスの詳細についてご教示いただけますでしょうか。	作業範囲の確認のため	仕様書に記載する機種に搭載されている機能及びライセンスから類推していただきますようお願いいたします。 なお、機器やサービスの詳細については機微情報にあたるため、閲覧対象とはしないことといたします。
37	質問	01_調達仕様書_ver1	11	2	5	4	1	「④ 通知に際しては、デジタル庁担当者の要求に応じて、特定した被疑要件の種別や頻度、重要度、通知を行う時間帯による通知ポリシーの設定ができること。また、ポリシーの設定はWeb ポータル等を用いて随時設定変更できること」とありますが、ポリシーの設定をするWebポータルは③にあるデジタル庁専用Webポータルと同じく専用となっていることが求められますでしょうか？	作業範囲の確認のため	デジタル庁専用Webポータルと同じく専用であることを求めます。
38	質問	01_調達仕様書_ver1	9	2	3	（1） ⑧	1	「デジタル庁の担当者の～フォレンジックを提供すること。」とありますが、調査対象はMicrosoft Defender for Endpointがインストールされている端末又はサーバである認識で良いでしょうか。	調査対象を把握したいためです。	ご認識のとおりです。
39	質問	01_調達仕様書_ver1	9	2	3	（1） ⑧	1	「デジタル庁の担当者の～フォレンジックを提供すること。」とありますが、Microsoft Defender for Endpointを利用しての調査である認識でよろしいでしょうか。	調査対象を把握したいためです。	デジタル庁で導入済みのMicrosoft Defender for Endpointを利用することが前提と想定しております。
40	質問	01_調達仕様書_ver1	6	1	4	-	-	監視対象により、一斉の運用開始ができない場合は段階的な運用開始とすることは可能でしょうか。 例）2023年4月運用開始　PAN-PA-5260、Thunder 3040S 　　2023年8月運用開始　Microsoft 365 E5関連のログ	対象によっては運用準備に時間を要するためです。	段階的な運用開始を妨げるものではないですが、早期の運用開始が望ましいです。
41	質問	令和４年度ガバメントソリューションサービスにおけるセキュリティ脅威の検知・分析・遮断サービスの提供 調達仕様書	6	1	4		1	構築期間と運用開始の想定時期を教えていただけますでしょうか。	サービスご提供の準備期間として、どの程度の時間があるかを踏まえて導入計画を検討したいためです。	構築期間は令和５年３月末まで、本格運用開始は令和５年４月からが望ましいと考えておりますが、対応不可である場合は、段階的な運用開始等も含めて協議させていただければと考えております。

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
42	質問	同上	9	2	3	(1) ②	1	「指定される方法」とは、2.3（5）の要件を指しているという理解でよいでしょうか。	「指定される方法」の要件を明確にさせていただきたいためです。	ご理解のとおりです。 仕様に明記いたします。
43	質問	同上	9	2	3	(1) ④	1	「ブラックリストを監視対象装置①に適用し」の①は②と想定しますが、こちらの理解でよいでしょうか。	ブラックリストの適用対象を明確にさせていただきたいためです。	ご指摘ありがとうございます。 （2）側の記載を修正いたしました。
44	質問	同上	9	2	3	(1) ④	1	「なお、②にも適用できる場合は」の②は③と想定しますが、こちらの理解でよいでしょうか。	ブラックリストの適用対象を明確にさせていただきたいためです。	ご指摘ありがとうございます。 （2）側の記載を修正いたしました。
45	質問	同上	9	2	3	(1) ④	1	この要件の意図としては、独自に作成したブラックリストを用いたインシデント検知であり、ブラックリストの適用方法自体は事業者の提案によるものと理解しますが、その認識でよろしいでしょうか。	ブラックリストの適用方法についての理解を確認したいためです。	ご指摘のとおりです。
46	質問	同上	9	2	3	(1) ⑦	1	ポータルはSaaSと連携してプラットフォームを用意し、コンテンツ部分の運用は弊社で責任を持って行う形を想定しています。 ISMAPに準拠しているSaaSであれば連携利用は可能でしょうか。	ポータルはSaaS連携した形でのご提供を検討しているためです。	利用可能です。 なお、この場合においては加点といたします。
47	質問	同上	10	2	3	(2) ⑤	1	「①から生成されるログ」の①は②という理解で相違ないでしょうか。	どこから生成されるログなのかを明確にしておきたいためです。	ご指摘ありがとうございます。 （2）側の記載を修正いたしました。
48	質問	同上	10	2	3	(2) ⑤	1	「③から生成されるログ」の③は③、④のどちらを指しているでしょうか。	どこから生成されるログなのかを明確にしておきたいためです。	ご指摘ありがとうございます。 （2）側の記載を修正いたしました。
49	質問	01_調達仕様書_ver1.0.pdf	6	1.4	-	-	1	＜仕様書＞ デジタル庁が想定する本調達のスケジュールは、以下のとおり。受注者は、運用計画において、本調達で必要となる作業を整理し、適切な作業スケジュールを提案すること。 ＜質問＞ より高品質な運用をするために運用と並行しアセスメント等を行い、運用計画書の中で、優先的に具備すべき機能を貴庁と議論の上段階的に運用開始するようなご提案は可能でしょうか。	本調達では標準的なSOCサービスに加えて、貴庁にカスタマイズした運用も発生します。そのため、より貴庁にあった運用に向けてアセスメント等をしたうえで運用を高度化することが良いと考えています。	段階的な運用開始を妨げるものではないですが、早期の運用開始が望ましいです。
50	質問	01_調達仕様書_ver1.0.pdf	6	1.4	-	-	1	＜仕様書＞ スケジュール表の項番3「月次報告会議事及び」 ＜質問＞ 及びの後に続く記載について教えていただけないでしょうか。また、月次報告会は運用開始の翌月からの開催の認識で良いでしょうか。	「及び」の後の記載がなかったため。また、スケジュールに2月と3月の間に最初の月次報告会がおかれており、想定されている月次報告会の開始タイミングを確認したいと考えています。	ご意見ありがとうございます。 以下のとおり修正いたします。 「月次報告会議事及び」→「月次報告会」

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
51	質問	01_調達仕様書_ver1.0.pdf	7	1.5	-	-	2	＜仕様書＞ 本調達の方式は総合評価落札方式とし、価格点と技術点の配点割合を１：１とする。なお、提案書提出の要領及び評価基準については「別添資料4.提案書作成要領」、「別添資料5.総合評価基準書」及び「別添資料6.総合評価基準書総合評価基準表」を参照すること。 ＜質問＞ 「別添資料4.提案書作成要領」は同封されてませんでしたが、提案書は縦向き/横向きなどの指定はありますでしょうか。	-	用紙サイズは、日本工業規格（JIS）A 列４番横又は縦置きとするようにお願いいたします。なお、大きな図面等は A 列 3 番横又は縦置きを使用して差し支えございません。
52	質問	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	④	1	＜仕様書＞ 下記（2）で示す機器やサービス以外に、自社にて独自に作成したIP アドレスやURLに関するブラックリストを監視対象装置①に適用し、インシデント検知を行うこと。なお、②にも適用できる場合は加点とする ＜質問＞ 「下記（2）で示す機器やサービス以外に、自社にて独自に作成したIPアドレスやURLに関するブラックリストを監視対象装置②に適用し、インシデント検知を行うこと。なお、③にも適用できる場合は加点とする」の誤記と認識しておりますがよろしいでしょうか。 （参考） ②パロアルトネットワークス社　PAN-PA-5260 ③A10ネットワークス社Thunder 3040S	①は説明文となっているため。	ご記載のとおり、誤りであるため修正いたします。
53	質問	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	⑤	1	＜仕様書＞ チケット作成後のインシデント対応として、デジタル庁担当者からの依頼に基づく追加調査への対応を行うこと ＜質問＞ 追加調査の範囲を教えていただけないでしょうか。	-	対応の範囲は、協議の上決定することとし、仕様書に以下のとおり追記いたします。 「なお、本件追加調査の対応要否はデジタル庁担当者と協議の上決定することとする。」
54	質問	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	⑦	1	＜仕様書＞ 受注社が自社で開発・運用しているサービスであり、受注者がポータルを構成する機器及びソフトウェアの保守を適切に実施し、不具合発生時も受注者で対応するなど、受注者が管理責任を負うこと。 ＜質問＞ 受注者が自社で開発・運用しているサービスの定義は、外部のSaaSサービス（ISMAP取得）などを利用して、構築しているような場合も含まれるとの認識で宜しいでしょうか。	オンプレミスや内製開発でのアプリケーションでのポータルサイト提供となった場合、セキュリティ的なリスクが増加しかつ、対応できる会社が限定されるため。	含まれます（仕様の要件を満たすのであれば、利用可能です。）。
55	質問	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	⑧	1	＜仕様書＞ デジタル庁の担当者の求めに応じ、ダークウェブ等の特殊な環境を用いたアクセスが必要なネットワーク等で公開されている情報について、年２回までの調査を実施し、ガバメントソリューションサービスの影響有無等の結果を報告すること。 ＜質問＞ ダークウェブ検索の要件が記載されておりますが、具体的なサービスイメージや、調査の内容などについてイメージされているものがあれば、ご教示頂けますでしょうか？ TOR等でアクセスできる情報やOSINT等の情報を利用し、合法的に収集できる範囲で、貴庁に影響及ぼすような情報を収集するような認識でよろしいでしょうか。	ダークウェブ等で公開されているガバメントソリューションサービスに影響のある情報の調査及び試算に必要となるため。	御認識のとおりです。
56	質問	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	⑧	1	＜仕様書＞ デジタル庁の担当者の求めに応じ、ダークウェブ等の特殊な環境を用いたアクセスが必要なネットワーク等で公開されている情報について、年２回までの調査を実施し、ガバメントソリューションサービスの影響有無等の結果を報告すること。 ＜質問＞ ダークウェブでの調査は、調査範囲等により費用は変動となるため、事前に必要な情報を頂きたいと考えております。 資料閲覧時に、必要な情報が全て確認できれば、正確な見積もりが可能ですが、確認できない場合は、応札時点では、想定されるお見積り条件をつけてご提案させて頂く形となりますが、それで問題ございませんでしょうか？	ダークウェブ等で公開されているガバメントソリューションサービスに影響のある情報の調査及び試算に必要となるため。	お示しする機器やサービスの詳細については機微情報にあたり、資料閲覧等による開示ができないことから、仕様書に記載の要件を満たす範囲で実施する前提で算定いただければと存じます。

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
57	質問	01_調達仕様書_ver1.0.pdf	9	2.3	(1)	⑧	1	＜仕様書＞ デジタル庁の担当者の求めに応じ、端末、Windows サーバの調査・報告ができる簡易的なフォレンジックを提供すること。 ＜質問＞ フォレンジックを提供する際に受注者が提供する調査ツールをデジタル庁様端末内保存していだく必要がありますが問題ないでしょうか インストールは実施致しません。	デジタル庁様端末内に受注者提供ソフトウェアを保存していただくためセキュリティポリシーなどに抵触しないか事前の確認のため。	感染調査等を目的として一時的にツールを利用することは問題ございません。
58	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 各監視装置については、弊社でログを分析する際には、弊社が指定するフォーマットとさせて頂いてもよろしいでしょうか？ 特に以下の監視対象装置に関して、ログの出力形式等を指定しますがよろしいでしょうか。 ②パロアルトネットワークス社 PAN-PA-5260 2台 ③A10 ネットワークス社Thunder 3040S 2 台	SOCで精度よく分析するために、弊社SOCよりログ出力形式を指定しております。	機器でサポートされている形式であれば、対応可能です。
59	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 特に以下の監視対象装置に関して、ファームウェアバージョンは弊社指定のバージョンをご利用いただくことは可能でしょうか。 ②パロアルトネットワークス社 PAN-PA-5260 2台 ③A10 ネットワークス社Thunder 3040S 2 台	バージョンによってログの出力フォーマットが変わり、弊社SOCでの分析に影響があるため。	原則は現行の運用・保守事業者が指定するファームウェアバージョンをご利用いただきますが、協議の上、要件を満たすものであれば変更できる場合もございます。
60	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 以下の監視対象装置に関して、ご利用中のファームウェアバージョンを教えていただけないでしょうか。 ②パロアルトネットワークス社 PAN-PA-5260 2台 ③A10 ネットワークス社Thunder 3040S 2 台	-	機微情報であるため契約後に情報共有させていただきます。
61	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 以下の監視対象装置に関して、弊社の分析基盤に転送していただくことは可能でしょうか。 ②パロアルトネットワークス社 PAN-PA-5260 2台 ③A10 ネットワークス社Thunder 3040S 2 台	-	可能です。
62	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 以下の監視対象装置に関して、現在SSL復号をしていますでしょうか。 現状復号しておらず、今後する予定の場合は、一旦現状ベースでの積算を行い。変更時に改めて影響を確認して別途貴庁と調整との理解でよろしいでしょうか？ ②パロアルトネットワークス社 PAN-PA-5260 2台 ③A10 ネットワークス社Thunder 3040S 2 台	-	機微情報であるため契約後に情報共有させていただきます。
63	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 以下の監視対象装置に関して、SOC分析のために必要な設定変更等は貴庁にて実施される想定で良いでしょうか。 ②パロアルトネットワークス社 PAN-PA-5260 2台 ③A10 ネットワークス社Thunder 3040S 2 台 ④Microsoft 365 E5 に含まれる下記のサービスに関連するログ	-	ご想定のとおりで問題ございません。

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
64	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 以下の監視対象装置に関して、メーカーサポートまたはサービス終了となった場合は、原則として、SOC分析の対象外とさせていただく想定でよろしいでしょうか。 ②パロアルトネットワークス社 PAN-PA-5260 2台 ③A10 ネットワークス社Thunder 3040S 2 台 ④Microsoft 365 E5 に含まれる下記のサービスに関連するログ	-	ご想定のとおりで問題ございません。
65	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 弊社内の解析基盤でログ解析を行う場合は、送信されるログ量により、コストが変わることとなります。そのため、事前にどの程度のログ量かを確認できる必要がございます。 以下の監視対象装置に関して、公告時には利用者情報を資料閲覧等で確認し、その時点の利用者情報をもとにログ量を試算し、ログ量の見積もり条件をつけたうえで提案する形も良いとの認識でよろしいでしょうか？ ②パロアルトネットワークス社 PAN-PA-5260 2台 ③A10 ネットワークス社Thunder 3040S 2 台	SOCサービスの試算に必要となるため。	現時点ログ料想定は月当たりおよそ26TBと仮定いたします。 その旨仕様書に記載いたします。 なお、お示しする機器やサービスの詳細については機微情報にあたり、資料閲覧等による開示ができないことから、仕様書に記載の要件を満たす範囲で実施する前提で算定及びご提案いただければと存じます。
66	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 以下の監視対象装置に関して、公告時には利用者情報を資料閲覧等で確認することができる想定で良いでしょうか。また、その時点の利用者情報をもとに試算し、ユーザ数の見積もり条件をつけたうえで提案することは可能でしょうか。 ④Microsoft 365 E5 に含まれる下記のサービスに関連するログ	SOCサービスの試算に必要となるため。	以下を仕様書に追記いたします。 「契約期間中において想定される最大デバイス数、ユーザー数は約40,000とする。」 なお、お示しする機器やサービスの詳細については機微情報にあたり、資料閲覧等による開示ができないことから、仕様書に記載の要件を満たす範囲で実施する前提で算定及びご提案いただければと存じます。
67	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	1	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 以下の監視対象装置に関して、海外拠点のログは含まれない理解で良いでしょうか。	海外拠点のログが含まれる場合には各国の法律によってはサービス提供できない場合があるため。	ご理解のとおりです。
68	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	-	2	＜仕様書＞ 監視対象装置等に関する要件 ＜質問＞ 事前に受領した条件をもとに見積条件を作成いたしますが、条件には移行の人数の推移は含まれますでしょうか。また、条件の変更が生じた場合には契約変更等によるご対応は可能でしょうか。	SOCサービスの試算に必要となるため。	含まれます。 なお、契約後の事情の変更において、対象となるユーザー数問わず、条件の変更が必要となる場合、双方の合意に基づき、契約変更により対応する場合がありますが、詳細は協議の上決定いたします。
69	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	②	1	＜仕様書＞ パロアルトネットワークス社 PAN-PA-5260 2台 ＜質問＞ PaloAltoの機器は1筐体で一つの設定で稼働しており、vsysなどはご利用されていないとの認識でよろしいでしょうか？	SOCサービスの試算に必要となるため。	vsysを利用しております。
70	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	②	1	＜仕様書＞ パロアルトネットワークス社 PAN-PA-5260 2台 ＜質問＞ 弊社SOCで分析するために、SOC専用アカウントを作成いただき、APIキーの作成しご提出いただくことは可能でしょうか。 また、WildFireポータルよりWildFireAPIキーを取得しご提出いただくことは可能でしょうか。	SOCサービスの試算に必要となるため。	可能です。

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
71	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	④	1	＜仕様書＞ Microsoft 365 E5 に含まれる下記のサービスに関連するログ ・Microsoft Defender for Endpoint ＜質問＞ 弊社SOCで分析するために、APIを作成いただき、必要なアクセス許可を付与して作成した情報を弊社にご提示いただく必要がありますが可能でしょうか。 また、弊社SOC専用ユーザを作成いただき、要件を満たすグループ、ロールを作成いただく必要がありますが可能でしょうか。	SOCサービスの試算に必要となるため。	可能です。
72	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	⑤	1	＜仕様書＞ ①から生成されるログは全て相関分析に利用すること。③から生成されるログを相関分析の対象とする場合には加点とする ＜質問＞ 「すべてのログを相関分析に利用すること」とありますが、「すべて」の定義は、PAN-PA-5260から発生するログで受託者が脅威検知するのに有益と判断もできるもの全てとの理解でよろしいでしょうか？	要件を明確化しコスト積算の精度を高めるため	ご理解のとおりです。 仕様書を修正いたしました（「すべて」を削除。）。
73	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(2)	⑤	1	【仕様書内に記載の以下の表現】 『①から生成されるログは全て相関分析に利用すること。③から生成されるログを相関分析の対象とする場合には加点とする』 【質問】 モニタリングするログの対象はv6対応が必要となりますでしょうか。	-	必要です。
74	質問	01_調達仕様書_ver1.0.pdf	10	2.3	(3)	①	1	＜仕様書＞ 監視対象装置やサービスから送出されるログメッセージを合計して毎秒 3000 件以上受信できること ＜質問＞ 貴庁のSentinelを使って分析する場合には、本項目は対象外という理解で良いでしょうか。	ログによっては弊社環境に転送せずに、貴庁のSentinelを使った分析を想定しております。	ご理解のとおりです。 ご指摘を踏まえて仕様書を修正いたします。
75	質問	01_調達仕様書_ver1.0.pdf	11	2.3	(3)	⑤	1	＜仕様書＞ 受信したログメッセージは最低3 ヶ月間保存し、デジタル庁専用Web ポータルから閲覧できる、もしくはデジタル庁担当者の要求に応じて開示できること ＜質問＞ 貴庁はMicrosoft Sentinelにすべてのログを転送しているため、ログの確認はMicrosoft Sentinelで可能な想定でおります。そのためSentinelのログを提示することで、本要件は満たすとの理解でよろしいでしょうか。	-	ご理解のとおりです。 ご指摘を踏まえて仕様書を修正いたします。
76	質問	01_調達仕様書_ver1.0.pdf	11	2.3	(4)	①	1	＜仕様書＞ 監視対象装置から送出されるログメッセージを毎秒 100 件以上分析処理できること ＜質問＞ 貴庁のSentinelを使って分析する場合には、本項目は対象外という理解で良いでしょうか。	ログによっては弊社環境に転送せずに、貴庁のSentinelを使った分析を想定しております。	デジタル庁のSentinelを使って分析する場合には不要な記載となるため、当該記載は削除いたします。
77	質問	01_調達仕様書_ver1.0.pdf	11	2.3	(4)	②	1	＜仕様書＞ 監視対象装置から送出されるログメッセージを相関分析し少なくとも次の4種類の被疑通信を特定できること ＜質問＞ 記載されている4種類の分類は、国際標準等で定義されている攻撃とも異なる独自な分類との認識です。 検知した通信が、仕様書で規定された4種類の被疑通信相当の内容のどれにあたるかを貴庁で理解できれば、必ずしもこの分類通りに報告はしなくても問題ないでしょうか？	各事業者では、それぞれで攻撃の分類をしており、同様の攻撃を把握できれば、報告時に必ずしもこの通りに分類することが必須ではないと思われるため。	問題ございません。

項	意見/質問	文　書　名	頁番号	章番号	節番号	小節番号	種 別	意　　見	理　　由	回答
78	質問	01_調達仕様書_ver1.0.pdf	11	2.3	(4)	⑤	1	＜仕様書＞ 監視対象装置もしくは監視対象装置と同様なセキュリティ装置から送出されたログメッセージを分析するSOC 業務を3年以上行っている経験を有すること ＜質問＞ 「同様なセキュリティ装置」とありますが、例えばMicrosoft Defender for Cloud Appsの場合は完全一致ではなく、その特性を鑑み同種と受託者にて判断する経験を3年以上行っていると判断する形でよろしいでしょうか？	-	御認識のとおりです。
79	質問	01_調達仕様書_ver1.0.pdf	12	2.3	(7)	②	1	＜仕様書＞ 受注者が監視している同一機器の監視傾向分析 ＜質問＞ 完全に同一機器ではなく、SOCとしての傾向や全体の傾向と比較してお客様の状況を記載するようなレポートを提出するとの理解でよろしいでしょうか	-	完全に同一機器（型番まで同一）である必要はなく、同一ベンダーが提供する機器に係る監視傾向分析であれば問題ございません。
80	質問	01_調達仕様書_ver1.0.pdf	14	2.4	(4)	②	1	＜仕様書＞ 必要に応じて別の成果物の提出を求める場合があるため、調査結果等は常に管理し、最新状態に保っておくこと。 ＜質問＞ 調査結果等とはWindowsサーバのフォレンジック調査の結果などを想定しておりますが、貴庁が想定されている調査の定義を教えていただけないでしょうか。	-	例えばインシデント（疑義案件含む）の調査結果を想定しています。
81	質問	01_調達仕様書_ver1.0.pdf	16	3.4	(2)	-	1	＜仕様書＞ 受注者は、本業務で知り得た情報を適切に管理するため、情報管理体制として、デジタル庁に対し「別添資料2.情報管理体制」により、「情報取扱者名簿」（氏名、住所、生年月日、所属部署、役職等が記載されたもの）及び「情報セキュリティを確保するための体制を定めた書面（情報管理体制図）」を提出し、担当職員の承認を得ること。なお、情報取扱者名簿には、本業務の遂行のため最低限必要な範囲で情報取扱者を掲載すること。 ＜質問＞ サービス提供する場合の範囲においては、サービスに関わるすべての人員の名簿の提供は現実的ではないため、代表者や主な担当者を提示することとなりますが許容されますでしょうか。	-	本業務で知り得た情報を適切に管理するため、代表者や主な担当者だけではなく、サービスに関わるすべての人員の名簿をご提示願います。
82	質問	01_調達仕様書_ver1.0.pdf	18	3.5	(1)	⑧	1	＜仕様書＞ サプライチェーン・リスクに係る確認のため、本調達において導入する「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成30 年12 月10 日関係省庁申合せ（最終改定令和2 年6 月30 日））別紙2 に掲げる情報システム・機器・役務等に関し、製造業者名、製造業者の法人番号、製品名及び型番等の情報を、「別添資料9.機器等リスト」に記載し、提案書の提出期限の5 開庁日前までに提出すること。提出された機器等リストについて、デジタル庁がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、当該リスクに対応するため、代替品又はリスク低減対策の提出を求めることがあるので留意すること。なお、提出した機器等リストの機器等を提案書の提出までに変更する場合には、事前にデジタル庁に申請し、承認を得ること。 ＜質問＞ 本項目は貴庁のDC等に設置する機器が対象となる理解でよろしいでしょうか。	弊社の内部の基盤環境は、社外秘に関る情報が含まれており、開示するのが困難であるため。	御認識のとおりです。
83	質問	03_調達仕様書_別添資料2_情報	1	1.2	-	-	1	＜仕様書＞ 情報管理規則等を有している場合で上記例を満たす情報については、情報管理規則等の内規の添付で代用可能。 ＜質問＞ 情報管理規則等そのものの提示が難しい場合には、該当箇所の抜粋をまとめてご提示することで代用可能でしょうか。	情報管理規則等に社外秘が含まれるため	代用可能です。 なお、提示に当たっては、全体の提示が困難であることを記載いただき、代用である旨を明示願います。