調達件名：ガバメントソリューションサービスにおけるSOCサービス

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
1	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	17	6	3	（7）	1	「引継ぎ」とは本調達を弊社が受注した場合、本契約期間後（令和９年9月30日以降）を想定し、他社に引継ぐことを想定した必要作業と経費を提案するということでしょうか？	引継ぎに関する提案および費用に関して、どのような想定をすればよいか不明確のためです。	本契約期間後（令和９年9月30日以降）を想定し、他社に引継ぐことを想定した提案を記載してください。
2	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	24	7	1	（3）⑦	1	データの保存はシェアードSOCの特性上ハードウェア資源は共用となります。このため完全消去にエビデンスを出すことはできません。専用に作成したシステムの廃棄時などにHDD消去証明を出すなどは可能ですが、SOCでSIEMやポータルなどに保存したデータに関しては削除操作コマンドによるログ提示などでの対応は可能でしょうか？	シェアードSOCの特性上データの完全消去エビデンスを出すことは現実的ではないためです。	データ消去作業終了後、受注者はデータの消去完了を明記した証明書を提出してください。
3	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	1	④	1	パロアルトネットワークス社 PAN-PA-5450およびA10 ネットワークス社Thunder 3040Sの1日あたりの平均ログ量（1セット分）を教えてください。	分析に必要な所要工数（コスト）を見積もるためです。	ご指摘の点については、本公告の閲覧資料をご確認ください。
4	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	7	2	2	④	1	「調査対象ログの受け取り後、ログフォーマットの確認や成形等準備に十分な期間を設け、ネットワーク構成図等を確認し、その他事象に関連しそうなログも補足で確認する」に関して、本項目のフォレンジック調査は、責庁経由で提供された調査対象ログのみで調査をする予定でしょうか、それとも被疑端末の保全は受託者にて実施することを想定しているでしょうか？	サービスを提供するにあたり要件の意味するところを明らかにしたいためです。	要件定義書2.2④ⅱの（通常の）フォレンジック調査については、被疑端末の保全はデジタル庁にて行う想定です。
5	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	7	2	2	④	1	No.４の質問において、被疑端末の保全を受託者にて実施する場合、被疑端末の受け取りは都内のみを想定しているか、あるいは都内以外も想定している場合、想定している地域を提示して頂きたい。	サービスを提供するにあたり要件の意味するところを明らかにしたいためです。	東京都内及びその近郊を想定しております。
6	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	8	2	3	⑤	1	「デジタル庁から提示するGSSが使用する暗号方式」とは、例えばどの様なもでしょうか。独自の暗号方式なのか、それとも一般に使われている暗号方式なのでしょうか？	サービスを提供するにあたり要件の意味するところを明らかにしたいためです。	一般的に使用されている暗号方式となります。
7	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	8	2	3	⑤	1	「ダークウェブ等の特殊な手法によるアクセスが必要なネットワーク等で公開されているAttackSurface 関連やブランド棄損関連」 で指すAttackSurface関連は以下の2通りの解釈ができるが、どちらを意図しているのでしょうか？ (A)ダークウェブ等においてデジタル庁のAttackSurfaceに関して言及されていないか情報収集を行う (B)GSSにおけるAttackSurfaceをスキャン等して脆弱になっていないのか・意図せず公開されているものは無いかを確認する	サービスを提供するにあたり要件の意味するところを明らかにしたいためです。	（A）を想定しております。
8	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	8	2	3	⑤	1	No.７の質問において（A）となる場合、該当するAttackSurfaceが、ダークウェブ等において言及されていないか情報収集を行うため、貴庁が定義するAttackSurfaceとなる資産が提示されるのか、それとも貴庁と協議のうえ定常的にAttackSurfaceを調査し発見された資産を対象とするのでしょうか？	サービスを提供するにあたり要件の意味するところを明らかにしたいためです。	デジタル庁と協議のうえ、定常的にAttackSurfaceを調査し発見された資産を対象とします。
9	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	8	2	3	①	1	デジタル庁から提示するGSSで導入機器及びソフトウェアの一覧については、そのソフトウェアを使用している資産情報（重要度、利用目的、場所、責任者など）、またソフトウェアのバージョン情報も含まれているものという理解でよいでしょうか？	資産情報や、利用しているソフトウェアのバージョンの記載が無い場合、対象ソフトウェアに関連するどの脆弱性情報の影響を受けるのか、また資産の情報が無い場合、優先度などがそれぞれ特定できず、正しい危険性の判断ができないためです。	導入機器及びソフトウェアの一覧については、脆弱性情報等の収集の際に、ソフトウェアの最新のバージョン情報を含む、受注者とも調整のうえ、必要となる情報を提示いたします。
10	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	8	2	3	①	1	デジタル庁から提示するGSSで導入機器及びソフトウェアの一覧については、どの程度の頻度で更新された情報が手に入るのでしょうか？	更新されていないソフトウェア一覧で脆弱性管理を行うと、運用の負荷が高くなるためです。	導入機器及びソフトウェアの一覧については、最新の情報を適切なタイミングで提供いたします。
11	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	3	②	1	「インシデント疑いの種別や頻度、重要度、通知を行う時間帯による通知ポリシーの設定」とありますが、「頻度」とは何を指すのでしょうか？	想定されているサービスレベルを把握するためです。	同一種類のインシデント疑いが一定期間内に発生する回数を指しております。
12	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	3	②	1	「インシデント疑いの種別や頻度、重要度、通知を行う時間帯による通知ポリシーの設定」とあるが、どの程度の粒度での設定となるのか例を教えて頂けますでしょうか？	想定されているサービスレベルを把握するためです。	ご指摘の点については、本公告の閲覧資料をご確認ください。
13	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	3	③	1	通知手段としては電子メール、電話、Microsoft Teams いずれかが利用できればよいでしょうか？	３つの通知手段すべてを使って連絡する必要があるかどうかの確認です。なお一般的なMSS監視サービスにおいてはポータル利用も想定されます。	通知手段として電子メール、電話および Microsoft Teamsすべてを利用できることを求めます。そのうえで実際の通知手段をデジタル庁と協議のうえ、決定します。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
14	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2	④	1	簡易フォレンジック調査を行うためのEDR製品は、1.1④ⅲにある、Microsoft Defender for Endpointでよろしいでしょうか？	サービス内容を明確にするために取り扱う製品を把握する必要があることからの質問になります。	Microsoft Defender for Endpointの想定となります。
15	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2	④	1	簡易フォレンジックの対象製品にも、iPhone、iPad、Adndoid スマートフォンは含まれますでしょうか？	サービス内容を明確にするために取り扱う製品を把握する必要があることからの質問になります。	簡易フォレンジックの対象製品に含まれます。
16	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	2	1	（2）①	1	″ii. GSS 利用者からの連絡や GSS 班の監視に基づき、当庁から調査依頼を行ったもの″につきまして、調査依頼は、GSS利用者から直接調査依頼を受けることはなく、GSS班からのみの調査依頼をいただく理解でよろしいでしょうか。	作業スコープを明確にするため	デジタル庁からの調査依頼は、デジタル庁のGSS担当者をとおした依頼を想定しております。
17	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	18	6	4	（1）①②	1	”①受注者は、本調達において構築するネットワークやシステム等について、 MSS 監視サービスを提供するための監視対応及び障害対応を保証するため、保守業務を実施すること。 ②受注者は、納入したハードウェア・ソフトウェアについて責任を持って保守を行うこと。” とのことですが、保守業務とはどのような業務を想定されておりますでしょうか。想定の業務内容についてご教示願います。（例：メーカー保守と連携した対応等）	作業範囲を明確にするため	保守業務の業務内容は、構築するネットワークやシステムによります。MSS監視サービスを提供するための監視対応及び障害対応を保証できるような保守業務を行っていただきます。
18	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	18	6	4	（1）⑦	1	”⑦受注者は、当庁の求めに応じて、技術的なサポートを行うこと。” とのことですが、技術サポートとはどのような業務を想定されておりますでしょうか。想定の業務内容についてご教示願います。（例：メーカーへの問合せ対応等）	作業スコープを確認するため	本調達において構築するネットワークやシステムに応じた技術的なサポートとなります。
19	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	18	6	4	（1）⑦	1	″⑦受注者は、当庁の求めに応じて、技術的なサポートを行うこと。″につきまして、既設SIEMの利用を前提としておりますが、技術的サポートの業務範囲に既設SIEMのサポートは含まれていない認識でよろしいでしょうか。	作業スコープを明確にするため	本調達において構築するネットワークやシステム等に含まれなければ、保守に係る技術的なサポートに含まれません。
20	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	26	7	3	（2）	1	貴庁に常駐する要員が業務で使用する作業端末の貸与はございますでしょうか。	事業者側の準備物を明確にするため	デジタル庁に指定する場所に常駐する技術者２名については、デジタル庁より作業端末を貸与する想定です。
21	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	1	2	1	″④で示す監視対象機器に対する死活監視を行い″につきまして、「令和 4 年度ガバメントソリューションサービスの運用・保守一式」にて実施している認識で合っておりますでしょうか。 当該業務にて対象機器の死活監視を行っている場合、指定の監視方法や死活監視要件（24/365監視、SLAなど）について、ご教示願います。また、本調達においても死活監視を行う目的についても併せてご教示願います。	作業スコープを明確にするため	セキュリティ関連機器の死活監視は、ログの記録に異常が発生した場合に、それが危機に依存するものかを迅速に判断していただくことを目的としております。
22	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	1	4	1	監視対象となる機器に含まれている「A10 ネットワークス社 Thunder 3040S」につきまして、ロードバランサー機能以外に現在利用されている機能（ファイアウォール・負荷分散・SSL復号・サイト間VPN等）がある場合は、ご教示願います。	システム構成の検討・確認のため	NAT、プロキシ機能のみ利用しており、SSL復号化は利用していない想定です。
23	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	1	4	1	監視対象となる機器やサービスのうち、iii. Microsoft M365 E5 に含まれる下記のセキュリティサービスにつきまして、「等」含まれる想定の監視対象製品をご教示願います。また、監視対象製品が追加となった場合、本調達の範囲内で監視対応を行うこととなりますでしょうか。 ”’ iii. Microsoft M365 E5 に含まれる下記のセキュリティサービス ・ Microsoft Defender for Endpoint ・ Microsoft Entra ID Protection ・ Microsoft Defender for Cloud Apps ・ Microsoft Defender for Office 365 ・ Microsoft Data Loss Prevention 等　”	監視費用の積算に影響するため	ご指摘を踏まえ、下記の記載に修正します。 「iii. Microsoft M365 E5 に含まれる下記のセキュリティサービス ・ Microsoft Defender for Endpoint ・ Microsoft Entra ID Protection ・ Microsoft Defender for Cloud Apps ・ Microsoft Defender for Office 365 ・ Microsoft Data Loss Prevention」
24	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	1	4	1	監視対象となるサービスに含まれている「Microsoft Data Loss Prevention」につきまして、ポリシーに反した不審な動きがあった際のアカウントロックを行う以外に、一次対応の業務内容について貴庁想定がございましらご教示願います。	遮断の要件を明確にするため	適宜、過検知等の対策などについて相談させていただく可能性があります。
25	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	2	5	1	日本国以外において本調達と同様のインシデント疑い調査および分析サービスを提供している場合にはその事例について紹介することとし、その紹介内容について加点対象とする、とありますが、これは下記１．２．のどちらが、もしくはどちらも加点対象となりますでしょうか。 1，サービス提供者が日本国以外の拠点を持ちサービスを提供している実績があるか 2，日本国以外の顧客を対象としたサービスを提供している実績があるか	評価基準確認のため	１及び２いずれも加点対象となります。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
26	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	3	2	1	″デジタル庁担当者の要求に応じて、特定したインシデント疑いの種別や頻度、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とし、ポリシーの設定は随時設定変更できること″につきまして、「ポリシーの設定」とは具体的にどのようなことを指しておりますでしょうか。また、設定変更の必要性についても併せてご教示願います。	MSS監視サービスの要件を明確にするため	ポリシーの設定とは、特定したインシデント疑いの種別や頻度、重要度、通知を行う時間帯によりMSS監視サービスの通知の方法や通知の内容のルールの設定です。インシデントの内容により、通知の方法や通知の内容を変えることができることを想定しています。
27	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	3	2	1	″デジタル庁担当者の要求に応じて、特定したインシデント疑いの種別や頻度、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とし、ポリシーの設定は随時設定変更できること″につきまして、既設SIEMの利用を前提としておりますが、設定変更ができるアカウントを付与いただき本調達の受託事業者にて実施する想定でしょうか。もしくは、既存の運用保守事業者様に依頼して実施されるか、どちらを想定されておりますでしょうか。	作業スコープを明確にするため	GSSにエスカレーションを行っていただく条件のポリシー設定を意図しており、インシデント判定自体のポリシー設定はGSSと協議の上行うことを想定しています。
28	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	4	3	1	Microsoft Defenderポータルへのアクセスを許可いただける事を前提としておりますが、そのうえでの接続要件はございますでしょうか。	接続要件確認のため	デジタル庁が貸与する端末を用いて接続することを要件と考えています。
29	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	1		1	体制に関する要件についてです。 ″専門の技術者２名″につきまして、現在も２名体制で実施されておりますでしょうか。 また、セキュリティに関する高度な知識を有する専門の技術者2名が貴庁の指定する場所に常駐することとなっておりますが、デバイス数とユーザー数がそれぞれ最終的に196,000迄拡大する中で、本調達とは別に常駐要員の増員は想定されておりますでしょうか。	要件の実現に向けた体制検討のため	現時点で本調達以外の今後の調達方針についてはお答えできません。 要件定義書1.1内の契約期間中のデバイス数とユーザー数を踏まえつつ、契約期間すべてにおいて本調達にかかる業務を実施できるよう提案してください。
30	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	1		1	″夜間休日は、インシデント発生の緊急対応などを行うために、デジタル庁からの問い合わせを行う窓口を用意すること。″となっておりますが、「インシデント発生の緊急対応」について具体的な作業内容をご教示願います。	作業スコープを明確にするため	夜間休日の対応は、インシデント発生時にデジタル庁から問い合わせを受け、日中業務日でのインシデント及びインシデント疑いに対するセキュリティ対策支援での実施では遅い対応など重要度を踏まえた対応をしていただく提案を想定しております。
31	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2		1	インシデント及びインシデント疑いに対するセキュリティ対策に関する要件において、①～⑦の調査フローを構築しますが、各段階について対応時間の定めはございますでしょうか。	作業スコープを明確にするため	インシデントの事案に応じて、求められる対応時間が変わってくる認識ですので、明確な対応時間の設定は儲けませんが、適切な対応時間で業務を実施できる体制を構築していただきますようお願いいたします。
32	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2	1	1	″①詳細な分析″につきまして、どの様な対応を想定されているか具体的な業務内容をご教示願います。「①詳細な分析」の段階では、インシデントの発生有無を切り分けるため、職員様へのヒアリングや端末等の調査も含まれると想定しております。	詳細な分析の要件を明確にするため	インシデントの発生の有無を判断するためにどのような「詳細な分析」を行うのかについての具体的な業務内容は、インシデント発生時の調査フローと併せて提案していただきます。
33	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2	3	1	″③被害の拡大の防止″につきまして、「当該機器について、デジタル庁からその検体の提供を受け、隔離保存を速やかに行い、デジタル庁の担当者に報告すること」となっておりますが、機器の検体を受け取り隔離保存を行い報告する作業は、被害の拡大の防止より、証拠保全を目的とした作業と考えております。項目名と作業の目的と合致していないと感じましたが、認識合っておりますでしょうか。	作業スコープを明確にするため	機器の検体を受け取り隔離保存することは、証拠保全とともに被害の拡大の防止にも含まれるため記載しております。 なお、2.2に記載の要件に基づきつつも、インシデント発生時の調査フローを提案していただくこととなります。
34	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2	4	1	④原因究明につきまして、原因究明のために、簡易フォレンジック、通常フォレンジックのほかに、検体解析も含まれると考えております。その際、別途ツールを用いた解析は想定されておりますでしょうか。	費用の積算に影響するため	検体解析も本調達の要件に含まれる認識ですが、使用するツールや解析方法はご提案によります。
35	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	8	2	3	1	1	″GSS で導入機器及びソフトウェアに関する脆弱性の情報等を収集し″ につきまして、利用する脆弱性診断ツールに指定がある場合は指定のツールをご教示願います。	構成確認のため	現時点で指定のツールの想定はありませんが、受注者はGSSの環境や構成を理解し、充分な脆弱性情報等の収集をしてください。
36	質問						2	貴庁環境の既設SIEMをリモート監視するにあたり、Microsoft社推奨のAzure LightHouseによる権限移譲を行うことは可能でしょうか。	最適な監視体制構築のため	検討の結果、不可とします。
37	質問	02_別添資料１．要件定義書		1	1.1	④	1	契約期間中に新たなログソースが追加となった場合、ログを取り込みための作業費（ログ要件の定義や取り込み自体の作業工数）を提案の中に見込む必要がありますでしょうか。	ログソースの追加予定や費用について明確化するため。	要件定義書内の契約期間中のデバイス数とユーザー数の見込み数の記載等の情報を用いて、契約期間内にセキュリティ監視の要件を満たすように、ご提案してください。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
38	質問	02_別添資料１．要件定義書		1	1.3	③	1	通知手段としては口頭では電話、テキストでは電子メールもしくはMicrosoft Teamsを利用するとの理解でよろしいでしょうか。	通知手段について明確化したいため。	通知手段として電子メールはテキスト、電話は口頭での利用となります。 Microsoft Teamsはテキスト、口頭での利用となります。
39	質問	02_別添資料１．要件定義書		2	2.1	①	1	貴庁への2名の常駐者は固定の人員である必要はありますでしょうか。例えば、専任のチームを組んで曜日によって常駐する人員をアサインする等の対応が可能であるか確認させてください。	2名に固定してしまうと突発的な休み等に対応ができなくなってしまうため。	技術者２名が常駐することを要件として求めますが、具体的な体制については提案によります。
40	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	1	1	2		1	緊急遮断対応は可能ですが、次のシグネチャの更新やファームウェアのバージョンアップ、パッチ当ても作業は含まれないと想定しております。 認識に祖語はないでしょうか？もし、含まれる場合、導入ベンダーとの保守契約などにより、当社のマネージドサービスと導入ベンダーとの責任分界点の整理が必要となります。	責任範囲の明確化のためにご教示ください。	シグネチャの更新やファームウェアのバージョンアップ、パッチ当ての作業については、要件に含むことを想定しておりません。
41	質問	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	18	6	4	（1）①	1	1. ロードバランサーが必要であるため以下の情報開示をお願いします。 ・Paloalto及びA10のログ量の情報提示 2. オンプレデバイス（FWやA10等）のログ収集に際して、ログ収集装置（仮想インフラ上のApplication）の設置が必要なため、以下の可否を提供ください。 ・デジタル庁が所有する仮想環境利用の有無	当社SOCサービスを提供するためのログ収集装置のサイジングに際して、ログ量の情報とログ収集装置の設置場所の有無についてご教示ください。	１．ご指摘については、本公告の閲覧資料をご確認ください。 ２．オンプレ利用を希望する場合は、デジタル庁と協議することになります。
42	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	2	④	1	インシデント疑いであると考えられる事象の調査と分析による最終的な結果は、デジタル庁が指定した方法で報告すること。 → SOCからの通知を受けて、常駐者が貴庁の指定のフォーマットで報告する対応という解釈で良いでしょうか？	貴庁の指定する方法の具体的な記載をお願いします。	常駐者がデジタル庁指定のフォーマットで報告する方法も想定しますが、具体的な報告の仕方については、業者からの提案も踏まえて、デジタル庁側で指定します。
43	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	3	①	1	インシデントの発生またはインシデント疑いを特定した場合、特定後 1 時間以内にインシデントの重要度判定を行い、デジタル庁が指定する担当者と方法にて連絡すること。 → 弊社サービスでは、SIEM基盤で生成された高レベルアラートをもとに、SOCアナリストが調査を開始してから、インシデント判定を含めた調査結果を報告するまで、1時間のSLAを設けておりますが、この条件での提供で合致しますでしょうか。	認識合わせのためにご教示ください。	御社のサービスによるインシデント判定が要件定義書で定める重要度判定の要件に合致するのか判断できないなど質問内容からは御社のサービスが明確でないため、合致するかどうか判断致しかねます。
44	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	3	②	1	重要度に応じた通知とは以下のどちらの認識となりますでしょうか？ A）SOCサービスを提供する業者→GSS運用・保守業者 B）GSS運用・保守業者→貴庁が定めたご担当者	通知プロセスやフローの明確化のためにご教示ください。	「重要度に応じた通知」とは、1.3通知に関する要件で定めるアラートとして本事業者からデジタル庁に通知されるものです。
45	質問	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2	④	1	i. 簡易フォレンジック調査（年 10 回程度の調査依頼を想定） ii.（通常の）フォレンジック調査（年１回程度の調査依頼を想定） → 記載のフォレンジック調査の回数を超過した場合、別途費用請求を行うことは可能でしょうか。	回数の予測が難しい為ためご教示ください。	仕様書に記載の回数を超過した場合は、事業者とデジタル庁で協議します。
46	質問	調達仕様書	14	6	2	（18）	1	「本仕様書において共用機器については、当庁担当者にて指定する場所に設置すること。また、新たな拠点の追加又は拠点の削減による設置機器の移動についても対応できること。なお、設置機器の移動に係る費用は、本調達に含まない。」とありますが、これは設置機器の移動に係る費用は本調達に含める必要はなく、発生した場合には別途調達を行うという意味でしょうか。また、「共用機器」に関する用語の定義がなく定義をお示しください。	調達に含める費用ではないことは分かりますが、発生したときの費用の扱いが不明瞭のため。	ご指摘の事象が生じた場合においては、生じた内容に応じて、デジタル庁と協議することとなります。 なお、共用機器とは、ご提案する内容によります。
47	質問	調達仕様書	2	1	6		1	「作業スケジュール：当庁が想定する本業務及び関連する業務の作業スケジュールは、図２のとおりである。」に関して、MSS監視サービスは2024年12月に開始し、12月は「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」を行う事業者と並行運用を実施の上で、2025年1月からは本件調達側のMSS監視サービスのみに切り替えるとの理解で良いでしょうか？	作業スケジュールを明確とするため。	デジタル庁側で想定するスケジュールは令和６年12月にMSS監視サービスを開始し、「令和6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」（令和６年12月末で契約終了）における監視との並走期間（引継ぎ期間）を経て、本調達における監視のみとなる想定です。
48	質問	調達仕様書	4	2	1	⑵②	1	「通常業務におけるセキュリティ対策支援：GSS で導入機器及びソフトウェアに関する脆弱性の情報等を収集し、危険性の判断、対策計画の策定・提案、対策の実施の支援等を行うこと。そのほ、当庁等が実施するセキュリティ監査等への対応支援等の前記に付帯する業務を行うこと。」に関して、ソフトウェアに関する脆弱性の情報等は本件提案者が準備するものとの理解で良いでしょうか？また、対象となるソフトウェア情報は貴庁から提供されるとの理解で良いでしょうか？	必要なツールの明確化と費用積算のため。	デジタル庁からGSSで導入機器及びソフトウェアの一覧を提示しますので、受注者がその知見や情報収集能力を活かして、脆弱性情報を随時収集していただきます。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
49	質問	調達仕様書	2	1	4		1	「当庁の指示の下、SOC サービスを提供する事業者とGSS 運用・保守業者は連携し、セキュリティ監視、インシデント対応や脆弱性発見時の対応等、セキュリティ関連の運用業務を行う。それぞれの役割は以下のとおりである。」 とありますが、7頁 「4.2 本調達案件と関連する調達案件」には令和６年度における「ガバメントソリューションサービスの運用・保守一式」の調達が記載ありません。これは、「令和3年度ガバメントソリューションサービスの運用・保守一式」が現在も随意契約等で継続しているもので、本件調達は当該事業者との連携することを求めるとの理解で良いでしょうか？	調達の背景・目的を正しく理解するため。	「仕様書別添資料３用語の定義」において、「GSS運用・保守業者」を「GSSの運用・保守を行う事業者。令和６年５月現在においては、「令和４年度ガバメントソリューションサービスの運用・保守一式」における事業者を指す。」としています。
50	質問	調達仕様書 別添資料１　要件定	6	2	2	④Ⅱ	1	（通常の）フォレンジック調査対象が「端末やサーバの HDD」と記載されていることから、Windows端末/サーバ、Linuxサーバが対象との理解で良いでしょうか？	調達の背景・目的を正しく理解するため。	Windows端末/サーバ、Linuxサーバが対象の想定です。
51	質問	調達仕様書 別添資料１　要件定	6	2	2	④Ⅱ	1	（通常の）フォレンジック調査を行う場所は貴庁が指定する場所で作業を行う理解でよろしいでしょうか。または調査対象となるHDDのコピ（保全）した情報を弊社環境にて調査することで良いでしょうか？ なお、フォレンジック調査自体を貴庁指定場所で実施することが必須の場合、調査に必要な機材は入札者が用意し、かつ当該場所に持ち込める理解でよろしいでしょうか。	調達の背景・目的を正しく理解するため。	デジタル庁と調整のうえ、デジタル庁が指定する場所あるいは受注者で用意する環境で実施していただくことを想定しています。 また、デジタル庁が指定する場所で実施する場合は、調査に必要な機材は受注者が用意し、デジタル庁と調整のうえ、当該場所に持ち込んでいただくことを考えています。
52	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	12	6	1	（3） （4）	4	プロジェクト実施計画書の記載対象はSOCサービスのためのシステム構築までという認識でよろしいでしょうか。 現在の記載だと、システム構築後のSOCサービス運用時も対象に含まれているように読み取れてしまうため、記載修正が必要と考えます。	SOCサービスに係る計画書については、プロジェクト計画書とは別に6.5(1)に記載の運用計画にて提示するものと考えます。	運用開始後にプロジェクト実施計画書で記載する必要があるネットワークやシステムの構築がなければ、運用計画書で記載する内容に含まれると整理してご提案いただいて構いません。
53	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	12	6	2	-	4	WBSでの予実管理の対象はSOCサービスのためのシステム構築までという認識でよろしいでしょうか。 現在の記載だと、システム構築後のSOCサービス運用時においてもWBSでの予実管理が必要なように読み取れてしまうため、記載修正が必要と考えます。	WBSでの予実管理は構築PJ等のタスクが決まっているPJで活用するものであり、運用業務においては不適であると考えます。	運用開始後にWBSで管理する必要があるネットワークやシステムの構築がなければ、運用開始後にかかるWBSの作成が不要であるとご提案していただいて構いません。
54	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	20	6	5	（3）① i	2	「検知内容については、詳細状況を記載し、不審な点がないかどうかの確認結果とその根拠も記載すること」の記載について、必要に応じて運用業者やエンドユーザへの直接確認を行う必要があると考えるため、その旨の追加が必要と考えます。 （修正イメージ） 「検知内容については、詳細状況を記載し、不審な点がないかどうかの確認結果とその根拠も記載すること。なお必要に応じて運用業者やエンドユーザへの直接確認を行うこと。」	本要件に限らず、必要に応じて運用業者やエンドユーザへの直接確認が必要であると考えます。この点が明確化されていない場合、ヒアリング対応しないで根拠（結論）を出すことは難しいと考えるため、デジタル庁様が対応することとなり得ます。	ご指摘をふまえ、下記のとおり追記いたします。 「なお、必要に応じて、デジタル庁に確認のもと、GSS運用・保守事業者や職員にヒアリングを行うこと。」
55	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	1	-	1	「24時間365日提供する体制」であり、「夜間休日は、インシデント発生の緊急対応などを行うために、デジタル庁からの問い合わせを行う窓口を用意」となっていることから、インシデント対応においては夜間休日も日中とほぼ同様なサービスを提供することが想定されているものと思われます。しかし、この夜間休日の対応において実施可能なサービスについては、例えば、MSS監視サービスによって通知されるインシデントへの対応のみを対象とする、対応は端末の隔離に限定する等、標準的な監視やインシデント対応の範囲に限定することが適当と考えます。	「総合的なセキュリティ対策支援サービス」を遂行する要員は、一般的なセキュリティ技術に加えて、監視対象システムの設定や運用についての十分な知識も必要です。このような要員を多数そろえて、特別、あるいは詳細な調査等を常時可能にすることは、非常にコストが高いものとなります。詳細な調査は若干遅れて日中の実施となっても、端末の隔離等の防御等が実施できれば被害を食い止めることができると思われるため、意見に記載のような範囲の対応であっても十分に安全性は確保できるものと考えます。	要件定義書2.1に記載のとおり、日中業務日はデジタル庁に指定する場所に常駐する技術者２名が本サービス（「インシデント及びインシデント疑いに対するセキュリティ対策支援」及び「通常業務におけるセキュリティ対策支援」）の提供を行うことを求めています。夜間休日は、窓口をとおしてデジタル庁からの問い合わせに応えてもらうことを求めています。 なお、夜間休日の対応は、インシデント発生時にデジタル庁から問い合わせを受け、日中業務日でのインシデント及びインシデント疑いに対するセキュリティ対策支援での実施では遅い対応など重要度を踏まえた対応をしていただく提案を想定しております。
56	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2	⑤⑥	1	再発防止等の策定について、「総合的なセキュリティ対策支援サービス」の作業範囲としては、一般的な対策案の提示と、GSS運用・保守事業者との連携や支援とするのが適切と思われます。すなわち、最終的な再発防止策の策定については、デジタル庁、GSS運用・保守事業者が主管となることが適当と考えます。	再発防止策の内容によっては、システム運用やユーザ利用へ影響する場合が考えられますが、その影響範囲や変更が許容されることの可否判断等は、システムの運用や設定を細かいところまで熟知している必要があり、「総合的なセキュリティ対策支援サービス」において、実施することは、一般的には困難と思われます。すなわち、再発防止策を決定するまでのプロセスにおいては、全関係者が協力をしながら作り上げるものですが、ただし、変化の影響を最も被る運用・保守事業者の判断が非常に重要であることから、その部署が主管となることが最も適切と考えます。	再発防止等の策定の要件は、再発防止策を策定してデジタル庁に提案することです。再発防止策についてはデジタル庁に説明と確認を行うことを求めており、再発防止策の実施の判断はデジタル庁で行います。 ご指摘を踏まえて、要件定義書2.2⑥の記載を明確化しました。 「⑥ 再発防止策の提案等」
57	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	7	2	2	①	2	デジタル庁様からの調査依頼の内容を明確化して頂けますでしょうか。 具体的には、「ユーザーや各省庁の情報システムから感染被疑の端末調査や不審メールの検体調査」、「NISC等外部機関からの情報に基づいてGSS環境が影響を受けていないかの調査」を明確に記載すべきと考えます。	見積の工数積算に影響がでるため。	ご指摘をふまえ、調達仕様書2.1（２）① ii に下記のとおり追記します。 「※当庁から調査依頼を行うものとして、感染被疑の端末調査、不審メールの検体調査や外部機関からの情報に基づいてGSS環境が影響を受けていないかの調査などを想定している。」

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
58	意見	その他	-	-	-	-	2	ファイルやメール等のサービスや、NWセンサー機器の過検知等によりブロックされた場合、ユーザー要望や必要に応じて、ブロックされないようにする対応が必要だと考えます。要件として具体的に明確化できますでしょうか。	現在のSOC運用において必要な作業であることと、見積の工数積算に影響がでるため、明確化して頂きたいと考えるため。	ご指摘のようなケースについては、本調達の要件には含みません。
59	意見	その他	-	-	-	-	2	朝会等必要会議への出席が明記されていないため、明記をお願いできますでしょうか。 具体的には、「朝会等必要な会議体に出席して、状況を報告すること。」のような記載追加をお願いいたします。	見積の工数積算に影響がでるため、明確化して頂きたいと考えるため。	必要な会議体への出席や会議での発言は、デジタル庁やGSSに関連する事業者との連携に含まれる認識です。 ご指摘を踏まえ、調達仕様書2.1（２）を明確化いたします。 「また、職員へのヒアリングの実施、GSSに関連する事業者との連携の他、必要な会議体への出席や発言を行う必要があるため、セキュリティに関する高度な知識を有する専門の技術者が当庁の指定する場所に常駐して下記の業務を行うことを求める。」
60	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	2	1	（2）	4	総合的なセキュリティ対策支援サービスの要件は、「令和4年度ガバメントソリューションサービスの運用・保守一式」に含まれる4.5セキュリティ運用支援業務とサービス内容が重複していると思われます。 「令和4年度ガバメントソリューションサービスの運用・保守一式」は2025年9月まで契約期間であるため、本項目の開始は2025年10月になると考えます。	「令和4年度ガバメントソリューションサービスの運用・保守一式」で2025年9月まで提供するセキュリティ運用支援業務と重複する内容となるためです。	本件仕様書における総合的なセキュリティ対策支援サービスの実施開始時期は、調達仕様書へ記載のとおり令和７年１月です。
61	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	25	7	1	（4）③	1	冒頭を以下の表現に変更をお願いします。 変更前 運用メンバ（MSS 監視サービス担当者）は、以下の要件を全て満たすこと。 変更後 運用メンバ（MSS 監視サービス担当者）は、以下の要件を全て満たす要員が常に運用メンバに含まれている事。	一般的なMSS監視サービスでは多数のユーザーのアラートをそれらを特に区別していません。また。アラートの分析難易度に応じて担当を分けることで多くのアラートを処理することを可能にしています。難易度の高いアラート調査はエキスパートが担当しておりかつ複数名でのチェック機能も設けているため、危険度の判断に誤りが発生する事がないことから意見のような記載としたいです。	ご指摘を踏まえ、下記のとおり記載を見直します。 「運用メンバ（MSS 監視サービス担当者）は、以下の要件を全て満たす要員が常に運用メンバに含まれていること。」
62	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	29	7	6	（2）①	1	以下の文章に変更をお願いします。 変更前 ①受注者は、当庁等が実施するセキュリティ監査、セキュリティ診断等を受けること。 変更後 ①受注者は、担当職員と協議の上当庁等が実施するセキュリティ監査、セキュリティ診断等を受けること。	一般的なMSS監視サービスを提供している場合、他のお客様に影響のあるような監査（情報の閲覧など）は受け入れられないケースもあるためです。	受注者は、当庁等が実施するセキュリティ監査、セキュリティ診断等を受けるなど対応していただきます。やむを得ない事情がある場合には、受注者とデジタル庁で協議します。
63	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	31	7	8	（5）②	1	「受注者は」以降を以下の文章に変更をお願いします。 変更前 ②契約履行過程で生じた納入成果物（契約履行に当たり作成・変更・修正した文書等を含む。）に関し、著作権法第27 条及び28 条に定める権利を含む全ての著作権及びノウハウ（営業秘密）は当庁に譲渡し、当庁が独占的に使用するものとする。受注者は、契約履行過程で生じた著作権及びノウハウ（営業秘密）を自ら使用又は第三者をして使用させる場合は、当庁と別に定める使用契約を締結するものとする。 なお、受注者は当庁に対し、一切の著作者人格権を行使しないこととし、また、第三者をして行使させないものとする。 変更後 ②受注者は、契約履行過程でデジタル庁固有の業務において発生した著作権及びノウハウ（営業秘密）を自ら使用又は第三者をして使用させる場合は、当庁と別に定める使用契約を締結するものとする。 なお、受注者は当庁に対し、一切の著作者人格権を行使しないこととし、また、第三者をして行使させないものとする。なお、契約締結前から受注者が保有している著作権、ノウハウ及び受託者が当庁限定ではなく他の契約者にも適用するために作成した著作物（IP アドレスブラックリストやURL ブラックリスト、シグネチャ等）は本対象に含めない。	MSS監視サービスにおいては、ノウハウを共通で利用するケースがございます。また契約履行前より受注者にて保持していた著作権は、そのままとすべきと考えます。（令和4年度調達仕様と同様の内容に変更頂きたい）	ご指摘を踏まえ、下記の記載に修正いたします。 「②契約履行過程で生じた納入成果物（契約履行に当たり作成・変更・修正した文書等を含む。）に関し、著作権法第27 条及び28 条に定める権利を含む全ての著作権及びノウハウ（営業秘密）は当庁に譲渡し、当庁が独占的に使用するものとする。受注者は、契約履行過程で生じた著作権及びノウハウ（営業秘密）を自ら使用又は第三者をして使用させる場合は、当庁と別に定める使用契約を締結するものとする。 また、受注者は当庁に対し、一切の著作者人格権を行使しないこととし、また、第三者をして行使させないものとする。なお、契約締結前から受注者が保有している著作権、ノウハウ及び受託者が当庁限定ではなく他の契約者にも適用するために作成した著作物（IPアドレスブラックリストやURLブラックリスト、シグネチャ等）は本対象に含めない。」
64	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	1	③	1	右記理由により以下の文章の追加をお願いします。 追加後 ③ ④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④ⅰに適用し、インシデント検知を行うこと。**または装置に直接登録しない場合でも既設SIEM等でのブラックリストを適用する事で同様のインシデント検知をできれば、それも可とする。**なお、④ⅱにも適用できる場合は加点対象とする。	装置に直接登録しなくても既設SIEM等にブラックリスト照合を可能とすることで、ログをもとに機器にブラックリスト適用する場合と同様の要件が実現可能です。また当該機器のログ以外へのブラックリスト活用など、効率的なサービス提供が可能となるためです。	検討の結果、仕様書への追記はしません。
65	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	2	①	2	インシデント疑いの調査や、インシデント発生時の対処を迅速化するような仕組み（例えばSOAR採用による自動化・高速化）が必須要件または提案が必要と考えます。	ランサムウェアなど一瞬で大きな被害をもたらすような事案が多発しており、インシデント発生時の対処には迅速な対応が求められると考えられます。	インシデント発生時の対処を迅速化するような仕組みを含め、事業者からの提案していただくこととします。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
66	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	2	②	2	以下の文章に変更をお願いします。 変更前 ② 1.1④の機器やサービスから生成されるログはデジタル庁GSS 班の既設SIEM に収集されており、この既設SIEM を用いて調査と分析を行うこと。なお、既設SIEM を用いず、それぞれのサービスからAPI 等を用いてログを取得して調査と分析を行わないこと。 変更後 ②1.1④の機器やサービスから生成されるログはデジタル庁GSS班の既設SIEMに収集されており、この既設SIEMを用いて調査と分析を行うことを基本とし、既設SIEMに無い情報を使った分析結果は全て既設SIEMに統合すること。	MDEの端末のアクティビティ情報や、Paloaltoのパケット情報など、既設SIEMに入っていないデータを使うことで高度な脅威の抽出や分析精度向上ができ、より高度なサービス提供が可能となります。その際にAPIを使ったデータ取得とMSS事業者のシステムへの取り込みが必要となるためです。 また、APIの利用は分析やレポート作成において効率的なサービス提供が可能となり、リーズナブルなサービス提案ができます。 ただし分析結果は既設SIEMに統合させることが望ましいと考えています。	1.2②の記載は下記のとおり、修正します。なお、既設SIEMに無い情報を用いて検知を行う場合には、取得したい情報をデジタル庁GSSと協議及び連携の上、既設SIEMに収集する設定を入れ、調査と分析に利用することを想定しております。 「1.1④の機器やサービスから生成されるログはデジタル庁GSS班の既設SIEMに収集されており、この既設SIEMを用いた調査と分析に対応できる場合は加点対象とする。既設SIEMを用いない場合は、調達仕様書1.6作業スケジュールに留意する他、転送するログを最小限にする等の工夫を行うこと。」
67	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	4	1	2	②	4	既設SIEMで分析するということは、分析結果や分析理由を既設SIEM上で確認できるよう、既設SIEMに記録を残す必要があると思われ、その旨明記する必要があると考えます。	既設SIEMで分析結果を確認できれば、分析結果の把握などが容易に行えるようになるためです。	1.2②の記載は下記のとおり、修正します。 なお、既設SIEMで調査と分析を行うにあたっては、調査結果やその履歴を既設SIEMに書き込むことを可とする想定です。 「1.1④の機器やサービスから生成されるログはデジタル庁GSS班の既設SIEMに収集されており、この既設SIEMを用いた調査と分析に対応できる場合は加点対象とする。既設SIEMを用いない場合は、調達仕様書1.6作業スケジュールに留意する他、転送するログを最小限にする等の工夫を行うこと。」
68	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	5	1	4	④	2	右記理由により以下の文章の追加をお願いします。 ④監視対象通信機器やサービスが提供する脅威検知シグネチャやブラックリスト以外に、自社において独自の通信先ブラックリストを構築し、監視対象装置やサービスに定期的に適用することで、リスクを未然に防ぐための通信防御設定を行うこと。**なお日々変化していく脅威に対して、運用期間中に継続して対応をしていくための具体的な提案をする事。**	サイバーに関する脅威は常に変化していること、組織によって想定する脅威が異なることから、組織に応じ、なおかつ脅威の変化に応じた独自のインシデント検知の仕組みを継続して作成することが必要と考えております。	ご指摘を踏まえ、下記の記載を追記します。 「なお、日々変化していく脅威に対して、運用期間中に継続して対応をしていくこと。」
69	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	-	-	4	総合的なセキュリティ対策支援サービスの要件は、「令和4年度ガバメントソリューションサービスの運用・保守一式」に含まれる4.5セキュリティ運用支援業務とサービス内容が重複していると思われます。（2.2 ④原因究明のフォレンジックを除く） 「令和4年度ガバメントソリューションサービスの運用・保守一式」は2025年9月まで契約期間であるため、フォレンジック対応を除く総合的なセキュリティ対策支援サービスの開始時期は2025年10月になると考えます。	「令和4年度ガバメントソリューションサービスの運用・保守一式」で2025年9月まで提供するセキュリティ運用支援業務と重複する内容となるためです。	本件仕様書における総合的なセキュリティ対策支援サービスの実施開始時期は、調達仕様書へ記載のとおり令和７年１月です。
70	意見	その他	-	-	-	-	2	一般的な記載事項ですが、必要要件と考えるため以下記載が必要と考えます。 「デジタル庁のシステム担当職員やNISCからの調査要求に応じて、既設SIEMからデータログを抽出して提出すること」	一般的に左記の記載は対応が必要と想定しており、見積の工数積算に影響がでるため、明確化して頂きたいと考えるため。	ご指摘については、デジタル庁から調査依頼やデジタル庁等が実施するセキュリティ監査等への対応支援の報告内容に含まれると考えております。
71	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	2	2	4	″既設 SIEM を用いず、それぞれのサービスから API 等を用いてログを取得して調査と分析を行わないこと。″とございますが、API 等を用いてログを取得できた場合、監視対象の機器やサービスにもよりますが、分析に有効となる情報量がSIEMのみの場合よりも圧倒的に多くなります。これにより、複数のログからの相関分析が可能となり、迅速なインシデント対応に繋がります。そのため、適切かつ効果的な監視を行えるようにAPIからログを取得して調査と分析を可能にすることを推奨いたします。	最適な監視や調査を行うため。	1.2②の記載は下記のとおり、修正します。 「1.1④の機器やサービスから生成されるログはデジタル庁GSS班の既設SIEMに収集されており、この既設SIEMを用いた調査と分析に対応できる場合は加点対象とする。既設SIEMを用いない場合は、調達仕様書1.6作業スケジュールに留意する他、転送するログを最小限にする等の工夫を行うこと。」
72	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	6	2	2	4	4	EDRを用いた簡易フォレンジックと比較して、（通常の）フォレンジック調査については、影響範囲（通常サーバ等の場合、複数機器に及ぶ）に応じて、ネットワーク構成図等の資料確認、対象機器の特定、ログ調査を行いますが、想定より調査規模や調査コストが高く算出される可能性がございます。 「年1回程度の調査依頼を想定」の範囲が不明確のため、本件は、本調達の範囲内で検討するよりも個別対応が可能であることを追記いただくことが望ましいと考えます。	フォレンジック調査の範囲を明確にし、最適なコストを検討するため。	検討の結果、記載のままとします。 なお、調査規模や調査コストを想定する際には、本公告の閲覧資料をご確認ください。
73	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）					4	″02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス） 1.1 セキュリティ監視に関する要件″ についてとなります。セキュリティ監視における分析ルールは、最新のサイバー攻撃に対応するため、脅威情報のトレンドやベストプラクティスが反映されたメーカー推奨のテンプレートを利用するお客様が増えております。これは様々なセキュリティインシデントに対し、最適な分析ルールが随時適用され、より安全で効率的な運用が可能となるためです。そのため、以下のような仕様書要件の追記をいただくことが望ましいと考えます。 ■仕様書案 ″1.1 セキュリティ監視に関する要件″ 今後、継続的にセキュリティインシデントに対し最適な分析ルールを適用していくために、既設のSaaS型 SIEM（Microsoft社）が推奨するテンプレートを使用すること	最適な分析ルールの随時適用や、より安全で効率的な運用に繋がると考えるため。	既設のSaaS型 SIEM（Microsoft社）が推奨するテンプレートを使用することも含め、「どのようにインシデント疑いを発見するかについて具体的に提案することとし、その提案内容について加点対象」とします。
74	意見						4	各製品のコンソールへのアクセスについては現状記載がございませんが、各製品のコンソールへのアクセスが可能であることを追記いただくことが望ましいと考えます。	MSS監視サービスの人員や常駐人員が各製品のコンソールへアクセスすることで、製品固有の詳細情報や判断根拠を確認することが可能になり、高度なセキュリティ監視、迅速な原因究明に繋がると考えるため。	各セキュリティ監視製品のコンソールへのアクセスは、基本的に許可する想定です。ただし、GSS 側から貸し出される端末を利用してのアクセスのみを考えています。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
75	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	2	1	4		1	脆弱性発見時の対応等はSOCサービス提供事業者ではなく、GSS運用・保守業者が実施する内容にご変更をお願い致します。 ■文言修正案 ○SOCサービスを提供する業者 GSSのセキュリティ関連の運用業務のうち、セキュリティ監視、インシデント発生時の対応や脆弱性発見時の対応等、セキュリティに関する専門的な知識が必要となる業務を行う。 ○GSS運用・保守業者 GSSのセキュリティ関連の運用業務のうち、GSSで導入機器及びソフトウェアの一覧の更新や脆弱性発見時の対応等、インシデント対応における再発防止策の検証及び実施等、運用保守業務と一体化となって行う業務を行う。	脆弱性対応は、保護対象の環境理解が必要なため、GSSの運用・保守業者の対応範囲と考えます。	本件の受注者は、GSSのセキュリティ関連の運用業務のうち、セキュリティに関する専門的な知識が必要となる業務を行うことを求めます。また、脆弱性対応のうち運用保守業務と一体化となって行う業務である対策の実施はGSS運用・保守業者で行うなど整理しております。 受注者においては、デジタル庁及びGSS運用・保守業者とのコミュニケーションなどを通してGSSの環境理解に努め、本調達の業務を行っていただきます。
76	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	23	7	1	（３）⑦	1	・データ消去作業およびデータの消去完了の証明書の提示は、SOC2 Type2等の外部監査資料のご提出で代用が可能な文言追加をご検討ください。 ■文言修正案 '⑦収集したデータ等を消去する際には、当庁から承認を得て、全て受注者が行い、第三者がデータ復元ソフトウェア等を利用してもデータが復元されないように完全にデータを消去すること。データ消去作業に必要な場所や機器等については、受注者の負担で用意すること。データ消去作業終了後、受注者はデータの消去完了を明記した証明書を当庁に提出すること。但し、定期的にSOC2 Type2などの監査を受けている場合はそのレポートを提出することでも対応可とする。	データ消去の手続きを簡略化するため。 ※SOC2 C1.2 機密情報の破棄に該当	検討の結果、記載のままとします。やむを得ない事情により証明書の提出が難しい場合は、デジタル庁と協議します。
77	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	27	7	5	（2）	1	バックグラウンドチェックは、どの調査会社を利用しているかにとどめてほしい。 ■文言追加案 '業務従事者の経歴（氏名、所属、役職、学歴、職歴、業務経験、研修実績その他の経歴、専門的知識その他の知見、母語及び外国語能力、国籍等が分かる資料）を提出すること。なお、本業務の実施期間中に業務従事者を変更等する場合は、事前にこれらの情報を担当職員に再提示すること。但し、外部のバックグラウンドチェックを行うサービスを利用している場合はサービス名の記載をすることで対応可とする。	提供する業者によってはカントリーレギュレーションにより個人情報の提示が制限されております。	検討の結果、記載のままとします。やむを得ない事情により経歴情報の提出が難しい場合は、デジタル庁と協議します。
78	意見	01_調達仕様書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	27	7	6	⑩	1	情報セキュリティ監査、システム監査はその他の認定（SOC2 Type2等）で代用可能とするか、メールやリモート会議などでの監査を認めてほしい。 ■文言修正案 '受注者は、当庁が実施する情報セキュリティ監査又はシステム監査を受け入れるとともに、指摘事項 への対応を行うこと。但し、定期的にSOC2 Type2などの監査を受けている場合はそのレポートを提出することでも対応可とする。	監査対応の簡略化のため。	検討の結果、記載のままとします。やむを得ない事情により当該監査の受け入れが難しい場合は、デジタル庁と協議します。
79	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	1	③	2	機器への適用のみならず、SOCシステム側のデータベースに脅威情報があり、その情報をもとに検知する方式の採用をご検討ください。' ■文言追加案 ④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④ⅰに適用し、インシデント検知を行うこと。なお、④ⅱにも適用できる場合は加点対象とする。	ブラックリストによる突合だけでなく複数のログ条件と脅威情報を突合させることでインシデント検知また予兆検知を行うことも重要と考えます。	検討の結果、仕様書への追記はしません。
80	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	2	②	1	監視にかかわるすべてのログがUSのAWS環境へ連携される事を許容ください。 ■文言追加案 但し、SOC側のSIEMを利用する場合は下記の条件を含めること ・庁側でも操作可能なSIEMの管理画面が閲覧可能なアカウントを提供すること ・SIEM基盤はISMAPに登録されているクラウドサービスを利用すること ・収集及び、解析されたデータはISMAPに登録のあるクラウドサービス内にのみ保管されること ・SIEMへのログ転送方式として庁側のSentinelを経由しない場合、MicrosoftのSaaS関連製品はAPIによるデータ連携を行い、オンプレにかかわる機器に関しては、SIEMへ連携するためのログ転送装置を用意すること	機器やサービスから生成されるログは、安全が確保されているSOCベンダー側にあるSIEM基盤に転送いただくことで、24時間、365日で検知・調査・運用を踏まえたセキュリティ運用の安定稼働につながると考えます。 また、重大インシデント発生時に、独自の脅威インテリジェンスとの突合などの付加価値付与や、インシデントハンドラーによる調査の迅速化が図れます。	1.2②の記載は下記のとおり、修正します。なお、クラウドサービスを利用する場合は、調達仕様書7.6（１）⑲や別添資料７「情報セキュリティ要件」も参考にしてください。 「1.1④の機器やサービスから生成されるログはデジタル庁GSS班の既設SIEMに収集されており、この既設SIEMを用いた調査と分析に対応できる場合は加点対象とする。既設SIEMを用いない場合は、調達仕様書1.6作業スケジュールに留意する他、転送するログを最小限にする等の工夫を行うこと。」
81	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	3	1	2	③	1	アラートを検知してから平均2時間以内などの記述に変更をお願いします。 ■文言修正案 'インシデント疑いであると考えられる事象に対する一次調査結果は、インシデント疑いであると考えられる事象を検知してから２時間以内に行うこと。但し複雑な攻撃時において分析や報告までに2時間を超過する場合は庁とコミュニケーションをとりながら時間のを最小限に抑えるように努めること	SIEM基盤による検知からのアラート発生と、それら発生した高レベルアラートをもとにした調査を行う場合、高度な相関分析及び詳細な報告の作成が必要となるため、複雑な攻撃においては報告まで2時間を超過するケースが考えられます。	インシデント対応においては詳細な分析だけでなく、迅速性も求められるため、一次調査結果は2時間以内に行うことを求めます。なお、一次調査結果に求める粒度については、デジタル庁側が了承する内容を業者に提案していただくことを考えています。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
82	意見	02_別添資料１．要件定義書（令和６年度ガバメントソリューションサービスにおけるSOCサービス）	8	2	3	⑤	1	インシデントに関する情報やダークウェブ上で漏洩していると考えられている関連キーワードでの調査とする内容へ変更は可能でしょうか？	調査を円滑にすすめるため、貴庁が漏洩や攻撃の予兆を気にされているサービス名やドメインをいただいた上での調査が効率的と考えております。 キーワードが無い場合、基本的には関連省庁名やドメイン名、IPアドレスなどがキーワードになりますが、特定のサービス名や製品名、関係グループ等は大体どのユーザも複数保持しており、弊社側で優先度や重要度の判断が難しい可能性が高いため。	ダークウェブ等で公開されている情報に関して、関連キーワードをもとにして、デジタル庁が提供するGSSに関する情報かつGSSへの危険性が脅かされると判断される情報を収集する方法も想定しますが、具体的な取集の仕方については、デジタル庁側が了承する方法を業者から提案していただくことを考えています。
83	意見	調達仕様書	16	6	3	②X	4	「全てのサービス（サービスを提供するためのハードウェア、ソフトウェア、ネットワーク等を含む。）について脆弱性検査を行い、問題が発見された場合は、是正した上で納品すること」 とありますが、サービスについては「デジタル庁に設置する機器やネットワーク」「サービス提供事業者の設備」の２つに分かれるかと思いますので、すべてを対象とするかどうかを明記することを検討してください。また、是正についてもすべての影響度の低い脆弱性を是正することはできないので、是正対象の脆弱性の内容についても記載することを検討してください（例：リスク評価も実施したうえで、直ちに是正が必要なものを対象とする）。	脆弱性診断の範囲をどこまでとするかによって、工数とスケジュールに大きく影響しますので、対象を明確にしていただきたいです。	当該記載箇所は、ネットワークやシステム構築を行い、デジタル庁に納品を行う場合の記載です。問題が発見された場合は、適切に是正していただく必要があります。
84	意見	調達仕様書	25	7	1	(4)③ｉ	1	「MSS 監視サービスの要件で定めるような情報セキュリティインシデントの対応業務を３年以上実施したことがある者。」とありますが、全ての業務担当者に３年以上の経験を求めるのはサービスとして提供する上で困難です。 従い、「上記の経験を有する者を運用メンバに含めること。」と条件を変更頂きたい。	デジタル庁様に専用のサービスを、専用の体制で提供しているわけでは無いので、全ての業務担当者に具体的な制限を持たせるのは困難であるためです。	ご指摘を踏まえ、下記のとおり記載を見直します。 「運用メンバ（MSS 監視サービス担当者）は、以下の要件を全て満たす要員が常に運用メンバに含まれていること。」
85	意見	要件定義書	4	1	2	②	4	「なお、既設 SIEM を用いず、それぞれのサービスから API 等を用いてログを取得して調査と分析を行わないこと。」とありますが、既設SIEMのログには検知したシグネチャのペイロード（悪意のあるデータ部分）が含まれないなど、既設SIEMのログだけでは正確な分析ができません。サービス提供者が適切なサービスを提供するためには、サービス提供事業者が用意するSIEMを「併用」したうえでの調査と分析を許容いただくなど、監視実現方法は提案に委ねていただきたく検討お願いします。	既設 SIEMのみを使用するという条件を設けることは、サービスの品質を落とすこととなり、本調達仕様の趣旨からかけ離れてしまうと考えます。	1.2②の記載は下記のとおり、修正します。 「1.1④の機器やサービスから生成されるログはデジタル庁GSS班の既設SIEMに収集されており、この既設SIEMを用いた調査と分析に対応できる場合は加点対象とする。既設SIEMを用いない場合は、調達仕様書1.6作業スケジュールに留意する他、転送するログを最小限にする等の工夫を行うこと。」
86	意見	要件定義書	4	1	2	④	4	「インシデント疑いであると考えられる事象の調査と分析による最終的な結果は、デジタル庁が指定した方法で報告すること。」とありますが、指定した方法が具体的に定義されておらず、これではマネージドサービスとして提供することが困難です。意図としては、インシデントの内容に応じて、報告内容や方法をその都度デジタル庁から指示するということだと考えますので、本要件は「総合的なセキュリティ対策支援サービスに関する要件」の業務内容とすべきだと考えます。	マネージドサービスでの提供は困難であるため。	ご指摘の点に懸念がある場合、たとえば、事前に業者から報告のフォーマット案や報告方法を提案のうえ、デジタル庁がそれを了承したうえで、原則それに則った報告で行うなど、都度デジタル庁から指示しない方法をご提案ください。
87	意見	要件定義書	4	1	3	③	4	「通知手段として電子メール、電話および Microsoft Teams を利用できること」とありますが、 電子メールと電話による通知で、もれなくインシデントの発生は把握できると思います。Microsoft Teamsによる通知は、インシデントの発生を把握するという意味では、必須では無いと考えますので、除外するか加点対象とするのが良いのではないでしょうか。	インシデントの把握という点では、Microsoft Teamsは必須ではないと考えるため。特に弊社標準業務ではTeamsを用いた通知に対応していないため、当該事項が必須となると入札参加自体が困難となるため。	通知手段として電子メール、電話および Microsoft Teamsを利用できることを求めます。
88	意見	要件定義書	5	1	4	⑤	3	⑤の要件に示されたPA-5260に対する通信遮断は、③の「ネットワーク機器」を指していると理解しています。そのため、⑤は削除して③を「緊急対応としての通信遮断は、ネットワーク機器（パロアルトネットワークス社 PA-5260）を用いた通信遮断～」とすべきかと思います。	仕様が重複しているので、纏めるべきと考えます。	検討の結果、記載のままとします。なお、⑤の要件は正しくはPAN-PA-5450及びPAN-PA-3430のため修正いたします。
89	意見	要件定義書	6	2	1	①	3	「デジタル庁の指定する場所」を具体的に記載してください。なお、指定する場所を秘匿する必要がある場合には、「東京都内」などの粒度で記載を検討お願いします。	常駐する場所によっては、業務担当者の要件が変わってくるためです。	東京都内及びその近郊を想定しております。
90	意見	要件定義書	4	1	3	①	2	「インシデントの発生またはインシデント疑いを特定した場合、特定後 1 時間以内にインシデントの重要度判定を行い、デジタル庁が指定する担当者と方法にて連絡すること」とありますが、より迅速な対応のため、「特定後1時間以内」→「特定後15分以内」に変更することを検討ください。	インシデント対応の速度向上のため。	インシデント対応は迅速性に加え、通知する内容も重要となる認識ですので、仕様書上は特定後1時間以内であることを求めます。なお、通知する内容も重視しつつ、より迅速性が高いサービスを提供していただければと思います。
91	意見	要件定義書	3	1	1	③	4	「④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④ｉに適用し、インシデント検知を行うこと。なお、④ｉにも適用できる場合は加点対象とする。」とあるが、④ｉｉ（A10 ネットワークス社Thunder 3040S）への適用は加点対象外とすることを検討いただきたい。	同機はインターネット接続しておらず、ブラックリストの適用は現地作業となると理解するため、同機の運用・保守を行っている「ガバメントソリューションサービスの運用・保守」のみ対応が容易であり、公平性を欠く懸念があるため。	検討の結果、記載のままとします。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
92	意見	要件定義書	3	1	1	④	3	契約期間中のデバイス数とユーザー数について記載ありますが、想定するログ量を記載お願いします。	MSS監視サービス費用の積算精度を向上させるため。	ご指摘の点については、本公告の閲覧資料をご確認ください。
93	意見	要件定義書	4	1	2	⑤	4	「日本国以外において本調達と同様のインシデント疑い調査および分析サービスを提供している場合にはその事例について紹介することとし、その紹介内容について加点対象とする。」とありますが、上記は加点対象から除外を検討お願いします。	日本国外で常駐者を含む類似業務を行っている事業者が極めて限定されること及び本業務の実効性や品質を確保する上で日本国内で政府機関向けに実績ではなく、日本国外で同様の業務を行っていることが有益となる必然性が薄いと考えられるため。	検討の結果、記載のままとします。
94	意見	要件定義書	5	1	4	④	2	「監視対象通信機器やサービスが提供する脅威検知シグネチャやブラックリスト以外に、自社において独自の通信先ブラックリストを構築し、監視対象装置やサービスに定期的に適用することで、リスクを未然に防ぐための通信防御設定を行うこと。」とあるが、独自の通信先ブラックリストのみではなく、独自シグネチャを定期的に適用することも追加を検討お願いします。	インシデントの検知力向上のため。	ご指摘をふまえ、下記のとおり修正いたします。 「監視対象通信機器やサービスが提供する脅威検知シグネチャやブラックリスト以外に、自社において独自のシグネチャまたは通信先ブラックリストを構築し、監視対象装置やサービスに定期的に適用することで、リスクを未然に防ぐための通信防御設定を行うこと。」
95	意見	要件定義書	6	2	1	①	3	「日中業務日は、セキュリティに関する高度な知識を有する専門の技術者２名がデジタル庁の指定する場所に常駐し、本サービスの提供を行うこと。」 とありますが、日中業務日の定義（例：開庁日９時から１７時３０分など）を追記検討お願いします。	体制検討及び費用積算精度向上のため。	「調達仕様書別添資料３用語の定義」において、「日中業務日」を「業務日の9:30～18:15とする。」としています。なお。業務日についても同資料内で定義しています。
96	意見	要件定義書	6	2	2	④	3	「（通常の）フォレンジック調査（年１回程度の調査依頼を想定）」 とありますが回数ではなく対象台数で記載することを検討お願いします	費用積算精度向上のため。	ご指摘の点については、本公告の閲覧資料をご確認ください。
97	意見	要件定義書	7	2	2	⑤	4	「発生したインシデントについて、その対処計画の提案を行い、デジタル庁の担当者に確認のうえで、デジタル庁指定の時間以内に対処を行うこと。」とありますが、対処ではなく、対処に係るアドバイスに変更を検討お願いします。	対処（例：脆弱性を排除するためのパッチ適用、バージョンアップなど）は「ガバメントソリューションサービスの運用・保守」事業者側の責任範囲と考えるため。	緊急性かつ専門性が求められるため、受注者には「対処」を行うことを求めます。なお、対処計画をデジタル庁で確認する際に、デジタル庁側から受注者が行う「対処」の作業範囲や作業内容を指示します。
98	意見	要件定義書	7	2	2	⑦	4	「①の結果、インシデントの発生とはいえないものの、サイバー攻撃が疑われる場合には、事象の内容、原因を追及し、影響範囲を見極めかつ対応策（同種の攻撃に備えた事前の対応策を含む）を検討し、デジタル庁の担当者に確認のうえで、デジタル庁指定の時間以内に対処を行うこと。」とありますが、対処ではなく、対処に係るアドバイスに変更を検討お願いします。	対処（例：脆弱性を排除するためのパッチ適用、バージョンアップなど）は「ガバメントソリューションサービスの運用・保守」事業者側の責任範囲と考えるため。	緊急性かつ専門性が求められるため、受注者には「対処」を行うことを求めます。なお、対応策をデジタル庁で確認する際に、デジタル庁側から受注者が行う「対処」の作業範囲や作業内容を指示します。
99	意見	要件定義書	8	2	3	②	4	「収集した脆弱性情報について、その危険性の判断を行うこと。危険性の判断を行うため、その判断基準を定め、事前にデジタル庁から承認を得ること。」とありますが、「貴庁から提供する判断基準を参考に定めること。」に変更を検討お願いします。	「ガバメントソリューションサービスの運用・保守」業務において既に当該業務は実施され、判断基準は存在すると考えるため、基準の継続性を確保するため。	判断基準は、事前にデジタル庁から承認を得たうえで、受注者で定めていただきます。なお、判断基準を定める際にデジタル庁側から必要な範囲内での情報連携を受けることは可能です。
100	意見	要件定義書	8	2	3	③	4	危険性の判断に基づいて、脆弱性に対する対策計画の策定を行い、デジタル庁の担「当者に説明と確認のうえで、提案すること。対策計画の策定を行う際には、その危険性を排除することを満たしつつ、GSS 運用・保守事業者の負担を必要最小限とするように留意すること。」とありますが、「ガバメントソリューションサービスの運用・保守事業者が作成する脆弱性に対する対策計画の作成に必要な助言をすること。」も変更を検討お願いします。	対処（例：脆弱性を排除するためのパッチ適用、バージョンアップなど）は「ガバメントソリューションサービスの運用・保守」事業者側の責任範囲と考えるため。	より専門性が求められるため、受注者には「対処計画の策定・提案」を行うことを求めます。
101	意見	要件定義書	3	1	1	②	4	「④で示す監視対象機器に対する死活監視を行い」とありますが、Microsoft 365 E5についてはサービス管理者が通知を受信したり、ポータルで確認するしか方法がありません。いずれにしても、MSSサービス提供事業者で死活監視をする必要は無く、デジタル庁もしくはMicrosoft 365に関する運用保守事業者で実施するのが適切と考えられるため、要件から削除することをご検討ください。	貴庁又はMicrosoft 365に関する運用保守事業者以外は実施不可能な要件であるため。	ご指摘をふまえ、下記のとおり修正いたします。 「④ⅰ～ⅳで示す監視対象機器に対する死活監視を行い」
102	意見	要件定義書	3	1	1	④	3	「PAN-PA-5450」とありますが、３セットとも同じ型番では無いと理解しています。「予定」や「PAシリーズ」という記載が良いのではないでしょうか。	仕様を明確にするため。	検討の結果、記載のままとします。
103	意見	要件定義書	5	1	4	⑤	3	「PAN-PA-5260」とありますが、型番が誤っています。また、全デバイスに対処が必要なものだと思いますので、明確に３セットであることを記載した方がよいのではないでしょうか。	仕様を明確にするため。	⑤の要件は正しくはPAN-PA-5450及びPAN-PA-3430のため修正いたします。

項	区分	文　書　名	頁番号	章番号	節番号	小節番号	種 別	質　　問　　等	理　　由	回答
104	意見	要件定義書	6	2	2	③	3	「デジタル庁からその検体の提供を受け、隔離保存を速やかに行い」とありますが、隔離保存の対象はマルウェア等と理解しています。前段の「デジタル庁からその検体の提供を受け」だとすでにマルウェアが隔離されている状態とも読めますので矛盾しているかと思います。「デジタル庁からの依頼を受け」が意図したことではないでしょうか。	仕様を明確にするため。	ご指摘をふまえ、下記のとおり修正いたします。 「デジタル庁から被疑検体の提供を受け、隔離保存を速やかに行い」