令和4年5月9日

奈良県総務部デジタル管理室
デジタル管理室長

質問回答書

次の調達について下記のとおり回答します。

物件名：奈良県自治体情報セキュリティクラウド再構築・運用業務

番号	項目	ページ、項目など	項目名、項番名など	質問内容	回答
1	仕様書	2.2.調達範囲 表.1必要機能一覧 4.3.必須機能		内部DNSの項目がありませんが、こちらについては、監視・分析は不要という認識で宜しいしょうか。	お見込みのとおりです。
2	仕様書	2.3.セキュリティクラウド利用自治体		「なお、FQDN数は各団体1つ(奈良県と生駒市のみ3つ)である。」とありますが、奈良県、生駒市はオプション機能の「追加WAFの利用」を考慮しての数字という理解で宜しいでしょうか。 WAFに関するFQDN数：基本機能　40、オプション 4	お見込みのとおりです。
3	仕様書	4.1.共通要件		本項で記載(6)の移行支援の内容は、現行のセキュリティクラウド運用事業者にも同様の条件で課せられていると認識してよろしいでしょうか。	お見込みのとおりです。
4	仕様書	4.1.共通要件 （7）		ログ情報保存のサーバについて、WAFやCDNにおいても日本国内にログ情報が保存されている必要がありますでしょうか。	原則日本国内保存とします。
5	仕様書	4.2.データセンター要件 (7)設備運用	項番1	「原則、24時間365日で常駐管理がされていること」とありますが、弊社データセンターは自社提供サービス以外に貸出をおこなっておらず契約者が入退館することがないため、常駐する必要はなく夜間休日においては、警備会社との連携で侵入警備を行うことで対処しております。 この場合においても、24時間365日の常駐が必要となりますでしょうか。	侵入警備だけでは要求要件を満たしていると認められません。
6	仕様書	4.2.データセンター要件 (7)設備運用	項番1	「原則、24時間365日で常駐管理がされていること」とありますが、弊社データセンターのインターネット接続点について外部の別データセンターからIXに接続しているものがあります。 このような場合において、別データセンターの運営事業者によって常駐がされている場合は、24 時間 365 日で常駐管理がされていることになるという認識でよろしいでしょうか。	要求要件を満たしていると認められません。

番号	項目	ページ、項目など	項目名、項番名など	質問内容	回答
7	仕様書	4.3.必須機能 (1)ウェブサーバの監視	項番8	「構成団体が提供するWebサーバの集約は行わない」とは、セキュリティクラウド内にハウジングやホスティング環境を準備して集約する必要は無いという意味で宜しいでしょうか？	お見込みのとおりです。
8	仕様書	4.3.必須機能 (3)プロキシサーバの監視	項番8	「セキュリティを考慮し、セキュリティクラウドからインターネットへ通信を行う際は、端末情報を削除すること」について、上位プロキシで復号されない通信からは、端末情報を削除できないかと思いますが、全ての通信について復号が必要でしょうか？	本項はXFF情報等により相手方Webサーバへ端末情報が届かないようにすることを意図しています。
9	仕様書	4.3.必須機能 (4)外部DNSサーバの監視	項番4	こちらに関しては、必ず外部DNSサーバ自体を監視する必要がありますでしょうか。不正な通信についてはUTMのログ分析等で代用可能かと思いますのでそのような形で代用する策も可としていただけないでしょうか。	サーバ本体のログを分析してください。
10	仕様書	4.3.必須機能 (4)外部DNSサーバの監視	項番9	マルチドメインのサポートについて、各団体ではなく、総合窓口を通して実施させていただいても宜しいでしょうか。	マルチドメインをサポートしているのであれば実施方法は受託者の提案によります。
11	仕様書	4.3.必須機能 (4)外部DNSサーバの監視		外部DNSのログについては、経路上に存在するUTMのログ(DDOSなど)を監視しての検知・分析でも宜しいでしょうか。	サーバ本体のログを分析してください。
12	仕様書	4.3.必須機能 (13)CDN	項番4	「コンテンツキャッシュサーバは、インターネット上の複数のサーバで構」とありますが、4.2 データセンター要件で定めるデータセンター以外のクラウドサービスを利用して良いという認識でよろしいでしょうか。 その場合でも、4.2. データセンター要件で定める「日本国内」「常駐管理」の仕様に準拠する必要があるという認識でよろしいでしょうか。	お見込みのとおりです。
13	仕様書	4.3.必須機能 (14)ログ収集・分析	項番1	対象の各サーバについては、WAFのログ分析でも宜しいでしょうか。	各サーバ本体のログを分析してください。
14	仕様書	4.3.必須要件 (14)ログ分析	項番4	『必要なルールを個別に作成できること』の記載がございますが、具体的にどういった内容を想定されておりますでしょうか。 (指定された脅威に対する分析ルールを追加する必要があるといった内容でしょうか)	お見込みのとおりです。

番号	項目	ページ、項目など	項目名、項番名など	質問内容	回答
15	仕様書	4.3.必須要件 (15)イベント監視	項番3	『OSのシステムイベント、アプリ―ションの起動や停止、エラー通知といったイベントを監視できること』と記載がありますが、左記以外にも監視項目があればご教示頂けますでしょうか。	必須の監視項目は仕様書記載のとおりです。 なお、本セキュリティクラウドに資する監視項目の提案がある場合は提案書の項目番号9番で記載いただければ評価する場合があります。
16	仕様書	4.4.オプション機能 (1)メール無害化	項番4	メール無害化機能とファイル無害化機能で両方の機能を求めている3団体様について、実際に項番4にてファイル無害化も行いますが、オプション機能（2）のファイル無害化の機能まで必要となりますでしょうか。	提供されるメール無害化の機能で4．4 オプション機能 （2）ファイル無害化の全ての要件を満たせるのであれば必要ありません。
17	仕様書	4.4.オプション機能 (2)ファイル無害化	全般	上記ご質問で、メール無害化機能に追加でファイル無害化の機能を利用希望の場合、費用を計算するために希望団体様の一般行政職員数をご教示いただけますでしょうか。	端末数を職員数として算定してください。
18	仕様書	4.4.オプション機 (4)EDR監視／運用	項番13	『TrendMicroやF-Secure等』の記載についてですが、可能であれば想定されるアンチウィルスソフトをご教示頂けないでしょうか？	表記以外のものについては、受託者決定後、現状調査の中でご確認ください。
19	仕様書	4.4.オプション機能 (4)EDR監視／運用	項番3	EDRの場合は論理的に隔離した後調査するためにはネットワークにつながっている必要があり、物理隔離されると調査続行が不可能になると考えます。また、物理隔離は現地で行っていただく必要があるので、しかるべき調査が終わった後必要であれば団体様に物理隔離をしていただくと考えてよろしいでしょうか。	各利用団体ごとに運用するセキュリティポリシーが異なるため、実際にどのような対応とするかは各利用団体と協議の上、決定することとします。
20	仕様書	4.4.オプション機能 (5)ActiveDirectoryの利用		初期の移行作業も含まれますでしょうか？	お見込みのとおりです。
21	仕様書	4.4.オプション機能 (5)ActiveDirectoryの利用		パッチ更新やアカウント追加や削除については市町村様側で対応で宜しいでしょうか？若しくはサービス事業者側の対応でしょうか？	原則受託者側の対応とします。
22	仕様書	4.4.オプション機能 (5)ActiveDirectoryの利用		設置場所は当社が構築するデータセンター内で宜しかったでしょうか？ (市町村様のサーバルーム等に設置する可能性が無いかの質問です)	お見込みのとおりです。

番号	項目	ページ、項目など	項目名、項番名など	質問内容	回答
23	仕様書	4.4.オプション機能 (6)メールサーバの利用		今回の作業範囲は、メールサーバの構築・市町村様側にてアカウント追加や削除が行えるようにするまでで宜しかったでしょうか？若しくは既存アカウントの移行作業も含まれますでしょうか？	メールサーバの構築並びに既存アカウントがある利用団体については移行作業も含みます。
24	仕様書	4.4.オプション機能 (6)メールサーバの利用		パッチ更新や故障以外の運用作業、アカウント追加や削除については市町村様側で対応で宜しいでしょうか？	原則受託者側の対応とします。
25	仕様書	4.4.オプション機能 (6)メールサーバの利用		設置場所は当社が構築するデータセンター内で宜しかったでしょうか？ (市町村様のサーバルーム等に設置する可能性が無いかの質問です)	お見込みのとおりです。
26	仕様書	4.4.オプション機能 (8)ウイルス対策ソフトの利用	項番7	サーバとは、ウィルスソフトの更新等の管理サーバのことで宜しかったでしょうか？ また、パッチ更新や故障以外の運用作業については市町村様側で対応で宜しいでしょうか？	対象サーバの認識についてはお見込みのとおりです。 また、運用作業については原則受託者側の対応ですが、端末側の設定等、受託者で行えない作業は利用団体側の作業となります。 詳細は利用団体と協議の上、決定します。
27	仕様書	4.4.オプション機能 (10)追加VPNの利用	項番1	市町村様側とセキュリティクラウドを結ぶ市町村様側ファイアウォールについては、市町村側様のご準備で宜しかったでしょうか？SLAは、このオプションについても適用でしょうか？	4.3.必須機能（6）各団体のセキュリティクラウド接続用ファイアウォールを参照してください。 SLAについてはお見込みのとおりです。
28	仕様書	4.4.オプション機能 (10)追加VPNの利用	項番1	「大和路情報ハイウェイを通らずに奈良県自治体情報セキュリティクラウドへ直接接続できる閉域回線」とありますが、市町村から大和路情報ハイウェイの自治体情報セキュリティクラウド接続点まで閉域回線という認識でよろしいでしょうか。 もしくは、市町村から自治体情報セキュリティクラウドを提供する受託者指定のデータセンターを直接接続する閉域回線となりますでしょうか。	後者となります。
29	仕様書	4.4.オプション機能 (10)追加VPNの利用	項番3	「100Mbpsベストエフォート、100Mbps帯域確保、1Gbpsベストエフォート、1Gbps帯域確保のメニューから選択可能であること」とありますが、他社提供のVPNサービスを利用し、市町村からVPNサービスへのアクセス回線をメニューから選択可能とするという認識でよろしいでしょうか。	お見込みのとおりです。 なお、回線サービスは可能であれば自社提供でも問題ありません。

番号	項目	ページ、項目など	項目名、項番名など	質問内容	回答
30	仕様書	4.5.運用保守要件 (1)統括窓口業務	※「対応レベル」表	「フォレンジック結果を提出する」と記載がありますが、全てのインシデントに対して実施するものでしょうか。また、どのような状況を以てフォレンジック完了とするのかご教示頂けますでしょうか？	フォレンジックの実施対象及び調査内容についてはインシデントが発生した利用団体と協議して決定するものとします。
31	仕様書	4.5.運用保守要件 (2)マネージドセキュリティサービス	項番11	『セキュリティ機器や監視対象サーバのログを全てマネージドセキュリティサービス事業者側に送り監視すること』と記載がありますが、4.3. 必須機能(14)ログ収集・分析に記載のある「監視対象サーバ、ゲートウェイ対策システム、メールセキュリティ対策システム」のログという認識で宜しいでしょうか？	4.3. 必須機能 (14)ログ収集・分析の項番3に記載されているファイウォール・IDS/IPS・メールリレーサーバ・WAF・プロキシサーバ・外部DNSサーバ等の主要なセキュリティ対策機器も対象となります。
32	仕様書	4.5.運用保守要件 (6)障害管理	項番2	セキュリティクラウドを構成する機器は冗長化を行い、と記載いただいておりますが、各団体に設置するセキュリティクラウド接続用ファイアウォールは冗長構成の対象外と考えてよろしいでしょうか。	お見込みのとおりです。 なお、当該機器について冗長化または可用性向上に資する提案がある場合は提案書の項目番号19番で記載いただければ評価する場合があります。
33	仕様書	4.5.運用保守要件 (8)ヘルプデスク機能	項番6	『構成団体のシステム更新、システム変更に対し柔軟に対応すること』と記載がありますが、現行のシステムでの更新および変更実績などをご教示頂けないでしょうか？	具体的な実績情報はありませんが、5年間の運用期間中にいずれの団体も1度はシステムの更新があると見込まれます。
34	仕様書	4.5.運用保守要件 (8)ヘルプデスク機能	項番8,9	問合せ対応や通知等を実施する際に、「電話又はメール」でとの記載がありますが、Webポータルによる提供は可能でしょうか？	Webポータルを併用することを妨げませんが、電話又はメールでの受付対応も提供してください。
35	仕様書	4.5.運用保守条件 (8)ヘルプデスク機能		ヘルプデスク、NOC、SOCに関する以下の情報について、可能な範囲で現状をご教示頂けないでしょうか？ ・問い合わせ件数 ・障害発生件数 ・参加団体の追加／脱退件数 ・参加団体のオプション機能の追加・削除申し込み件数	現行セキュリティクラウドに関しては以下のとおりです。 問い合わせ件数：約350件／年 障害発生件数：11件 参加団体の追加／脱退：なし オプション機能の追加・削除： WAFのFQDN追加4件 Webメール利用追加1件 メール無害化追加1件
36	仕様書	4.5.運用保守要件 (9)セキュリティレベルの自己点検の実施	項番5	『第三者による監査』と記載がありますが、第三者は本セキュリティクラウドにかかわっていない会社、資本提携のない会社等を想定しましたがその認識であっておりますでしょうか？	お見込みのとおりです。
37	仕様書	4.5.運用保守要件 (11)セキュリティ監視業務	※「危険度」表	危険度の分類の一例とありますが、提供事業者側で定義したものを事前合意の上利用する運用でも問題無いでしょうか？	お見込みのとおりです。

番号	項目	ページ、項目など	項目名、項番名など	質問内容	回答
38	仕様書	4.5.運用保守要件 (14)定例会議等の運営		各団体への月次報告は文書での報告とし、報告会は年1回集合型での開催とさせて頂いて宜しいでしょうか。	奈良県に対しては月に1回以上定例会議を開催してください。 奈良県以外の構成団体に対してはお見込みのとおりです。
39	仕様書	4.5.運用保守要件 (14)定例会議等の運営		現地で対応させていただく対応者とは別に、一部の対応者(NOC、SOC要因)がリモートで参加させていただく運用は可能でしょうか？	差し支えありません。 参加のための環境は受託者でご用意ください。
40	仕様書	5.移行作業要件		移行を検討するにあたり、オプション機能のメールに関する以下の情報について、可能な範囲でご教示頂けないでしょうか？ ・Webメール、メールスプールサーバ(IMAP、SMTP)の製品名とバージョン情報 ・移行元サーバとの間で、IMAPでの通信が可能か ・メールパスワードを既存事業者から平文でご提供頂けるか	受託者決定後、現状調査の中でご確認ください。
41	(参考資料)オプション機能　団体別導入一覧			オプションの無害化利用でのメールアドレス数の記載はありますが、基本機能としての全自治体のメールアドレス数をご教示頂けますでしょうか？	端末数をメールアドレス数として算定してください。
42	(参考資料)オプション機能　団体別導入一覧			お客様で利用されるグローバルIPアドレスの準備は必要でしょうか？ 必要な場合、数量をご教示頂けますでしょうか？	仕様書で示す機能の実現に必要な数量をご用意ください。