

第3期千葉県自治体情報セキュリティクラウドサービス提供業務に係る質問に対する回答

番号	質問日	資料名	質問内容	回答
1	令和8年10月9日	様式14 見積書、別紙 提案書記載事項一覧	オプション要件の費用について 様式14 見積書におきまして、オプション要件であるコンテンツ改ざん検知が含まれております。同資料の記載上の注意として、「11. オプション要件の金額を含めないよう提示してください。」とございますが、コンテンツ改ざん検知について費用の記載は不要でしょうか。	コンテンツ改ざん検知に係る費用は、オプション要件のため、見積書に含めないでください。 ただし、コンテンツ改ざん検知機能がWAFの標準機能の一部として一体的に実装されており、その利用の有無にかかわらずWAFの費用が変わらない場合は、当該機能に相当する費用をWAFの費用から分離又は控除する必要はありません。
2	令和8年10月9日	別紙 業務提案書記載事項一覧	必須要件への適合確認について 「別紙 業務提案書記載事項一覧」の「2 共通記載ルール」において、「各項目には、要求水準書及び別紙3 の必須要件への対応内容、実現方法及び適合を確認できる根拠を記載すること」とございます。一方で、同資料「3 提案書記載事項」の表には各大項目の「必須記載事項」が示されていますが、当該「必須記載事項」の内容を示すことで、全ての必須要件に適合しているという理解でよろしいでしょうか。「要求水準書」及び「別紙3 次期SC 要件」に記載された全ての要件について個別に対応内容等を記載することは、提案書の紙面の制約上困難と考えております。「様式15 証明書」で「要求水準書」及び「別紙3 次期SC 要件」の要件を満たす保証をしているため、2つを組み合わせることにより全ての要件を満たしていることを示す想定です。もしくは業務提案書から切り離し、要件適合表を別紙にて提出可能でしたら、そちらでの対応も検討させていただきます。	「別紙 業務提案書記載事項一覧」の「2 共通記載ルール」にかかわらず、必須要件への適合確認については、以下のとおり取り扱います。 基礎審査については、「様式15別紙(様式15-2)」の「対応可否」欄に、全ての必須要件について「可」又は「否」を記載してください。また、「可」と記載する場合であっても、実現方法や適合性が要求水準書等の記載から明確に確認できない要件については、同別紙の「記載欄」に、対応内容、実現方法及び適合を確認できる根拠等を記載してください。ただし、これらが明確な要件についてまで、全ての対応内容等を一律に個別記載する必要はありません。 要求水準を上回る提案については、業務提案書の該当する業務提案審査項目に記載し、「様式15別紙(様式15-2)」の「記載欄」には、対応する業務提案審査項目等を記載してください。 要件適合表を別紙として提出する必要はありません。
3	令和8年10月9日	別紙 業務提案書記載事項一覧	要求水準を上回る提案の記載方法について 「別紙 業務提案書記載事項一覧」の「2 共通記載ルール」において、「要求水準を上回る提案については、上回る内容、実現方法、期待効果及び実現可能性を確認できる根拠を記載すること。」と記載されています。一方、「3 提案書記載事項」の各提案項目には、「要求水準を上回る提案として記載する事項」が複数示されています。これらについて、各提案項目に記載された箇条書きの事項は、全てについて上回る提案の有無(上回る提案又は提案なし)を記載する必要があるとの理解でよろしいでしょうか。また、箇条書きで示された事項以外の内容について要求水準を上回る提案を行った場合、それらも業務提案審査における加点点評価の対象にならない認識ですが合いますでしょうか。併せて、箇条書きで示された事項以外の提案については、各提案項目内に記載すべきか、又は提案No.20「付加価値提案」に記載することを想定されているのかご教示ください。	業務提案については、該当する業務提案審査ナンバーを明記した上で、要求水準を上回る提案がある事項のみ記載してください。「別紙 業務提案書記載事項一覧」の「2 共通記載ルール」には、該当がない場合は「追加提案なし」と記載する旨を定めていますが、要求水準を上回る提案がない事項については、当該記載を省略できるものとします。また、「要求水準を上回る提案として記載する事項」に箇条書きで示された事項以外の提案であっても、各提案項目との関連性が認められるものについては、当該関連性を明確に説明した上で、該当する提案項目内に記載してください。この場合、当該提案項目における評価の対象となります。 提案No.20「付加価値提案」は、他のいずれの提案項目にも関連しない業務提案を包括的に評価するための項目です。このため、箇条書きで示された事項以外の提案については、既存の提案項目との関連性がある場合は当該提案項目に、いずれの提案項目にも関連しない場合は提案No.20「付加価値提案」に記載することを想定しています。
4	令和8年10月9日	第3期千葉県自治体情報セキュリティクラウド要求水準書	地方公共団体サイバーセキュリティ対策事業実施要領について 要求水準書「第2 章 概要」「1 調達背景と目的」におかれまして、「なお、本セキュリティクラウドの利用開始に伴う移行・設計・テスト等の移行業務については、本要求水準書のほか、地方公共団体サイバーセキュリティ対策事業実施要領(自治体情報セキュリティクラウド更新事業)の定めるところによるものとする。」と記載がございます。地方公共団体サイバーセキュリティ対策事業実施要領(自治体情報セキュリティクラウド更新事業)の内容をご共有いただくことは可能でしょうか。	当該要領は提供可能ですので、本回答に併せて提供させていただきます。

第3期千葉県自治体情報セキュリティクラウドサービス提供業務に係る質問に対する回答

番号	質問日	資料名	質問内容	回答
5	令和8年10月9日	第三期千葉県自治体情報セキュリティクラウド要求水準書	サプライチェーンリスク対策に関する提出資料について 「第4章 契約条件・制約条件等」「4 法令等の遵守」におかれまして、「(4)入札参加希望事業者は、本要求水準書及び別紙3「次期SC 要件」に定めるサプライチェーンリスク対策を含むセキュリティ対策に適合することを確認する書面を提出すること。」とありますが、具体的に提出が必要な書類をご教示いただけませんか。 弊社では「(様式15) 証明書」および「別記 データ保護及び管理に関する特記仕様書」に記載のある書類(品質保証体制を証明する書類(品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図))を想定しております。	「様式15 証明書」に加え、本業務のサービス提供に係るサプライチェーンリスク評価を実施し、「別紙3 次期SC要件」に定める対策を満たしていることを確認できる根拠資料を提出してください。根拠資料としては、サービス提供体制、関係事業者、主要な機器・サービス、リスク評価結果、セキュリティ管理体制等を示す資料が考えられます。これらの事項は、原則として全て確認できるようにしてください。ただし、事項ごとに個別の資料を作成する必要はありません。一つの資料に複数の事項をまとめるなど、提出する資料全体で必要な事項を客観的に確認できるようにしてください。また、入札時点で構成事業者又は製品・サービスを確定していない場合は、予定する構成、選定方針、評価方法及び契約締結後の確認方法を記載してください。 なお、「データ保護及び管理に関する特記仕様書」に基づく品質保証体制を証明する書類を、根拠資料の一部とすることも可能です。
6	令和8年10月9日	別紙3 次期SC 要件	リモートデスクトップに関する提案方式について No.17「利用団体ごとに、仮想端末又は提案方式に係る利用環境を個別に管理できること」と記載されています。下記の2つの考え方があると存じますが、前者①の認識でよろしいでしょうか。後者②には、各利用団体管理者による設定変更にてトラブルが発生した場合の切り分けが困難、復旧までに時間を要すなど運用上の課題がございます。 ①利用団体間で論理的に分離され、受注者が団体別に設定・管理できる状態 ②各利用団体の管理者が自利用団体分について直接操作(利用者登録、接続先制御の変更等)できる管理権限の委譲	No.17については、①のとおり、利用団体ごとに利用環境を個別に管理できることを想定しています。 (各利用団体の管理者が直接操作できる管理機能の実装や、管理権限の付与までを求めるものではありません。)
7	令和8年10月16日	要件水準書 P24	【サービス提供編】第1章 システムの要件 7 情報セキュリティ要件(1)セキュリティ体制 (イ) 本業務の運用体制において不正通信の早期発見及びインシデントへの対応を迅速に行う体制(CSIRT)を構築し、また本業務の運用体制とは別に情報セキュリティに関する体制を構築し協議会を通じ利用団体に報告すること。 (内容) 現行のセキュリティクラウドにおいて検知した利用団体のセキュリティインシデントへの対応について、直近1年間のCSIRTの活動実績(対応件数及び主な対応内容)をご教示いただけますでしょうか。	現行のセキュリティクラウドにおける直近1年間(2025年4月から2026年3月まで)のセキュリティインシデント検知件数は、合計1,957件(※)です。 主な対応内容は、公開Webサーバへの攻撃、不正なWebサイトへの通信、マルウェアのダウンロード、不審なDNS通信、マルウェア添付メールおよびスパムメール等の検知・分析のほか、必要に応じた攻撃元IPアドレス等の予防遮断・緊急遮断、過遮断時のホワイトリスト登録等です。 なお、上記件数はCSIRT・SOCが検知・確認したアラート等の件数であり、すべてが侵入や情報漏えい等の実被害を伴うものではありません。検知後は内容を分析し、「緊急遮断」「予防遮断」「ホワイトリスト登録」または「対処不要」のいずれかを判断しています。 (※)機器による自動ブロック件数は膨大であり、CSIRTのインシデント対応件数とは性質が異なるため、1,957件には含めていません。
8	令和8年10月16日	要求水準書 P27	(3) アクセス回線(利用団体からセキュリティクラウドの間の回線) (イ) アクセス回線はIP-VPN等の閉域網を基本とし、利用団体の状況を考慮し、安全性を損なうことなく適切な価格で提供される回線を選定すること。なお、アクセス回線は利用団体毎に別途契約を行うが、以下の点に留意すること。 ・冗長化を図れること (内容) アクセス回線の冗長化を行う場合、利用団体に設置するルータ等の通信機器についても冗長構成とする必要がありますでしょうか。	アクセス回線を冗長化する場合であっても、利用団体に設置するルータ等の通信機器を一律に冗長構成とすることは必須としていません。ただし、当該通信機器が単一障害点とならないよう、機器の冗長化、予備機の確保等により、障害時に通信を継続又は速やかに復旧できる構成としてください。具体的な構成は、利用団体の状況を踏まえ、利用団体と協議の上で決定するものとします。

第3期千葉県自治体情報セキュリティクラウドサービス提供業務に係る質問に対する回答

番号	質問日	資料名	質問内容	回答
9	令和8年10月16日	別紙3 次期SC要件 NO18	■見出し ログ収集・不正事象検知 ■機能要件 受託者は、ファイアウォール、IDS/IPS等のセキュリティ機器、プロキシサーバ、振る舞い検知装置及び監視対象サーバ(Webサーバ、メールリレーサーバ、外部DNSサーバ、利用団体ADサーバ等)が出力する各種ログを収集・管理し、不正又は不正が疑われる事象を検知できる仕組みを提供すること。また、保管したログ情報について、分析官が手動で分析を行うための検索機能を有すること。 (内 容) セキュリティクラウドの各機器から収集した通信ログ及びイベントログについて、1日あたりのログの最大生成容量(GB/日)をご教示いただけますでしょうか。	現行のセキュリティクラウドにおける通信ログ及びイベントログの生成容量は、概ね700GB/日から1TB/日の範囲で推移しており、この期間における最大実績は約1TB/日です。 なお、この数値は現行環境の実績値であり、次期環境の設計に当たっては、通信量の増加、ログ取得対象及びログ出力設定の変更を踏まえ、必要な拡張性を確保してください。
10	令和8年10月16日	別紙2 利用団体におけるインターネットの利用状況	次期SCで各団体毎に利用を選択するオプション機能 LBO(ローカルブレイクアウト) (内容) LBO(ローカルブレイクアウト)の利用を予定・検討している利用団体について、利用団体ごとの想定回線帯域をご教示いただけますでしょうか。	LBO(ローカルブレイクアウト)の利用を予定または検討している利用団体ごとの想定回線帯域は、以下のとおりです。 利用団体 想定回線帯域 利用団体A 100Mbps 利用団体B 1Gbps 利用団体C 1Gbps 利用団体D 未定 利用団体E 100Mbps(帯域保証)または1Gbps(ベストエフォート) 利用団体F 1Gbps 利用団体G 1Gbps 利用団体H 1Gbps(ベストエフォート) 利用団体I 1Gbps 利用団体J 1Gbps 利用団体K 1Gbps
11	令和8年10月16日	要求水準書 P26 第2章 システムの稼働環境要件	3 ネットワーク構成 (3)アクセス回線(利用団体からセキュリティクラウドの間の回線) (ア)各利用団体からセキュリティクラウドまでのアクセス回線は、本調達の範囲外であるが、受注者は費用面における負担軽減も含め全体構成を考慮した、アクセス回線の導入について検討を行うこと。また、その結果を基に利用団体へ現行と同等程度でより低廉な回線構成の導入提案を行い、利用団体との協議や導入支援を行うこと。 (内容) アクセス回線については、利用団体ごとに別途契約するものと認識しております。業務提案書におけるアクセス回線費用の提示については、利用団体が選択可能な回線種別及び帯域ごとの月額単価メニュー表を提示することよろしいでしょうか。	お見込みのとおりです。 業務提案書には、利用団体が選択可能な回線種別および帯域ごとの月額単価メニュー表を提示してください。併せて、初期費用、帯域保証・ベストエフォートの別、冗長化の可否・費用、契約条件およびその他の前提条件を明示してください。 なお、各利用団体からセキュリティクラウドまでのアクセス回線は本調達の範囲外であり、各利用団体が別途契約するため、当該回線費用は入札金額および見積書(様式14)には含めないでください。

第3期千葉県自治体情報セキュリティクラウドサービス提供業務に係る質問に対する回答

番号	質問日	資料名	質問内容	回答
12	令和8年10月16日	要求水準書 P26 第2章 システムの稼働環境要件	3 ネットワーク構成 一部のISPの変更ができない利用団体については、利用団体→セキュリティクラウド→利用団体→ISPという経路で折り返し通信するための設定を行うこと。折り返し通信の実現方法を検討するに当たっては、品質確保について十分留意すること。 (内容) 本構成の対象となる団体数をご教示いただけますでしょうか。	現時点において、本構成による折り返し通信の利用を予定している団体はありません。なお、今後の検討状況等により変更となる可能性があります。