三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務に係る意見招請
寄せられた意見と三重県の考え方

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
1	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	2　EDR 機能詳細 12項目目	【記載内容】 エージェントソフトウェアのCPU利用優先度を管理サーバ側で設定できること。 【意見】 ・必要な機能要件でないように思いますがどうでしょうか？弊社がご提案を想定している製品は、クライアントPCのCPUに負荷をかけない設計となっておりますので、機能としては必要ないと考えております。	・管理サーバ側から各クライアントに対して、（１）負荷が高いエージェントソフトウェアをクライアント側で強制的に稼働させたい時、（２）クライアント側で負荷が高い業務を実施している際に負荷が高いエージェントソフトウェアの優先度を下げるたい時、といった場合に設定を行うことを想定しています。そのため、エージェントソフトウェアにかかる負荷が十分に低い場合を想定し、記載内容を以下に変更します。 【変更内容】 エージェントソフトウェアのCPU利用優先度を管理サーバ側で設定できること。ただし、エージェントソフトウェアを導入することによるCPU負荷等への影響が軽微な場合は、不要とする。	あり
2	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	2　EDR 機能詳細 16項目目	【記載内容】 エージェントソフトウェアのインストーラーを管理サーバからダウンロードできること。 【意見】 ・弊社がご提案を想定している製品は、管理サーバからエージェントソフトウェアのインストーラを直接ダウンロードができません。ダウンロードサイトをご案内し、そこからダウンロードいただく形となりますので、機能要件のご変更をしていただけますでしょうか？	・記載内容を以下に変更します。 【変更内容】 エージェントソフトウェアのインストーラーを各端末からアクセス可能なサーバ（管理サーバ、イントラサーバ等）からダウンロードできること。	あり
3	仕様書(案)	P6 ３　事業概要 （２）業務範囲 カ　追加セキュリティ対策のサービス構成例 表　追加セキュリティ対策における必須機能 機器・機能　EDR	【記載内容】 ・被害の検知・・・エクスプロイト攻撃や攻撃時における特徴的なふるまい（IOA　Indicator Of Attack）の検知の他、感染の痕跡（IOC　Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知する。 【意見】 記載内容の削除依頼・・・「IOA Indicator Of Attack」 を削除をお願いできますでしょうか。 理由としては、OpenIOCのように、IoCについてはオープンソースとして広く公開されている規格であることに対し、IOAについては各社によって使われ方/意味合いがばらばらであり、その中身は単純なふるまい検知になります。某社では、IOAは"コードの実行、永続化、ステルス、コマンド＆コントロール、ラテラルムーブメント"を検知することと定義しておりますが、これらは元より弊社製品の検知エンジンで対応可能です。弊社製品ではあくまでオープンソース規格であるIOC内で十分に他社が定義するIOAに対応可能であり、規格の不十分なIOAという用語の意味合いもないと考えてます。	・記載内容を以下に変更します。 【変更内容】 ・被害の検知・・・収集したログを横断的に分析することで、エクスプロイト攻撃やファイルレス攻撃、攻撃時における特徴的なふるまい等による検知の他、感染の痕跡（IOC Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知する。	あり
4	仕様書(案)	P7 ３　事業概要 （２）業務範囲 カ　追加セキュリティ対策のサービス構成例 表　追加セキュリティ対策における任意機能の想定 機器・機能　SIEM	【記載内容】 ・SIEM（Security Information and Event Management）は、通常、さまざまな機器（ファイアウォール等）やソフトウェアのログを収集し、一元的に分析することで、セキュリティインシデントの検知を行うものであるが、EDRにて収集したログについても一元的に分析することで、検知機能が強化されると想定している。 ・なお、次期セキュリティクラウドにおいて、SIEMを導入予定のため、本委託業務における任意機能として求めるSIEMは、さまざまな機器やソフトウェアのログに加えてEDRのログの分析を行うことで初めて検知機能が強化されることになると考えているため、注意すること。 【意見】 ・SIEMに関してですが、今回提案させて頂く内容にSIEMは任意の機能として別提案を想定されておりますでしょうか。 ・弊社製品による提案では、次期セキュリティクラウドで導入される予定のSIEMでEDR以外の関連するセキュリティ装置（ADサーバーやUTM・ファイアウォール、プロキシなど）とのログの突合調査も対応可能とさせて頂く予定です。本内容であれば問題ございませんでしょうか。	・SIEMの定義として、単一の機器を分析するのではなく、異なる種別の機器や同種の機器でも複数台の機器から収集したログを相互に分析することと定義しています。 ・この内、本委託業務におけるEDRの機能として、「複数の端末」からログを収集し、分析を行うこととしていますが、この機能自体もSIEMと考えているため、この機能については、必須機能に含まれると考えています。 ・ただし、「複数の端末」以外の機器（例えば、セキュリティ装置やネットワーク機器等）からログを収集し、「複数の端末」から得られるログも含めて分析を行う場合は、必須機能を超えた提案要素になり、任意機能に該当すると考えています。 ・以上のことから、ご指摘の「EDR以外のログと、EDRで得られるログを突合調査」いただく場合は、任意機能に該当すると考えています。	なし
5	仕様書(案)	P8 ３　事業概要 （２）業務範囲 カ　追加セキュリティ対策のサービス構成例 表　追加セキュリティ対策における任意機能の想定 機器・機能　ITハイジーン	【記載内容】 ・ITハイジーンは、エンドポイントにおける「衛生管理」を意味し、各エンドポイントにおける、セキュリティパッチの適用状況や、マルウェア対策ソフトウェアにおけるパターンファイル等の更新状況を一元管理するとともに、対応が不十分なエンドポイントを把握するための機能や、それらの端末に対して、適正な状態にするための機能（アプリケーションの一斉配布、強制配布、未対応の端末に対する機能制限など）が提供されることで、セキュリティインシデントの未然防止につながると想定している。 ・ITハイジーンは、マルウェア対策やEDRのオプション機能として提供される場合もあれば、全く別のソフトウェアとして提供される場合もあると想定している。 【意見】 ・ITハイジーンに関してですが、任意の想定機能で必須事項ではございませんでしょうか。 ・今回提案させて頂く弊社製品では(マルウェア対策ソフトウェアにおけるパターンファイル等の更新状況)は可能ですが、それ以外の機能は持ち合わせて頂いておりません。 ・必須機能であれば他のソフトウェアと提案をさせて頂きます。	・お見込みのとおり、ITハイジーンにかかる機能については、必須機能ではなく、任意機能としています。	なし
6	仕様書(案)	P8 ３　事業概要 （２）業務範囲 キ　実績及び認証取得等 要件　認証取得	【記載内容】 ・以下のいずれかの認証を受けていることが望ましい。 　・経済産業省の情報セキュリティサービス審査登録制度の情報セキュリティサービス基準を満たす事業者であること。 　・一般社団法人情報マネジメントシステム認定センターが運用する情報セキュリティマネジメントシステム適合性評価制度（ISMS）の認証を取得していること。 　・ISO/IEC27001 又はJIS Q 27001 に基づく認証（事業部単位で認証を受けている場合は、当該事業部が本委託業務の実施体制に参画できること。） のいずれか、またはそれらと同等であると証明可能な情報セキュリティに関する規格を、本委託業務の実施組織・部門が認証取得していること。また、ISO/IEC27017に基づくISMSクラウドセキュリティ認証についても取得していることが望ましい。 　・プライバシーマーク制度の認定事業者又はこれと同等以上のISO Guide72:2001 に従った第三者適合性評価制度の認証取得事業者であること。 【意見】 ・認証取得に関してですが、ISMAPへの対応の有無(対応予定を含む)を追加お願いいたします。 ・背景としてデジタル省(内閣官房情報通信技術総合戦略室を含む)推進している、地方自治体のガバメントクラウドでのセキュリティ対策としてとISMAPの評価/登録を受けることが必須事項で進んでいるかと思われます。今後ガバメントクラウドを利用する端末のEDRに関しても ログの保管先観点で制限の対象になる可能性もございます。 ISMAPはクラウドサービスを展開するベンダーのセキュリティレベルが問題無いようであれば、どのベンダーでも登録は可能かと思われます。 ・参考資料　https://www.soumu.go.jp/main_content/000731217.pdf	・記載内容に以下の内容を追記します。 【追記内容】 　・政府情報システムのためのセキュリティ評価精度（ISMAP）による、ISMAPクラウドサービスリストに掲載されているサービスを提供できること。	あり

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
7	仕様書(案)	P10 ６　納品物件 （２）各エンドポイントにインストールするエージェントソフトウェア	【記載内容】 【提案】エージェントソフトウェアの追加購入時の単価について提案すること。 【想定】三重県が利用する、エージェントソフトウェアとして、令和4年度に9,000ライセンスを追加購入（一年分）することを想定している。また、令和5年度以降においても一年分ずつ追加購入を行う形を想定している。 【意見】 ・ライセンスの購入に関して、２つのパターンで提示することは可能にして頂くことはできますでしょうか。 ・理由としては初期に複数年契約(3年の想定)をすることによって、単価をさげることが可能であり、4年目以降も同様のディスカウント提示が可能な為、初期1年で購入の場合より単価を下げることができます。 ・以下の２つの形で提案を検討しております。 ①初期購入分(12000ライセンス)初回3年令和4年4月~令和6年3月で購入して頂き、その後1年更新を想定 ②初期購入分(12000ライセンス)初回1年:令和4年4月~令和5年3月で購入して頂き、その後1年更新	・記載内容を以下に変更します。 【変更内容】 三重県の追加購入後、三重県及び他の接続団体が、さらなる追加調達を行う場合には、同価格、又は、同価格以下にて購入が可能であること。また、ライセンスの追加調達に伴い、SOC(NOC)における利用費用の増大が見込まれるが、「３事業概要（２）業務範囲 ウ 利用者数、端末数」に記載の端末数をあらかじめ見込み、SOC(NOC)にかかる追加費用が発生しないよう、あらかじめ、本委託業務にかかる費用に見込んでおくこと。 【提案】エージェントソフトウェアにおける追加購入時の単価として、令和4年度に三重県が、9,000ライセンスを追加購入（最大60か月分）する際に提供可能な価格を提案すること。	あり
8	仕様書(案)	P19 12　業務詳細 （３）全体構成と機能要件 イ　機能要件	【記載内容】 ・SOC（NOC）が提供する各種業務の詳細や、提供される各種業務に対するSLA（サービスレベル協定 Service Level Agreement）について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル協定（案）」を参考として設計に盛り込むこと。また、毎月、本サービスレベル協定にかかる実績を管理し、報告を行うこと。なお、SLA内に減額ポイントを盛り込んだ場合で、かつ、減額ポイントの要件を満たした場合（SLAを満たせなかった場合）は、当該減額ポイントに基づき、運用保守費の減額を実施することになるため、注意すること。 ・【提案】SOC（NOC）が提供する業務内容の詳細とその業務に対するSLAについて、提案を行うこと。 【意見】 ・機能要件のSLA(サービスレベル協定 Service Level Agreement）に関して、削除いただくか、SLO（Service Level Objective)へ変更、または[SLAもしくはSLO]へ変更は可能でしょうか。 ・理由としてSOCの仕様書上SLAではなくSLOとなります。SOC現在EDR監視台数数十万台となりますが、アラート受信後の一次対応にて60分を超えて対応になってことは1度もございませんが仕様書上どうしてもSLAは設けかねます。	・記載内容を以下に変更します。 【変更内容】 ・SOC（NOC）が提供する各種業務の詳細や、提供される各種業務に対するSLA（サービスレベル協定 Service Level Agreement）、又は、SLO（サービスレベル目標 Service Level objective）について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル（案）」を参考として設計に盛り込むこと。また、毎月、本SLA、又は、SLOにかかる実績を管理し、報告を行うこと。なお、SLAとして減額ポイントを盛り込んだ場合で、かつ、減額ポイントの要件を満たした場合（SLAを満たせなかった場合）は、当該減額ポイントに基づき、運用保守費の減額を実施することになるため、注意すること。 ・【提案】SOC（NOC）が提供する業務内容の詳細とその業務に対するSLA、又は、SLOについて、提案を行うこと。なお、SLOによる提案を行う場合は、可能な限り、過去の実績値についても記載すること。 ・【想定】SLAとSLOの違いとして、SLAは目標を達成できない場合に減額が発生するが、SLOにおける目標はあくまで努力目標のため目標を達成できない場合でも減額は発生しない、と想定している。逆に、SLOはSLAと比較して、（達成できなくても減額等が発生しないため）目標が高くなると想定している。 ----------【関連項目】---------- ・P16「11　調達全般に関する共通要件（４）ドキュメント　表　ドキュメントの詳細 種別/提出時期　運用・保守設計書（令和4年3月末）」に記載の「・本県と受託事業者との間で締結するSLA（Service Level Agreement）についても記載すること。」を以下に変更します。 【変更内容】 ・本県と受託事業者との間で締結するSLA（Service Level Agreement）、又は、SLO（Service Level objective）についても記載すること。 ----------【関連項目】---------- ・別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル協定（案）」を「別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル（案）」に変更します。 ・また、記載注意事項を以下の内容に変更します。 ※記載注意事項 ・変更や追加した部分には、太字、下線を記載すること。 ・減額ポイントの記載については、原案どおり「なし」のままでも問題ないが、記載を行う場合は、以下の例を参考として記載すること。 例：〇〇までの時間が60分を上回った回数が、全件数の5%以上を占める場合は、次の計算式に従って「運用保守費」を減額する。 当該年度にかかる運用保守費 ＝（１－（60分を上回った件数 - 10）/全体件数）×運用保守費（年額） 運用保守費（年額）の上限は、契約額となるため、注意すること。 ・「【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件」における「3　SOC(NOC)」の内容を下回る提案も可とするが、評価が低くなるため注意すること。 ----------【関連項目】---------- ・資料4別紙1「提案書評価基準表　提案要素3　SOC（NOC）が提供するサービス内容 目次」に記載の「SOC（NOC)にかかるSLA」を「SOC（NOC)にかかるサービスレベル」に変更するとともに、同「記載依頼事項」に記載の「SOC（NOC）が担当する業務について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル協定（案）」を参考に、本委託業務で実現可能なSLAについて記載すること。」について、以下の内容に変更します。 【変更内容】 SOC（NOC）が担当する業務について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル（案）」を参考に、本委託業務で実現可能なサービスレベルについて記載すること。	あり
9	仕様書(案)	P25 12　業務詳細 （６）セキュリティインシデント対応支援業務の設計にかかる要件 ス　訓練対応	【記載内容】 ・年に1回以上、各接続団体の担当職員に対し、セキュリティインシデント発生を想定した対応模擬訓練を実施できること。 【意見】 ・各接続団体への訓練対応について。接続団体が複数あるため開催を1度にまとめていただくなどご検討いただきたければ幸いです。 ・SOCで提供可能なサービスにおいて、模擬訓練はメニューに含まれておりませんが、年に4回までの報告会を実施しております。その中で事前にお題をいただければ、柔軟に対応が可能となります。	・訓練は、団体数に関係なく、年1回以上開催していただく必要があります。（各団体で1回ずつではありません。ご注意ください。）	なし
10	仕様書(案)	P26 12　業務詳細 （７）セキュリティ監視等業務の設計にかかる要件 ア　基本方針	【記載内容】 ・SOCは24時間365日の有人運用とすること。また、十分に新型コロナウイルス等の感染症対策がなされており、2つ以上の拠点・フロア等に分かれた分散オペレーション体制が構築されていること。 【意見】 ・「[2つ以上の拠点・フロア等に分かれた分散オペレーション体制が構築されていること」とありますが、削除をお願いいたします。 ・SOCは同一フロア内に1つの拠点として設置しております。空気清浄機の設置や、入退室時の消毒、マスク着用、作業スペースを個人個人でパーティションで分けるなどコロナ対策は講じております。	・記載内容を以下に修正します。 【変更内容】 ・ SOCは24時間365日の有人運用とすること。また、十分に新型コロナウイルス等の感染症対策がなされており、2つ以上の拠点・フロア等に分かれた分散オペレーション体制、又は、一つのチームの影響によりサービスの全停止やサービスレベルの低下を招かない仕組み（濃厚接触者とならない仕組み）が構築されていること。	あり

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
11	仕様書(案)	P27 12　業務詳細 （７）セキュリティ監視等業務の設計にかかる要件 イ　セキュリティ監視、調査、及び、解析	【記載内容】 ・重大なセキュリティインシデントと判断してから60分以内に、受託事業者の専門技術者から当該接続団体の担当者に電話やメール等の方法により緊急連絡を実施し、担当者に対してセキュリティインシデントの内容等について、確実に伝達すること。 【意見】 ・「60分以内に、受託事業者の専門技術者から当該接続団体の担当者に電話やメール等の方法により緊急連絡を実施し、担当者に対して セキュリティインシデント の内容等について、確実に伝達すること」についてですが、[専門技術者]の削除をお願いいたします。 ・危険度「高」のアラートに対して、ご指定いただいた管理者・ご担当者へ自動音声のお電話で「危険度高のアラートを受信しました。詳細はメールをご確認くださいという内容を通知しておりますため専門技術者が架電することではありません。一方お客様からの確認等はSOCアナリストにてお電話等の対応は致しております。	・記載内容を以下の内容に変更します。 【変更内容】 ・重大なセキュリティインシデントと判断してから60分以内に、受託事業者から当該接続団体の担当者に電話やメール等の方法により緊急連絡を実施し、担当者に対してセキュリティインシデントの内容等について、確実に伝達すること。	あり
12	【別紙1】提案書評価基準表	提案要素2　追加セキュリティ対策の機能詳細（900点） 【必須機能】マルウェア対策 【必須機能】EDR	【記載内容】 マルウェア対策　対象OS等 「検知機能」「マルウェアの診断」にて記載した機能について、OS毎の利用可否を記載すること。なお、OSとして、Windows（クライアントOS,サーバOS）、Mac OS、Linuxを含めること。また、iOS、iPadOS、Androidについても記載に含めることが望ましい。 EDR　対象OS等 「検知機能」と「調査、解析機能」で示した機能について、OS毎の利用可否を記載すること。なお、OSとして、Windows（クライアントOS,サーバOS）、Mac OS、Linuxを含めること。また、iOS、iPadOS、Androidについても記載に含めることが望ましい。 【意見】 ・「また、iOS、iPadOS、Androidについても記載に含めることが望ましい」との記載がございますが、削除をお願いできますでしょうか。 ・三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務に関する仕様書（案）ではモバイル端末に対する要件が基より記載されていないこと。 また、弊社製品では、ただ単純に製品に対応したエージェントを開発をするということではなく、重要なインシデントやサイバー脅威、ランサムウェア等の脅威のほとんどがWindowsに関連していることを認識した上で製品開発を進めておりますため、モバイルデバイスへのマルウェア対策、EDRを対象として含めておりません。	・提案を求めている項目のため、記載内容の変更はなしとします。	なし
13	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	2　EDR 機能詳細 2項目目	【記載内容】 収集したログを横断的に分析することで、エクスプロイト攻撃やファイルレス攻撃、攻撃時における特徴的なふるまい（IOA　Indicator Of Attack）による検知の他、感染の痕跡（IOC　Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知できること。 【意見】 記載内容の削除依頼・・・「IOA Indicator Of Attack」 を削除をお願いできますでしょうか。 理由としては、OpenIOCのように、IoCについてはオープンソースとして広く公開されている規格であることに対し、IOAについては各社によって使われ方/意味合いがばらばらであり、その中身は単純なふるまい検知になります。某社では、IOAは"コードの実行、永続化、ステルス、コマンド＆コントロール、ラテラルムーブメント"を検知することと定義しておりますが、これらは元より弊社製品の検知エンジンで対応可能です。弊社製品ではあくまでオープンソース規格であるIOC内で十分に他社が定義するIOAに対応可能であり、規格の不十分なIOAという用語の意味合いもないと考えてます。	・記載内容を以下に変更します 【変更内容】 収集したログを横断的に分析することで、エクスプロイト攻撃やファイルレス攻撃、攻撃時における特徴的なふるまい等による検知の他、感染の痕跡（IOC　Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知できること。	あり
14	仕様書(案)	P6 ３　事業概要 （２）業務範囲 カ　追加セキュリティ対策のサービス構成例 表　追加セキュリティ対策における必須機能 機器・機能　EDR	【記載内容】 ・被害の検知・・・エクスプロイト攻撃や攻撃時における特徴的なふるまい（IOA　Indicator Of Attack）の検知の他、感染の痕跡（IOC　Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知する。 【意見】 特徴的なふるまい（IOA　Indicator Of Attack）の検知について、IOAは必須でしょうか。必須であれば、必須と記載してください。	・特徴的なふるまいによる検知は、EDRの必須機能ではありません。（マルウェア対策の必須機能ですが、IoAという記述は削除します。） ・記載内容を以下に変更します。 【変更内容】 ・被害の検知・・・収集したログを横断的に分析することで、エクスプロイト攻撃やファイルレス攻撃、攻撃時における特徴的なふるまい等による検知の他、感染の痕跡（IOC Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知する。	あり
15	仕様書(案)	P7 ３　事業概要 （２）業務範囲 カ　追加セキュリティ対策のサービス構成例 表　追加セキュリティ対策の必須機能を実現するために必要になる設備 設備　ログ収集	【記載内容】 ・各エンドポイント（業務端末）のログを収集・保管できること。 ・データセンター内、又は、SOC(NOC)等のクラウドサービス上に設置すること。 【意見】 ・弊社製品のログは基本的に端末上に保持され、有事の際のオペレーションによって、当該端末のログのみを管理サーバに収集する動作となります。 ・２つの要件が並記されているため、端末のログを”常時”データセンター内のサーバに収集して保管する必要があるようにも読み取れますが、必須機能でしょうか。	・必要に応じてログを収集することで必須機能の要件を満たす場合は、「常時」ログを管理サーバに保存する必要はありません。なお、どのような形にせよ、調査・解析を実施するために「ログ収集」を行う設備は必要になると考えています。 ・記載内容を以下に変更します。 【変更内容】 ・各エンドポイント（業務端末）のログを必要に応じて収集・保管できること。 ・データセンター内、又は、SOC(NOC)等のクラウドサービス上に設置すること。	あり
16	仕様書(案)	P.18 12　業務詳細 （２）事前調査にかかる要件 ア　各接続団体に対する追加セキュリティ対策の利用意向調査	【記載内容】 ・意向調査の結果に基づき、必要に応じて詳細ヒアリングを実施し、追加セキュリティ対策の利用範囲や端末数、導入時期（利用を開始したい時期）、ライセンスの追加調達の有無、既存のマルウェア対策の状況、今後の機器更新の変更予定、必要な連絡体制等の詳細について、確認を行うこと。 【意見】 ・導入時期をヒアリングすることは可能だと考えていますが、各市町様の要望が重複した場合は、ご要望に応えるのが困難になる旨ご認識頂ければと存じます。「確認を行うこと」との記載のため、要望を必ず満たす必要はないと考えておりますが、それでも利用開始希望を必ず満たせるわけでないため、可能であれば本記載を削除いただきたいと考えています。	・開始したい時期を調査し、調整を行う必要があると考えています。逆に、調査を実施しない場合、同時期に開始要望が来る可能性があり、調整ができなくなると考えています。 ・以上のことから、仕様書の変更はなしとします。	なし

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
17	仕様書(案)	P.19 12　業務詳細 （３）全体構成と機能要件 イ　機能要件	【記載内容】 ・SOC（NOC）が提供する各種業務の詳細や、提供される各種業務に対するSLA（サービスレベル協定 Service Level Agreement）について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル協定（案）」を参考として設計に盛り込むこと。また、毎月、本サービスレベル協定にかかる実績を管理し、報告を行うこと。なお、SLA内に減額ポイントを盛り込んだ場合で、かつ、減額ポイントの要件を満たした場合（SLAを満たせなかった場合）は、当該減額ポイントに基づき、運用保守費の減額を実施することになるため、注意すること。 【意見】 ・弊社のSOC運用においては、SLAではなくSLO(Service Level Objective)を設定しております。SLOには罰則が存在しないため、これを達成できなかったとしても運用保守費の減額を実施することはできません。 ・本案件においては、SLAを守れなかった場合の罰則が定義されているように見受けられますが、仮に本規約に則ってに罰金を請求されても支払い等の対応できませんが、ご認識相違ございませんでしょうか。	・記載内容を以下に変更します。 【変更内容】 ・SOC（NOC）が提供する各種業務の詳細や、提供される各種業務に対するSLA（サービスレベル協定 Service Level Agreement）、又は、SLO（サービスレベル目標 Service Level objective）について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル（案）」を参考として設計に盛り込むこと。また、毎月、本SLA、又は、SLOにかかる実績を管理し、報告を行うこと。なお、SLAとして減額ポイントを盛り込んだ場合で、かつ、減額ポイントの要件を満たした場合（SLAを満たせなかった場合）は、当該減額ポイントに基づき、運用保守費の減額を実施することになるため、注意すること。 ・【提案】SOC（NOC）が提供する業務内容の詳細とその業務に対するSLA、又は、SLOについて、提案を行うこと。なお、SLOによる提案を行う場合は、可能な限り、過去の実績値についても記載すること。 ・【想定】SLAとSLOの違いとして、SLAは目標を達成できない場合に減額が発生するが、SLOにおける目標はあくまで努力目標のため目標を達成できない場合でも減額は発生しない、と想定している。逆に、SLOはSLAと比較して、（達成できなくても減額等が発生しないため）目標が高くなると想定している。 ----------【関連項目】---------- ・P16「11　調達全般に関する共通要件（４）ドキュメント　表　ドキュメントの詳細 種別/提出時期　運用・保守設計書（令和4年3月末）」に記載の「・本県と受託事業者との間で締結するSLA（Service Level Agreement）についても記載すること。」を以下に変更します。 【変更内容】 ・本県と受託事業者との間で締結するSLA（Service Level Agreement）、又は、SLO（Service Level objective）についても記載すること。 ----------【関連項目】---------- ・別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル協定（案）」を「別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル（案）」に変更します。 ・また、記載注意事項を以下の内容に変更します。 ※記載注意事項 　・変更や追加した部分には、太字、下線を記載すること。 　・減額ポイントの記載については、原案どおり「なし」のままでも問題ないが、記載を行う場合は、以下の例を参考として記載すること。 　　例：〇〇までの時間が60分を上回った回数が、全件数の5%以上を占める場合は、次の計算式に従って「運用保守費」を減額する。 　　当該年度にかかる運用保守費 　　=（１－（60分を上回った件数 - 10）/全体件数）×運用保守費（年額） 　　運用保守費（年額）の上限は、契約額となるため、注意すること。 　・「【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件」における「3　SOC(NOC)」の内容を下回る提案も可とするが、評価が低くなるため注意すること。 ----------【関連項目】---------- ・資料4別紙1「提案書評価基準表　提案要素3　SOC（NOC）が提供するサービス内容 目次」に記載の「SOC（NOC)にかかるSLA」を「SOC（NOC)にかかるサービスレベル」に変更するとともに、同「記載依頼事項」に記載の「SOC（NOC）が担当する業務について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル協定（案）」を参考に、本委託業務で実現可能なSLAについて記載すること。」について、以下の内容に変更します。 【変更内容】 SOC（NOC）が担当する業務について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル（案）」を参考に、本委託業務で実現可能なサービスレベルについて記載すること。	あり
18	仕様書(案)	P.26 12　業務詳細 （７）セキュリティ監視等業務の設計にかかる要件 イ　セキュリティ監視、調査、及び、解析	【記載内容】 ・セキュリティ監視等業務における危険度の分析基準は、検知シグネチャに定義された危険度ではなく、不正な動作に対する調査、解析の結果から監視等の対象となるエンドポイントに対する影響度や不正アクセス等の成否によって4段階以上で定義し、危険度に応じた対応ができること。 【意見】 ・弊社のSOCにおいて、アラート検知に危険度を設定する想定ではありますが、「4段階以上」という文言がない方が望ましいです。	・セキュリティ監視業務において、検知したセキュリティインシデントを複数の危険度で判定する必要があると考えていますが、その目的は、判定した危険度に応じて、その後の対応を変化させる必要があると考えているためです。つまり、直ちに連絡し対応を行う必要があるか、詳細を調査してから連絡するか、翌日以降にメールで報告で良いか、等の判断基準として、危険度の判定を求めています。 ・以上のことから、仕様書の変更はなしとします。	なし
19	仕様書(案)	P.26 12　業務詳細 （７）セキュリティ監視等業務の設計にかかる要件 イ　セキュリティ監視、調査、及び、解析	【記載内容】 ・危険度の分析において、重大なセキュリティインシデント（攻撃が成功した可能性が高いまたは攻撃が成功）を判断する場合は、不正な動作に対する調査、解析結果とともに、当該エンドポイントに影響を与えない範囲において対象となる機器における脆弱性の有無を確認し最終的な判断を行えるようにすること。 【意見】 ・最終的な判断のために、脆弱性の有無を確認する必要があるとのことですが、弊社製品において脆弱性の有無を確認するためには、基本モジュールに加えて、追加モジュールを使用する必要があります。 ・したがって、脆弱性の調査に関する記載は削除いただきたいと考えております。	・重大なセキュリティインシデントが発生した場合、その調査、解析として、侵入経路の調査や被害を把握するための全端末調査、被害状況の調査などの実施を求めています。また、再発防止策として、根本解決の実施等についても求めています。この根本解決を行うために、調査の過程にて、既知の脆弱性を狙ったものである場合は脆弱性への対応が必要になると考えており、さらに、侵入経路が不明な場合であっても、ソフトウェアのバージョンアップ、パッチ当ての他、クリーンインストール等を実施することによる対応を検討する必要があると考えていることから、被害にあった端末に対する脆弱性の有無の確認は、必要な作業であると考えています。なお、全台の脆弱性を一元管理する機能は、任意機能の一つである「ITハイジーン」に該当する機能と考えています。 ・以上のことから、仕様書の変更はなしとします。	なし
20	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	1　マルウェア対策 機能詳細 2項目目	【記載内容】 Mac OS、Linuxに対してもパターンマッチング方式のスキャン機能を提供できること。 【意見】 ・弊社製品において、Mac OS、Linux共に、別途マルウェア対策ソフトが必要になる想定ですが、必須でしょうか？	・本委託業務で導入いただくマルウェア対策ソフトウェアにて、Mac OS、Linuxのパターンマッチング方式のスキャン機能の対応ができない場合は、別製品の納入を行っていただく必要があります。 ・以上のことから、仕様書の変更はなしとします。	なし

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
21	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	1　マルウェア対策 機能詳細 11～16項目目	【記載内容】 一定期間、管理サーバと通信していない対象端末の台数を管理サーバ上で確認できること。 管理サーバにより、対象端末に対して即時スキャン及びスケジュールスキャンの設定ができること。 管理サーバにより、全ての対象端末の一元管理ができること。（管理サーバの台数は問わない。） 対象端末を管理サーバ側でグルーピングして、グループごとに異なる設定を適用できること。 エージェントソフトウェアのアップグレードや設定変更について、管理サーバから実施できること。 エージェントソフトウェアのインストーラーを管理サーバからダウンロードできること。 【意見】 ・管理サーバは必須でしょうか。	・多くのマルウェア対策ソフトウェアにおいて、管理サーバによるライセンス管理機能、端末の一元管理機能、パターンファイル等の配信機能等が提供されていますが、管理サーバによらない方法にて各種機能の提供ができる場合は、管理サーバ自体は不要です。 ・なお、管理サーバによらない方法の詳細については、提案書にて説明をいただくようお願いします。 ・以上のことから、仕様書の変更はなしとします。 ・なお、「エージェントソフトウェアのアップグレードや設定変更について、管理サーバから実施できること。」「エージェントソフトウェアのインストーラーを管理サーバからダウンロードできること。」については、No2にて変更を行っていますので、ご確認ください。	なし
22	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	2　EDR 機能詳細 8項目目	【記載内容】 情報漏洩対策として、ファイル変更にかかる情報だけでなく、ファイルアクセスにかかる情報も取得できること。 【意見】 ・ファイルの書き込みだけでなく、アクセスにかかる情報の取得も必要でしょうか？通常、情報漏洩はアクセスだけで発生するものではなく、書き込みが必要です。	・記載内容を以下の内容に変更します。 【変更内容】 情報漏洩対策として、ファイル変更にかかる情報だけでなく、ファイル書き込みにかかる情報も取得できること。	あり
23	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	2　EDR 機能詳細 12項目目	【記載内容】 エージェントソフトウェアのCPU利用優先度を管理サーバ側で設定できること。 【意見】 ・弊社製品において、CPU利用優先度の設定を行う機能はありません。必須の機能でしょうか。	・管理サーバ側から各クライアントに対して、（1）負荷が高いエージェントソフトウェアをクライアント側で強制的に稼働させたい時、（2）クライアント側で負荷が高い業務を実施している際に負荷が高いエージェントソフトウェアの優先度を下げるたい時、といった場合に設定を行うことを想定しています。そのため、エージェントソフトウェアにかかる負荷が十分に低い場合を想定し、記載内容を以下に変更します。 【変更内容】 エージェントソフトウェアのCPU利用優先度を管理サーバ側で設定できること。ただし、エージェントソフトウェアを導入することによるCPU負荷等への影響が軽微な場合は、不要とする。	あり
24	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	3　SOC 機能概要	【記載内容】 マルウェア対策によるアラートを監視するとともに、EDRにより収集したログの常時監視、又は、全エンドポイントに対するログ分析等を通じて、セキュリティインシデントが発生した際に、具体的な影響の把握、当該対象端末の隔離による脅威の拡散抑止、全対象端末を対象とした被害範囲の特定、脅威除去支援および回復支援等のセキュリティ監視等業務を提供できること。 【意見】 ・「マルウェア対策によるアラートを監視」とありますが、必須機能でしょうか。マルウェア対策ソフトによる検知後、被害状況の調査等にかかる支援は実施できますが、全てのアラートを監視することは困難です。	・これまでマルウェア対策ソフトウェアによる検知後は、「LAN配線の抜去」「各団体内情報担当者、インシデント担当者への報告」「パターンファイルの最新化」「フルスキャン」を実施しており、「フルスキャン」を実施したとき、マルウェアが再検知されなければ、問題なしとしているところです。しかし、「本当に安全か不安が残る」「脆弱性対応等の根本解決につながらない」などといった課題があるため、マルウェア対策ソフトウェアによる検知があった場合、SOCによる迅速な調査、解析が必要と考えています。また、検知後は迅速な対応が必要になることから、アラートによる自動通知が望ましいと考えています。 ・以上のことから、本仕様の変更はなしとしますが、「マルウェア対策によるアラート」に代わる機能の提案も可としますので、提案書にて説明をいただくようお願いします。 （例えば、画面にマルウェアの検知情報が表示された後、発見した職員用の手順を整備し、24時間365日SOCへの電話連絡を受ける体制をもって代える、などの提案を想定しています。）	なし
25	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	3　SOC 機能詳細 4項目目	【記載内容】 危険度に応じて、接続団体毎に対応フローを策定でき、運用できること。なお、対応フローには、隔離措置時における運用管理者の承認確認や、危険度、重大度、時間帯などの条件等による、初期通知や初期対応の内容を盛り込めること。 【意見】 ・「接続団体毎に対応フローを策定」とありますが、必須機能でしょうか。単一のフローに対して、接続団体ごとに通知先を変更する形を想定していますが、問題ないでしょうか。	・本内容の詳細は、提案項目となるため、提案書にて説明をいただくようお願いします。 ・以上のことから仕様書の変更はなしとします。	なし
26	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	3　SOC 機能詳細 6項目目	【記載内容】 初期通知は、危険度の判定後60分以内の通知を目標とし、通知内容に「セキュリティインシデント概要」、「対応状況」、「対策の必要性と推奨される対策内容」を含めること。 【意見】 ・「対応状況」「対策の必要性と推奨される対策内容」については、初期通知の段階で判明していないこともあると想定していますが、必須機能でしょうか。	・記載内容を以下に変更します。 【変更内容】 初期通知は、危険度の判定後60分以内の通知を目標とし、通知内容に「セキュリティインシデント概要」、「対応状況」、「対策の必要性と推奨される対策内容」を可能な限り含めること。	あり
27	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	3　SOC 機能詳細 13項目目	【記載内容】 解析等により特定されたマルウェア等について、セキュリティ対策やEDRで駆除できなかった場合、脅威を除去するための支援ができること。このとき、マルウェア本体の除去だけでなく、侵害の痕跡を含めた完全な除去作業が可能であること。また、再発防止策等（検出された検体のファイルハッシュ値などを用いたブラックリストの登録、攻撃に用いられたC&CサーバーのURL情報や適用すべきパッチ、ソフトウェア情報の提供等）の対応ができること。 【意見】 ・「マルウェア本体の除去だけでなく、侵害の痕跡を含めた完全な除去作業が可能であること。」とありますが、脅威を除去するための支援は可能ですが、保証まではできません。完全な除去作業が必要な場合は端末のクリーンインストールを推奨いたしますが、弊社SOCでは対応できません。	・「完全な除去作業」とは、全てのマルウェアに対して再発防止策を含めて、完全な除去を保証する必要があるということではなく、マルウェアに感染したと判断された＝マルウェアが特定された＝その時点でそのマルウェアに特徴的な痕跡が把握されている、と想定しているため、その痕跡を完全に駆除するための支援をしていただくことを想定しています。（要は、再検知されないための支援を行っていただくということです。） ・また、最終的にクリーンインストールしてください、という指示になるということでも、問題ありません。 ・記載内容を以下に変更します。 【変更内容】 解析等により特定されたマルウェア等について、セキュリティ対策やEDRで駆除できなかった場合、脅威を除去するための支援ができること。このとき、マルウェア本体の除去だけでなく、侵害の痕跡を含めた除去作業について支援し、再検知されない状態にできること。また、再発防止策等（検出された検体のファイルハッシュ値などを用いたブラックリストの登録、攻撃に用いられたC&CサーバーのURL情報や適用すべきパッチ、ソフトウェア情報の提供等）の対応ができること。	あり
28	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	3　SOC 機能詳細 15項目目	【記載内容】 追加セキュリティ対策で検知したセキュリティインシデントに対する支援について、費用の追加なしに回数無制限で対応できること。 【意見】 ・検知後のファスト・フォレンジックは、回数の上限を設定することは可能でしょうか。	・回数の制限を行う場合は、これまでの同種同規模団体等における実績等から、セキュリティインシデントの発生回数を見込むなど、十分な回数を実施できるようにしてください。なお、その回数を越えたセキュリティインシデントが発生した場合でも追加料金が発生しないようにしてください。 ・以上のことから、仕様書の変更はなしとします。	なし
29	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	3　SOC 機能詳細 16項目目	【記載内容】 組織内に侵入潜伏している未検知のマルウェア等に対して、本県からの要望に応じて、月に1回以上、全端末の一斉調査（脅威ハンティング）が実施できること。 【意見】 ・弊社にて追加の脅威情報等をご準備する想定はございません。調査のためにプロセス名やハッシュ値をいただく前提であれば、実施可能です。	・お見込みのとおり、脅威情報等の提供までを求めているものではなく、こちらからの依頼による対応を求めています。 ・以上のことから、仕様書の変更はなしとします。	なし
30	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	3　SOC 機能詳細 17項目目	【記載内容】 業界団体から早期警戒情報など緊急情報を入手した際、回数無制限で脅威ハンティングが実施できること。 【意見】 ・回数について、ご相談させていただきたくことは可能でしょうか。	・回数の制限を行う場合は、これまでの実績等から、十分な回数を実施できるようにしてください。なお、その回数を越えた場合でも追加料金が発生しないようにしてください。 ・以上のことから、仕様書の変更はなしとします。	なし

No	寄せられた意見			三重県の考え方	仕様書の追記または修正有無
	書類名	ページ等	意見		
31	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	3　SOC 機能詳細 18項目目	【記載内容】 月次レポートを翌月初5営業日以内に提出すること。 【意見】 ・月次報告内容について合意させていただき、その上で提示目安を協議させていただく形でよろしいでしょうか。	・月次レポートは、仕様書「12　業務詳細　（7）セキュリティ監視等業務の設計にかかる要件　ウ　監視報告」に記載されている「全体傾向」「詳細情報」について、5営業日以内で提出いただく必要があります。 ・なお、想定している報告内容が仕様書記載の内容を超えたものである場合は、5営業日以内に提出いただく必要はありませんが、どの程度の日数で提出されるかについて、提案書にて説明をいただくようお願いします。 ・以上のことから、仕様書の変更はなしとします。	なし
32	仕様書(案)	P.28 12　業務詳細 （7）セキュリティ監視等業務の設計にかかる要件 イ　セキュリティ監視、調査、及び、解析	【記載内容】 ・【想定】セキュリティ監視による検知以外に、マルウェア対策のパターンマッチング等により検知を行った場合も、SOC において、EDR によ る検知と同様の対応を行うことを想定している。 【意見】 ・マルウェア対策のソフトウェアについては複数種類が混在することとなりますでしょうか。種別の明記を頂ければ幸いです。また、今後の利用想定として、OS付帯のアンチウイルス・ソフトウェアの管理は必要でしょうか。仮に必要であれば、「OS付帯のアンチウイルスソフト」への管理必要性の有無について、また、同一コンソールでの集中管理について明記を頂きたく願います。	・マルウェア対策ソフトウェアについては、本委託業務で導入いただくことになりますので、導入いただくマルウェア対策ソフトウェアのみの管理が本委託業務の範囲となります。 ・なお、導入したマルウェア対策ソフトウェアをSOC（NOC）で監視する際、その手段についての規定はありません。（別々の管理コンソールによる管理でも問題ありません。） ・以上のことから、仕様書の変更はなしとします。	なし
33	【仕様書 別紙】追加セキュリティ対策の必須機能にかかる詳細な機能要件	2　EDR 機能詳細 11項目目	【記載内容】 一定期間、管理サーバと通信していない対象端末の台数を管理サーバ上で確認できること。 【意見】 ・一定期間、管理サーバと通信していない対象端末の台数を即座に確認することは可能ですが、その場合何かしらの処置を求めるのであれば追記をお願い致します。	・通信していない対象端末の台数を確認後、即時の処置は求めていません。 ・以上のことから、仕様書の変更はなしとします。	なし
34	仕様書(案)	P.28 12　業務詳細 （7）セキュリティ監視等業務の設計にかかる要件 イ　セキュリティ監視、調査、及び、解析	【記載内容】 ・検知したイベントについて、月次監視報告書として取りまとめ、翌月中に報告すること。報告内容として、全体傾向（セキュリティインシデントの発生件数や推移、危険度別件数等）と詳細情報（発生したセキュリティインシデントに対する詳細情報）を含めること。 【意見】 ・発生件数が多かった際、減らすための対策は不要か。	・記載内容を以下の内容に変更します。 【変更内容】 ・検知したイベントについて、月次監視報告書として取りまとめ、翌月中に報告すること。報告内容として、全体傾向（セキュリティインシデントの発生件数や推移、危険度別件数等）と詳細情報（発生したセキュリティインシデントに対する詳細情報）を含めること。また、発生したセキュリティインシデントに対して、事前対策が可能な場合は、その対策案についても必要に応じて報告内容に含めること。	あり
35	落札候補者決定基準（案）	P4 ４．落札候補者の決定方法	【記載内容】 （２）技術評価点が600点未満。 【意見】 ・落札候補者としない要件として、「技術評価点が600点未満」と記載されていますが、600点の根拠は何でしょうか。 ・また、必須機能で0点の項目があっても、合計600点以上なら、失格にならないのでしょうか。	・落札候補者にしない要件として、全ての評価が1点の場合を想定し「600点未満」としていましたが、十分なセキュリティ対策を実現できない提案を排除するため、少なくとも全ての評価が2点以上の場合を想定し、「1,200点未満」に変更します。 ・提案内容に0点の項目があった場合（記述がなかった場合）、当該項目以外の項目においても、悪影響があると考えられること、さらに、上述の「1,200点未満」の要件と併せて失格になる可能性が高いと考えられること、などが考えられますが、0点の項目（記述がない項目）があった場合でも、評価を行うことが、よりよい審査につながると考えられるため、「0点の項目があった場合でも失格にはしない」こととします。 【変更内容】 （２）技術評価点が1,200点未満。	あり
36	【別紙1】提案書評価基準表	提案要素5 必要ライセンス数とライセンス価格 1　購入単価 評価の視点	【記載内容】 ※最大600点 【意見】 ・「最大600点」はどういう意味でしょうか。	・「※最大500点」の記載誤りです。記載内容を以下の内容に変更します。 【変更内容】 ※最大500点	あり
37	【別紙1】提案書評価基準表	提案要素5 必要ライセンス数とライセンス価格 1　購入単価 評価の視点	【記載内容】 提案されたライセンス単価を基に、以下の計算式により求めた点数を本提案要素における評価点とする。 （1-提案単価/ライセンス基準単価）×500点 ※ライセンス基準単価：1,200円/年（税抜き） ※最大600点 ※有効数字は、小数点以下1桁までを有効とし、小数点以下2桁目で四捨五入する。 【意見】 ・記載がない場合の他、ライセンス基準単価を越えた場合はどうなりますか。	・記載内容を以下の内容に変更します。 【変更内容】 提案されたライセンス価格を基に、以下の計算式により求めた点数を本提案要素における評価点とする。 （1-提案されたライセンス価格/ライセンス基準単価）×500点 ※ライセンス基準単価：1,200円/年（税抜き） ※最大500点 ※有効数字は、小数点以下1桁までを有効とし、小数点以下2桁目で四捨五入する。 ※ライセンス価格にかかる提案がない場合、本項目評価点は0点とする。 ※ライセンス基準単価を超えるライセンス価格を提案した場合は、落札候補者としないため、注意すること。	あり