三重県自治体情報セキュリティクラウド（第3期）構築及び運用・保守業務に係る意見招請の結果（寄せられた意見と三重県の考え方）

No	書類名	ページ等	意　見	三重県の考え方	修正有無	変更前	変更後
1	仕様書	p.33/ 11.業務詳細 （11）データセンターの要件 イ 設備要件	地震対策について「耐震構造の建築物であること」と記載があります。 一般的に耐震構造は建物の倒壊防止を主目的とした構造であり、地震時の揺れ自体を大きく低減するものではありません。 一方、免震構造は建物に伝わる地震動を大幅に低減できるため、サーバ等のICT機器や電源・空調設備などの精密設備への影響を抑制し、地震発生時の設備保護およびサービス継続性の向上が期待できます。 そのため、データセンターの可用性および継続運用性の観点から、免震構造の建築物についても対象とする仕様への修正を提案します。 （仕様修正案） ・建物は、震度6強の地震に対して建物の仕上げ及び設備に損傷を与えない設計(耐震構造または免震構造)の建築物であること。	ご意見を参考に修正します。	有	建物は、震度6の地震に対して建物の仕上げ及び設備に損傷を与えない設計の耐震構造の建築物であること。	建物は、震度6強の地震に対して建物の仕上げ及び設備に損傷を与えない設計(耐震構造または免震構造)の建築物であること。
2	仕様書	P.24/ 11 業務詳細 （７）運用・保守業務の設計の要件 ス　訓練対応	第2期で実施されている具体的な実施事項を追記いただくことは可能でしょうか。 ■記載例 ・対応訓練にかかる役割分担や連絡フロー等の事前検討資料の作成 ・訓練当日の連絡フロー資料の作成	ご意見を参考に記載します。	有	記載なし	インシデント発生時の連絡フローの確認等を目的とし、SOCから各接続団体に電話連絡し、ポータルサイト上で発生から完了までの連絡フローの対応を行う。1団体あたり1時間程度を想定する。
3	仕様書	P.24/ 11 業務詳細 （７）運用・保守業務の設計の要件 カ 設定変更対応	別途三重県様の指示により、設定事項の棚卸しや不要設定の整理・削除が随時発生する可能性はありますか。 ■記載例 ・設定事項の棚卸や不要設定の整理・削除内容を随時、管理資料に反映する事	ご意見を参考に記載します。	有	記載なし	設定事項の棚卸や不要設定の整理・削除内容を随時、管理資料に反映すること。
4	仕様書	P.24/ 11 業務詳細 （2）運用・保守業務の設計の要件 カ 設定変更対応	「システム更新（セキュリティパッチ適用）対応」に関して、土日祝日の取り扱いをご教示ください。	22ページ　「キ　調達した機器に対するリスク管理」24ページ　「シ　対応時間帯」に記載のとおりです。	無		
5	仕様書	P.3/ ２ 事業概要 （２）業務範囲 イ 現行（第２期）セキュリティクラウドの構成概要	「リバースプロキシ」は2期構成では存在せず、「WAF」「CDN」の機能に包含されている。その旨記載し、「リバースプロキシ」は削除する事を推奨します。	ご意見を参考に修正します。	有	リバースプロキシ・接続団体の公開Webサーバに対するインターネットからのアクセスを統合し、公開Webの代理としてインターネットとの通信を行う機器	削除
6	仕様書	P.7/ ２ 事業概要 （３）受託要件 ウ NOC 及びSOC	「5年以上の国内外でのリモート監視オペレーションの実績を有すること。」 2期仕様の10年から5年に変更されています。NOC及びSOCの品質低下に影響する事や、セキュリティクラウドの事業は3期目であり、各NOC及びSOC事業者も経験年数を積んでいる事から、10年の記載に戻す事を推奨します。	5年以上で一定の品質は確保できていると思われることから、見直しは行いません。	無		
7	仕様書	P.7/ ２ 事業概要 （３）受託要件 ウ NOC 及びSOC	「自治体を含む、100社・団体程度の監視運用実績を有すること。」の記載が2期仕様から削除されています。 No.6同様にNOC及びSOCの品質低下に影響する事や、セキュリティクラウドの事業は3期目であり、各NOC及びSOC事業者も経験年数を積んでいる事から、10年の記載に戻す事を推奨します。	ご意見を参考に記載します。	有	記載なし	自治体を含む、100社・団体以上の監視運用実績を有すること。
8	仕様書	P.20/ 11 業務詳細 （７）運用・保守業務の設計の要件 ア 基本方針	「NOCは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できること。」の記載が2期仕様から削除されています。コロナ終息後ではありますが、同様のパンデミックはいつ発生するかわからない為、上記記載の再掲載を推奨します。	見直しは行いません。	無		
9	仕様書	P.20/ 11 業務詳細 （７）運用・保守業務の設計の要件 ウ ポータルサイト	「障害発生時等、接続団体からセキュリティクラウドを利用できない場合を想定し、セキュリティクラウド以外からのアクセス方法も用意すること。」の記載が2期仕様から削除されています。ポータルサイトへのアクセス可用性を考慮すると、上記記載の再掲載を推奨します。	ご意見を参考に記載します。	有	記載なし	障害発生時等、接続団体からセキュリティクラウドを利用できない場合を想定し、セキュリティクラウド以外からのアクセス方法も用意すること。
10	仕様書	P.22/ 11 業務詳細 （７）運用・保守業務の設計の要件 カ 設定変更対応	「権威DNS情報の変更」項目が追加されています。本業務について、ドメイン種別によって、県市町と契約しているドメイン事業者、もしくはJ-LISが管理している為、そこへ依頼する事となる。尚、上記の通り、県市町ごとやドメインの種別によって依頼先が異なる為、注意する事。	ご意見を参考に修正します。	有	権威DNS情報の変更	権威DNS情報の変更（接続団体ごとやドメインの種別によって依頼先が異なる）

三重県自治体情報セキュリティクラウド（第3期）構築及び運用・保守業務に係る意見招請の結果（寄せられた意見と三重県の考え方）

No	書類名	ページ等	意　見	三重県の考え方	修正有無	変更前	変更後
11	仕様書	P.22/ 11 業務詳細 （７）運用・保守業務の設計の要件 カ 設定変更対応	「WAF機能におけるホワイトリスト対応やSSL証明書更新作業」が追記されています。今後の更新期限短縮に向けて、証明書については自動更新機能を利用する旨の記載を推奨します。	別紙「次期（第３期）自治体情報セキュリティクラウド要件シート」 No14,15に記載しています。	無		
12	仕様書	P.23/ 11 業務詳細 （７）運用・保守業務の設計の要件 ケ 定例報告	「対面またはWEB会議・・・」との記載がありますが、2期仕様では原則対面との記載となっている、お客様との円滑なコミュニケーション等を考慮すると、原則対面の記載に戻す事を推奨します。	見直しは行いません。	無		
13	仕様書	P.23/ 11 業務詳細 （７）運用・保守業務の設計の要件 ケ 定例報告	「なお、日程調整等は、本県が実施する。」が2期仕様から削除されています。日程調整は本案件の受託事業者が実施する事を想定されていますか。その場合、その旨を記載する事を推奨します。	ご意見を参考に記載します。	有	記載なし	なお、日程調整は受託事業者が実施すること。
14	仕様書	P.24/ 11 業務詳細 （７）運用・保守業務の設計の要件 サ 職員研修対応	No.12同様「対面またはWEB会議・・・」との記載がありますが、2期仕様では原則対面との記載となっている、お客様との円滑なコミュニケーション等を考慮すると、原則対面の記載に戻す事を推奨します。	見直しは行いません。	無		
15	仕様書	P.24/ 11 業務詳細 （８）セキュリティ監視等業務の設計の要件 ア 基本方針	No.8同様「SOCは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できること。」の記載が2期仕様から削除されています。コロナ終息後ではありますが、同様のパンデミックはいつ発生するかわからない為、上記記載の再掲載を推奨します。	見直しは行いません。	無		
16	仕様書	P.25/ 11 業務詳細 （８）セキュリティ監視等業務の設計の要件 イ SOC の詳細	「本県と同規模程度の組織に対するセキュリティ監視等業務の経験を5 年以上持つこと。」 2期仕様の10年から5年に変更されています。NOC及びSOCの品質低下に影響する事や、セキュリティクラウドの事業は3期目であり、各NOC及びSOC事業者も経験年数を積んでいる事から、10年の記載に戻す事を推奨します。	見直しは行いません。	無		
17	仕様書	P.25/ 11 業務詳細 （８）セキュリティ監視等業務の設計の要件 ウ セキュリティ監視等の詳細	・EDRの監視運用業務の追記をお願いします。	ご意見を参考に修正します。	有	Webサーバ、メールリレーサーバ、プロキシサーバ、外部DNSサーバ等、主にセキュリティクラウドとインターネット間における通信を、セキュリティ監視等（監視、調査、解析）の対象とすること。具体的には、ファイアウォール、IDS/IPS、マルウェア対策、通信の復号対応、URLフィルタ、アンチウィルス/スパム対策、振る舞い検知機能、WAF、CDN等の各機能に対する監視を行うこと。	Webサーバ、メールリレーサーバ、プロキシサーバ、外部DNSサーバ等、主にセキュリティクラウドとインターネット間における通信及び利用者PCを、セキュリティ監視等（監視、調査、解析）の対象とすること。具体的には、ファイアウォール、IDS/IPS、マルウェア対策、通信の復号対応、URLフィルタ、アンチウィルス/スパム対策、振る舞い検知機能、WAF、CDN、EDR、マルウェア対策等の各機能に対する監視を行うこと。
18	仕様書	P.25/ 11 業務詳細 （８）セキュリティ監視等業務の設計の要件 オ 監視報告	「・ セキュリティ監視等業務における、インシデント発生時における詳細情報の情報共有を行うため、専用Webポータルを受託事業者側で用意することが望ましい。なお、専用Webポータルの認証は、セキュリティ維持のためワンタイムパスワード等の多要素認証とすること。 ・ 専用Webポータルを用意しない場合は、別途、遅滞なく情報共有ができる仕組みを用意すること。」が2期仕様から削除されています。現行のSOC運用を考慮すると、要件は必須の為、再掲載を推奨します。	11 業務詳細（７）運用・保守業務の設計の要件　ウ　ポータルサイトに記載します。	有	記載なし	セキュリティ監視等業務における、インシデント発生時の詳細情報の情報共有を行える機能を有すること。
19	仕様書	P.17/ 11.業務詳細 （４）三重県情報ネットワークとの接続設計の要件	回線サービスの提供方法の精査および見積作成のため、下記2点の情報についてご教示をお願い致します。 ・現行三重県情報セキュリティクラウドのネットワーク構成が分かる資料（物理構成およびVLAN等の論理構成等が分かる資料）。 ・三重県情報ネットワークと情報セキュリティクラウドを接続するために必要となる情報（スイッチを設置するためのラック情報、アクセスポイントとの物理結線や構内配線方法、VLAN方式や冗長化方式、ケーブル手配等を含めた責任分界点など）を確認およびご相談させていただくためのご連絡先、および各種見積のご依頼先。	左記資料は、公告後、競争入札参加資格確認申請により有資格者と確認され、守秘義務に関する誓約書を提出した場合に開示します。	無		

三重県自治体情報セキュリティクラウド（第3期）構築及び運用・保守業務に係る意見招請の結果（寄せられた意見と三重県の考え方）

No	書類名	ページ等	意　見	三重県の考え方	修正有無	変更前	変更後
20	仕様書	p.20/ 11.業務詳細 （７）運用・保守業務の設計の要件 ア 基本方針	「NOC の所在地は、県内を原則とするが、現地対応が必要な保守要員以外の要員（問い合わせ対応、遠隔での対応が可能な業務を行う要員）が勤務するNOCは、県外、かつ、複数拠点設置も可とする。ただし、少なくとも1 拠点は県内へ設置すること。」と記載がございますが、現地対応が必要な保守要員が勤務するNOCが三重県内に設置していればよいという解釈でよろしいでしょうか。	お見込みのとおりです。	無		
21	仕様書	p.29/ 11.業務詳細 （９）利用サービスの詳細の要件 イ 機能要件	WAF/CDNについて、見積積算上必要な情報のため、全サイト分の利用帯域(byte)及び通信量(byte)の情報をご教示お願い致します。	ご意見を参考に以下を修正します。 11 業務詳細(9) ウ	有	CDNは、接続団体数×2（公式Webサイト、防災サイト）に加えて、20サイト程度が利用できること。また、転送量によらず、固定料金での提供が可能であること。また、WAFやDDoS対策についても、同数のサイトに対応が可能なこと。	WAFやCDN、DDoS対策は、接続団体数×2（公式Webサイト、防災サイト）に加えて、20サイト程度が利用できること。WAFやCDN、DDoS対策は、利用帯域や通信量の増減に関わらず、本業務の範囲内とする。なお、2026年1月の1か月あたりの通信量は21TB(テラバイト)程度、利用帯域は平均65Mbps程度、95パーセンタイル（P95）115Mbps程度である。
22	仕様書	p.36/ 11.業務詳細 （16）契約終了時の要件	「データの抹消作業は、三重県が指定する場所で行うこと」と記載がございますが、 クラウドサービス及び共有機器にてご提供させて頂く機能もございますため「サービス提供型の場合を除く」という補足を追記、サービス提供型の場合は「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群」に準拠した方法で消去することとし、各機能毎の消去方法につきましては協議の上で決定させて頂きたく存じます。 (仕様書案) サービス提供型の場合は「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群」に準拠した方法で消去すること。	ご意見を参考に記載します。	有	記載なし	クラウドサービスなどサービス提供型の場合は、暗号化消去など論理的消去により復元不可能な状態にすること。
23	別紙_次期（第３期）自治体情報セキュリティクラウド要件シート	2 / 3 ページ No.14 インシデントの予防 Webサーバセキュリティ対策 ①WAF	「・Webサーバ用の証明書発行が出来ること。」と記載がございますが、WAF側に適用する証明書のことを指しているという解釈でよろしいでしょうか。	お見込みのとおりです。	無		
24	別紙_マルウェア対策およびEDRの機能要件	P.2/ 3　SOC(NOC)_機能詳細	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。 --- 上記記載について、対応フローは接続団体様共通のフローを想定しています。接続団体様毎に対応フローを必要とされる理由・背景を伺えますと幸いです。ご回答踏まえ対応可否について改めて検討いたします。 また、隔離措置時における運用管理者様の承認確認については、スピーディな対応を目的に行わず即時遮断を想定します。（遮断NG端末は事前に遮断対象外リストに登録いただく運用を想定）	同じ危険度でも接続団体毎または対象端末毎に、隔離措置後に電話やメールで連絡する場合もあれば、隔離措置までは実施せずに電話やメールで確認後に隔離措置を実施する場合があると想定します。ご意見を参考に修正します。	有	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。	危険度に応じて、接続団体毎または対象端末毎に対応フローを策定でき、運用できること。
25	別紙_マルウェア対策およびEDRの機能要件	P.2/ 3　SOC(NOC)_機能詳細	「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」に関して、「・また詳細調査・フォレンジックは本調達の範囲外とする。」の追記をお願いします。	ご意見を参考に記載します。	有	記載なし	フォレンジックなどの詳細調査は本業務の範囲外とする。
26	別紙_マルウェア対策およびEDRの機能要件	P.2/ 3　SOC(NOC)_機能詳細	「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。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。」に関して、「・また詳細調査・フォレンジックは本調達の範囲外とする。」の追記をお願いします。	ご意見を参考に記載します。	有	記載なし	フォレンジックなどの詳細調査は本業務の範囲外とする。
27	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能概要 2 EDR/機能概要 （1/3,2/3,3/3）	追加要件として意見します。 昨年、ランサムウェア被害を受けられたアスクル様が公表されている攻撃の内容にもありますが、攻撃に業務委託先アカウント（正規アカウント）を利用されています。このように攻撃手法が年々、進化していることから、契約期間中にエンドポイントセキュリティに関し、別途対策が必要となる場合があると考えます。正規アカウントを利用する攻撃手法に対応するソリューション等が必要になる場合を想定しています。その場合、導入に掛かる工数や、費用を考慮し、要件には以下が必要と考えます。 『契約期間中に別途セキュリティ対策が必要となった場合の拡張性を考慮し、ランサムウェア対策・EDRに追加するエージェントが必要なく、機能を追加できること。』	ご意見を参考に記載します。	有	記載なし	契約期間中に別途セキュリティ対策が必要となった場合、ランサムウェア対策やMDRなどの機能をEDRに追加できる拡張性があること。

三重県自治体情報セキュリティクラウド（第3期）構築及び運用・保守業務に係る意見招請の結果（寄せられた意見と三重県の考え方）

No	書類名	ページ等	意　見	三重県の考え方	修正有無	変更前	変更後
28	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『パターンファイルやシグネチャ等のパターンマッチング方式に加えて、ふるまい検知（脆弱性を突いた不審な動作を検知）やサンドボックス等の機械学習方式により、マルウェアの検知ができること。』について意見します。 パターンファイルやシグネチャ等のパターンマッチング方式が前提となっていますが、それらの検知手法には管理サーバが必要になります。管理サーバを設置することによる運用負荷や脆弱性の対策が必要になる為、管理サーバや、パターンファイルを有することを前提とするものではなく、SaaS型で管理サーバが不要であり、パターンマッチング方式ではないソリューションの提案も受け入れるようにして頂けないでしょうか。クライアント端末では、シグネチャファイルによるネットワーク負荷、リアルタイムスキャン、定期スキャンによる端末負荷と、インストールやアップデートに伴う再起動による運用負荷が発生します。それらの負荷を考慮し、最近のエンドポイントセキュリティ対策の仕様書では、シグネチャの配信をしない「クラウドサービス（SaaS）型のシステムであること。」と要件に書かれている県庁様もあります。	ご意見を参考に修正します。	有	パターンファイルやシグネチャ等のパターンマッチング方式に加えて、ふるまい検知（脆弱性を突いた不審な動作を検知）やサンドボックス等の機械学習方式により、マルウェアの検知ができること。	パターンマッチング方式、AI（機械学習）、ふるまい検知（脆弱性を突いた不審な動作を検知）、サンドボックス等の方式により、既知及び未知のマルウェアの検知ができること。
29	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『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。』について意見します。 パターンファイルやシグネチャ等のパターンマッチング方式が前提となっていますが、それらの検知手法には管理サーバが必要になります。管理サーバを設置することによる運用負荷や脆弱性の対策が必要になる為、管理サーバや、パターンファイルを有することを前提とするものではなく、SaaS型で管理サーバが不要であり、パターンマッチング方式ではないソリューションの提案も受け入れるようにして頂けないでしょうか。	ご意見を参考に修正します。	有	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。	Mac OS、Linuxに対しても、パターンマッチング方式、AI（機械学習）、ふるまい検知（脆弱性を突いた不審な動作を検知）、サンドボックス等の方式により、既知及び未知のマルウェアの検知ができること。
30	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『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。』について意見します。 管理サーバを設置することによる運用負荷や脆弱性の対策が必要になる為、管理サーバや、パターンファイルを有することを前提とするものではなく、SaaS型で管理サーバが不要であり、パターンマッチング方式ではないソリューションの提案も受け入れるようにして頂けないでしょうか。管理サーバではなく、『ダッシュボード上で確認できること』も可としてください。	ご意見を参考に修正します。	有	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。	一定期間、通信していない対象端末の台数を管理サーバまたはダッシュボードなどで確認できること。
31	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『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。』について意見します。 管理サーバを設置することによる運用負荷や脆弱性の対策が必要になる為、管理サーバや、パターンファイルを有することを前提とするものではなく、SaaS型で管理サーバが不要であり、パターンマッチング方式ではないソリューションの提案も受け入れるようにして頂けないでしょうか。SaaS型ソリューションの場合、コンソール上で設定が可能です。	ご意見を参考に修正します。	有	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。	管理サーバまたはコンソールにより、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。
32	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『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。）』について意見します。 管理サーバを設置することによる運用負荷や脆弱性の対策が必要になる為、管理サーバや、パターンファイルを有することを前提とするものではなく、SaaS型で管理サーバが不要であり、パターンマッチング方式ではないソリューションの提案も受け入れるようにして頂けないでしょうか。SaaS型ソリューションの場合、コンソール上で管理が可能です。	ご意見を参考に修正します。	有	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。）	管理サーバまたはコンソールにより、全ての対象端末の一元管理ができること。
33	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『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。』について意見します。 管理サーバを設置することによる運用負荷や脆弱性の対策が必要になる為、管理サーバや、パターンファイルを有することを前提とするものではなく、SaaS型で管理サーバが不要であり、パターンマッチング方式ではないソリューションの提案も受け入れるようにして頂けないでしょうか。SaaS型ソリューションの場合、コンソール上で設定が可能です。	ご意見を参考に修正します。	有	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。	対象端末を管理サーバまたはコンソール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。
34	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『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。』について意見します。 管理サーバを設置することによる運用負荷や脆弱性の対策が必要になる為、管理サーバや、パターンファイルを有することを前提とするものではなく、SaaS型で管理サーバが不要であり、パターンマッチング方式ではないソリューションの提案も受け入れるようにして頂けないでしょうか。SaaS型ソリューションの場合、コンソール上で設定が可能です。その際、端末の再起動は不要です。	ご意見を参考に修正します。	有	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アップグレードや設定変更について、管理サーバまたはコンソールから実施できること。
35	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『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。』について意見します。 管理サーバを設置することによる運用負荷や脆弱性の対策が必要になる為、管理サーバや、パターンファイルを有することを前提とするものではなく、SaaS型で管理サーバが不要であり、パターンマッチング方式ではないソリューションの提案も受け入れるようにして頂けないでしょうか。SaaS型ソリューションの場合、コンソール上からダウンロードが可能です。	ご意見を参考に修正します。	有	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。	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またはコンソールからダウンロードできること。
36	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 (1/3)	『パターンファイルやシグネチャ等のパターンマッチング方式に加えて、ふるまい検知（脆弱性を突いた不審な動作を検知）やサンドボックス等の機械学習方式により、マルウェアの検知ができること。』について意見します。 機械学習では検知できない攻撃への対策として、脅威ハンティングが必要と考えます。例えば、ゼロディ攻撃に対しての対策です。脅威ハンティングを採用することにより、より強固なセキュリティ対策が実現できます。従いまして、要件には以下が必要と考えます。 『24時間365日、専門家による脅威ハンティングを提供すること。』	別紙「マルウェア対策及びEDRの機能要件」3　SOC(NOC)　機能詳細に記載しています。	無		

三重県自治体情報セキュリティクラウド（第3期）構築及び運用・保守業務に係る意見招請の結果（寄せられた意見と三重県の考え方）

No	書類名	ページ等	意　見	三重県の考え方	修正有無	変更前	変更後
37	別紙_マルウェア対策およびEDRの機能要件	3 SOC(NOC)機能詳細 (2/3)	『危険度は4段階（0～3）以上で定義し、危険度に応じた対応ができること。』について意見します。 危険度が低いものであっても調査・対応することで、攻撃が深刻化する前に防御することができると考えます。従いまして、要件には以下が必要と考えます。 『危険度に関わらず、全ての攻撃に対し調査・対応ができること。』	ご意見を参考に修正します。	有	危険度は4段階（0～3）以上で定義し、危険度に応じた対応ができること。	危険度は4段階（0～3）以上で定義し、危険度に応じた対応ができること。また、危険度に関わらず、全ての攻撃に対し調査・対応ができること。
38	別紙_マルウェア対策およびEDRの機能要件	3 SOC(NOC)機能詳細 (3/3)	『初期対応として、判定された危険度に応じて、脅威（検体）や被疑端末の隔離等の措置が60分以内に可能なこと。』について意見します。 自動隔離の設定で多くのソリューションが実現可能になると考えます。しかし、自動隔離をしてしまうと誤検知の場合、利用者の業務の妨げになると考えます。隔離までを対応範囲とするのではなく、侵害を止めるためには、隔離だけではなく端末の修復までが必要ですが、それを60分以内とするのは難しいケースが多いと想像します。対応についての早さを求められるのであれば、SOCを提供する各社に、これまでの実績ベースで、平均修復時間（MTTR）を提示させる、または指定してはいかがでしょうか。 『昨年度、あるいは一昨年度における実績ベースの平均修復時間（MTTR）が60分以内であること（SLAではない）。修復とは、自動修復、自動隔離ではなく、脅威を取り除く為の調査、対応作業を実施し、安全に端末を運用できる状態にすることと定義する』	ご意見を参考に、数字を修正し目標としたうえで記載します。	有	記載なし	平均修復時間（MTTR）は危険度の判定後240分以内を目標とし、脅威を取り除く為の調査、対応作業を実施し、安全に端末を運用できる状態にすること。
39	別紙_マルウェア対策およびEDRの機能要件	3 SOC(NOC)機能詳細 (3/3)	『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。』について意見します。 従来は、多くのSOCベンダーが「通知」のSLAを示していますが、通知することより、対応・修復を優先してはいかがでしょうか。実績ベースで、平均修復時間（MTTR）を提示させる、または指定することをお勧めします。	ご意見を参考に、数字を修正し目標としたうえで記載します。	有	記載なし	平均修復時間（MTTR）は危険度の判定後240分以内を目標とし、脅威を取り除く為の調査、対応作業を実施し、安全に端末を運用できる状態にすること。
40	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 2 EDR/機能詳細	追加要件として意見します。 以下のセキュリティの国際機関の公開情報（以下URL）に記載の通り、攻撃者はグローバルで176グループ存在します。（これ以上存在すると言われています） https://attack.mitre.org/groups/ ランサムウェア対策やEDRを提供するメーカーは脅威インテリジェンスを有していることが必須と考えます。攻撃グループを追跡し、その攻撃手法が検知判断に入っていることで、最新の脅威にも対応できると考えます。 従いまして、要件には以下が必要と考えます。 『最低170グループ以上の攻撃グループを追跡し、脅威インテリジェンスを有していること、且つ、その情報を検知エンジンに取り込んでいること。』	見直しは行いません。	無		
41	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 2 EDR/機能詳細	追加要件として意見します。 昨今のランサム被害の報道でもありましたが、EDRを止めるという攻撃が存在します。また、カーネル上で動くマルウェアも存在します。それらを考慮し、要件には以下が必要と考えます。 『マルウェア対策及びEDRはカーネルモードで動作すること。』	ご意見を参考に記載します。	有	記載なし	マルウェア対策はカーネルモードで動作すること。 EDRはカーネルモードで動作すること。
42	別紙_マルウェア対策およびEDRの機能要件	2 EDR/機能詳細	追加要件として意見します。 対象の全端末にランサムウェア対策及びEDRが導入されていることが望ましいですが、未導入の端末から侵害されるケースが発生すると想定されます。従いまして、要件には以下が必要と考えます。 『セキュリティ対策ソフトウェアが導入されていない端末からの侵害を、導入されている端末で検知した場合、未管理端末を特定し通知が可能であること。』	ご意見を参考に記載します。	有	記載なし	セキュリティ対策ソフトウェアが導入されていない端末からの侵害を、導入されている端末で検知した場合、未管理端末を特定することが可能であること。
43	別紙_マルウェア対策およびEDRの機能要件	1 マルウェア対策/機能詳細 2 EDR/機能詳細	追加要件として意見します。 SaaS提供の場合は、端末とクラウド側の通信におけるセッション数は、1～2にすることで、Proxy経由で通信させる場合でも、ネットワーク負荷を抑えることが可能です。従いまして、SaaS提供の場合は、要件に以下が必要と考えます。 『SaaS提供の場合は、端末とクラウド側の通信におけるセッション数は、端末１台あたり、通常1セッション、最大2セッションであること。』	見直しは行いません。	無		