三重県自治体情報セキュリティクラウド（令和3年度）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(案)	P27 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 イ　SOCの詳細	【記載内容】 ・分析結果の内容について、24時間365日技術的な問合せについて対応できること。また、不正アクセス等の内容について詳細に説明できる技術者を24時間体制で常駐させること。 【意見】 ・「不正アクセス等の内容を詳細に説明できる技術者」の常駐について記載がありますが、問い合わせ対応できる人材が常駐したうえで、連絡できる体制をとる形では不十分でしょうか。	・記載内容を以下に変更します 【変更内容】 ・分析結果の内容について、24時間365日技術的な問合せについて対応できること。また、不正アクセス等の内容について詳細に説明できる技術者と24時間体制で連絡がとれること。	あり
2	仕様書(案)	P29 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 エ　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、不正な通信に対する調査、解析の結果から監視等の対象となる機器やネットワーク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。以下、例を記述する。 【意見】 ・「4段階以上で定義し」とありますが、3段階の定義で十分な対応が可能と考えています。4段階が必須の場合、どのような意図があるか確認させてください。	・P29における危険度0と危険度1について、一つの危険度にまとめることは問題ありません。ただし、危険度2と危険度3については、SOC側での攻撃成否確認をしていただくための要件として設定しているため、分類を行っていただく必要があると考えています。 ・以上のことから、記載内容を以下に変更します。 【変更内容】 ・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、不正な通信に対する調査、解析の結果から監視等の対象となる機器やネットワーク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。なお、3段階での定義も可とするが、以下の例に示す危険度2と危険度3について、分類可能とすること。以下、例を記述する。	あり
3	仕様書(案)	P25 11　業務詳細 （７）運用・保守業務の設計にかかる要件 コ　セキュリティ監視業務にかかる対応	【記載内容】 ・その他、被害状況の確認や、既存ネットワークや既存システムにかかる受託事業者への説明、根本的な対応策にかかる提案や根本対応等の実施にかかる支援まで、各接続団体からの要望に応じて、対応できること。 【意見】 ・セキュリティクラウド責任分解点を超える、接続団体既存NW・システムに関する対応に関しては、SCログ分析から想定される範囲にて「受託事業者への説明、根本的な対応策にかかる提案」は実施可能ですが、接続団体側システムのフォレンジックや根本対処等の作業は見込んでいないため、「根本対応等の実施にかかる支援」は削除頂くか、その前提での補足（「SCログ分析範囲での情報提供など」等）を記載いただけないでしょうか。	・「根本的な対応策にかかる提案や根本対応等の実施にかかる支援まで」と記載がありますが、あくまで支援であり、対処は必要ありません。 ・現行セキュリティクラウドにおける運用時の反省を含めて、これまで本県担当職員が実施していた業務を実施する目的で記載しています。 ・以上のことから、仕様の変更はなしとします。	なし
4	仕様書(案)	P27 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 イ　SOCの詳細	【記載内容】 ・セキュリティ監視等を専門とする技術者は、情報セキュリティ監視に関する十分な専門知識を有し、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10年以上持つこと。 【意見】 ・経済産業省の情報セキュリティサービス基準適合認定(セキュリティ監視・運用サービス)の審査基準では、技術者の知識・経験（10年以上実績）は認定要件となっている為、本項は経産省認定を満たしていない場合の対応項目と考えられます。 ・認定を前提とする場合は、本項を削除して良いかと考えます。 [参考]情報セキュリティサービス基準⇒P6（1）ア（ウ） <https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf>	・情報セキュリティサービス基準の記載と矛盾しないため、仕様の変更はなしとします。	なし
5	仕様書(案)	P27 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 イ　SOCの詳細	（質問事項重複のため、削除）	–	
6	仕様書(案)	P27 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 ウ　セキュリティ監視等の詳細	【記載内容】 ・ セキュリティ監視等（監視、調査、解析）の対象として、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。 【意見】 ・WAFシグネチャは原則ブロック設定であり、「攻撃検知」＝「防御できている」となる為、リアルタイム分析対象の必要性は無いのではと考えます。 ・一方、Proxyサーバログは、昨今のマルウェア感染フローにおいても監視上非常に重要なログの為（大半がブランジング通信を介する）、24時間365日の「リアルタイム監視」対象として追加すべきと考えます。	・本要件にて、セキュリティ監視等の対象として、機器や機能を例示していますが、詳細な対応方法については、設計段階で決定するものと考えています。 ・お見込みのとおり、さまざまな監視方法（リアルタイムによるログ分析、UTMによる監視、SOCによる監視など）があるため、トータルとして、十分なセキュリティ対策が維持できる構成としてください。なお、設計内容については、本県に説明のうえ、承認を得る必要がありますので、ご注意ください。 ・以上のことから、仕様の変更はなしとします。	なし
7	仕様書(案)	P27 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 ウ　セキュリティ監視等の詳細	【記載内容】 ・セキュリティ監視等の対象となる機器の検知ポリシーは、日常的なセキュリティ監視等業務において能動的に見直しを行い、変更がある場合は、その内容を本県の担当者に報告すること。また、検知ポリシーはセキュリティ監視等における対象機器の検知精度を向上させるため、検知及び分析結果をもとに検討を実施し、変更がある場合は、その内容を本県の担当者に報告すること。 ・検知ポリシーの変更等について、本県の担当者より受託事業者に対して要請があった場合、専門の技術者にて受け付ける体制をとれること。 【意見】 相関分析機器（SIEM）の検知ポリシーは、弊社側で有効性等の観点から見直しを実施していますが、弊社仕様上その内容はユーザに開示するものではありません。 2点目の「県担当者への報告」、および3点目の記載を削除頂けないでしょうか。	・記載内容を以下に変更します 【変更内容】 ・セキュリティ監視等の対象となる機器の検知ポリシーは、日常的なセキュリティ監視等業務において能動的に見直しを行うこと。また、検知ポリシーはセキュリティ監視等における対象機器の検知精度を向上させるため、検知及び分析結果をもとに検討を実施すること。 ・検知ポリシーにおける変更等について、本県の担当者からの照会があった場合、その運用方法等の概要を説明できること。	あり
8	仕様書(案)	P28 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 エ　セキュリティ監視、調査、及び、解析 表　不正な通信を検知した際の対応方針	【記載内容】 〇不正な通信の種別 不審な通信またはマルウェアへの感染・活動等及びその兆候を検知した場合 〇対応 ・速やかに不審な通信等か否かを解析すること。 ・不審な通信等であると判断した場合は、各接続団体における担当者に報告するとともに、該当端末利用者等に対する対処方法についても報告すること。 【意見】 ・GW機器のログ監視分析を実施するため、外部⇔内部の通信から不審な兆候を検知します。表の1行目は、外部⇔内部いずれかの通信方向から検知される場合なので、記載は不要かと考えます。	・マルウェアに対する記載であり、他の要件と矛盾しないため、仕様の変更はなしとします。	なし
9	仕様書(案)	P29 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 エ　セキュリティ監視、調査、及び、解析	（質問事項重複のため、削除）	ー	

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		
10	仕様書(案)	P29 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 エ　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15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またはメールにて緊急連絡を行うこと。また、セキュリティインシデント発生元の特定が可能であり、かつ、その端末が接続団体内の端末と判断できる場合は、可能な範囲で端末を特定した上で電話またはメールにて報告すること。 【意見】 ・通知は、危険度判断後15分以内を目標としているものの、より的確なポイントを絞った通知とするため、XFFでの端末特定などに時間を有する可能性があります。 15分目途／目標等の記述として頂けないでしょうか。	・「重大なセキュリティインシデントと判断」されるのは、攻撃が成功しているなど、調査よりも報告が優先される場合と想定しているため、「判断」がなされてからの第一報は、15分以内のままとします。なお、調査に時間を要する場合は、第一報時にその旨を告げていただき、その後、第二報以降にて、詳細な調査結果にかかる報告を行っていただくことを想定しています。 ・なお、別の質問（No55）により、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15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、担当者に対してインシデントの内容等について、確実に伝達すること。また、セキュリティインシデント発生元の特定が可能であり、かつ、その端末が接続団体内の端末と判断できる場合は、可能な範囲で端末を特定した上で電話やメール等の方法により、報告すること。	あり
11	仕様書(案)	P30 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 オ　監視報告 表　月例監視報告書の詳細	【記載内容】 〇項目名 ・全体傾向 〇詳細 ・受託事業者監視センターの全体にて確認した不正アクセス件数推移、危険度別件数 〇項目名 ・個別傾向 〇詳細 ・不正アクセス件数推移、危険度別件数、上位検知シグネチャ、担当者・受託事業者間の連絡、対応履歴 【意見】 ・弊社月次レポートでは、民需ユーザ含めたセンター全体の「全体傾向」は意義あるものと考えておらず、記載していません。（複数県SC運用監視を踏まえたプロアクティブな運用は実施想定です） 月例監視報告書の記載から、「全体傾向」を削除頂くか、例として頂けないでしょうか。	・「全体傾向」は三重県自治体情報セキュリティクラウド全体を、「個別傾向」は各接続団体を、「詳細情報」は個々のインシデント等について記載するものとします。 ・以上のことから、記載内容を以下に変更します 【変更内容】 全体傾向 ・セキュリティクラウド全体にて確認した不正アクセス件数推移、危険度別件数 個別傾向 ・各接続団体における不正アクセス件数推移、危険度別件数、上位検知シグネチャ、担当者・受託事業者間の連絡、対応履歴	あり
12	仕様書(案)	P6 ２　事業概要 （２）業務範囲 エ　サービス構成例	【記載内容】 ・（省略） 【意見】 ・リバースプロキシ機能は、想定図ではWAF機能に集約されると思われるため、クラウドサービス提供施設内の機能としては無くなるものと考えます。 ・データ領域を保持するサーバの、定期的なバックアップが想定されるため、バックアップサーバを記載されてはどうでしょうか。	・サービス構成例はあくまで例であり、不要な機器や冗長な機能が記載されている場合の他、逆に、必要な機器や機能が記載されていない場合もあります。さらに、応札をいただく各事業者のサービス構成についても異なるものと想定しているため、リバースプロキシの削除とバックアップサーバの追加についても、ケースバイケースになると想定しています。 ・以上のことから、仕様の変更はなしとします。	なし
13	仕様書(案)	P19 11　業務詳細 （５）構築設計	【記載内容】 ・各接続団体からインターネット上の各種サービス（例えば、Slack Technologies社Slack、Google社GoogleWorkspace、Microsoft社Office365、Cisco社WebEX等）へのアクセスについては、後述する「ブレイクアウト接続回線」から接続可能とすること。なお、処理能力に余裕を持たせることで、ブレイクアウト接続回線を利用せず、全てをインターネット接続回線から接続する構成とすることについても可とするが、今後の利用量の増加等も考慮して、十分な余裕を持たせること。 【意見】 ・ブレイクアウト接続回線は必須となっておらず、「処理能力に十分な余裕を持たせる場合はブレイクアウト無しでも可」との記載ですが、回線およびUTM/PROXY等の関連機器の「十分に余裕のある」性能処理条件が明らかになっておらず、三重県様にとって性能リスクを抱えてしまう記載と思われます。 ブレイクアウト機能を必須とすることを推奨します。	・ブレイクアウト接続回線を必須とするため、「なお、処理能力・・・持たせること」までを削除します。 ・以上のことから、記載内容を、以下のように修正します。 【変更内容】 ・各接続団体からインターネット上の各種サービス（例えば、Slack Technologies社Slack、Google社GoogleWorkspace、Microsoft社Office365、Cisco社WebEX等）へのアクセスについては、後述する「ブレイクアウト接続回線」から接続可能とすること。 ---------- ・また、性能要件については、「11業務詳細（９）利用サービスの詳細にかかる要件　ウ性能要件」に記載する形に変更します。 【記載内容】 ・各接続団体からのインターネットに向けた通信、及び、インターネットからセキュリティクラウド内に向けた通信について、後述する「（10）通信回線にかかる要件　ア　インターネット接続回線」で用意する帯域以上の処理性能を有すること。（通信回線以外のサービスでボトルネックが発生しないような処理能力を有すること。） 【変更内容】 ・ 各接続団体からのインターネットに向けた通信、及び、インターネットからセキュリティクラウド内に向けた通信について、後述する「（10）通信回線にかかる要件　ア　インターネット接続回線」で用意する帯域以上の処理性能を有すること。（インターネット接続回線、および、ブレイクアウト接続回線以外のサービスでボトルネックが発生しないような処理能力を有すること。例えば、想定される通信量から逆算し、クラウド接続回線の増強やファイアウォールの機器スペックを向上させるなどの対応を行うこと。） ・ インターネット接続回線については、運用期間内において、適切な上限帯域設定や、フィルタリング、ローカルブレイクアウトの実施等を行うことで、インターネット接続回線がボトルネックとならないような対応を行うこととしているが、運用期間内において、クラウド接続回線がボトルネックとなる場合は、本委託業務の範囲内で増強を行うこと。	あり
14	仕様書(案)	P23 11　業務詳細 （７）運用・保守業務の設計にかかる要件 カ　設定変更対応	【記載内容】 ・設定変更対応として、現時点で想定している内容は、以下のとおり。 ・ファイアウォールへのアクセス制限設定 ・URLフィルタのフィルタルール設定 ・IDSまたはIPSの検知・遮断設定 ・リバースプロキシの接続団体向けIP設定 ・DNSサーバのレコード登録 ・メールリレーサーバのリレー設定 ・マルウェア/スパム対策の除外設定 【意見】 ・新設される機能として、以下変更作業が想定されます。 〇WAF機能：当該機能のホワイトリスト対応やSSL証明書更新作業 〇ブレイクアウト機能：ブレイクアウト対象通信の追加・変更	・記載内容を以下に変更します。 【変更内容】 ・設定変更対応として、現時点で想定している内容は、以下のとおり。 ・ファイアウォールへのアクセス制限設定 ・URLフィルタのフィルタルール設定 ・IDSまたはIPSの検知・遮断設定 ・リバースプロキシの接続団体向けIP設定 ・DNSサーバのレコード登録 ・メールリレーサーバのリレー設定 ・マルウェア/スパム対策の除外設定 ・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 ・ブレイクアウト対象通信の追加・変更	あり
15	仕様書(案)	P23 11　業務詳細 （７）運用・保守業務の設計にかかる要件 カ　設定変更対応	【記載内容】 ・設定変更の実施後、対象機器の設定情報（Config情報）や設定データ等のバックアップを実施するようにすること。また、バックアップは設定変更を行った機器等に対して、2世代以上の管理を行うこと。 【意見】 ・バックアップについては、設定データ以外の日々更新されるデータも対象とすべきと考えます。以下記載を追記をご提案します。 「また、設定情報以外の日々蓄積するデータを有するサーバ群（ログサーバ等）は、2週間前程度までのデータに復旧できるようにしておくこととし、業務上影響のない時間帯を考慮したうえでバックアップを取得すること。 バックアップソフトウェアはメーカーサポートを受けれる有償のものを活用すること。」	・本項目は、「設定変更対応」にかかるバックアップ等の要件を記載しており、また、設定変更対応に伴うバックアップについては、2世代以上の管理で十分と考えています。 ・ご意見をいただきました、「設定データ以外の日々更新されるデータ」にかかるバックアップについては、別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」における「対応と復旧　－　バックアップとリストア」に要件が記載されており、この中で、サイバー攻撃やデータ消失、マルウェア被害等の対策としてバックアップを取得することとしています。また、バックアップの手法については、構築される構成により、複数の考え方・方法があると想定していることから、設計段階にて詳細を決定することとなります。 ・以上のとおり、設定変更対応のバックアップにかかる要件変更はないことから、仕様の変更はなしとします。	なし

<table>
<tr><th rowspan="2">No</th><th colspan="3">寄せられた意見</th><th rowspan="2">三重県の考え方</th><th rowspan="2">仕様書の追記または修正有無</th></tr>
<tr><th>書類名</th><th>ページ等</th><th>意見</th></tr>
<tr><td>16</td><td>仕様書(案)</td><td>P24
11　業務詳細
（７）運用・保守
業務の設計にかかる要件
キ　調達した機器に対するリスク管理</td><td>【記載内容】
・本委託業務にて調達した機器に対するリスク管理を行うため、脆弱性情報等の収集を行うこと。

【意見】
・脆弱性情報の収集に関しては網羅性に関する記載も必要と考えます。「脆弱性配信サービスや外部データベースを活用し、対象製品に関する網羅的な脆弱性情報を収集すること」などの追記をご提案します。</td><td>・記載内容を以下に変更します。

【変更内容】
・本委託業務にて調達した機器に対するリスク管理を行うため、脆弱性情報等の収集を行うこと。なお、脆弱性配信サービスや外部データベースを活用し、対象製品に関する網羅的な脆弱性情報を収集すること。</td><td>あり</td></tr>
<tr><td>17</td><td>仕様書(案)</td><td>P24
11　業務詳細
（７）運用・保守
業務の設計にかかる要件
ケ　定例報告会</td><td>【記載内容】
・運用期間において、定期的に、本県、及び、各接続団体に対して報告会を行うこと。

【意見】
・報告会は、効率的な会議運営や緊密なコミューニケーションが実現できるよう、オンサイトでの対応者を準備することを必須とするようご提案します。（県がリモート対応を指示する場合はその限りではない）</td><td>・記載内容を以下に変更します。

【変更内容】
・運用期間において、定期的に、本県、及び、各接続団体に対して報告会を行うこと。なお、特に指定のない限り、オンサイトでの開催を原則とすること。</td><td>あり</td></tr>
<tr><td>18</td><td>仕様書(案)</td><td>P24
11　業務詳細
（７）運用・保守
業務の設計にかかる要件
サ　職員研修対応</td><td>【記載内容】
・開催は年2回以内とし、開催日及び内容は県と調整すること。

【意見】
・上記コメント同様に、オンサイトでの対応者を準備することを必須とするようご提案します。</td><td>・記載内容を以下に変更します。

【変更内容】
・開催は年2回以内とし、開催日及び内容は県と調整すること。なお、特に指定のない限り、オンサイトでの開催を原則とすること。</td><td>あり</td></tr>
<tr><td>19</td><td>仕様書(案)</td><td>P30
11　業務詳細
（９）利用サービスの詳細にかかる要件
ア　基本要件</td><td>【記載内容】
・各接続団体に提供するサービスは原則として同内容とするが、通信量に関しては、接続団体毎に上限設定が可能なこと。

【意見】
・通信量の接続団体毎の上限設定は、現実的ではなく、特定団体のブラウジングが多いなどの場合はブレイクアウトで対象通信を迂回させる等の対応が現実的と思います。</td><td>・誤記（通信量　→　通信帯域）がありましたので修正します。また、帯域制限以外の制限方法であっても要件を満たすことが明らかになるように、記載内容を以下に変更します。

【変更内容】
・各接続団体に提供するサービスは原則として同内容とするが、通信帯域に関して接続団体毎に上限設定が行えるなど、特定の接続団体がセキュリティクラウドの機能を占有できないような制限が可能なこと。</td><td>あり</td></tr>
<tr><td>20</td><td>仕様書(案)</td><td>P30
11　業務詳細
（９）利用サービスの詳細にかかる要件
イ　機能要件</td><td>【記載内容】
・なお、利用サービスの詳細要件に記載されていないものについても、セキュリティクラウドによるサービス提供を行うために必要となる機能があれば、適宜、提供を行うこと。

【意見】
・機能に関して、詳細要件シートには共通的な要件（冗長化・サーバウイルス対策）が記載されていません。本項に以下記載をご提案します。
「・接続団体通信に影響がでる機能群は冗長化構成とし、単一障害時は事業継続可能とすること」
「・汎用OSにて構築するサーバには、有償のアンチウイルス対策を実施すること」</td><td>・記載内容に以下の内容を追記します。

【追記内容】
・特に、単一障害によるサービス停止とならないための冗長化構成等や、ウィルス対策等の対応等については、必須と考えているため、留意すること。</td><td>あり</td></tr>
<tr><td>21</td><td>仕様書(案)</td><td>P31
11　業務詳細
（９）利用サービスの詳細にかかる要件
ウ　性能要件</td><td>【記載内容】
・CDNについて、接続団体数×2（公式Webサイト、防災サイト）に加えて、10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。

【意見】
・CDNの対象FQDN数が規定されていますが、WAF・DdoS対策を同サービスで実現する場合、同FQDN数を前提とするという補足を追記することをご提案します。</td><td>・記載内容に以下の内容を追記します。

【追記内容】
・また、WAFやDDOS対策についても、同数のサイトについて対応が可能なこと。</td><td>あり</td></tr>
<tr><td>22</td><td>仕様書(案)</td><td>P19
11　業務詳細
（５）構築設計</td><td>【記載内容】
・各接続団体からインターネット上の各種サービス（例えば、Slack Technologies社Slack、Google社GoogleWorkspace、Microsoft社Office365、Cisco社WebEX等）へのアクセスについては、後述する「ブレイクアウト接続回線」から接続可能とすること。なお、処理能力に余裕を持たせることで、ブレイクアウト接続回線を利用せず、全てをインターネット接続回線から接続する構成とすることについても可とするが、今後の利用量の増加等も考慮して、十分な余裕を持たせること。

【意見】
・ブレイクアウト環境（ブレイクアウト用機器）対するセキュリティー要件（機能要件）が抜けている。少なくとも「ファイアウォール」「IDS/IPS」は必要と思われる。また、想定されるセッション数に対する性能要件の記載を提案します。</td><td>・ブレイクアウト接続回線を必須とするため、「なお、処理能力・・・持たせること」までを削除します。
・以上のことから、記載内容を、以下のように修正します。

【変更内容】
・各接続団体からインターネット上の各種サービス（例えば、Slack Technologies社Slack、Google社GoogleWorkspace、Microsoft社Office365、Cisco社WebEX等）へのアクセスについては、後述する「ブレイクアウト接続回線」から接続可能とすること。

・また、セキュリティ要件については、「11業務詳細（９）利用サービスの詳細にかかる要件　イ　機能要件」に記載する形に変更します。

【追記内容】
・ブレイクアウト接続回線にかかる通信について、接続先となる利用サービス、及び、接続元となる接続団体による細かな利用制限（フィルタリング）や「IDS/IPS」等のセキュリティ対策が実施できること。ただし、制限等を実現する機能等については、全ての接続団体が利用する場合を想定し、十分な処理能力を有したものとすること。（運用期間当初は、ほとんど利用がないと想定しているが、徐々に利用が増えてくると考えられることから、綿密な容量計算等を行う必要があると想定している。）
・ブレイクアウト接続回線からの通信について通信ログの採取とレポート作成が可能なこと。また、「IDS/IPS」で異常な通信を検知した際は、セキュリティ監視等業務として、調査・分析が行えること。</td><td>あり</td></tr>
<tr><td>23</td><td>仕様書(案)</td><td>P31
11　業務詳細
（10）通信回線にかかる要件
ア　インターネット接続回線</td><td>【記載内容】
・後述する「ブレイクアウト回線」と合わせて計4Gbps のベストエフォート回線（この内、インターネット接続回線用として1Gbps は帯域確保または帯域保証回線、さらに、ブレイクアウト接続回線用として1Gbps は帯域確保または帯域保証回線とすること）を用意すること。

【意見】
・ブレイクアウト構成の場合
　ブレイクアウト接続回線3Gbps（内1Gbps保証）
　インターネット接続回線1Gbps（保証）
　合計：3Gbps+1Gbps＝合計4Gbps（内2Gbps保証）
という認識で問題無いでしょうか。</td><td>・想定される構成について「11業務詳細（10）通信回線にかかる要件　ア　インターネット接続回線　表　インターネット接続回線とブレイクアウト接続回線の構成例」に追記します。
・提案の構成の他、いくつかの構成が想定されますが、どのような構成とするかについては、設計段階において、将来予想も踏まえて提案をいただいたうえで、本県の承認を得る必要があるため、注意してください。

【追記内容】
<table><tr><th>分類</th><th>インターネット接続回線</th><th>ブレイクアウト接続回線</th><th>計</th><th>クラウド接続回線</th></tr><tr><td rowspan="3">ブレイクアウト接続回線をDC（津市内）で接続</td><td>1Gbps（帯域保証）
1Gbps（ベスト）</td><td>1Gbps（帯域保証）
1Gbps（ベスト）</td><td>4Gbps</td><td>1Gbps（帯域保証）と
1Gbps（ベスト）が必要</td></tr><tr><td>1Gbps（帯域保証）
2Gbps（ベスト）</td><td>1Gbps（帯域保証）</td><td>4Gbps</td><td>1Gbps（帯域保証）と
2Gbps（ベスト）が必要</td></tr><tr><td>1Gbps（帯域保証）</td><td>1Gbps（帯域保証）
2Gbps（ベスト）</td><td>4Gbps</td><td>1Gbps（帯域保証）が必要</td></tr><tr><td rowspan="3">ブレイクアウト接続回線をクラウド提供施設で接続</td><td>1Gbps（帯域保証）
1Gbps（ベスト）</td><td>1Gbps（帯域保証）
1Gbps（ベスト）</td><td>4Gbps</td><td rowspan="3"><u>2Gbps（帯域保証）と
2Gbps（ベスト）が必要</u></td></tr><tr><td>1Gbps（帯域保証）
2Gbps（ベスト）</td><td>1Gbps（帯域保証）</td><td>4Gbps</td></tr><tr><td>1Gbps（帯域保証）</td><td>1Gbps（帯域保証）
2Gbps（ベスト）</td><td>4Gbps</td></tr></table>表　インターネット接続回線とブレイクアウト接続回線の構成例</td><td>あり</td></tr>
</table>

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		
24	仕様書(案)	P32 11　業務詳細 （10）通信回線にかかる要件 イ　クラウド接続回線	【記載内容】 ・クラウドサービス提供施設を本県が別途調達しているデータセンター（津市内）内に設置する場合は、クラウド接続回線に代えて、データセンター内配線を行うこと。 【意見】 ・県が別途調達しているラック等を利用可能なのか、受託者にて対象データセンターに新たに有償準備する必要があるのかが読み取れない。	・本県が別途調達しているデータセンターにおいて、本委託業務の受託事業者が利用できるスペースはありません。「11　業務詳細（４）三重県情報ネットワークとの接続設計にかかる要件」に示したとおり、クラウドサービス提供施設を本県が別途調達しているデータセンター内に設置する、または、設置しないのいずれの場合においても、受託事業者側で「データセンター内受託事業者契約ラック」が調達されているものと想定していますので、そのラックからクラウド接続回線と接続を行うためのラックとの配線が必要となります。	なし
25	仕様書(案)	P32 11　業務詳細 （10）通信回線にかかる要件 ウ　ブレイクアウト接続回線	【記載内容】 ・グローバル IP アドレスを 128 個以上利用できること。但しクラウドサービス等の提供方式によって、同等のサービスが提供できる場合はこの限りでない。 【意見】 ・固定IP128個の用途（必要性）が読み取れない。	・インターネット上の各種サービスを利用する際、各接続団体からの送信元IPアドレスとして利用することで、フィルタリング等の対応を行うことを想定しています。 ・以上のことから、記載内容に以下の内容を追記します。 【追記内容】 ・また、各接続団体からインターネット上の各種サービスを利用する際、接続団体毎に固定の送信元IPアドレスを設定できること。	あり
26	仕様書(案)	P32 11　業務詳細 （10）通信回線にかかる要件 ウ　ブレイクアウト接続回線	【記載内容】 ・ブレイクアウト接続回線として、冗長性を確保した回線を用意すること。 【意見】 ・直接接続の構成を考慮し、以下の記載追加を希望します。 「もしくは、クラウド接続回線同様に（冗長化された上位回線と）同一施設内で接続を行う。」	・ブレイクアウト接続回線が不通になった場合を想定し、ブレイクアウト接続回線自体の冗長性確保を要件としていましたが、ブレイクアウト接続回線を冗長化させるのではなく、インターネット接続回線から通信を行うことができれば要件を満たすことから、記載内容を以下のとおりに変更します。 【変更内容】 ・ブレイクアウト接続回線が不通となった場合を想定し、インターネット接続回線等を経由する形への経路変更の対応や、迅速な障害対応（機器の予備機の確保、現地常駐SEによる機器交換等）が実施できること。また、インターネット接続回線とブレイクアウト接続回線は別キャリアとすること。	あり
27	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No3　プロキシサーバ	【記載内容】 ・構成団体とインターネットのメールを中継するメールリレーサーバを設置し、通信内容を監視すること ・ログ分析を行うためアクセス情報（アクセス日時、接続元IPなど）を記録すること ・ログを分析し、セキュリティインシデントが発生した場合に報告すること ・不正中継を防止すること ・なりすましメールに対する対策を講じること ・構成団体ごとのマルチドメインをサポートすること ・中継を許可するドメインは、構成団体が管理するドメインのみとすること ・なりすましメールに対する対策として、送信ドメイン認証方式は、普及率が最も高いSPF方式を選択できること ・外部サービスを利用する場合は同等の機能を有すること 【意見】 ・「Outgoing IPを接続団体ごとに専有IPアドレスに固定化できること」を追記することをご提案します。（クラウドサービス利用時のグローバルIPでのアクセス制御等を想定）	・「11　業務詳細（10）通信回線にかかる要件　ア　インターネット接続回線」内の「グローバルIPアドレスを256個以上利用できるようにすること。但しクラウドサービスの提供方式によって、同等のサービスが提供できる場合はこの限りでない。」に、以下の内容を追記します。 【追記内容】 ・また、各接続団体からインターネット上の各種サービスを利用する際、接続団体毎に固定の送信元IPアドレスを設定できること。	あり
28	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No4　外部DNSサーバ	【記載内容】 ・構成団体のキャッシュDNSサーバとしてインターネットに対して再帰問合せを行い通信内容を監視すること ・ログ分析を行うためアクセス情報（アクセス日時、接続元IPなど）を記録すること ・C&Cサーバ等へのDNS問合せなど不正な通信を監視し検知すること ・ログを分析し、セキュリティインシデントが発生した場合に報告すること 【意見】 ・内部DNSサーバの記載が混在しているため、2点目～5点目は内部サーバ向けの項目とすることをご提案します。 ・管理ゾーン数を定義することをご提案します。	・本要件は、外部DNSに求められる要件ですが、DNSの構成として、内部DNSと機能を分離させ別途構築する方法や、接続団体のDNSと連携して構築する方法等、いくつかの構成が考えられます。しかし、どのような構成であっても、DNS機能の全体で本要件を満たすようにしていただく必要があります。 ・また、管理するゾーン数は増減すると想定されるため、運用期間中において、各接続団体からの要望に応えられるよう十分な量のゾーン数が扱えるようにしていただく必要があります。 ・以上のことから、仕様の修正はなしとします。	なし
29	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No8　通信の復号対応	【記載内容】 ・SSL/TLSで暗号化された通信内容を復号し通信内容を監視可能とすること ・通信の復号処理により業務に支障が出る場合は迂回方法を検討すること ・通信先が信頼できると判断される場合は、復号処理の対象外としてよい 【意見】 ・復号対象の機能が明確になっていないため、以下記載追記をご提案します。 「HTTPS通信に対するセキュリティ機能（IDS/IPS、マルウェア検知、URLフィルタ、Proxy）を対象に復号対応を実施すること」	・監視対象は、ゲートウェイにおける「SSL/TLS」通信と考えてください。 ・記載内容に矛盾がないことから、仕様の修正はなしとします。	なし
30	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No10　アンチウイルス／スパム対策	【記載内容】 ・インターネットからのメールについて、アンチウイルス検査を行い、不正なメールの検知及び隔離、削除を行うこと ・インターネットからのメールについて、スパムメールの判別を行い、レベルに応じた隔離、遮断を行うこと ・業務に不要な広告メール等を検知し隔離、遮断できること ・ブラックリスト方式、ホワイトリスト方式に対応すること ・メール原本は隔離されたサーバに転送できること ・セキュリティクラウド共通の迷惑メールフィルタリングを設定すること ・隔離されたメールは一定期間保存され、必要に応じて確認ができること 【意見】 ・「メール原本は隔離されたサーバに転送できること」とありますが、メール無害化時以外には必要ない項目かと思われます。	・こちらの記載は、メールに対する検査、隔離、削除を行う内の、「隔離」を行ったメールに対する要件です。全てのメールに対する対応を求めるものではありません。なお、隔離が必要ない形での運用を行う場合についても、要件を満たすと考えています。 ・ただし、そのような場合は、設計段階において、隔離が不要な理由等について説明し、本県の承認を受けていただく必要がありますので、ご注意ください。 ・以上のことから、仕様書の修正はなしとします。	なし
31	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No12　WAF	【記載内容】 ・構成団体が提供するWebサイトに対して、Web アプリケーションの脆弱性を狙った不正な通信等の検知・防御すること ・管理する構成団体のWebサーバに合わせて必要なチューニング等を行うこと ・Webアプリケーションの脆弱性を突いた以下の攻撃を防御する。 SQLインジェクション／OSコマンド・インジェクション／ディレクトリ・トラバーサル／セッション管理の不備／クロスサイト・スクリプティング／CSRF（クロスサイト・リクエスト・フォージェリ）／HTTPヘッダ・インジェクション／メールヘッダ・インジェクション／クリックジャッキング／バッファオーバーフロー／アクセス制御や認可制御の欠落 【意見】 ・1FQDNに対してオリジンが2サーバ存在する接続団体が想定される場合、以下記載追記をご提案します。 「1FQDNに対してオリジンサーバが2サーバ存在する場合も分散制御に対応すること」 ・WAFによって通信影響を受ける場合のホワイトリスト化などを想定し、以下記載追記をご提案します。 「送信元IPアドレス、送信元の国ベース、宛先URLによるアクセス制御が可能なこと」	・「11　業務詳細（９）利用サービスの詳細にかかる要件　ウ　性能要件」に以下の内容を追記します。 【追記内容】 ・WAFについて、1FQDNに対するオリジンサーバが複数ある場合、分散制御に対応できること（複数あるオリジンサーバの内、2サーバ以上に対して、分散制御ができれば要件を満たす）。また、送信元IPアドレス、宛先URL等によるアクセス制御が可能なこと。	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		
32	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No13　CDN	【記載内容】 ・大規模なリクエストが発生した場合でも継続的な情報発信ができるようWebサーバの負荷分散を行う ・構成団体のWebサイト（Webサーバ）に急激なアクセスがあった場合においても、住民に対してWebサイトから情報が継続的に発信可能なサービスであること ・CDNを利用するWebサーバは構成団体の公式Webサーバおよびアクセス集中が想定されるサーバを対象とすること ・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成され高速な配信を実現すること ・CDNサービスが提供されるサービスは、耐震、免震などの構造上の安全性に配慮された設備で運用された可用性が高いサービスであること ・HTTPSでコンテンツを配信可能であること ・HTTPSの場合はサーバ証明書も提供できること ・アクセス元のIPアドレスに応じたアクセスの拒否、許可の設定が可能であること ・アクセスログを取得可能であること ・市町村等の環境でオリジンサーバを運営しているケース、及び、外部サービスを利用しているケースにおいて、CDNサービスが提供可能なこと ・転送量によらず、固定料金での提供が可能であること 【意見】 ・オリジンサーバへのURLアクセスは、CDN（クラウドWAF）経由でのアクセスとなりますが、オリジンサーバIPアドレス指定での直接アクセスが抜け道となる可能性がある為、CDN（クラウドWAF）サービスIPアドレスからのアクセスのみを許可するよう、オリジン側でアクセス制御することが望ましいと考えます。 当該アクセス制御が可能なように、以下記載追記をご提案します。 「Webサーバーへのアクセスを CDNサービスからの通信に限定するためサービスが使用しているIPアドレスレンジを全て公開していること」	・「11　業務詳細（９）利用サービスの詳細にかかる要件　イ　機能要件」に以下の内容を追記します。 【追記内容】 ・CDNについて、各接続団体におけるWebサーバへのアクセスをCDNサービスからの通信に限定するため、CDNサービスが使用しているIPアドレスレンジを全て確認できること。	あり
33	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	その他　機能要件項目追加のご提案	【記載内容】 （なし） 【意見】 ・仕様案本紙P6図にも記載のあるDDoS対策について要件記載が無いため、記載することをご提案します。 「・公開Webサーバへの DDoS対策を実施すること。 　・DDoS 攻撃が発生してもDDoSトラフィックのみ排除し通常ユーザーのトラフィックは正常にCDN処理がされるようCDN機能と連携可能なこと。 　・DDoS対策はインターネット側での対策とし、分散対策が可能であること」。 （注：DDoS攻撃がCDN処理に影響を与えないように、またGW装置でのDDoS対策は入り口回線容量が埋め尽くされる攻撃がくると無力化する可能性がある為、インターネット側（CDNの前）でのDDoS対策を推奨します） ・NTPサーバに関する要件がないため、記載することをご提案します。 「・インターネット上の信頼できる機器と時刻同期を行い、導入機器の時刻同期を行うこと。 ・時刻同期のアクセスについて、特定のホストやネットワークからのみ許可する設定を施すこと。」	・「11　業務詳細（９）利用サービスの詳細にかかる要件　イ　機能要件」に以下の内容を追記します。 【追記内容】 ・公開Webサーバへの DDoS対策を実施すること。 ・DDoS対策として、DDoS 攻撃が発生してもDDoSトラフィックのみ排除し通常ユーザのトラフィックは正常にCDNにて処理がされるようCDN機能と連携可能なこと。CDN全体による分散対応が可能なこと。 ・インターネット上の信頼できる機器と時刻同期を行い、導入機器の時刻同期を行うこと。 ・時刻同期のアクセスについて、特定のホストやネットワークからのみ許可する設定を施すこと。	あり
34	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No14～16　高度な人材による監視と検知 No17～24　対応と復旧	【記載内容】 （記載内容が多いため省略） 【意見】 ・No14～24は、仕様案本紙の「運用・保守業務要件」「セキュリティ監視等業務にかかる要件」と重複する記載となっています。 別紙のNo14～24は削除し、本紙での記載要件を有効とされることをご提案します。	・仕様書に記載の内容は、別紙の内容をベースとして、必要とされる内容を追記している形としているため、仕様書の修正はなしとします。	なし
35			・以下、NOC/SOC観点で仕様書本紙に重複記載が無いと思われる項目についての補足 　No36～No40	－	－
36	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No14　ログ収集・分析	【記載内容】 ・ログは最低5年分保存できること 【意見】 ・「ログは最低5年分保存」と記載がありますが、実際の運用経験やコスト最適化の観点を踏まえ、ログの保存期間は有事の際に実効的に分析可能な範囲で1年保存としてはどうでしょうか。	・ログは最低5年分保存できることとしてください。なお、1年ごとに媒体等で納品する形も可とします。	なし
37	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No15　イベント監視	【記載内容】 ・ファイアウォール、IDS/IPSといったセキュリティ機器や監視対象サーバ(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)のイベントを監視し、異常を検知した際に通知できること ・パターンマッチングやしきい値等のルールに基づき、許可していないイベントの発生を検知できること ・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 ・検知したイベントはログとして保存すること ・インシデントの兆候をつかむために有用でないイベントは除外(フィルタリング)できることが望ましい 【意見】 ・セキュリティ機器のイベント監視については、仕様書本紙「P24 オ 稼働監視・障害対応」に記載がありますが、別紙記載のパターンマッチング等のセキュリティ検知については記載が無いため、汎用OSでのサーバ構築時はウイルス対策を要件とされることをご提案します（No20に記載済み）。	・（No20で回答）	
38	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No19　不正通信の早期検知を行う運用体制の確立(CSIRT)	【記載内容】 ・セキュリティインシデント発生時の対応を迅速に行うため運用体制(CSIRT)を構築すること ・運用体制を書面にて関係者に共有すること ・運用フローを年１回以上検証すること ・インシデント発生時、必要に応じてファイアウォールのポリシー追加、変更により通信を遮断する。ポリシー変更は関係者と協議の上、決定する。また、事前決定された対応案に基づいて実施する 【意見】 ・CSIRT構築は自治体様での対応事項のため、本項記載内容の受託者側での対応は難しいと考えます。弊社ではSOCでの連携サポートを想定しています。	・CSIRT（Computer Security Incident Response Team）とは、セキュリティクラウド上で発生したインシデントへの対応を行う体制であると考えています。そのため、接続団体と受託事業者（NOC,SOC）を交えて検討し、確立することを要件としています。 ・以上のことから、仕様書の修正はなしとします。	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		
39	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No21　バックアップとリストア	【記載内容】 ・機器障害などによりセキュリティクラウドの運用が停止することを防ぐためバックアップを取得すること ・ログ等日々の保存データを日次でバックアップすること ・システム変更が生じた場合、随時システムバックアップを行うこと ・バックアップからのリストアを検証すること ・バックアップは本体とは別の場所に保管し本体障害時に復旧できること 【意見】 ・仕様書本紙にはバックアップを主体とした項目はありませんが、「P23 カ 設定変更」内にバックアップの記載をされています。No15にて、別紙記載の内容と同等レベルの運用要件化についてのご提案をしております。	・（No15で回答）	
40	別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」	No24　セキュリティレベルの自己点検の実施	【記載内容】 ・年１回、構成する機器に対しての脆弱性診断を実施して脆弱性がないか検証すること ・脆弱性が検知された場合、速やかに是正すること ・システム停止等が困難な場合、設定変更等による脆弱性の回避策についても検討する ・脆弱性への対応はバージョンアップ、セキュリティパッチ適用等による恒久対応が望ましい ・第三者の監査を受けることが望ましい 【意見】 ・パブリッククラウドサービスには、脆弱性診断は許容されないケースもあります。脆弱性対応については、仕様書本紙「P24 キ」の記載を要件とされることをご提案します。 （網羅的な脆弱性対応の実現については、No16にてご提案内容を記載しています）	・本要件については、セキュリティクラウドの機能を維持するための要件であり、点検漏れのないことを求めるものです。そのため、パブリッククラウドサービス等の利用を検討する場合は、点検等の頻度を要件として、その要件を満たすサービスを利用することで、本要件を満たすものと考えています。 ・以上のことから、仕様の修正はなしとします。 ・（その他の内容については、No16で回答）	なし
41	仕様書(案)	P14 10　調達全般に関する共通要件 （４）他の受託事業者との調整 ウ　設定変更等の依頼	【記載内容】 ・実際の設定変更作業は関係する受託事業者との既存契約の範囲内の内容に限り、接続団体を通じて依頼することが可能だが、契約の範囲を越える内容については、受託事業者の責により実施することとなるため注意すること。なお、当該調整に関する費用を本県に請求することはできない。 【意見】 「接続団体の契約の範囲を超える内容については・・・」とありますが、接続団体側の機器等の設定変更は契約外となる為、「支援する事」等に変更する事を推奨します。	・本委託業務では、各接続団体を次期セキュリティクラウドへ移行する作業を行うこととしていますが、移行の際は、各接続団体における既存ネットワークや既存システムの設定変更が発生すると想定しています。この作業について、各接続団体が既存ネットワークや既存システムにかかる受託事業者と運用・保守契約等を締結していなかったり、締結していても、その契約の中で対応ができない場合は、本委託業務にかかる受託事業者が対応を行うことになります。そのため、その際に発生する費用は、本委託業務内に含まれているとお考えください。（これは、既存ネットワークや既存システムに対して、できるだけ設定変更が生じないような設計としていたくこと、本委託業務の受託事業者が、最終的な責任を負っていただくこと、などを意図しています。） ・なお、本委託業務の範囲外の内容や、本委託業務と関係なしに、発生する業務等については、各接続団体が実施することとなりますが、その詳細については、設計段階にて役割分担を行っていただく必要があります。 ・以上のことから、仕様の修正はなしとします。	なし
42	仕様書(案)	P19 11　業務詳細 （５）構築設計	【記載内容】 （なし） 【意見】 セキュリティの観点から、接続団体間の通信を禁止してはどうでしょうか。	・「11　業務詳細（９）利用サービスの詳細にかかる要件　イ　機能要件」に以下の内容を追記します。 【追記内容】 ・セキュリティの観点から、接続団体間の直接通信を禁止できること。なお、一部の通信のみ、直接通信を許可できること。	あり
43	仕様書(案)	P22 11　業務詳細 （７）運用・保守業務の設計にかかる要件 ウ　ポータルサイト	【記載内容】 ・全ての接続団体に対して、複数のアカウントを発行できること。なお、通常は各接続団体に対して1つのアカウント発行を想定しているが、通常運用時に利用するアカウントの他、インシデント発生時に利用するアカウントなど、複数アカウント発行を希望する団体にのみ、発行することを想定している。 【意見】 アカウント数単位で課金される為、必要最低限数の提示を推奨します。 算出例：35アカウント（接続団体33+受託事業者1+α1）	・各接続団体で最大5つ程度と想定しています。 ・以上のことから、記載内容を以下に変更します。 【変更内容】 ・全ての接続団体に対して、複数のアカウント（最大5つ程度）を発行できること。なお、通常は各接続団体に対して1つのアカウント発行を想定しているが、通常運用時に利用するアカウントの他、インシデント発生時に利用するアカウントなど、複数アカウント発行を希望する団体にのみ、発行することを想定している。	あり
44	仕様書(案)	P31 11　業務詳細 （10）通信回線にかかる要件 ア　インターネット接続回線	【記載内容】 ・インターネット接続回線として、冗長性を確保した回線を用意すること。 【意見】 可用性を考慮し、「インターネット接続回線」と「ブレイクアウト接続回線」は、異キャリアで提供する事を推奨します。いずれかの回線が故障しても、もう一方の回線で縮退稼働を想定。	・記載内容に以下の内容を追記します。 【追記内容】 ・また、インターネット接続回線とブレイクアウト接続回線は別キャリアとすること。	あり
45	仕様書(案)	P31 11　業務詳細 （10）通信回線にかかる要件 ア　インターネット接続回線	【記載内容】 ・グローバルIPアドレスを256個以上利用できるようにすること。但しクラウドサービスの提供方式によって、同等のサービスが提供できる場合はこの限りでない。 【意見】 各接続団体が、グローバルIPアドレスに紐づいたインターネットサービスを契約する必要性が想定されるため、各接続団体毎に固定のグローバルIPアドレス設定が必要と考えます。	・記載内容に以下の内容を追記します。 【追記内容】 ・また、各接続団体からインターネット上の各種サービスを利用する際、接続団体毎に固定の送信元IPアドレスを設定できること。	あり
46	仕様書(案)	P23 11　業務詳細 （７）運用・保守業務の設計にかかる要件 カ　設定変更対応	【記載内容】 ・ 各接続団体における担当職員からの依頼に基づき、各種設定変更を行うこと。 【意見】 対応時間について記載することを推奨	・記載内容に以下の内容を追記します。 【追記内容】 ・なお、疑義のない設定変更依頼については、原則として翌営業日中に対応を行うこと。	あり
47	仕様書(案)	P7 ２　事業概要 （３）受託要件 ア　運用実績	【記載内容】 ・受託事業者は本県または他都道府県を含め、自治体情報セキュリティクラウドの構築・運用実績があること。 【意見】 ・情報セキュリティクラウドの運用・保守実績がある事業者を必須要件とすると先回のセキュリティクラウド受託事業者のみと限定されてしまい、三重県内本店企業等の参加が困難となることから、上記の受託条件について、記載の変更をお願いできますでしょうか。 「受託事業者は本県または地方自治体に対して、SOC（セキュリティオペレーションセンター）によるログの監視・分析を行っているクラウドサービスの構築・運用実績があること。」	・以下の内容に修正します。 【変更内容】 ・受託事業者は本県または他都道府県を含め、自治体情報セキュリティクラウドの構築・運用実績があること。または、本県または地方自治体に対して、後述するセキュリティ監視等業務を伴ったクラウドサービスの構築・運用実績があること。	あり
48	仕様書(案)	P7 ２　事業概要 （３）受託要件 イ　認証取得	【記載内容】 ・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。 【意見】 「11　業務詳細（９）利用サービスの詳細にかかる要件　ア　基本要件」にて、「クラウドサービスは、受託事業者が提供するサービスの他、外部事業者が提供するサービスにより提供することも可とする。なお、複数のクラウドサービスを組み合わせて各種サービスを提供する場合でも、本委託業務にかかる受託事業者は、全てのサービスに対し、責任をもって提供を行うこと。」と定義されています。 そうしますと、受託元はいわゆる情報セキュリティマネージメントシステム（ISMS）だけではなく、クラウドサービスに特化した「ISMSクラウドセキュリティ認証」も必要不可欠であると考えております。 特にクラウドセキュリティ認証は、受託業者側の日常運用にまでつながる運用規定を所有する必要があり、厳格な規格と考えておりますので、加筆をお願いいたします。	・ご指摘の「ISO/IEC 27017:2015に基づくISMSクラウドセキュリティ認証」について、本委託業務においては、努力目標とします。 ・そのため、以下のように記載内容を変更します。 【変更内容】 ・ 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。	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		
49	仕様書(案)	P7 2　事業概要 （3）受託要件 ウ　NOC及びSOC	【記載内容】 （なし） 【意見】 　NOC、SOCについての運用実績については求められておりますが、NOC、SOCは三重県様および参加団体様の情報資産を扱うこととなります。この為、受託者だけではなく、NOC提供事業者にもISMSの認証取得義務を負うべきかと考えておりますので、加筆ください。（SOCについてはP27(8)イ5点目に記載有り）	・ご指摘のとおり、NOCについてもなんらかの情報セキュリティに関する認証を受けていることが望ましいと考えます。しかし、NOCはSOCと異なり複数拠点での運用を想定しており、また、各接続団体における既存ネットワークや既存システムにかかる受託事業者等との協力体制による運用を想定していることから、全ての拠点に対してなんらかの認証を求めることは、既存事業者等とのスムーズな連携の妨げになると考えています。なお、全てのNOC拠点の運用においては、セキュリティクラウドにおける重要情報を扱うことから、受託事業者が他の事業者へ運用等を委託する場合は、当然、守秘義務等の情報漏洩対策を契約等により、対応されるものと考えています。 ・以上のことから、仕様書の修正はなしとします。	なし
50	仕様書(案)	P7 2　事業概要 （3）受託要件 ウ　NOC及びSOC	【記載内容】 ・10万台端末規模の監視運用実績を有すること ・10年以上の国内でのリモート監視オペレーションの実績を有すること ・自治体を含む、1000社・団体を超える監視運用実績を有すること 【意見】 この3点の受託条件について、記載の変更をお願いできますでしょうか。 「都道府県など自治体におけるセキュリティ機能を有するネットワークインフラにおいて、各市町村と直接やり取りを含めた運用・保守サービスの提供実績を有すること。また、市町村のネットワークインフラの構築・保守・運用の実績があり、自治体の情報セキュリティの知識を有することが望ましい。10年以上のリモート監視オペレーションの実績を有すること。」 これらの要件ですが、P5 ウの通り、三重県様の参加団体様を含めた端末台数が「26,500台」とご指定頂いています。10万台という算定根拠・理由が不明瞭と思われますが、このような大規模監視実績をご要望された場合は大手企業様のみ入札参加できることとなり三重県様企業育成頂いている県内企業様に対して不公平な条件かと存じます。 また、提供するセキュリティクラウド機器類の数量、および、該当機器で抽出される各接続端末からのログによる監視ということであれば理解できますが、「10万台の端末台数の監視運用実績」をご指定された理由もご明示ください。 各市町様の端末、三重県庁様の端末については各導入業者様・保守業者様が実施されているものと考えておりまして、セキュリティクラウドの受託要件として端末台数に限定されているのは矛盾していると考えています。 10年以上の国内リモート監視オペレーション実績については、国内に限定した実績で有る必要性が不明瞭であり、さらに、セキュリティクラウド導入機器については国外製の機器も多く存在しておりますので、国内外問わず10年以上のリモート監視オペレーション実績として差支えないかと考えております。 また、1000社・団体を超える監視運用実績の数量基準も明示頂きたいと考えますが、三重県様の本調達仕様では団体様が約33程度でございますので、同数規模での運用実績とさせて頂きたい。	・本委託業務における要件として、各接続団体で運用法用や設定、セキュリティ対策等が異なる業務端末に対して、C&Cサーバやマルウェア等の通信を検知し、遮断することなどを求めています。 ・また、インシデントは複数の団体で同時多発的に発生することが想定されるため、国内における相当数の団体、及び、複数団体にまたがる業務端末に対してリモート監視やオペレーションに対する実績が必要と考えています。 ・以上のことから、本仕様書の要件としたところですが、ご指摘の内容を踏まえ、以下の内容に修正します。 【変更内容】 ・延べ数万台端末規模の監視運用実績を有すること。 ・10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。 ・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。	あり
51	仕様書(案)	P7 2　事業概要 （3）受託要件 ア　運用実績 イ　認証取得 ウ　NOC及びSOC	【記載内容】 （省略） 【意見】 　入札参加資格・受託資格を満たせば日本国内企業の参加は認めて頂いておりますが、この受託要件ですと、国内大手企業様のみが参加可能で、該当企業様が受託される可能性が高いと推察されます。 　県内企業が参加することができたとしても、価格競争力だけでは大手企業様のように持っておらず、結果、受注可能性が低くなると思われます。 　県民の税金を用いて本事業を遂行される県庁様としては、そういう事態となれば、地域振興が損なわれる可能性が高くなると感じております。 　そこで県土整備部が公共工事を発注するにあたって、県内企業にアドバンテージをつけているやり方や、県内企業を育成強化する為にも国内大手企業と三重県内本店企業の共同体での入札方式等を検討していただいてはどうかと思います。 　本事業を遂行できる企業は全国に多く存在し、現在のセキュリティクラウド全国調達状況を拝見しますと、大手企業が参入されてくることも考えられます。 　三重県様におかれましては、情報通信系の事業にあたっては県内情報通信関連企業の育成強化も同時に図って頂くことを強く希望し、一方で、三重県様の当該事業の発注にあたっても、ただ単に該当事業の完遂を達成するだけでなく、県内本社設置の情報通信関連企業の育成も同時に図っていく、地域振興を同時に進めていくということを考えて頂きたく、本県調達にあたっては、県外企業参入時には、三重県内本店企業との共同体（ＪＶ）を前提条件とした入札をご検討頂きたくお願いいたします。	・本委託業務においては、地方公共団体の締結する契約のうち、政府調達に関する協定の適用を受ける契約に該当するため、「物品等又は特定役務の調達手続きの特例を定める規則」及び「地方公共団体の物品等又は特定役務の調達手続の特例を定める政令」（以下、「政令」という。）に基づき調達手続きを行う必要があります。このため、政令第五条第１項において「（中略）当該入札に参加する者の事業所の所在地に関する必要な資格を定めることができない。」と規定されていることから、地域要件等による優遇措置を設けることができませんので、ご理解ください。 ・一方で、県内の情報通信関連企業の育成や振興は重要な課題と考えています。今後、県内においてもDXの取組が大小織り交ぜ様々な形で展開されることが想定されますので、県内事業者の皆さまにもご協力をいただく中で、県内情報通信産業の振興にもつなげられるよう引き続き取組の検討を進めていきたいと考えています。	なし
52	仕様書(案)	P10 7　機密保持	【記載内容】 ・本委託業務は、三重県電子情報安全対策基準（情報セキュリティポリシー）を遵守して行うこと。 【意見】 ・参加申請するにあたり、本件遵守可能か事前に確認をいたしたく、上記について、開示頂きたくお願いいたします。	・「三重県電子情報安全対策基準（情報セキュリティポリシー）」は、本県における情報セキュリティに対する対策等について記載したものであり、本資料を公開することは、サイバー攻撃等を実施する者に対して情報を与えることになることから、非公開としています。	なし
53	仕様書(案)	P14 10　調達全般に関する共通要件 （4）他の受託事業者との調整 イ　既存事業者との調整 ウ　設定変更等の依頼	【記載内容】 ・実際の設定変更作業は関係する受託事業者との既存契約の範囲内の内容に限り、接続団体を通じて依頼することが可能だが、契約の範囲を越える内容については、受託事業者の責により実施することとなるため注意すること。なお、当該調整に関する費用を本県に請求することはできない。 ・契約の範囲の目安としては、日常的に発生しうる設定変更 や協議への参加、問い合わせ対応については既存契約による対応が可能だが、作業時の立会等については、受託事業者ごとに対応が分かれるため、注意すること。 【意見】 ・システムリプレース時において既存システムにて必要な調整等は、基本的には既存契約の範囲内に含まれると考えて宜しいでしょうか？ ・既存業者様との調整は受託事業者が図るものとは存じますが、何等か既存業者様側へのご費用が発生するのでしょうか。この場合、現在の三重県様と既存業者様間の委託契約内容に従うものと存じますが、どのようなケースにおいて本件受託者側で既存業者様への負担が発生するものか、詳細項目を明示頂きたくお願い申し上げます。	・次期セキュリティクラウドへの移行において、各接続団体では本委託業務以外の発注費用は見込んでいません。 ・また、各接続団体における既存ネットワークや既存システムへの影響を考慮せずに次期セキュリティクラウドを構築し、既存ネットワークや既存システムに対して大規模な設定変更作業が発生したり、新たな機器導入が発生したりするような事態も避ける必要があります。 ・以上のことから、本委託業務において発生する、既存ネットワーク、及び、既存システムに対する全ての設定変更等の業務について、本委託業務の受託事業者が負担することとしています。 ・なお、設定変更等の業務の内、各接続団体において、日常的に発生しているであろう業務（ルーティングの変更、DNSの変更、プロキシの設定等）については、各接続団体において、対応を行うことが可能と想定していますが、詳細な役割分担については、設計時に確認していただくことを想定しています。	なし
54	仕様書(案)	P18 11　業務詳細 （4）三重県情報ネットワークとの接続設計にかかる要件	【記載内容】 ・三重県情報ネットワークとの接続場所は、本県が別途調達しているデータセンター（津市内）とし、三重県情報ネットワークとの接続インタフェースは 10GBASESR × 2 本として設計すること。 なお、三重県情報ネットワーク機器側に必要な SFPモジュール（ 2 本）も本委託業務の中で準備すること。（三重県情報ネットワーク機器の詳細については、契約締結後に詳細を開示する。） 【意見】 ・NW機器(三情)へのSFPモジュール（ 2 本）の取り付けと設定変更は、三重県情報ネットワーク受託事業者にて実施頂ける認識と考えおりますが差支えございませんでしょうか。	・お見込みのとおり、三重県情報ネットワークに対してSFPモジュールの取り付け作業、及び、三重県情報ネットワーク側の機器にかかる設定変更作業については、三重県情報ネットワークにかかる受託事業者が実施します。 ・なお、実際の作業にあたっては、あらかじめ三重県情報ネットワークにかかる受託事業者と調整等を実施したうえで、接続に必要となる接続設計を行っていただき、本県、及び、三重県情報ネットワークにかかる受託事業者へ説明を実施し、承認を受けていただく必要があるので、注意してください。	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		
55	仕様書(案)	P26 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 エ　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15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またはメールにて緊急連絡を行うこと。また、セキュリティインシデント発生元の特定が可能であり、かつ、その端末が接続団体内の端末と判断できる場合は、可能な範囲で端末を特定した上で電話またはメールにて報告すること。 【意見】 ・緊急時の状況に応じて、柔軟に連絡方法を選択できる方が望ましいと考える為、緊急連絡の際に電話とメールの他に「ポータルサイトの機能（例えばチャット等）」を連絡方法の候補に含めて頂けないでしょうか。	・緊急時は、当該接続団体の担当者への「連絡」が必要と考えており、どのようなツールを利用する場合でも、担当者へ伝わったことを確認していただく必要があります。 ・そのため、チャットやポータルサイトの機能で、通知等を行い、かつ、閲覧確認等ができるのであれば、それらの機能を利用しても問題ありません。ただし、各接続団体における担当者が当該ツールを利用できない場合は、別の方法で連絡を実施していただくことになりますので、ご注意ください。 ・以上のことから、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15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、担当者に対してインシデントの内容等について、確実に伝達すること。また、セキュリティインシデント発生元の特定が可能であり、かつ、その端末が接続団体内の端末と判断できる場合は、可能な範囲で端末を特定した上で電話やメール等の方法により、報告すること。	あり
56	仕様書(案)	P29 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 エ　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、不正な通信に対する調査、解析結果とともに、監視対象ネットワーク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】 調査・解析は本件で導入した機器のログにて行います。導入していない機器のログ確認は対象外という想定でおりますがよろしいでしょうか。	・お見込みのとおり、セキュリティ監視等業務におけるリアルタイム監視を実施する対象ログは、本委託業務で導入した機器等のログとなりますので、各接続団体における既存ネットワークや既存機器については、対象外とお考えください。 ・なお、インシデントの対応時において、詳細ログが提供された場合には、調査・分析を行っていただくことを想定していますので、ご注意ください。 ・以上のことから、仕様書の修正はなしとします。	なし
57	仕様書(案)	P30 11　業務詳細 （９）利用サービスの詳細にかかる要件 ア　基本要件	【記載内容】 ・各接続団体に提供するサービスは原則として同内容とするが、通信量に関しては、接続団体毎に上限設定が可能なこと。 【意見】 ・通信量の上限制限より、通信速度による上限制限の方が、回線輻輳時におけるトラヒックコントロールの効果を得やすいと考えておりますので、通信量の上限以外に、帯域制限等による通信速度（bps）の上限設定でも可として頂けないでしょうか。	・誤記（通信量　→　通信帯域）がありましたので修正します。また、帯域制限以外の制限方法であっても要件を満たすことが明らかになるように、記載内容を以下に変更します。 【変更内容】 ・各接続団体に提供するサービスは原則として同内容とするが、通信帯域に関して接続団体毎に上限設定が行えるなど、特定の接続団体がセキュリティクラウドの機能を占有できないような制限が可能なこと。	あり
58	仕様書(案)	P30 11　業務詳細 （９）利用サービスの詳細にかかる要件 ウ　性能要件	【記載内容】 ・CDNについて、接続団体数× 2（公式 Web サイト、防災サイト）に加えて、10 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。 【意見】 ・CDNについて、以下のような条件も追記頂けると幸いです。 ①運用期間中において、CDNの対象となるWebサイトの増減やFQDNの変更に追加請求なく対応すること。 ②「CDN導入に伴い証明書が必要となる場合、追加請求なく証明書を提供すること。5年間の運用で必要な証明書の更新手続きを行い、更新した証明書を提供すること。」 もしくは、「5年間該当団体よりCDN利用の際は、対象のオリジンサーバの証明書を提供すること。」 どちらかに決めて頂きたい。 ③CDNコントロールパネルのアカウントを、接続団体個別に追加請求なく発行すること。 ④CDNコントロールパネルの利用方法について、接続団体用の問合せ窓口を用意すること。 ⑤CDNのトラヒック転送状況など運用レポートを接続団体個別に出力できること。 ⑥CDNの障害を検知し、接続団体へ通知する運用とすること。	・各接続団体のWebサーバにかかる証明書については、各接続団体が調達するため本委託業務にかかる受託事業者での準備は不要です。 ・各接続団体における運用レポートの発行については、「11　業務詳細（７）運用・保守業務の設計にかかる要件　ケ　定期報告」に含まれていますので、ご確認ください。 ・CDNを含む、クラウドサービス等に対する稼働監視・障害対応については、「11　業務詳細（７）運用・保守業務の設計にかかる要件　オ　稼働監視・障害対応」に含まれていますので、ご確認ください。 ・CDNにかかる設定や問い合わせ窓口について、及び、その他の意見については、「11　業務詳細（９）利用サービスの詳細にかかる要件　イ　機能要件」に以下の内容を追記します。 【追記内容】 ・CDNについて、運用期間中における設定変更（CDNの対象となるサイト数の増減、FQDNの変更等）についても、本委託業務の範囲内とすること。 ・CDNについて、各接続団体用のアカウントを作成し、各接続団体から直接、設定変更ができること。また、問い合わせ窓口を用意し、それぞれの接続団体で利用できること。なお、設定変更を直接、実施する接続団体はほとんどないと想定しているため注意すること。（多くの場合は、他の設定変更依頼への対応と同じく、受託事業者で対応を行うこととなる。）	あり
59	仕様書(案)	P31 11　業務詳細 （10）通信回線にかかる要件 ア　インターネット接続回線	【記載内容】 ・グローバルIPアドレスを256個以上利用できるようにすること。但しクラウドサービスの提供方式によって、同等のサービスが提供できる場合はこの限りでない。 【意見】 ・インターネット回線や公開WEBサーバ回線の冗長化の設計を行うにあたり、必要なグローバルIPアドレス数が増え、グローバルIPアドレス不足とならないようにしたい為、事前にグローバルIPアドレスの用途の使用状況を開示頂きたい。	・現在の想定としては、インバウンド用の通信に必要となるアドレスの他、各接続団体からのアウトバウンド用通信における送信元アドレスとしても、必要になると想定しています。 ・さらに、「自治体情報セキュリティ対策の見直しについて https://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000098.html」等により、各接続団体がセキュリティ対策の見直しを行うこととなったとき、現時点での詳細は不明ですが、必要になると想定しています。	なし
60	仕様書(案)	P31 11　業務詳細 （９）利用サービスの詳細にかかる要件 ウ　性能要件	【記載内容】 ・ 各接続団体からのインターネットに向けた通信、及び、インターネットからセキュリティクラウド内に向けた通信について、後述する「（10）通信回線にかかる要件　ア　インターネット接続回線」で用意する帯域以上の処理性能を有すること。（通信回線以外のサービスでボトルネックが発生しないような性能とすること。） 【意見】 「（通信回線以外のサービスでボトルネックが発生しないような性能とすること）」とございます。 クラウド接続回線（帯域確保1Gbps/1GpsﾍﾞｽﾄｴﾌｫｰﾄのActive/Stanbyで実質1Gbps）等でのボトルネックが発生するであろうと想定されますが、参加団体様（市町様等）に向けては県民サービス向上の一助につながるものであると考えておりますので、利用サービスに係る性能要件と同様として、クラウド接続回線の要件見直しをお願いいたします。 トラフィック過多が想定されている場合であれば、「クラウドサービス提供施設」を三重県様情報ネットワーク集約ポイントである津DC内とし、その間を広帯域構内配線等で結ぶ方がより効率的な方策かと考えております。	・ご指摘のとおり、インターネット接続回線をクラウド接続回線以上の帯域とした場合、クラウド接続回線がボトルネックになり、インターネット接続回線において十分な通信ができなくなる可能性はありますが、運用期間中において、インターネット接続回線の増強は想定していないことから、各接続団体における適切な上限帯域設定や、フィルタリング、ローカルブレイクアウトの実施等を行うことで、上限に至らないような運用を行うことを想定しています。とはいえ、クラウド接続回線がボトルネックにならないよう、以下の内容に修正します。 【変更内容】 ・ 各接続団体からのインターネットに向けた通信、及び、インターネットからセキュリティクラウド内に向けた通信について、後述する「（10）通信回線にかかる要件　ア　インターネット接続回線」で用意する帯域以上の処理性能を有すること。（インターネット接続回線、および、ブレイクアウト接続回線以外のサービスでボトルネックが発生しないような処理能力を有すること。例えば、想定される通信量から逆算し、クラウド接続回線の増強やファイアウォールの機器スペックを向上させるなどの対応を行うこと。） ・インターネット接続回線については、運用期間内において、適切な上限帯域設定や、フィルタリング、ローカルブレイクアウトの実施等を行うことで、インターネット接続回線がボトルネックとならないような対応を行うこととしているが、運用期間内において、クラウド接続回線がボトルネックとなる場合は、本委託業務の範囲内で増強を行うこと。 ---------- ・また、データセンターの指定にかかるご意見についてですが、本委託業務は、そもそも各種サービスをクラウドサービスにより提供いただくことを要件としており、また、クラウドサービスによる提供とは、受託事業者が「クラウドサービス提供施設」にて、新規に機器導入を行うほか、既存の設備やサービス等を組み合わせて各種サービスを提供する等、様々な形態があると想定しています。このとき、クラウドサービス提供施設として利用するデータセンターについても自由に組み合わせて利用することを否定するものではないため、クラウドサービス提供施設として利用するデータセンターについて、1か所に指定することはしておりませんのでご理解ください。 ・なお、ご指摘の通り、本県が別途調達しているデータセンター（津市内）とクラウドサービス提供施設間の通信回線がボトルネックになる恐れがあることから、十分な帯域のクラウド接続回線を提供することについて、別途、要件を追記します。	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		
61	仕様書(案)	P31 11　業務詳細 （９）利用サービスの詳細にかかる要件 ウ　性能要件	【記載内容】 （なし） 【意見】 　具体的な数値要件のご提示が無く、受託者側で準備する機器類のスペック算定ができません。この仕様ですと、既存業者様のみが知る情報で全入札参加者様に不公平な条件になろうかと考えます。 　あくまで一例ですが、現在の各市町様からの通信トラフィックの主たるプロトコル別にピーク時の通信量、セッション数等、機器類に関わる全体の情報（マルウェア検知数、IDS・IPS検知・遮断数、メールリレーサーバのトランザクション量等も）開示を頂きたくお願いします。 　また、今後5年間で三重県様が想定されている通信量や、セッション数の増加等もご指定頂きたくお願いいたします。	・現在の通信トラフィックとして、トラフィック情報、メール流量、ファイアウォール詳細等について、可能な限り、公告時に公開するようにします。なお、今後5年間の想定通信量について、上限は、各接続回線の上限となりますが、セッション数等の上限については、設計段階での検討事項と考えていますので、受託事業者において、トラフィック調査やこれまでのノウハウ、データや根拠等を示していただいたうえで、設計を行っていただき、本県の承認を得ていただくことになりますので、ご注意ください。 ----------（R3.6.3追記） ・通信トラフィックの主なものは以下のとおりです。なお、機器等の構成については、「２事業概要（２）業務範囲　イ　現行セキュリティクラウドの構成概要」を参照してください。 ・ファイアウォールセッション数：50,000～60,000（繁忙期である12時～13時のデータ） ・メール流量：340万件/月（送信40万件、受信300万件） ・トラフィック情報　ISP1（各接続団体からインターネット）： 　インバウンド　業務時間中平均300Mbps、月間平均90Mbps、 　アウトバウンド　業務時間中平均60Mbps、月間平均30Mbps ・トラフィック情報　ISP2（インターネットから各接続団体Webサーバ等）： 　インバウンド　業務時間中平均45Mbps、月間平均25Mbps、 　アウトバウンド　業務時間中平均65Mbps、月間平均40Mbps	なし
62	仕様書(案)	P32 11　業務詳細 （10）通信回線にかかる要件 イ　クラウド接続回線	【記載内容】 ・1Gbpsの帯域が確保されている回線と、1Gbpsのベストエフォート回線を2回線準備すること。なお、それぞれの回線については、Active/Standby構成とすること。 ・上記2回線を閉域網で提供すること。 【意見】 　クラウドサービス提供施設のインターネット接続回線がブレイク回線と併せて4Gbpsのベストエフォート回線となっています。ところが、クラウド接続回線は1Gbps帯域確保・1GbpsﾍﾞｽﾄｴﾌｫｰﾄのActive/Stanbyとご指定になっておりまして、三重県様が別途調達している津市内データセンター・クラウドサービス提供施設間は、実質1Gbpsの帯域となります。 　三重県様参加団体様庁舎側から外部、外部から参加団体様庁舎側のトラフィックは年々増加している傾向にあろうかと存じますが、1Gbpsとされた明確な理由はございますでしょうか。キャッシュできるような通信ではなく、動的コンテンツ類の通信増となっていようかと存じており、1Gbpsでは不足すると推察されます。 　既に津市内データセンターには、参加団体様を結ぶ三重県情報ネットワークの収容拠点でもあると存じ上げておりますが、各参加団体様と該当三重県情報ネットワークのアクセスポイントは最大1Gpbsの帯域で接続されていらっしゃると思います。 　トラフィック確保の観点で、クラウド接続回線が1Gbpsというのは無理がある構成かと考えております。 　受託事業者側には、クラウド接続回線を4Gbpsと同等以上のクラウド接続回線をお求めになられる方が各市町様を通じた県民サービス向上に寄与されることとなろうかと思います。 　このため、津市内データセンターには既に各団体様を接続する三重県様がご準備された三重県情報ネットワークインフラが整備されており、津市内データセンター内でクラウドサービス提供をするのが最も効率的かと存じますので、「クラウドサービス提供施設」を既設の津市内データセンター内とご指定頂くことはできますでしょうか。	・各接続団体からのアウトバウンド通信にかかる通信量は、増加する一方ですが、各接続団体における適切な通信帯域の上限設定やローカルブレイクアウト等の対応を実施することにより、運用期間中に上限に達しないような運用が可能であると考えています。 ・とはいえ、ご指摘の通り、クラウド接続回線について、ボトルネックになる可能性があることから、「1Gbpsの帯域が～Active/Standby構成とすること。」及び「上記2回線を閉域網で提供すること。」までを削除したうえで、記載内容を以下に変更します。 【変更内容】 ・ インターネット接続回線、及び、ブレイクアウト接続回線の構成に応じて、クラウド接続回線として十分な帯域の回線を閉域網にて用意すること。 ---------- ・また、データセンターの指定にかかるご意見についてですが、本委託業務は、そもそも各種サービスをクラウドサービスにより提供いただくことを要件としており、また、クラウドサービスによる提供とは、受託事業者が「クラウドサービス提供施設」にて、新規に機器導入を行うほか、既存の設備やサービス等を組み合わせて各種サービスを提供する等、様々な形態があると想定しています。このとき、クラウドサービス提供施設として利用するデータセンターについても自由に組み合わせて利用することを否定するものではないため、クラウドサービス提供施設として利用するデータセンターについて、1か所に指定することはしておりませんのでご理解ください。 ・なお、ご指摘の通り、本県が別途調達しているデータセンター（津市内）とクラウドサービス提供施設間の通信回線がボトルネックになる恐れがあることから、十分な帯域のクラウド接続回線を提供することについて、別途、要件を追記します。	あり
63	仕様書(案)	P32 11　業務詳細 （10）通信回線にかかる要件 ウ　ブレイクアウト接続回線	【記載内容】 ・ブレイクアウト接続回線として、冗長性を確保した回線を用意すること。 【意見】 ・ブレイクアウト接続回線について、ローカルブレイクアウト回線を利用した攻撃のリスクを増加させたり、可用性や運用性を損なうような事がないよう対策が必要と考える為、以下の要件など追記の検討を頂きたい。 ①ローカルブレイクアウト回線用にもインターネット回線と同等程度のセキュリティ機能を実装すること（セキュリティのクラウドサービスの利用も可） ②ローカルブレイクアウト回線経由の特定の通信を必要に応じて遮断できる機能を有すること。 ③ローカルブレイクアウト回線において接続団体毎に通信量、もしくは通信速度の上限設定が可能なこと。また、送信元アドレスに基づきブレイクアウト回線の利用可否などのコンロールが可能なこと。 ④ローカルブレイクアウト回線の通信について通信ログの採取とレポート作成が可能な事。また、想定外の通信や攻撃が無かったか通信ログの監視を行う事。 ⑤ローカルブレイクアウト回線において、NW機器(三情)の接続部分やブレイクアウト用機器やブレイクアウト用の回線(GIP含む)が冗長化されシングルポイント障害で停止する事が無い事。また、通常のインターネット回線への通信へ影響が無い事。	・「11　業務詳細（９）利用サービスの詳細にかかる要件　イ　機能要件」に以下の内容を追記します。 【追記内容】 ・ ブレイクアウト接続回線にかかる通信について、接続先となる利用サービス、及び、接続元となる接続団体による細かな利用制限（フィルタリング）や「IDS/IPS」等のセキュリティ対策が実施できること。ただし、制限等を実現する機能等については、全ての接続団体が利用する場合を想定し、十分な処理能力を有したものとすること。（運用期間当初は、ほとんど利用がないと想定しているが、徐々に利用が増えてくると考えられることから、綿密な容量計算等を行う必要があると想定している。） ・ ブレイクアウト接続回線からの通信について通信ログの採取とレポート作成が可能なこと。また、「IDS/IPS」で異常な通信を検知した際は、セキュリティ監視等業務として、調査・分析が行えること。 ---------- ・冗長化については、記載内容を、以下の内容に修正します。 【変更内容】 ・ブレイクアウト接続回線が不通となった場合を想定し、インターネット接続回線等を経由する形への経路変更の対応や、迅速な障害対応（機器の予備機の確保、現地常駐SEによる機器交換等）が実施できること。また、インターネット接続回線とブレイクアウト接続回線は別キャリアとすること。	あり
64	仕様書(案)	P32 11　業務詳細 （10）通信回線にかかる要件 ウ　ブレイクアウト接続回線	【記載内容】 （なし） 【意見】 　一般的に「既にセキュリティが確保されているサービス間の通信用」として準備されるのかと認識しています。 　全参加団体様のどのようなサービスを該当回線で接続される予定でしょうか。 　また、該当回線に限ってですが、三重県様の閉域網内に直接接続されることとなりますが、この回線で利用されるグローバルIP（128個）についてセキュリティ対策は要件に入っていないよう見られます。 　セキュリティ対策は必要かと存じ上げますが、セキュリティ対策を講じる場合は「クラウドサービス提供施設」に存在する各種セキュリティ機器へ一旦通信をルーティングさせてセキュリティ対策を取る必要があるという認識で宜しいでしょうか。そうしますと、クラウド接続回線をブレイクアウト接続回線トラフィックが折り返しで利用することとなり、帯域圧迫に繋がると懸念されようかと思います。 　「クラウドサービス提供施設」側でブレイクアウト接続回線を提供するのが効率的かと存じますが、現在、三重県様の三重県情報ネットワークインフラの集約拠点とされております津DCに集約するのが最も効果的であると考えており、「クラウドサービス提供施設」自体も津DCであるべきと考えておりますが、津DCでは無い他拠点で「クラウドサービス提供施設」を準備されることをお認めされている背景や目的などを明確に頂きたくお願いするとともに、効率性を考えると、津DCの方が「クラウドサービス提供施設」として良いと考えらえる為、「クラウドサービス提供施設」を津DCと限定頂きたくお願いします。	・ブレイクアウト接続回線に対するセキュリティ対策については、No63にて記載しています。 ・ブレイクアウト接続回線の利用について、詳細は未定ですが、十分なセキュリティ対策を実施できる特定のサービスのみに限定することを想定しています。そのため、当該トラフィックについては、クラウドサービス提供施設への折り返しは不要と考えています。 ・ブレイクアウト接続回線をクラウドサービス提供施設から接続するよう指定することについて、本委託業務は、各種サービスをクラウドサービスにより提供いただくことを要件としており、また、クラウドサービスによる提供とは、受託事業者がクラウドサービス提供施設にて、新規に機器導入を行うほか、既存の設備やサービス等を組み合わせて各種サービスを提供する形態を想定しています。そのため、ブレイクアウト接続回線についても、クラウドサービス提供施設での接続の他、本県が別途調達しているデータセンター（津市内）での接続についても否定するものではないため、ブレイクアウト接続回線を接続するデータセンター、及び、クラウドサービス提供施設として利用するデータセンターについて、1か所に指定することはしておりませんのでご理解ください。	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		
65	仕様書(案)	全体	【記載内容】 （省略） 【意見】 本件の調達にあたっては、委託業務とされておりますが、「仕様書P9　6支払い」には年度毎の上限割合率を提示頂いております。 実際の調達にあたっては、三重県様予算上限額の設定はあろうかと思いますが、品質維持を目的として、最低限度額を設定頂くことはできないでしょうか。	・本委託業務は、地方公共団体の締結する契約のうち、政府調達に関する協定の適用を受ける契約に該当するため、「物品等又は特定役務の調達手続きの特例を定める規則」及び「地方公共団体の物品等又は特定役務の調達手続の特例を定める政令」に基づき調達手続きを行う必要があります。 ・そのため、最低制限価格制度の対象外となりますので、ご理解ください。	なし
66	仕様書(案)	P22 11　業務詳細 （７）運用・保守業務の設計にかかる要件 ウ　ポータルサイト	【記載内容】 ・問合せ・ファイル授受機能を受託事業者が更新した際は、当該接続団体に紐づくメールアドレスへ通知を行えること。 【意見】 ・メールアドレスへ通知を行えることとするとツールが限定されてしまう為、上記の受託条件について、記載の変更をお願いできますでしょうか。 「問合せ・ファイル授受機能を受託事業者が更新した際は、当該接続団体に紐づく メールアドレスへ通知を行えること。また、メール通知が難しい場合、アプリアイコンバッチやWindowsのバナーやサウンドによる通知も可能とする。」	・通知について、メールでの通知だけでなく、アプリ等によるPush型通知も要件を満たすことから、記載内容について、以下の内容に変更します。 ・なお、他の通知等にかかる要件についても同様の変更を行います。（メールアドレスへ通知を行えること　→　メール等による通知が行えること） 【変更内容】 ・問合せ・ファイル授受機能を受託事業者が更新した際は、当該接続団体に紐づく メール等による通知が行えること。	あり
67	仕様書(案)	P26 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 イ　SOCの詳細	【記載内容】 ・経済産業省の情報セキュリティサービス基準適合認定（セキュリティ監視・運用サービス）に登録されていること。 【意見】 ・上記の受託条件について、記載の変更をお願いできますでしょうか。 「経済産業省の情報セキュリティサービス基準適合認定（セキュリティ監視・運用サービス）に登録されていること。 登録や登録予定がない場合は、下記のいずれかの書類を提出すること。 ①下記URLの情報セキュリティサービス基準における「４ セキュリティ監視・運用サービスに係る審査基準」を満たす書類 https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html ②総務省のクラウドサービス提供における情報セキュリティ対策ガイドライン（第２版）で定義のSOC2Report https://www.soumu.go.jp/main_content/000566969.pdf」	・本要件は、SOCにかかる要件とすることで、一定のサービスレベルを確保することを目的としています。しかしながら、①の書類が提出できる（取得できる見込みがある）、②の書類が提出できる（外部機関によるクラウドサービスの提供事業者として認証を受けている）などの対応が可能な事業者を制限するものではないため、記載内容について、以下の内容に変更します。 【変更内容】 ・経済産業省の情報セキュリティサービス基準適合認定（セキュリティ監視・運用サービス）に登録されている、または、登録見込みであること。	あり
68	仕様書(案)	P29 11　業務詳細 （８）セキュリティ監視等業務の設計にかかる要件 エ　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、不正な通信に対する調査、解析の結果から監視等の対象となる機器やネットワーク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SOCのサービスでは、インシデントはSIEMエンジンとアナリストの分析にて原則3段階の重要度で分類となりますが、実運用に合わせて（検知対象など）条件による分類変更や通知ポリシーのカスタマイズが可能です。 そのため、上記の受託条件について、以下の通り記載の変更をお願いできますでしょうか。 「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、不正な通信に対する調査、解析の結果から監視等の対象となる機器やネットワーク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。危険度の分析基準は4段階以上が望ましいものの3段階となる場合は、実運用に合わせて通知する危険度の変更や通知ポリシーのカスタマイズを行い、インシデントの内容に応じて柔軟に対応すること。」	・P29における危険度0と危険度1について、一つの危険度にまとめることは問題ありません。ただし、危険度2と危険度3については、SOC側での攻撃成否確認をしていただくための要件として設定しているため、分類を行っていただく必要があると考えています。 ・以上のことから、記載内容を以下に変更します。 【変更内容】 ・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、不正な通信に対する調査、解析の結果から監視等の対象となる機器やネットワーク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。なお、3段階での定義も可とするが、以下の例に示す危険度2と危険度3について、分類可能とすること。	あり
69	仕様書(案)	P29 11　業務詳細 （10）通信回線にかかる要件 ア　インターネット接続回線	【記載内容】 ・インターネット接続回線として 、冗長性を確保した回線を用意すること。 【意見】 冗長性が必要な範囲を明確にする為、次の内容を承諾頂けますでしょうか。 ・インターネット接続回線の障害時に公開WEBサーバ用回線をバックアップとして利用しても宜しいでしょうか？ ・公開WEBサーバ用回線の障害時に、インターネット接続回線をバックアップとして利用しても宜しいでしょうか？	・インターネット接続回線として、複数の回線を別々のケーブルで用意いただく構成であれば、要件を満たします。 ・なお、インターネットへの冗長性を確保する目的から、記載内容に以下の内容を追記します。 【追記内容】 ・また、インターネット接続回線とブレイクアウト接続回線は別キャリアとすること。	あり
70	仕様書(案)	P6 2　事業概要 （２）業務範囲 エ　サービス構成例	【記載内容】 （省略） 【意見】 サービス構成例として、CDNおよびWAFは「クラウドサービス提供施設」上ではなく、インターネット（SaaS）側に構成されておりますが、クラウドサービスとしてCDN/WAFは提供してもよいでしょうか。	・CDN、WAFを含む、全てのサービスについて、サービス利用型での提供であれば、どのような構成であっても問題ありません。 ・なお、クラウドサービス提供施設にてCDNやWAFを提供する場合は、DDoS攻撃時に正常な通信が遮断されないよう、十分な対応を行うようにしてください。	なし
71	仕様書(案)	P6 2　事業概要 （２）業務範囲 エ　サービス構成例	【記載内容】 （省略） 【意見】 リバースプロキシについては、CDN/WAFと同じくインターネット側のSaaSでもよいでしょうか。 市町のWebサーバが外部にある場合は、セキュリティクラウド提供設備側にて通信を終端すると、インターネット回線の非効率化につながります。	・CDN、WAFを含む、全てのサービスについて、サービス利用型での提供であれば、どのような構成であっても問題ありません。	なし
72	仕様書(案)	P6 2　事業概要 （２）業務範囲 エ　サービス構成例	【記載内容】 （省略） 【意見】 ブレイクアウト用機器については、セキュリティクラウドのセキュリティ機能を実施せず（SOC対象外）インターネット側へ通信をブレイクアウトすることとなりますが、ログの取得は必須化と考えます。ブレイクアウト用機器専用のログ収集装置を要件に組み入れることをご提案いたします。	・いただいたご意見を踏まえて、「11　業務詳細（９）利用サービスの詳細にかかる要件イ　機能要件」に以下の内容を追記します。 【追記内容】 ・ ブレイクアウト接続回線にかかる通信について、接続先となる利用サービス、及び、接続元となる接続団体による細かな利用制限（フィルタリング）や「IDS/IPS」等のセキュリティ対策が実施できること。ただし、制限等を実現する機能等については、全ての接続団体が利用する場合を想定し、十分な処理能力を有したものとすること。（運用期間当初は、ほとんど利用がないと想定しているが、徐々に利用が増えてくると考えられることから、綿密な容量計算等を行う必要があると想定している。） ・ ブレイクアウト接続回線からの通信について通信ログの採取とレポート作成が可能なこと。また、「IDS/IPS」で異常な通信を検知した際は、セキュリティ監視等業務として、調査・分析が行えること。	あり
73	仕様書(案)	P6 2　事業概要 （２）業務範囲 エ　サービス構成例	【記載内容】 （省略） 【意見】 ローカルブレイクアウトについては、クラウドアプリケーションを判別して通信制御する機能が必須と考えてよいでしょうか。	・お見込みのとおりです。	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		
74	仕様書(案)	P8 ４　履行場所	【記載内容】 ・NOCについては、迅速な運用・保守を行うため、原則として三重県内に設置すること。 【意見】 こちらについてですが、NOCについては、駆け付け含めて三重県内にあるのが最適かと考えますが、提案者の範囲を広げるため、隣接県（愛知県等）も許容いただけないでしょうか。	・本県は、南北、東西に長い地形であり、また、接続団体によっては、アクセスに時間がかかることが想定されるため、迅速な対応を行うことを目的として、NOCの設置場所を県内としています。（どのような配置であっても、県外の拠点のみでは、迅速な対応は不可能と考えています。） ・以上のことから、仕様書の修正はなしとします。	なし
75	仕様書(案)	P19 11 業務詳細 （５）構築設計	【記載内容】 ・各接続団体からインターネット上の各種サービス（例えば、Slack Technologies社Slack、Google社GoogleWorkspace、Microsoft社Office365、Cisco社WebEX等）へのアクセスについては、後述する「ブレイクアウト接続回線」から接続可能とすること。なお、処理能力に余裕を持たせることで、ブレイクアウト接続回線を利用せず、全てをインターネット接続回線から接続する構成とすることについても可とするが、今後の利用量の増加等も考慮して、十分な余裕を持たせること。 【意見】 こちらについてですが、Web会議や各市町が安全性を判断し利用を許可するクラウドサービス通信を対象とするということでよいでしょうか。	・お見込みのとおりです。	なし
76	仕様書(案)	P31 11　業務詳細 （９）利用サービスの詳細にかかる要件 ウ　性能要件	【記載内容】 ・選定するファイアウォールについて、本仕様書に記載された帯域、及び、機能を提供するにあたり、十分な性能を有すること。なお、本県が要求した場合、カタログスペックではなく、受託事業者による検証等により、性能を証明できること。 【意見】 こちらについてですが、ファイアウォールについて暗号化/復号化を実施する状況において検証した結果を、お示しすればよいでしょうか。	・お見込みのとおりです。	なし
77	仕様書(案)	全体	【記載内容】 （省略） 【意見】 セキュリティクラウドを構成する機器に対しての、詳細機能要件や負荷要件などはありますでしょうか。	・本県に対する機器の納品はないものと考えています。そのため、機器の詳細についての要件等はありません。	なし
78	仕様書(案)	全体	【記載内容】 （省略） 【意見】 各種機器については、仮想化基盤上の仮想アプライアンスの提供でも良いのでしょうか。 各機器についてはトラフィック量により相当パフォーマンスに影響が出ます。そのため、物理アプライアンスでの提供を推奨させていただきます。	・本県に対する機器の納品はないものと考えています。そのため、機器の詳細についての要件等はありません。	なし
79	仕様書(案)	P4 ２　事業概要 （２）業務範囲 イ　現行セキュリティクラウドの構成概要 表　現行システムにかか る機能等一覧	【記載内容】 （省略） 【意見】 DDoS対策についてISP側で実施すると回線コスト増に繋がる可能性があり、DDoS対策の柔軟性を確保するためISP側でという文言を外していただくことは可能でしょうか？	・本表に記載の要件は、現行システムにかかる要件であり、次期システムの要件ではありません。	なし
80	仕様書(案)	P21 11　業務詳細 （７）運用・保守業務の設計にかかる要件 ア　基本方針	【記載内容】 ・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については、県外、かつ、複数での設置も可とする。ただし、少なくとも1拠点は県内へ設置すること。 【意見】 NOCの所在地は、県内を原則とするとありますが、コストの観点からNOCの配置場所は県外も可能という形にできないでしょうか?障害発生により現地への駆けつけが必要な場合は迅速に駆けつけるようにいたします。	・本県は、南北、東西に長い地形であり、また、接続団体によっては、アクセスに時間がかかることが想定されるため、NOCの設置場所については、迅速な対応を行うことを目的として、県内としています。 ・以上のことから、仕様書の修正はなしとします。	なし
81	仕様書(案)	P4,P8	表記ゆれの対応 　DDoS　に統一します。	・該当箇所を修正します。	あり
82	仕様書(案)	P31	誤字・脱字・誤植対応 　ブレイクアウト回線　→　ブレイクアウト接続回線	・該当箇所を修正します。	あり
83	仕様書(案)	P30 11　業務詳細 （９）利用サービスの詳細にかかる要件 イ　機能要件	【記載内容】 ・各利用サービスにおける詳細な機能要件については、別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」を参照すること。 【意見】 ・デジタル基盤改革支援補助金（次期自治体情報セキュリティクラウド移行事業）関連の修正	・以下のように修正します。 【変更内容】 ・各利用サービスにおける詳細な機能要件については、別紙「次期セキュリティクラウドにかかる利用サービスの詳細要件」を参照すること。また、令和2年8月18日総行情109号総務省自治行政局地域情報政策室長通知「次期自治体情報セキュリティクラウドの標準要件について」で示された必須要件を満たすこと。	あり
84	仕様書(案)	P9 ６　支払い （２）内訳資料の提出	【記載内容】 ・上記支払条件を踏まえて、契約締結後、速やかに、契約額の内訳資料（税抜き金額を明記すること）を作成し提出すること。 ・特に初期費用の内、構築費用と移行費用、さらに、保守費用について、明確に分離した内訳資料を作成すること。 【意見】 ・デジタル基盤改革支援補助金（次期自治体情報セキュリティクラウド移行事業）関連の修正	・以下のように修正します。 【変更内容】 ・上記支払条件を踏まえて、契約締結後、速やかに、契約額の内訳資料（税抜き金額を明記すること）を作成し提出すること。 ・特に初期費用の内、提供するサービス単位で「設計」「設定」「テスト」「移行」「その他」、さらに、保守費用について、明確に分離した内訳資料を作成すること。	あり