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・保守業務契約に

関する仕様書（案）

令和３年４月

三重県デジタル社会推進局

スマート改革推進課

１　背景と目的

（１）はじめに

本仕様書は、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（以下、「本委託業務」という。）の仕様について記載している。

（２）三重県自治体情報セキュリティクラウドとは

自治体情報セキュリティクラウドとは、都道府県と市町村が共同して、都道府県ごとにインターネットへの接続口を一つに集約し、高度なセキュリティ監視を行うものであり、このうち、「三重県自治体情報セキュリティクラウド」とは、三重県、及び、県内各市町（29 市町）と広域連合（3 団体）の計 33 団体（以下、「接続団体」という。）が利用する三重県版の自治体情報セキュリティクラウドのことである。（以下、特に注釈のない限り、「三重県自治体情報セキュリティクラウド」を「セキュリティクラウド」という。）

現行のセキュリティクラウドは、接続団体が管理する個人情報等の重要なデータの漏えいを未然に防止することを目的とし、接続団体が必要とする情報セキュリティ水準を確保しつつ、迅速な初動対応を行うため、

- 各自治体のインターネット業務用ネットワークを不正アクセスから保護する
- 各自治体のインターネット業務用ネットワークにおいて、情報セキュリティインシデントが発生した場合、これを検知し事前に登録した職員等へ通報する
- 情報セキュリティインシデントへの適切な対応を判断するため、具体的な状況の把握と影響範囲の調査を支援する

といった機能を有する。

（３）本委託業務の目的

現行のセキュリティクラウドは、平成 28 年度にオンプレミス構成により、構築し、運用を行っているが、運用期限である令和 3 年度末が迫っている。

さらに、総務省から、次期セキュリティクラウドにかかる機能要件として、

- 災害時等の公式Web サイト等におけるアクセス集中を想定した安定した情報発信
- 外部環境の変化への対応（大規模サイバー攻撃、手口の巧妙化）
- 可能性、コスト等を考慮した回線サービスの選定
- クラウドサービスの活用
- 都道府県と市区町村が一体となったセキュリティ対策とインシデント対応

等が示され、その対応を求められている。

以上のことから、これら機能を実現した次期セキュリティクラウドを構築したうえで、現行セキュリティクラウドから次期セキュリティクラウドへ移行することで、各接続団体が安定的に利用できるセキュリティクラウドを提供し、運用を行うことを本委託業務の目的とする。

２　事業概要

（１）契約名

契約名は、「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・保守業務契約」とする。

（２）業務範囲

ア　業務概要

- 本委託業務について、業務全体に対する業務計画書を作成のうえ、進行管理を行うこと。
- 本委託業務を実施するにあたり、現地調査、各接続団体からのヒアリング、各接続団体のインターネット接続環境にかかる受託事業者等、関係者等との事前調整を行ったうえで、必要な設計を行うこと。
- セキュリティクラウドとして、必要な機能をクラウドサービスにより提供を行うこと。また、通信回線についても提供を行うこと。
- 現行セキュリティクラウドを利用している各接続団体について、次期セキュリティクラウドへの移行作業を行うこと。
- 接続団体の移行後、契約期間終了日まで、セキュリティクラウドの安定的な運用を行うとともに、接続団体からの設定変更依頼、操作方法等の問い合わせ対応等の運用・保守業務を行うこと。
- セキュリティクラウド上の各機能等にかかる運用監視を行い、インシデント発生時には、事前の設計内容に基づき、担当者への通知、ネットワークの制限、復旧までの支援等の作業を行うこと。
- 業務の詳細については、「11　業務詳細」を確認すること。

イ　現行セキュリティクラウドの構成概要

・ 現行セキュリティクラウドの構成概要は、以下のとおり。

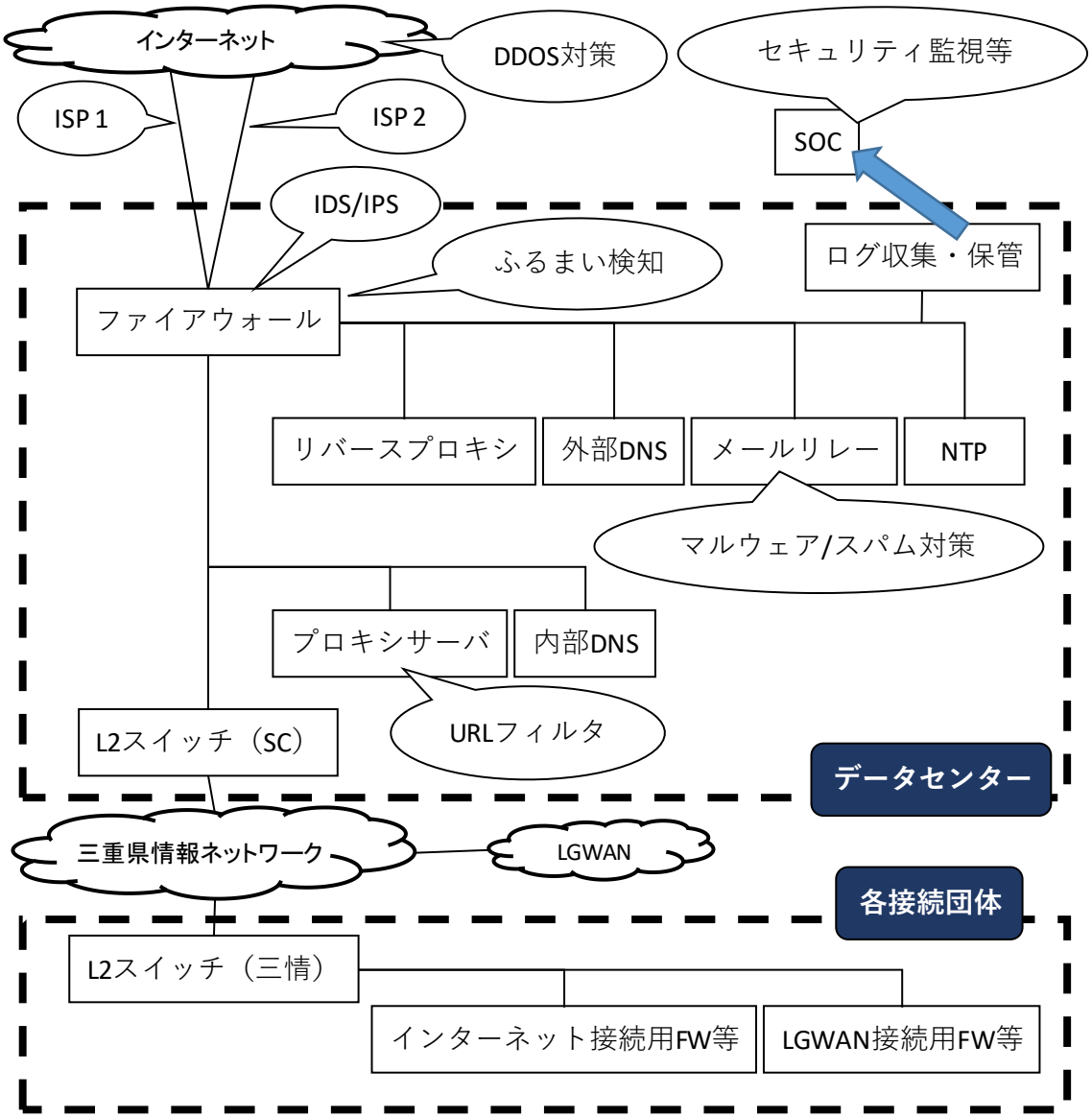

図　現行セキュリティクラウドの構成概要

機器・機能	内容
ファイアウォール（FW）	・三重県セキュリティクラウドとインターネットの境界にあり、プロトコル単位で通信を制御する機器 ・インターネット閲覧（ブラウンジング通信）におけるマルウェア対策も実施
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

外部 DNS	・接続団体の DNS 情報（URL とグローバル IP の変換情報）を集約した DNS 機能を持った機器
メールリレー	・インターネットを経由して送信・受信するメールを市町のメールサーバへリレーする機器
NTP	・インターネット上の信頼できる機器と時刻同期を行い、接続団体の各機器へ時刻同期を行う機器
ログ収集・保管	・各機器から出力されるログを収集、保管する機器（保存期間は 1 年間）
プロキシサーバ	・インターネット閲覧（ブラウジング通信）において、端末の代理としてインターネットとの通信を行う機器
内部 DNS	・再帰検索を行いドメイン情報の解決要求を行う機器
L2 スイッチ（SC）	・セキュリティクラウドと三重県情報ネットワークとを接続するための機器
L2 スイッチ（三情）	・三重県情報ネットワークと各接続団体とを接続するための機器 ・当初、セキュリティクラウドの一部として整備したが、現在は、三重県情報ネットワークの一部として別途整備済み
SOC	・Security Operation Center ・セキュリティ監視等を行う拠点
インターネット接続用 FW 等	・各接続団体におけるインターネット用ネットワークを三重県情報ネットワーク経由でセキュリティクラウドへ接続するための機器等
LGWAN 接続用 FW 等	・各接続団体における LGWAN 業務用ネットワークを三重県情報ネットワーク経由で LGWAN へ接続するための機器等

表　現行システムにかかる機器等一覧

機器・機能	内容
ISP 1	・Web ブラウジング等のアウトバウンド通信用回線 ・接続団体毎に異なるグローバル IP アドレスを付与
ISP 2	・公開サーバ等のインバウンド通信用回線
DDoS 対策	・公開 Web サーバに対する DDos 攻撃トラフィックを ISP 側で緩和する機能
IDS/IPS	・インターネットとの通信において、不正に侵入しようとする異常な通信を検知及び遮断する機能
ふるまい検知	・インターネットとの通信に含まれるファイルなどを隔離した疑似空間において動作を確認し、不正か否かを検知する機能
マルウェア/スパム対策	・メールに対するスパム対策やマルウェア対策を行う機能
URL フィルタ	・URL フィルタ機能（共通ブラックリスト）
セキュリティ監視等	・セキュリティアラートの監視・分析や、セキュリティ機能の性能維持・メンテナンス業務を実施する機能

表　現行システムにかかる機能等一覧

ウ　接続団体

- 三重県、津市、四日市市、伊勢市、松阪市、桑名市、鈴鹿市、名張市、尾鷲市、亀山市、鳥羽市、熊野市、いなべ市、志摩市、伊賀市、木曽岬町、東員町、菰野町、朝日町、川越町、多気町、明和町、大台町、玉城町、度会町、大紀町、南伊勢町、紀北町、御浜町、紀宝町、紀北広域連合、紀南介護保険広域連合、三重県後期高齢者医療広域連合（計 33 団体）
- 利用者数 約 15,000 人
- 端末数 約 15,000 台
- 今後、参加団体における利用者数、端末数の増減が予想されるが、その最大の利用者数として、30,000 アカウント、及び、26,500 台としてライセンスの調達を行うこと。（最大数は、1 ユーザあたり 2 アカウントと想定して 30,000 アカウント、将来的に全ての接続団体がβモデル（各自治体における 3 層分離ネットワークの内、業務端末をインターネット接続系ネットワークに接続して利用する構成のこと）へ移行し、かつ、リモートワーク等による端末台数の増加を想定して 26,500 台とした。）

エ　サービス構成例

・ 現時点で想定している次期セキュリティクラウドにかかるサービス構成例については、以下のとおり。

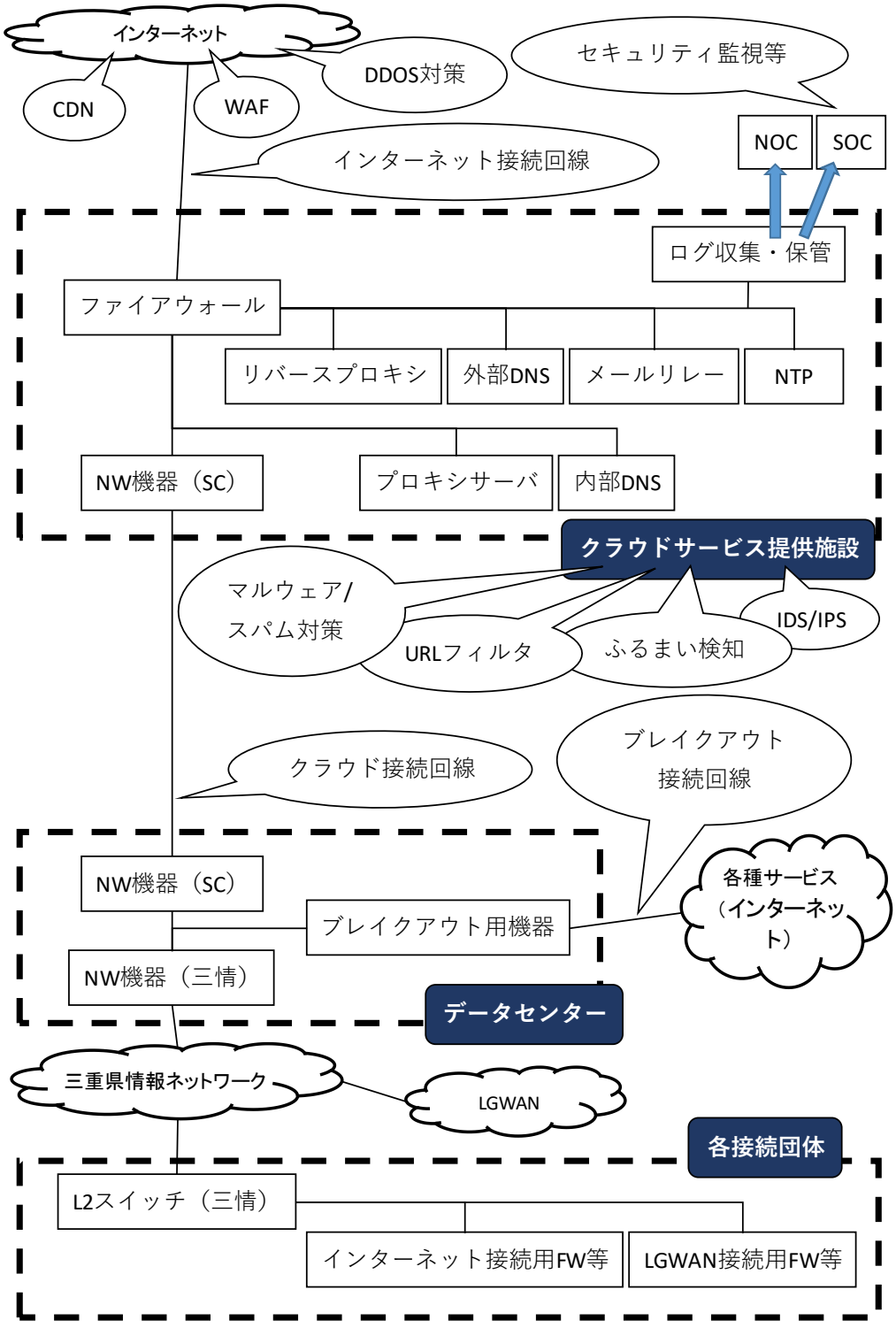

図　次期セキュリティクラウドのサービス構成例

※ 上図はあくまで例であり、本構成に限定するものではないため、注意すること。なお、詳細要件については、「11　業務詳細（9）利用サービスの詳細にかかる要件」を確認すること。

（3）受託要件

本委託業務の受託要件は、以下のとおりとする。

ア　運用実績

- 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。

イ　認証取得

- 以下のいずれかの認証を受けていること。
  - 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。
  - 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。

ウ　NOC 及び SOC

- 受託事業者が提供する NOC、及び、SOC について、自治体情報セキュリティクラウドの運用・保守実績を有すること。（NOC、及び、SOC の詳細については、「4　履行場所」を参照のこと。）
- 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。

３　調達スケジュール

期間名	詳細
契約履行期間	・本契約の締結日から令和９年３月 31 日までとする。
構築期間	・本契約の締結日から令和４年１月 31 日までとする。 ・構築期間において、各種設計、必要な機器やサービスの調達、構築作業、各種試験等を完了すること。
移行期間	・令和４年２月から令和４年３月 31 日までとする。 ・移行期間内に、全接続団体の移行を完了すること。 ・移行が完了した接続団体に対しては、運用期間と同様の機能を提供すること。
運用期間	・令和４年４月１日から令和９年３月 31 日までとする。

４　履行場所

本業務の履行場所は、本県及び各接続団体（県内）、本県が別途調達しているデータセンター（津市内）、クラウドサービス提供施設、NOC、SOC とする。

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。なお、現地対応が必要な保守要員以外の要員（問い合わせ対応、設定変更等、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、県外での設置も可とする。

SOC については、受託事業者が準備した場所とするが、日本国内とし、また、その場所を本県に開示できること。

本県が別途調達しているデータセンター、及び、受託事業者が利用するデータセンターにかかる要件については、「11　業務詳細（１１）データセンターにかかる要件」を参照すること。

施設名	詳細
クラウドサービス提供施設	・クラウドサービスを提供するための施設のこと。各受託事業者が契約するデータセンターを想定している。
インターネット上の各種サービス	・クラウドサービス提供施設以外で展開されている各種サービスのこと。 ・DDOS 対策サービスや CDN 等が該当する。
NOC（Network Operation Center）	・セキュリティクラウドを保守・運用していくうえで必要となる、運用・保守要員等が勤務する施設のこと。
SOC（Security Operation Center）	・セキュリティ上の監視を行うための監視装置等を設置した施設のこと。 ・クラウドサービス提供施設と同一の場合もあれば、別拠点の場合もあると想定している。
本県が別途調達しているデータセンター	・津市内にあるデータセンターのこと。
本庁舎	・三重県の本庁舎のこと。

表　履行場所の詳細

５　納品物件

（１）ハードウェア及びソフトウェア

本業務に必要となる全てのハードウェア及びソフトウェアを調達すること。

調達するハードウェア及びソフトウェアは、履行期間内において、保守可能であることを前提とする。契約期間中に調達した製品のサポートが終了する場合は、受託事業者の責において後継製品や同等の性能を持った代替製品への移行を行い、継続してサービスが提供できるよう対応を行うこと。なお、当該製品にかかるサポート終了についての情報を知りえた段階で、本県に対して報告をおこない、サポートが終了するまでに、本県に今後の対応策について説明を行い、承認を受けること。

ソフトウェアライセンスについては、接続団体の利用者数、または、端末数の最大数を考慮して、必要十分な数量を調達すること。なお、ほとんどのハードウェア及びソフトウェアについては、受託事業者との資産となる形（本県への納品がない形）を想定している。

（２）ドキュメント

受託事業者は本委託業務を実施するうえで、必要となるドキュメントについて、本県に納品すること。

納品方法は、電子媒体と紙面での納品を各１部とする。なお、電子媒体のファイル形式については、本県と事前に協議を行い、決定すること。

ドキュメントの詳細は「10　調達全般に関する共通要件（５）ドキュメント」を参照すること。

６　支払い

（１）支払条件

本委託業務における費用は、各年度末に当該年度分の費用を支払うこととする。

消費税法が改正された場合は、当該期間の費用について改正後の税率を適用する。

各年度の支払額（税抜き額）は、以下の割合を目安とし契約時に協議するものとする。各年度の割合は、契約総額から消費税及び地方消費税額に相当する金額を減じた金額（税抜き額）を基準として算出する。

- 令和３年度 37.5%
- 令和４年度 12.5%
- 令和５年度 12.5%
- 令和６年度 12.5%
- 令和７年度 12.5%
- 令和８年度 12.5%

（２）内訳資料の提出

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。

７　機密保持

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。当該ポリシーに抵触する行為又は事象が発生した場合や、そのようなおそれがある場合は、本県に報告を行い、本県の指示のもと速やかに対応すること。

業務遂行上知り得た個人情報、三重県及び接続団体に関するすべての機密事項について、本委託業務のみに利用するものとし、契約期間中又は契約終了後を問わずに第三者に漏えいしないこと。

それぞれの契約による事務を処理するための個人情報の取り扱いについては、契約書別記「個人情報の取り扱いに関する特記事項」を遵守すること。

８　暴力団等による不当介入に対する対応

（１）受託事業者は、業務の履行にあたって暴力団、暴力団関係者又は暴力団関係法人等（以下、「暴力団等」という。）による不当介入を受けたときは、次の義務を負うものとする。

ア　断固として不当介入を拒否すること。

イ　警察に通報するとともに捜査上必要な協力をすること。

ウ　委託者に報告すること。

エ　業務の履行において、暴力団等による不当介入を受けたことにより、工程納期等に遅れが生じる等の被害が生じるおそれがある場合は、委託者と協議を行うこと。

（２）受託事業者が（１）のイ又はウの義務を怠ったときは、三重県の締結する物件関係契約からの暴力団等排除要綱第７条の規定により三重県物件関係落札資格停止要綱に基づく落札資格停止等の措置を講じる。

９　注意事項

本委託業務について、契約書及び仕様書に明示されていない事項でも、その履行上当然必要な事項については、受託事業者が責任を持って対応すること。

受託事業者は、運用開始までの作業スケジュールを本県と協議の上、決定すること。

本仕様書に記載されている全ての業務に対し、いかなるケースにおいても本県に対し、別途費用を請求することはできない。ただし、本県の要求仕様変更による追加費用については別途協議を行うこととする。

本仕様書に定めのない事項が発生した場合、及び、疑義が発生した場合は、本県と協議の上、定めるものとする。

現行セキュリティクラウドの停止を伴う作業は、閉庁日もしくは夜間での実施を前提にすること。

10　調達全般に関する共通要件

（1）プロジェクト管理に関する要件

ア　プロジェクトの体制

・ 本委託業務のプロジェクト体制に関する要件は以下のとおり。

- 受託事業者は、本委託業務の遂行を確実に実施できる履行体制（支援体制含む）を確保すること。
- 十分な知識を有するものを責任ある立場としてプロジェクトに専任で参加させ、業務を実施すること。
- 作業に従事する者が、本県並びに関係者と充分な協力が取れる体制とすること。

イ　プロジェクト管理

・ 本委託業務のプロジェクト管理に関する要件は以下のとおり。

- 受託事業者は契約締結後速やかに、業務計画書を作成のうえ、本県に提出し、本県の承認を得たうえで業務を実施すること。
- 原則として、本県と合意した業務計画書にしたがって業務を実施すること。
- 業務の実施に当たり、以下の、進捗管理、品質管理、変更管理を徹底すること。なお、業務計画書の内容に変更が必要となる場合は、本県と協議し、承認を得たうえで、変更を行うこと。

種別	詳細
進捗管理	・業務計画策定時に定義する業務スケジュールに基づく進捗管理を実施すること。 ・受託事業者は、実施スケジュールと現状の差を把握するとともに、進捗の自己評価を実施し、定例報告会において本県に報告すること。 ・進捗及び進捗管理に是正の必要がある場合は、その原因と対応策を明らかにし、速やかに是正の計画を策定し、本県の承認を得たうえで、実施すること。
品質管理	・業務計画書策定時に定義する品質管理方針及び品質管理基準に基づく品質管理を実施すること。 ・受託事業者は、品質基準と現状の差を把握するとともに、品質の自己評価を実施し、各工程完了報告会において本県に報告すること。 ・品質及び品質管理に是正の必要がある場合は、その原因と対応策を明らかにし、速やかに是正の計画を策定し、本県の承認を得たうえで、実施すること。
変更管理	・仕様確定後に仕様変更の必要が生じた場合において、受託事業者はその影響範囲及び対応に必要な工数等を識別した上で、本県と協議のうえ対応方針を確定すること。

表　プロジェクト管理の詳細

- プロジェクト全般の品質状況を監査する品質管理体制を整え、品質管理責任者を設置すること。
- 必要に応じて適宜ミーティング等を実施し、本県に対し報告及び作業内容の説明・協議を行うこと。なお、構築期間においては、週 1 回以上、運用期間においては、月 1 回以上の間隔で報告会を開催すること。また、運用期間における年度末の報告会において品質判定会議を開催すること。
- 各報告会等における議事録について、受託事業者側で速やかに作成し、関係者へと共有すること。
- 全ての作業において、本県が提供した、個人情報を含む業務上の情報は細心の注意をもって管理し、第三者に開示又は漏洩しないこと。また、そのために必要な措置を講ずること。

（２）本県からの提供資料

現行セキュリティクラウドに関する構成詳細や、公開情報等については、以下の資料を参照すること。なお、以下の資料で提供されていない設計構成情報、ハードウェア・ソフトウェア構成にかかる情報、監視・運用・保守にかかる情報については、競争入札参加資格確認申請により有資格者であることが確認され、守秘義務に関する誓約書を提出した者に対して開示することが可能である。

- 現行セキュリティクラウドにかかる接続団体向け説明資料（三重県自治体情報セキュリティクラウド接続団体向け説明会資料（運用編））
- 三重県自治体情報現行セキュリティクラウド接続申請書

（３）責任分界点

本県では、各接続団体からセキュリティクラウドへ接続するためのアクセス回線として、本県が別途構築した情報スーパーハイウェイである、「三重県情報ネットワーク」を利用している。

各接続団体には三重県情報ネットワークの接続口である「L2 スイッチ（三情）」が整備されており、また、本県が別途調達しているデータセンターにも、「NW 機器（三情）」が整備されている。そのため、セキュリティクラウド側からは、三重県情報ネットワークに接続できれば、全ての接続団体との通信が可能となっている。

以上のことから、本委託業務における責任分界点を、「NW 機器（三情）」における接続ポートとし、責任分界点からインターネット側における、全ての機器とラックの準備及び配線を受託事業者の責任で実施すること。

なお、クラウドサービス提供施設とデータセンターが同一施設の場合等、下図の構成によらない場合であっても「NW 機器（三情）」の接続ポートが責任分界点となるので注意すること。

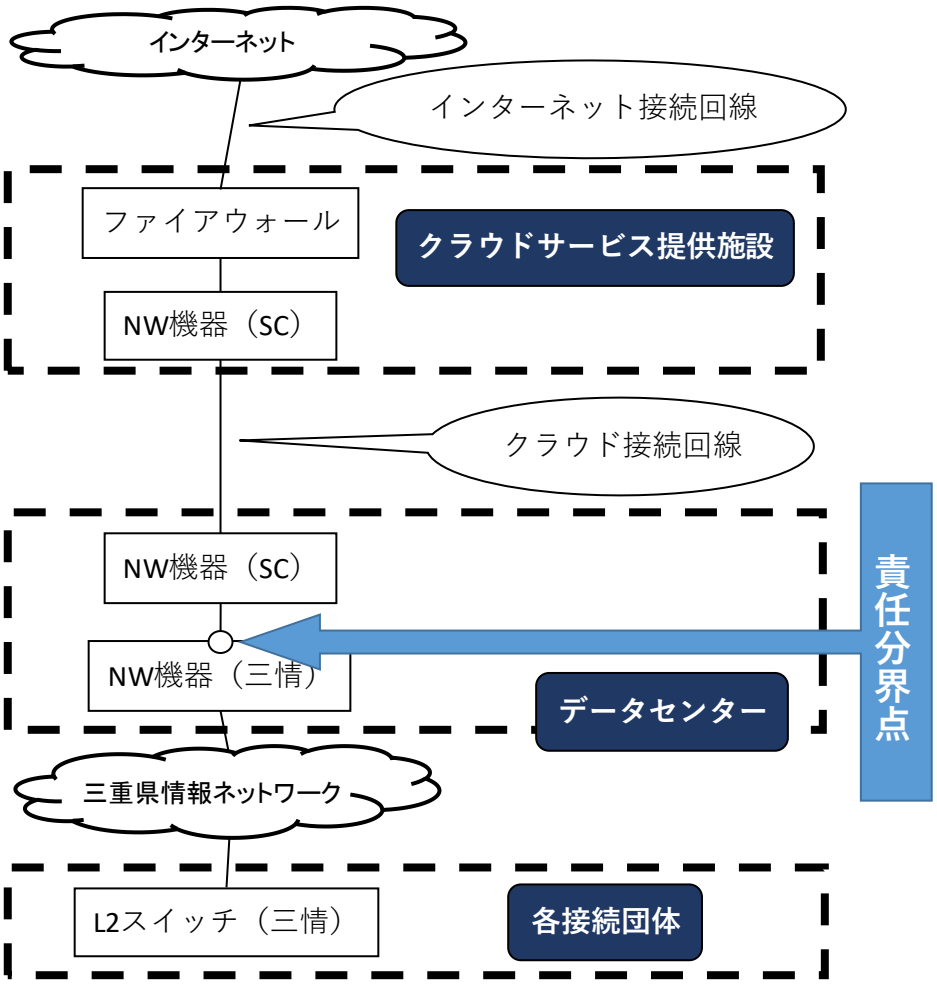

図　責任分界点

（４）他の受託事業者との調整

ア　接続団体関連

- 各接続団体の担当者の他、各接続団体における既存ネットワークまたは既存システム（公式 Web サイト、メールシステム等）の保守担当事業者等と協議等が必要となる場合は、本県に報告し、承認を得た後に、受託事業者の責により調整を行い、実施すること。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。
- 接続団体関連との協議等を行う場合は、各接続団体が指定する場所での協議となるため、注意すること。なお、相手先が Web 会議等を指定した場合は、その指示に従うこと。

イ　既存事業者との調整

- 現行セキュリティクラウドにかかる受託事業者及び三重県情報ネットワークにかかる受託事業者等、本県がこれまでに調達を行っている既存事業者と協議等が必要となる場合は、本県に報告し、承認を得た後に、受託事業者の責により調整行い、実施すること。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。

ウ　設定変更等の依頼

- 他の受託事業者が導入した機器等について、本委託業務を実施するうえで設定変更等が必要となる場合は、本県に報告し、承認を得た後に、それらの機器を所管する受託事業者と協議等を実施すること。なお、機器等の設定変更に関する設計については、受託事業者が主体的に実施すること。また、これら設計については、本県、接続団体、及び、関係する受託事業者に対して説明を行い、設定変更内容についての承認を受けること。
- 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。
- 運用期間において、既存ネットワークまたは既存システムの再構築が行われる可能性があり、その際、セキュリティクラウドの設定変更や立会い等が必要になる場合がある。その場合についても、各接続団体等との協議や、セキュリティクラウド側の設定変更等について、各接続団体等の依頼に基づき、対応を行うこと。なお、ハードウェアの増設やソフトウェアにかかるライセンスの追加等が必要になる場合は、本業務の範囲外とする。

（5）ドキュメント

受託事業者は以下のドキュメントを指定された期日までに、本県に納品すること。

ア　業務計画書

- 業務計画書の内容は以下のとおりとする。
  - 業務スケジュール
  - 業務遂行体制、業務従事者名簿
  - 機器及びソフトウェア等一覧
  - 進捗管理基準
  - 品質管理方針、品質管理基準
  - 変更管理基準
  - 工程完了判定基準
  - コミュニケーション計画
- 業務計画書の内容のうち、セキュリティクラウドの構築・移行等の作業に関するものは契約締結後 10 開庁日以内、運用保守等に関するものは令和３年８月末までに提出すること。

イ　各種設計書、完成図書及び報告書

- 受託事業者は各工程の計画、成果を示すドキュメントを作成すること。想定するドキュメントは以下のとおり。ただし、各工程に着手する前に、当該工程において作成するドキュメントに関し、本県と協議を行うこと。
- 内容に関しては、レビュー会を設けて本県に対し十分な説明を行い、内容の承認を得てから納品すること。特に、設計、構築、移行等の重要工程完了時の納品物については、余裕をもって本県に提出し、県の承認を得ること。

種別/提出時期	詳細
サービス定義書（令和３年９月末）	・セキュリティクラウドにて提供される各サービスの詳細について定義したもの。 ・各種サービスの性能要件（〇〇Mbps まで処理可能等）についても、漏れなく記載すること。 ・運用・保守業務の他、セキュリティ監視等業務の詳細についても、記載すること。
構築設計書（令和３年９月末）	・サービス定義書で定義した各種サービスを提供するために必要となる次期セキュリティクラウドについて、構築を行うために必要となる各種設計について記載したもの。
移行設計書・移行手順書（令和３年 12 月末）	・現行セキュリティクラウドから次期セキュリティクラウドへ各接続団体を移行するために必要となる各種設計及び手順等について記載したもの。 ・各接続団体に対する、それぞれの移行設計書及び移行手順書についても作成すること。

運用・保守設計書（令和3年12月末）	・運用期間における運用・保守にかかる業務内容について記載したもの。 ・各接続団体からの問い合わせ対応、設定変更依頼への対応、障害発生時への対応等についても記載すること。
セキュリティ等監視設計書（令和3年12月末）	・運用期間におけるセキュリティ等の業務内容について記載したもの。 ・利用者からの通報や攻撃等の検知に対する一次対応の他、既存ネットワークや既存システム等に対する根本対策等の二次対応等についても記載すること。
接続申請書（令和4年3月末）	・現行セキュリティクラウドにて各接続団体との接続用に用意した接続申請書について、次期セキュリティクラウド用に内容を更新したもの。 ・作成する接続申請書には、各接続団体における接続構成図についても記載すること。
接続団体向け説明資料（令和 3年12月末）	・接続団体向け説明会用の資料のこと。内容として、セキュリティクラウドの機能概要、設定変更等にかかる流れ、緊急時対応等とし、詳細については、本県と協議を実施したうえで、作成すること。 ・本資料については、毎年度更新を行うこと。
各種設定一覧（令和3年12月末）	・セキュリティクラウドを利用するために必要となる各種設定一覧について記載したもの。 ・ハードウェアを納品している場合は、ラック構成図の他、必要な内容等についても記載すること。
運用・保守体制表（令和3年12月末）	・セキュリティクラウドを運用・保守するために必要となる運用・保守体制について記載したもの。 ・通常時の体制の他、緊急時体制についても記載すること。 ・本資料については、毎年度更新を行うこと。
各種報告資料（報告会ごと）	・セキュリティ監視等にかかる定期レポート、トラフィックレポート、運用報告書、課題管理表等、定期的に作成する資料のこと。 ・議事録についても、適宜、作成すること。

表　ドキュメントの詳細

11　業務詳細

（１）設計業務全体にかかる要件

ア　基本方針

- セキュリティクラウドの安定した稼動、業務の継続性を第一とし、構築期間、移行期間、運用期間を通じて、安全で確実な運用が可能となるような設計とすること。
- 設定変更等の作業を実施する場合は、サービス設定ミス等に起因するリスクや、作業に伴うサービス停止時間の短縮を考慮し、必ず、作業手順書を作成し、各作業に対するテストやリハーサルが可能となるようにすること。
- 本業務を実施する中で、障害等の発生により作業が中断した場合を考慮し、可能な限り、切り戻し手順についても設計を行うこと。
- 本県の担当職員が実施しなければならない作業がある場合は、作業時間を考慮し、余裕をもって依頼を行うこと。
- 各接続団体の担当職員、及び、関係する受託事業者等に対して、作業の依頼や立会等の依頼を行う場合は、拘束時間を短くするなど、負担が極力少なくなるよう留意すること。
- 作成した設計書、手順書等については、作成の都度、本県に対して説明を行い、承認を得ること。

（２）事前調査にかかる要件

ア　各接続団体における事前調査及びヒアリング

- セキュリティクラウドを利用する各接続団体にかかる事前調査として、既存の接続申請書の内容を確認すること。
- 接続申請書の内容確認後、現地確認を行い、現状との差異について確認し、接続申請書を最新状態に更新すること。
- 現地確認の際は、各接続団体のセキュリティクラウドにかかる担当者の他、各接続団体における既存ネットワークまたは既存システム（公式Webサイト、メールシステム等）の保守担当事業者等からヒアリングを行い、現時点における意見・要望等の他、障害情報、機器更新等の変更予定等の情報についても収集するとともに、必要な連絡体制についても確認すること。
- 移行期間において想定される、各接続団体における既存ネットワークおよび既存システム等の設定変更時における、立ち合いの可否や、設定変更等に対する作業依頼の可否についても確認すること。

イ　その他の既存事業者に対する事前調査

- 本県が別途提供する、三重県情報ネットワーク等に関する資料について、内容を確認すること。
- 確認した内容等について、既存事業者との協議を行い、詳細な内容について確認すること。
- 移行期間において想定される、設定変更時における、立ち合いの可否や、設定変更等に対する業務依頼の可否についても確認すること。

（３）サービス設計にかかる要件

サービス設計として、本委託業務における要件について、本県との最終確認を実施後、具体的なサービス提供方式の決定を踏まえて、設計を行うこと。

各種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。

各種サービスに対して、機能要件だけでなく、冗長化構成に基づき可能となる障害時の業務継続性や、それぞれのサービスに対する性能要件についても記載すること。

NOC、及び、SOC が提供する各種サービスについても、業務内容の他、提供可能なサービスレベルについても記載すること。（例えば、インシデント発生時の初動対応時間等の努力目標について記載すること。）

本内容を「サービス定義書」に反映すること。また、作成したサービス定義書について、本県に対して報告し、承認を得ること。

（４）三重県情報ネットワークとの接続設計にかかる要件

三重県情報ネットワークとの接続に必要となる接続設計を行うこと。このとき、必要に応じてラック構成図についても作成すること。

接続設計にあたっては、三重県情報ネットワークにかかる受託事業者と調整を行い、可能な限り、シンプルな構成となるよう留意すること。

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 10GBASE-SR×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。）

三重県情報ネットワークとの物理的な配線には、ラック間配線が必要になるが、ラック間配線については、データセンター側に依頼する必要があるため、注意すること。なお、ラック配線にかかる費用についても、本委託業務の範囲内で受託事業者が準備すること。（各ラックに光パッチパネルがあらかじめ設置されているため、各ラック間の光パッチパネル間でラック間配線を依頼することになる。）

ラック間配線の申請から接続までは 2 週間程度を要するため、余裕をもって発注を行うこと。

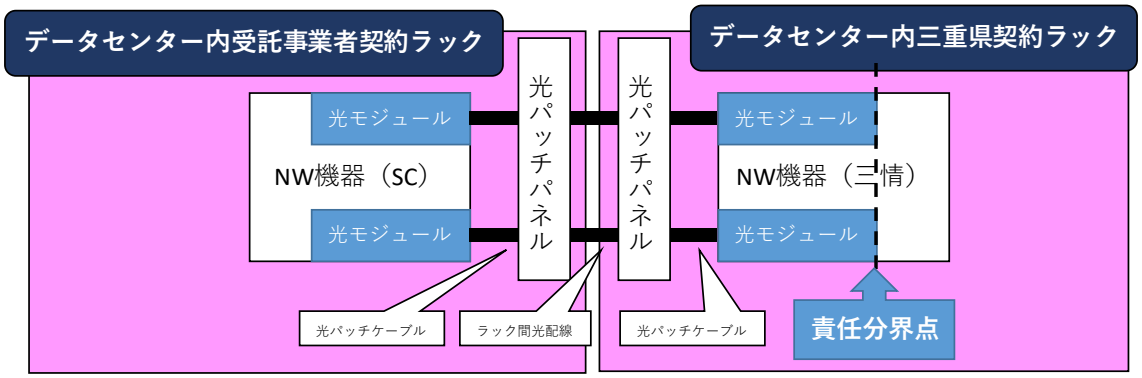

図　三重県情報ネットワークとの接続詳細

（５）構築設計

次期セキュリティクラウドにかかる構築業務にかかる設計として、現行セキュリティクラウド、各接続団体における既存ネットワークや既存システム、三重県情報ネットワークなどの設定及び構成を踏まえたうえで、実現可能で、かつ、既存の構成等にできるだけ影響を与えないような構成に留意して構築設計を行うこと。

「（３）サービス設計にかかる要件」にて策定した「サービス定義書」に定義した各種サービスを提供するために必要となる、全ての設計（物理構成、論理構成、機器配置図、ラック構成、IP アドレス構成、ルーティング構成、セキュリティポリシー（ファイアウォール、IDS 等）、サービス構成図等）について記載すること。なお、数団体分の新規接続に耐えられる構成とすること。

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。

本仕様書において、各種サービスに対する要件のみが記載され、詳細な構成等が記載されていない部分があるが、その場合は、要件を満たす構成であれば、どのような構成であっても構わない。ただし、全ての構成を実現するために必要となる費用等についても本委託業務の範囲内となるので注意すること。

各接続団体におけるプロキシサーバについて、端末の特定を行うため HTTP ヘッダ領域の送信元 IP アドレス情報（X-Forwarded-For）の設定についても設計を行うこと。なお、設定変更等の作業自体は、各接続団体の既存システムにおける受託事業者が実施することを想定している。

次期セキュリティクラウドの構築後、提供される各種サービスに対する機能要件、性能要件等について確認が行えるよう、稼働試験及び性能試験の内容についても設計を行うこと。特に、性能試験については、各種サービスにかかる単体テスト、疎通テスト等の他、できる限り実環境に近い構成による試験ができるよう留意すること。

次期セキュリティクラウド内に、冗長化された部分がある場合（例えば、Active/Standby 構成の機器や通信回線など）、切り替え作業にかかる試験、及び、切り戻し試験についても設計を行うこと。特に、機器故障の場合は、機器だけでなく、通信回線の切り替え等も発生すると想定されるが、全体の切り戻しを行う際の判断基準（切り戻しにかかる時間、通信断の時間など）についての情報を取得するため、現行セキュリティクラウドへの影響が大きい場合を除き、可能な限り実環境に近い形で試験を実施できるよう留意すること。

運用期間における機器の不具合や障害の発生を想定し、監視や検知の動作確認、さらに、それに伴うアラート通知等にかかる試験についても設計を行うこと。

全ての構築作業及び各種試験が完了した段階で、構築されたセキュリティクラウドが、機能面、運用面等において要求仕様を満たし、かつ、正常に稼動していることを最終的に判断することができる稼働試験についても設計を行うこと。特に、セキュリティクラウドに対する確認事項等を記載した「稼動判定基準（案）」の作成を行うとともに、当該判定基準に対して、本県に対し説明を行い、承認を得ること。

（６）移行業務等の設計にかかる要件

各接続団体が現行のセキュリティクラウドから、次期セキュリティクラウドへ移行するために必要となる移行業務にかかる設計として、移行設計を行うこと。

各接続団体の準備遅延や、悪天候による日程順延、移行後の障害発生による切り戻しの実施等、さまざまな理由により、予定通りの移行が進まないと想定されるが、移行期間内に全ての作業が完了するよう、余裕を持った柔軟な設計とすること。

手戻りをなくし、かつ、障害発生をできる限り発生させない、または、発生した際の影響を小さくするため、現行セキュリティクラウドから次期セキュリティクラウドへの移行作業が軽微な接続団体の移行を優先すること。

接続団体への影響が小さくなるよう、各接続団体におけるネットワークや各種サービス停止時間を最小限に抑え、かつ、安全で確実に実施可能な移行作業が実施できるよう留意すること。

移行作業の実施当日において、障害発生等により作業が中断した場合、迅速にその原因を明らかにし、作業を再開できるよう、または、次の機会へとつなげられるよう、あらかじめ、発生する障害等を想定し、その調査等の内容を手順書等として準備しておくこと。

移行作業実施時には、各接続団体における既存ネットワーク機器や既存システム等において、設定変更等の現地作業が発生すると想定しているが、各接続団体の担当職員、及び、既存ネットワークや既存システムに対する受託事業者に対して、できる限り作業を依頼しなくてもよい形での設計を行うこと。やむを得ず、各接続団体の担当職員、及び、既存ネットワークや既存システムに対する受託事業者に対して、作業を依頼する場合は、説明用の資料や手順書等を用意し、事前説明を行ったり、事前リハーサルや当日の作業立会等を予定したりするなど、確実な移行作業が実施できるよう留意すること。

接続申請書自体について、各接続団体の移行後の状態を記載できるよう様式自体を修正したうえで、各接続団体における移行設計を反映させること。

本委託業務における受託事業者が、各接続団体内での現地作業を行う場合は、入館方法や作業開始時、及び、終了時の連絡方法、障害等が発生した際の対応、設定変更後の稼働確認方法等について、事前調整を行い、設計に反映させること。

移行作業にかかる詳細について、設計を行うとともに、移行後の試験として、各種サービスに対する稼働試験の他、可能な限り、性能要件についても試験が実施できるよう設計を行うこと。

接続団体によっては、セキュリティクラウドが利用できない場合のバックアップ回線等の冗長化構成を持ったネットワーク構成となっている場合があるため、必要に応じて、試験内容に盛り込むこと。

作成した移行設計書及び各種手順書、接続申請書、各種試験等をもとに、各接続団体における移行作業の実施日時や各担当者名、連絡先等を網羅した接続団体それぞれの移行計画を策定すること。

策定した移行計画については、各接続団体に対して説明し、承認を得ること。

（7）運用・保守業務の設計にかかる要件

セキュリティクラウドについて、運用・保守業務を行うために必要となる運用・保守設計を行うこと。

運用・保守設計にあたっては、以下の要件を満たす設計とすること。

ア　基本方針

- セキュリティクラウドにかかる運用･保守業務を行ううえで必要となる、運用・保守要員等が勤務する施設として、NOC（Network Operation Center）を設置すること。
- 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。
- NOC は 24 時間 365 日の有人運用とすること。なお、NOC を複数拠点設置する場合は、その内、少なくとも 1 拠点は、24 時間 365 日の有人運用とすること。
- 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。
- 現行セキュリティクラウドにおける課題として、問い合わせ内容や作業内容等により、問い合わせ先が本県や現行セキュリティクラウドの受託事業者に変更になるなど、総合窓口の設置やワンストップサービスの提供ができておらず、迅速なサービス提供ができなかったり、業務負荷の増大を招いたりしたことを踏まえて、問い合わせや各種申請に対応するためのポータルサイトの構築や、ワンストップサービスを提供できる総合窓口の設置を行うこと。
- セキュリティ監視等の業務を行う施設として、後述する SOC（Security Operation Center）を設置することとしているが、NOC と緊密な連携が取れること。なお、NOC と同一施設とする必要はない。
- 各接続団体の担当者にかかる業務負荷軽減とセキュリティ・可用性の向上のそれぞれを考慮すること。
- 運用期間において 運用・保守業務に対する PDCA サイクルを実施し、実施内容を継続的に評価、改善することで長期にわたっての安定的、効率的かつ高品質なサービス提供を実現できること。
- テスト期間、運用期間に関わらず、移行が完了した接続団体に対しては、運用・保守業務を実施できること。

イ　総合窓口

- 接続団体における担当職員からの問合せ、障害申告の受付及びインシデント登録、対応等を受け付けることができる総合窓口を用意すること。
- 接続団体からの問い合わせに直接対応できること。

- 窓口への連絡手段は主にメール、及び、電話の他、柔軟な連絡手段を用意することとし、運用期間中に継続して利用できる連絡先として、電話番号及びメールアドレスを用意すること。
- 障害発生時や、緊急度の高いセキュリティインシデント発生時への対応として、24 時間 365 日の受付対応ができること。

ウ　ポータルサイト

- 総合窓口とは別に、各種設定変更等の申請等について、双方向でやり取りが可能なポータルサイトを用意すること。
- ポータルサイトの機能として、掲示板機能、問い合わせ管理機能等、運用上必要になる機能を持たせること。
- ポータルサイトへのアクセスについて、ID パスワードに加え、SMS による認証など、多要素認証による認証機能を持たせること。
- 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。
- 掲示板機能として、全接続団体が閲覧可能な掲示版機能を有すること。
- 掲示板へのお知らせ事項等の掲示は受託事業者もしくは本県の担当者が実施できること。
- 掲示板が更新された際は、全アカウントに紐づくメールアドレスへ通知を行えること。
- 接続団体毎の問合せ管理、ファイル授受を実現できるコミュニケーション機能を有すること。
- 対象となる接続団体のみに閲覧権限を割り振ることができること。
- 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。
- 問合せの進捗状況・ステータス、および対応履歴が確認できること。
- ポータルサイトへの接続は、セキュリティクラウドを経由したアクセスが可能なこと。なお、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。
- モバイル端末からポータルサイトへのアクセスが可能であり、全ての機能を利用できること。

エ　進捗管理

- 総合窓口やポータルサイト等からの問い合わせ対応や作業依頼、障害時の調査依頼など、それぞれの対応については進捗を管理し、完了まで責任を持って対応を行えるようにすること。
- 問合せに対する一次回答は、原則として翌営業日中に回答できること。

オ　稼動監視・障害対応

- セキュリティクラウドで提供される各種サービスに対してステータスを監視し、不具合の予兆等に対し、メール等による通知（アラートメールの発信）が実施できること。
- アラートメールや、各接続団体からの障害等の報告を受けた後は、障害の一時切り分け、障害発生ポイント等の特定、暫定対応等の実施、各関係団体の担当者への報告など、速やかに行えるよう、対応フロー等について整理しておくこと。
- 監視対象として、各サービスの提供状態の他、本委託業務にて調達した機器に対する疎通確認や、CPU 使用率、トラフィック量、セッション数等のステータス等についても監視対象とし、その他、安定的な運用のために、監視が必要と考えられる項目についても監視対象とすること。
- 障害等に対する一次切り分けの結果、本委託業務の範囲外の要因による障害の場合は、あらかじめ、決められた対応フローにより、関係機関への報告を行えるようにすること。
- セキュリティクラウドで提供する各種サービスが提供できなくなるなどの重大な事案（機器障害、外部からの攻撃等によるサービス停止など）については、24 時間 365 日の対応を行うこと。ただし、予備系への切り替えにより各種サービスの提供が再開した場合や、軽微な障害等については、翌営業日以降の対応も可とする。
- 障害対応については進捗を管理し、完了まで責任を持った対応を行えるようにすること。

カ　設定変更対応

- 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。
- 設定変更の内、軽微なものを除き、依頼内容、及び、実施する変更内容について、本県の担当者の承認を得てから作業を実施するようにすること。
- 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
- 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。

キ　調達した機器に対するリスク管理

- 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。
- 安定的な運用のために適用が必要なセキュリティパッチやファームウェアバージョンアップ等については、セキュリティ上のリスクを考慮のうえ、定期的に実施できること。なお、緊急対応が必要な場合は、随時対応が実施できること。
- セキュリティパッチ等の適用は、可能な限り、セキュリティクラウドの運用に影響を与えないよう、土日祝日や業務時間外帯での対応とすること。
- セキュリティパッチ等の適用後は構成ドキュメントの修正を実施するようにすること。

ク　構成情報の更新対応

- 運用期間中において、稼働監視・障害対応、設定変更対応、調達した機器に対するリスク管理等の業務により、セキュリティクラウドにおけるシステム構成や設定内容等に対して変更があった場合、更新履歴を残したうえで、各種設計書における必要な情報の更新を行うこと。
- 各種設計書については、常に最新版の情報を閲覧できるようにするとともに、本県の指示により、常に最新状態のものを共有できること。

ケ　定例報告

- 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。
- 報告会では、運用・保守の対応状況として、問合せ件数、進捗管理状況の他、障害やインシデントの発生状況や対応状況についての報告書を取りまとめ、報告書として提出できるようにすること。また、各接続団体における各種サービスの利用状況や稼働状況（負荷情報など）の他、通信回線等にかかるトラフィック情報等についても報告し、設計に基づいた性能が出ているかを確認できるようにすること。
- 報告内容の種類によっては、全ての報告会での報告を求めるものではないが、少なくとも半年に１度以上は、全ての項目に対して報告を行うようにすること。
- 後述するセキュリティ監視等業務にかかる内容についても、本報告会にて、定期的に報告するようにすること。
- 年に１回以上、セキュリティクラウドの年間運用サマリを作成し、報告するようにすること。
- 本県に対する報告会は、月に１回以上実施すること。なお、運用期間中の開催日は別途調整を行う。
- 各接続団体に対する報告会は、年に１回以上実施すること。この時、本県に対する報告会と同様の内容について、報告を行うこと。なお、日程調整等は、本県が実施する。

コ　セキュリティ監視等業務にかかる対応業務

- 後述する「（8）セキュリティ監視等業務の設計にかかる要件」により、現地対応を含めた緊急対応が必要になった場合、SOC と情報共有を行いながら、運用・保守業務の一環として、必要な対応が実施できること。なお、通常、現地対応は、各接続団体の担当者、及び、既存ネットワークや既存システムに対する受託事業者が対応を行うこととなっており、また、リモートによる対応で十分な対応が可能な場合が大多数と考えているため、現地対応は、ほぼ発生しないと想定している。
- 本県からの指示により現地での対応が必要と判断される場合に備えて、対応フロー等について整理しておくこと。
- 緊急時連絡は、SOC から各接続団体における担当者や関係する受託事業者等に直接連絡を行う形を想定しているが、SOC からの支援だけでは十分な支援ができないと見込まれる場合は、NOC 要員が SOC からの連絡を受けた後、各接続団体に対して報告・支援を行う形も可とする。ただし、その場合は、SOC と情報共有を行い、SOC に代わって復旧までの支援にかかる業務を実施できること。
- 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。
- SOC との迅速な連携や、迅速な初動を実現できるよう、平時においても、外部からの攻撃や、インシデント発生時におけるアラート通知などの情報について SOC と情報共有しておくこと。

サ　職員研修対応

- 県が主催する各接続団体のシステム管理者や新任者を対象とした研修会に、セキュリティクラウドの概要や問い合わせ方法、作業依頼方法、障害時対応等について説明を実施できること。
- 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。

シ　対応時間帯

- 対応時間として、下記を目安とするが、安定的な運用・保守を行うために必要となる体制を構築すること。

種別	対応時間の目安
総合窓口（一次受付）	24 時間・365 日
問合せに対する回答	平日 8:30～17:15
稼動監視・障害対応	24 時間・365 日
システム変更対応	平日 8:30～17:15
定例報告	平日 8:30～17:15
セキュリティ監視等対応	24 時間・365 日

表　対応時間の目安

ス　訓練対応

- 年に 1 回以上、各接続団体の担当職員に対し、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。
- 場合によっては、実施しない場合もあるため、注意すること。

セ　その他

- その他、運用・保守業務を実施するうえで、必要となる設計があれば、必要に応じて、対応を行うこと。

（8）セキュリティ監視等業務の設計にかかる要件

セキュリティクラウドにおけるセキュリティ監視、調査、解析等のセキュリティ監視等の業務を行うために必要となるセキュリティ監視等設計を行うこと。

セキュリティ監視等設計にあたっては、以下の要件を満たす設計とすること。

ア　基本方針

- セキュリティクラウドにかかるセキュリティ監視等を実施していくうえで必要となる、セキュリティ監視要員等が勤務する施設として、SOC（Security Operation Center）を設置すること。
- SOC の所在地は、日本国内とし、また、その場所を本県に開示できること。
- 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。
- 各接続団体の担当者にかかる業務負荷軽減とセキュリティ・可用性の向上のそれぞれを考慮した設計とすること。
- 運用期間において 運用・保守業務に対する PDCA サイクルを実施し、実施内容を継続的に評価、改善することで長期にわたっての安定的、効率的かつ高品質なサービス提供を実現すること。
- テスト期間、運用期間に関わらず、移行が完了した接続団体に対しては、セキュリティ監視等業務を行えること。

イ　SOC の詳細

- 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。
- SOC におけるセキュリティ監視等業務について、以下のいずれかの資格を有する者を 1 名以上従事させること。
  - (ISC)2 の情報セキュリティプロフェッショナル認定資格「CISSP」
  - 日本行政情報セキュリティプロフェッショナル認定資格「JGISP」
  - 米国 SANS Institute 社の情報セキュリティ認定資格「GIAC」
  - 米国 Guidance Software 社の認定資格「EnCace Certified Examinar」（EnCE）
  - 米国 AccessData 社の認定資格「AccessData　Cerified Examinar」（ACE）
  - ISACA（情報システム監査コントロール協会）の認定資格「CISA」

- 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。
- 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。
- SOC におけるログ分析として、ログ分析機能(SIEM)による相関分析が 24 時間 365 日可能であること。
- 情報セキュリティマネジメントについて、ISO/IEC 27001、JIS Q 27001 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、本業務の実施組織・部門が認証取得していること。
- 各接続団体等の担当者に対する対応については、全て日本語で実施すること。

ウ　セキュリティ監視等の詳細

- 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。
- 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。
- 機器メーカーから検知シグネチャ等が提供される場合は、セキュリティ監視等の対象となる機器等に対して、正常な通信に影響を及ぼさないよう、受託事業者が十分留意したうえで、適用できるようにすること。なお、適用する検知シグネチャ等については、セキュリティクラウドにて利用している通信プロトコルや監視対象ネットワークに最適化したものを適用できるようにすること。
- セキュリティ監視等の対象となる機器に対し、リモートから Ping による稼働監視を実施できるようすること。また、リモートから SNMP による、CPU 利用率、セッション数、インタフェース毎のトラフィック量等の性能監視を実施できるようすること。

エ　セキュリティ監視、調査、及び、解析

- 各機器が出力するセキュリティログについて、24 時間 365 日有人によるリアルタイムセキュリティ監視を実施し、必要に応じて、インターネットと各接続団体間における双方向の通信を調査・解析できること。また、危険度に応じて、各接続団体の担当者に報告を行うとともに、対策等にかかる助言が実施できること。
- 現行セキュリティクラウドにおけるセキュリティ監視等業務において、インシデント発生の報告は、SOC から本県担当者に実施されており、かつ、本県担当者では、当該接続団体に対する的確なフォローができなかったことへの反省を踏まえて、SOC から当該接続団体に対して直接報告を行い、対応策等に対する支援が実施できるようにすること。さらに、上述の「運用・保守設計」にも記載しているとおり、本県からの指示により、SOC からの連絡を受けた NOC 要員による現地対応を含めた緊急対応が実現できるようにすること。
- 緊急度の高いアラートのみではなく、出力される全てのセキュリティログを監視対象とすること。
- セキュリティ監視等の対象となる機器において、不正な通信を検知、遮断できるようにすること。ただし、ネットワーク全体の停止ではなく、当該通信等に限った遮断ができるようにすること。
- 不正な通信に対する調査を実施し、その結果に基づいて、攻撃の可能性があるログの抽出を行うとともに、以下のケースに応じた対応等を実施できること。

不正な通信の種別	対応
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	・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。
外部から内部への不審な通信及びその兆候を検知した場合	・速やかに不審な通信等か否かを解析すること。 ・不審な通信であると判断した場合は、ただちに各接続団体における担当者に報告するとともに、通信元を特定し、通信元に対する対処方法を報告すること。
内部から外部への不審な通信及びその兆候を検知した場合	・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、通信元及び通信先を特定し、通信元及び通信先に対する対処方法を報告すること。

表　不正な通信を検知した際の対応方針

・ 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。

分析結果	対応
危険度 0 （Low）	・安全なイベント ・調査活動など、実害が発生しなかった行為
危険度 1 （Medium）	・安全と思われるイベント ・実害を狙った攻撃だが、攻撃の失敗が確認できたもの
危険度 2 （High）	・重大なセキュリティイベント ・攻撃が成功した可能性が非常に高い、あるいは攻撃の失敗が確認できない場合などに該当するもの
危険度 3 （Critical）	・重大なセキュリティイベント ・明らかに攻撃が成功した場合、踏み台や Web サイト改ざん等が該当する

表　危険度と対応方針

・ 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。
・ 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。
・ 接続団体側に Proxy サーバが設置されている多段 Proxy 構成において、XFF 情報を利用している場合は、可能な限り被疑端末を特定し通知すること。
・ 危険度が高い（危険度が 3 である）場合は、インシデントの要因となるマルウェアサイト(C&C サーバ等)への緊急通信遮断を実施すること。

オ　監視報告

・ 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。

・ 月例監視報告書には以下の内容を含めること。

項目名	詳細
全体傾向	・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
個別傾向	・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
詳細情報	・不正アクセスに関する検知内容、推奨確認方法、推奨対処方法

表　月例監視報告書の詳細

・ 月例監視報告書の記載内容に関する問い合わせ対応を行うこと。
・ 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。

カ　その他

・ その他、セキュリティ監視等業務を実施するうえで、必要となる設計があれば、必要に応じて、対応を行うこと。

（９）利用サービスの詳細にかかる要件

セキュリティクラウドで提供される各種サービスについて以下の要件を満たすこと。

ア　基本要件

・ セキュリティクラウドで提供される各種サービスについてクラウドサービスにより提供すること。
・ 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、責任を持って提供を行うこと。
・ 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。

イ　機能要件

・ 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。
・ 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。

ウ　性能要件

- 「2　事業概要（2）業務範囲　ウ　接続団体」における接続団体が、契約期間終了時まで利用できる十分な性能とすること。
- 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。)
- 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。
- 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。

(10) 通信回線にかかる要件

通信回線として、以下の要件を満たした回線を用意し、移行期間、運用期間において、利用できるようにすること。なお、各通信回線に対する接続イメージは、「2 事業概要（2）業務範囲　エ　サービス構成例」を参照すること。

ア　インターネット接続回線

- クラウドサービス提供施設とインターネットを接続するための回線として、以下の要件を満たすものを調達し、利用できるようにすること。
- 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。
- 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。
- 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。
- インターネットから各接続団体の Web サーバに対する Web サーバアクセスには、200Mbps 以上の通信帯域を確保すること。なお、Web サーバとして ASP サービスを利用している場合などにおいて、Web サーバアクセスにおける全ての通信がインターネット上で完結する場合（セキュリティクラウド内に通信が発生しない場合）については、Web サーバアクセス全体にかかる処理能力として読み替えること。
- 現行のセキュリティクラウドにおいて、利用中のドメイン（mie-sec-cloud.jp）を踏襲し、次期セキュリティクラウドにおいても、利用できるようにすること。なお、踏襲するにあたり、現行セキュリティクラウドにかかる受託事業者からドメイン管理業務を引き継ぎ、運用期間における管理費用（5 年間）についても本委託業務の範囲内とすること。

イ　クラウド接続回線

- 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とを接続する回線として、以下の要件を満たすものを調達し、利用できるようにすること。
- 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。
- 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。

ウ　ブレイクアウト接続回線

- 本県が別途調達しているデータセンター（津市内）とインターネットを接続する回線として、以下の要件を満たすものを調達し、利用できるようにすること。
- 前述した「インターネット接続回線」と合わせて計 4Gbps のベストエフォート回線（このうち、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。
- 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。
- 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。

（11）データセンターにかかる要件

クラウドサービス提供施設として本県が別途調達するデータセンター以外のデータセンターを利用する場合、当該データセンターについては、以下の要件を満たすこと。

ア　基本要件

- 受託事業者の入退館及び館内作業が可能であること。
- 受託事業者による機器設置室内での作業は、土日祝日を含めた 24 時間 365 日可能であること。
- 計画的な定期保守点検などによる設置機器のサービス停止がないこと。
- データセンター事業者は、5 年以上の運用実績を有すること。
- データセンターファシリティスタンダードのティア 3 相当以上のティアレベルに準拠していること。なお、設備に関するその他の要件については「イ　設備要件」を参照すること。

イ　設備要件

要件	詳細
情報セキュリティマネジメント	・JIS Q 27001 又は ISO/IEC 27001 に基づく認証を取得している組織によって運用されていること。

システム	
立地	・国内に設置された施設を利用することとし、データ保管場所が特定できる場所であること。 ・データセンターは活断層上に建設・設置されていないこと。
地震対策	・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の耐震構造の建築物であること。
火災対策	・火災の予兆を検知できるシステムが設置されており、ガス消化設備を有していること。
災害発生時の避難対策	・建物は、非常口、非常照明設備及び避難誘導標識等が設置されており、保守作業員が災害時に円滑な避難ができること。
落雷対策	・建物には、落雷の被害を受けない対策がなされていること。
防水対策	・建物には、水害の被害を受けないような防水対策を施していること。ただし、河川、高潮、津波の氾濫想定水位に対し、データセンタービルの 1 階床標高が上回っている場合はその限りではない。
防犯対策	・建物への入館、機器設置室への入退室、建物からの退館において、入室者を識別及び記録できる複数段階のセキュリティ設備（IC カード等）により許可されたもののみ入退室が可能なこと。 ・入退館管理は、24 時間 365 日行っていること。 ・主要な出入口は、監視カメラ等により映像を記録すること。
電源対策	・2 系統以上で、冗長性を確保していること。 ・建物の電源設備の法定点検及び工事の際においても、機器の停電時対策をとる必要のないこと。 ・停電時にシステムを運用するために十分な電源容量を持つ非常用自家発電装置を備えていること。 ・停電時に自家発電装置が安定的に起動するまでの間、瞬断することなくシステムに十分な電力供給が可能な無停電電源装置を設置していること。無停電電源装置は冗長構成がとられていること。
空調設備	・機器設置室は空調設備からの漏水対策を行っていること。または空冷式の空調機を採用していること。 ・機器設置室の主要な空調設備機器については、予備機が設置されており、主要機器が故障の場合でも必要な冷却能力を確保できること。

表　データセンターの設備要件

（12）次期セキュリティクラウドの構築にかかる要件

次期セキュリティクラウドの構築作業として、「サービス定義書」に定義した各種サービスを提供するために必要となる全ての構築作業を行うこと。

構築作業は、先に作成した「構築設計」に従い、確実に実施すること。

構築作業終了後、構築設計に従い、各種試験を実施し、その結果を本県に対して報告し、承認を得ること。

障害対応試験、負荷試験、冗長化構成等にかかる切り替え試験等、現行セキュリティクラウド等に影響を与える可能性がある試験を実施する場合は、各接続団体等に対して、極力影響を与えない時間で実施すること。

三重県が別途調達するデータセンターでの作業を実施する際は、入館申請が必要となるため、注意すること。なお、機器搬入等を行う際は、データセンターが指定する搬入口及びエレベータを使用し、設備、器物破損を防止するための処置を講じること。また、搬入にあたり発生した不要物（梱包材）は速やかに回収し、受託事業者の責任、負担において、安全に破棄すること。

現行セキュリティクラウド、及び、三重県情報ネットワークとの接続時には、各受託事業者と綿密な連絡を取りながら、現行ネットワーク等への影響を与えないよう、細心の注意を払うこと。

障害発生等の理由により、作業を中断、中止、切り戻し等を行う必要がある場合は、速やかに本県の担当者宛連絡を行うこと。また、速やかに、構築設計を修正し、本県に対して説明を行い、承認を得ること。

通信回線の接続等、外部への通信を開始する場合や、他のネットワークと接続する場合、既存機器の設定変更を行う場合等は、間違った設定変更が各種サービスの停止などの重大なインシデントを発生させる恐れがあるため、作成した手順書の最終確認や、作業実施時のダブルチェック等、細心の注意を払うこと。

構築作業に伴い、重大なインシデントが発生した場合は、遅滞なく本県に報告を行うとともに、直ちに切り戻し作業を行い、被害が最小限になるよう、一次対応を行うこと。その後、速やかに、インシデント発生状況、影響範囲、根本解決策等について本県に報告を行うこと。

構築後、しばらくの間は、現行セキュリティクラウドにかかる受託事業者と連携し、問題等が発生していないか、継続して確認を行うこと。また、問題が発生した場合は、関係者と協力して原因調査及び対応にあたること。

全ての構築作業が完了後、「稼働判定基準」に基づき試験を実施し、その結果について、本県に対して説明を行い、承認を得ること。

（13）接続団体の移行にかかる要件

全ての接続団体について、現行のセキュリティクラウドから次期セキュリティクラウドへ移行を行うこと。

移行作業は、先に作成した「移行計画」に従い、確実に実施すること。

三重県が別途調達するデータセンターでの作業を実施する際は、入館申請が必要となるため、あらかじめ留意すること。なお、機器搬入等を行う際は、データセンターが指定する搬入口及びエレベータを使用し、設備、器物破損を防止するための処置を講じること。また、搬入にあたり発生した不要物（梱包材）は速やかに回収し、受託事業者の責任、負担において、安全に破棄すること。

各接続団体、及び、各接続団体にかかる既存ネットワークや既存システムが設置されている施設で作業を実施する際は、各接続団体の指示に従い、事前連絡、入館申請等の対応を行うこと。なお、機器搬入等を行う際は、当該施設の管理者が指定する搬入口及びエレベータを使用し、設備、器物破損を防止するための処置を講じること。また、搬入にあたり発生した不要物（梱包材）は速やかに回収し、受託事業者の責任、負担において、安全に破棄すること。

各接続団体等の準備遅延、悪天候、障害等の発生により、移行作業を中断、中止、切り戻し等を行う必要がある場合は、速やかに本県及び各接続団体の担当者宛連絡を行うこと。また、速やかに、移行計画を修正し、本県及び該当接続団体に対して説明を行い、承認を得ること。

各種試験の結果については、移行作業の進捗状況に応じて、速やかに本県、及び、該当接続団体へと報告を行うこと。

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対して、各種サービスの切り替え等を行う場合等は、間違った設定変更が各種サービスの停止などの重大なインシデントを発生させる恐れがあるため、作成した手順書の最終確認や、作業実施時のダブルチェック等、細心の注意を払うこと。

移行作業に伴い、重大なインシデントが発生した場合は、遅滞なく本県及び各接続団体に報告を行うとともに、直ちに切り戻し作業を行い、被害が最小限になるよう、一次対応を行うこと。その後、速やかに、インシデント発生状況、影響範囲、根本解決策等について本県及び各接続団体に報告を行うこと。

移行後、しばらくの間は、接続団体からセキュリティクラウドへの接続について、問題が発生していないか、定期的に確認を行うこと。また、問題が発生した場合は、関係者と協力して原因調査及び対応にあたること。

移行計画にかかる全ての作業が完了後、本県及び当該接続団体に対して説明を行い、承認を得ること。

（14）運用・保守業務要件

セキュリティクラウドの安定的な運用を行うため、運用・保守業務を行うこと。

運用・保守業務は、先に作成した「運用・保守設計」に従い、確実に実施すること。

運用・保守設計の内容については、各接続団体の組織改正等に応じて、適宜修正すること。

運用・保守業務を実施する保守要員に変更がある場合は、引継ぎ作業として、「運用・保守設計」の内容だけでなく、各接続団体担当者への挨拶の他、必要に応じて、現地確認等についても実施し、サービスレベルを低下させないよう、留意すること。

（15）セキュリティ監視等業務にかかる要件

セキュリティクラウドの安定的な運用を行うため、セキュリティ監視等業務を行うこと。

セキュリティ監視等業務は、先に作成した「セキュリティ監視等設計」に従い、確実に実施すること。

セキュリティ監視等設計の内容については、各接続団体の組織改正等に応じて、適宜修正すること。

セキュリティ監視等業務を実施する要員に変更がある場合は、引継ぎ作業として、「セキュリティ監視等設計」の内容の他、各接続団体における詳細構成等についても引継ぎを実施し、要員変更によるサービスレベルを低下させないよう、留意すること。