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・保守業務契約に関する仕様書

令和８年５月

三重県総務部デジタル推進局

デジタル改革推進課

1　背景と目的 1
（1）はじめに 1
（2）三重県自治体情報セキュリティクラウドとは 1
（3）本委託業務の目的 1
2　事業概要 2
（1）契約名 2
（2）業務範囲 2
（3）受託要件 6
3　調達スケジュール 7
4　履行場所 7
5　納品物件 8
（1）ハードウェア及びソフトウェア 8
（2）各エンドポイントにインストールするエージェントソフトウェア 8
（3）ドキュメント 9
6　支払い 9
（1）支払条件 9
（2）内訳資料の提出 10
7　機密保持 10
8　暴力団等による不当介入に対する対応 10
9　注意事項 10
10　調達全般に関する共通要件 11
（1）プロジェクト管理に関する要件 11
（2）本県からの提供資料 12
（3）責任分界点 12
（4）他の受託事業者との調整 13
（5）ドキュメント 14
11　業務詳細 16
（1）設計業務全体の要件 16
（2）事前調査の要件 17
（3）サービス設計の要件 17
（4）三重県情報ネットワークとの接続設計の要件 17
（5）構築設計 18
（6）移行業務等の設計の要件 19
（7）運用・保守業務の設計の要件 20
（8）セキュリティ監視等業務の設計の要件 25
（9）利用サービスの詳細の要件 28
（10）通信回線の要件 30

（11）データセンターの要件 33
（12）次期（第３期）セキュリティクラウドの構築の要件 34
（13）接続団体の移行の要件 35
（14）運用・保守業務要件 36
（15）セキュリティ監視等業務の要件 36
（16）契約終了時の要件 36

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（第３期）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（第２期）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、以下の機能を有する。

- 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機能を有する。また、総務省からセキュリティクラウドの標準要件として以下が示されている。
  - ✧ 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
  - ✧ EDR（Endpoint Detection and Response）の導入（β/β'モデル（業務端末をインターネット接続系ネットワークへ設置する構成）の場合）

（3）本委託業務の目的

現行（第２期）セキュリティクラウドは、令和３年度に構築し、運用を行っているが、令和８年度末に運用期限を迎えることから次期（第３期）セキュリティクラウドを構築したうえで、現行（第２期）セキュリティクラウドから次期（第３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（第３期）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

- 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。
- 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の受託事業者等、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。
- 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、通信回線も提供を行うこと。
- 現行（第２期）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（第３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の運用監視を行い、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。
- 接続団体のうち EDR 参加団体には、エンドポイントにおける EDR 機能及びマルウェア対策機能を提供すること。また、ライセンス等についても必要数を納入すること。
  参加団体及び必要ライセンス数は別紙「EDR 参加団体」参照
- 業務の詳細は、「11　業務詳細」を確認すること。

イ　現行（第２期）セキュリティクラウドの構成概要

- 現行（第２期）セキュリティクラウドの構成概要は、以下のとおり。なお、現行（第２期）セキュリティクラウドでは、EDR と EDR の SOC は別契約（追加セキュリティ対策）としているが、図では簡略化して記載している。
- リバースプロキシの機能は、WAF、CDN に内包されている。

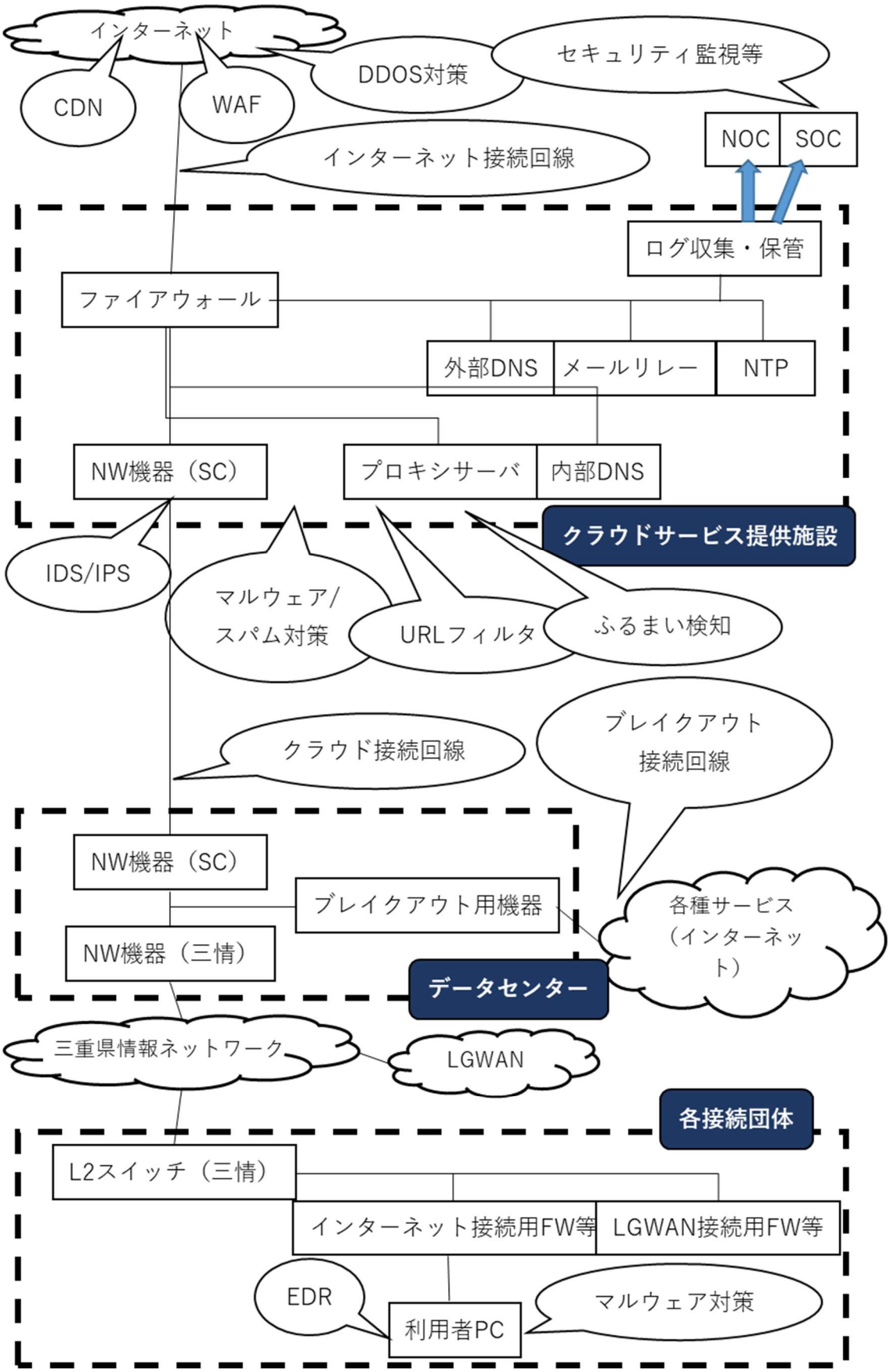
インターネット
CDN
WAF
DDOS対策
セキュリティ監視等
NOC
SOC
インターネット接続回線
ログ収集・保管
ファイアウォール
外部DNS
メールリレー
NTP
NW機器（SC）
プロキシサーバ
内部DNS
クラウドサービス提供施設
IDS/IPS
マルウェア/
スパム対策
URLフィルタ
ふるまい検知
クラウド接続回線
ブレイクアウト
接続回線
NW機器（SC）
ブレイクアウト用機器
各種サービス
（インターネット）
NW機器（三情）
データセンター
三重県情報ネットワーク
LGWAN
各接続団体
L2スイッチ（三情）
インターネット接続用FW等
LGWAN接続用FW等
EDR
利用者PC
マルウェア対策

図　現行（第２期）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５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
NW 機器（SC）	・セキュリティクラウドと三重県情報ネットワークを接続する機器
NW 機器（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機器
SOC（NOC）	・SOC として、収集したログの常時監視または全エンドポイントに対するログ分析等を通じて、セキュリティインシデント等を検知できること。 ・NOC として、各接続団体におけるセキュリティインシデント発生時における必要な対応の支援が実施できること。
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 へ接続する機器等

表　現行（第２期）システムの機器等一覧

機器・機能	内容
インターネット接続回線	・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 ・公開サーバ等のインバウンド通信用回線
CDN	・インターネット上のコンテンツを効率的かつ高速に配信する機能
WAF	・Web アプリケーションへの不正アクセスを防ぐ機能
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 ・エンドポイントにおける、マルウェア（コンピュータウィルス等の悪意ある動作を行うソフトウェア）対策機能として、主に「侵入されないための機能」を提供できること。 ・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。
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
EDR	・EDR として、エンドポイントにおいてマルウェア等の脅威が侵入した後に「被害を拡大させないための機能」を提供できること。 ・具体的には、各エンドポイントからの「ログの収集・分析」を通じて、「被害の検知」「不審な通信や動作の遮断」「侵入経路や被害範囲の調査」といった機能を提供できること。 ・EDR の運用において、セキュリティ等の専門的な知識や経験が必要となる場合は「SOC(NOC)」を設置し、必要な作業が実施できること。

表　現行（第 2 期）システムの機能等一覧

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）

エ　利用者数・端末数

・ 利用者数・端末数は以下のとおりとする。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ため、最大数が利用可能なこと。

項目	現在の数	最大数
利用者数	約 15,000 人	約 30,000 人
端末数	約 15,000 台	約 26,500 台
端末数（EDR 及びマルウェア対策）	約 11,500 台	約 20,000 台

オ　次期（第３期）サービス構成例

・ 現行（第２期）では EDR と EDR の SOC は別契約（追加セキュリティ対策）としていたが、次期（第３期）では EDR と EDR の SOC も含めた構成とする。なお、あくまで想定であり、本構成に限定するものではない。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の要件」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。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。

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 または 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を取得していることが望ましい。
  - プライバシーマーク制度の認定事業者また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 は、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 の詳細は、「4　履行場所」を参照のこと。）
- 延べ数万台端末規模の監視運用実績を有すること。
- 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。
- 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。
- セキュリティクラウド本体と EDR の SOC は同一事業者とし、問合せ窓口も一元化すること。

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 14 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 9 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 9 年 2 月から令和 9 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、運用期間と同様の機能を提供すること。
運用期間	・令和 9 年 4 月 1 日から令和 14 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 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 は、県外設置も可とする。

SOC の設置場所は日本国内とし、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の要件は、「11　業務詳細（１１）データセンターの要件」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場所、別場所でも可とする。
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。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、当該製品のサポート終了の情報を知りえた段階で、本県に報告をおこない、サポートが終了するまでに、本県に今後の対応策の説明を行い、承認を受けること。

ソフトウェアライセンスは、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。

運用開始は令和９年４月１日からであるが、少なくとも移行開始時期には各種ライセンスが必要になると想定される。このため、サブスクリプション形式の１年単位ライセンスなどについて、運用期間終了（令和 14 年３月 31 日）までのライセンスの確保する必要があることに留意すること。

なお、ほとんどのハードウェア及びソフトウェアは、受託事業者の資産（本県への納品がない）となる想定をしている。

（２）各エンドポイントにインストールするエージェントソフトウェア

各エンドポイント（業務端末）にインストールするエージェントソフトウェアについては、以下の数量を調達し、納品すること。（詳細は、別紙「EDR 参加団体」を参照）なお、「３事業概要（２）業務範囲ウ 利用者数、端末数」に記載の端末数よりも少ないが、これは、調達するライセンス数を超えた端末で利用する場合は、その都度、各接続団体がライセンスの追加を行うことを想定しているためである。

項目	必要ライセンス	期間
エージェントソフトウェア	11,500 ライセンス	令和９年４月１日から 60 カ月分

表　調達するライセンス数

各接続団体が、エージェントソフトウェアを追加購入する方法として、利用初年度に複数年度分のライセンス費用を一括支払いする場合と、毎年一年分のライセンス費用を支払う場合があるため、柔軟な対応ができること。

運用開始は令和９年４月１日からであるが、移行開始時期から運用開始前までの移行期間中もライセンスが必要になると想定される。移行期間の間は、別紙「EDR 参加団体」及び表「調達するライセンス数」の必要ライセンスに加え、各接続団体が追加購入する予定の追加ライセンスについても本業務で提供できること。

項目	移行期間	運用期間
必要ライセンス	本業務の範囲	本業務の範囲
追加ライセンス	本業務の範囲	本業務の範囲外

エージェントソフトウェアは、本委託業務の履行期間終了時点まで追加購入が可能なこと。

三重県及び他の接続団体が、追加購入を行う場合には、同価格または同価格以下にて購入が可能であること。１ユーザ１年間当たり 4,600 円（税込）程度を想定している。ただし、物価や為替の変動により同価格以下の購入が困難である場合は別途協議する。また、ライセンスの追加購入に伴い、SOC(NOC)における利用費用の増大が見込まれるが、「２事業概要（２）業務範囲　エ 利用者数・端末数」に記載の端末数をあらかじめ見込み、SOC(NOC)にかかる追加費用が発生しないよう、あらかじめ、本委託業務にかかる費用に見込んでおくこと。

（３）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を、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三重県から一括して支払うこととする。なお、追加購入したライセンス費用については、購入時点の支払い条件に基づき、原則として、購入した団体から支払いを行う形になるため、注意すること。

消費税法が改正された場合は、当該期間の費用は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８年度 67.5%

- 令和９年度　6.5%
- 令和 10 年度 6.5%
- 令和 11 年度 6.5%
- 令和 12 年度 6.5%
- 令和 13 年度 6.5%

（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、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、保守費用は、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また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は、本委託業務のみに利用するものとし、契約期間中また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）受託者は、業務の履行にあたって「三重県の締結する物件関係契約からの暴力団等排除措置要綱」に規定する暴力団、暴力団関係者また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）のイまた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

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うえ、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、本県と協議のうえ、定めるものとする。

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。
  - 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者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十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。
  - 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、業務計画書の内容を変更する場合は、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。 ・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。 ・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は、その影響範囲及び対応に必要な工数等を識別したうえで、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。
- 適宜ミーティング等を実施し、本県に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 回程度、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。
- 各報告会等の議事録は、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、第三者に開示または漏洩しないこと。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（第２期）セキュリティクラウドに関する構成詳細や、公開情報等は、以下の資料を参照すること。なお、以下の資料にない設計構成情報、ハードウェア・ソフトウェア構成の情報、監視・運用・保守の情報は、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者に開示することができる。

- 現行（第２期）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（第２期）セキュリティクラウド接続申請書
- 三重県自治体情報セキュリティクラウド接続団体様追加セキュリティ対策（EDR）概要

（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、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である。

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）」の接続ポートとし、責任分界点からインターネット側の、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。

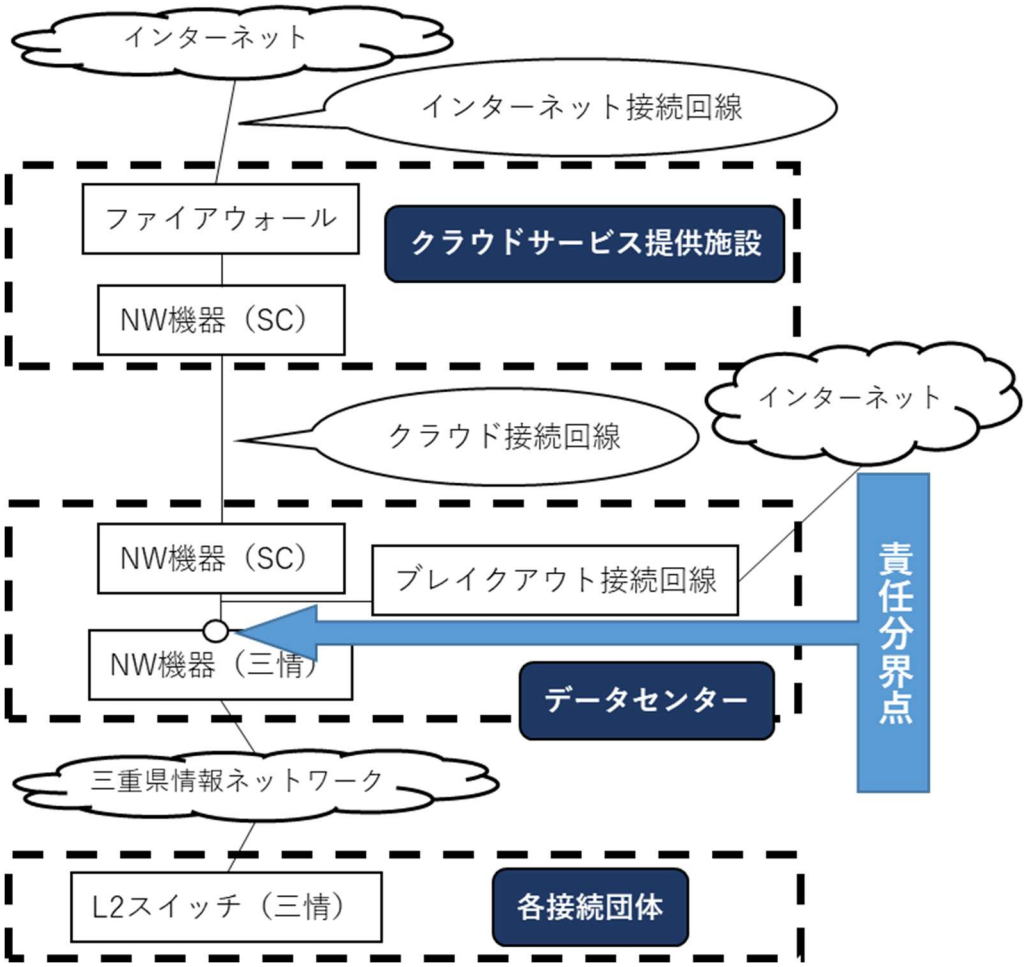

図　責任分界点

（4）他の受託事業者との調整

ア　接続団体関連

- 各接続団体担当者のほか、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な場合は、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協議すること。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。

・ 接続団体側の機器において、設定変更が必要であり、接続団体の既存契約の範囲を越える内容は、受託事業者の責により実施すること。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。

イ　既存事業者との調整

・ 現行（第 2 期）セキュリティクラウドの受託事業者及び三重県情報ネットワークの受託事業者等、本県がこれまでに調達を行った既存事業者と協議等が必要な場合は、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。

ウ　設定変更等の依頼

・ 他の受託事業者が導入した機器等の設定変更等が必要な場合は、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は、受託事業者が主体的に実施すること。また、これらの設計は、本県、接続団体、及び、関係する受託事業者に説明を行い、設定変更内容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であり、既存契約の範囲を越える内容は、受託事業者の責により実施すること。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。

・ 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、問い合わせ対応は既存契約による対応が可能だが、作業時の立会等は、受託事業者ごとに対応が分かれる。

・ 運用期間中に、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。その場合は、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は、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の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 8 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

・ 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である。ただし、各工程に着手する前に、当該工程にて作成するドキュメントに関し、本県と協議を行うこと。

・ 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 8 年 9 月末）	・セキュリティクラウドで提供される各種サービスの詳細を定義したもの。 ・各種サービスの性能要件を記載すること。 ・運用・保守業務のほか、セキュリティ監視等業務の詳細を記載すること。
構築設計書（令和 8 年 9 月末）	・サービス定義書で定義した各種サービスを構築するために必要となる各種設計を記載したもの。
移行設計書・移行手順書(令和 8 年 12 月末)	・現行（第 2 期）セキュリティクラウドから次期（第 3 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を記載したもの。 ・各接続団体に対する移行設計書及び移行手順書を作成すること。
運用・保守設計書（令和 8 年 12 月末）	・運用期間における運用・保守の業務内容を記載したもの。 ・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を記載すること。
セキュリティ等監視設計書（令和 8 年 12 月末）	・運用期間中のセキュリティ等監視の業務内容を記載したもの。 ・利用者からの通報や攻撃等の検知に対する一次対応のほか、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を記載すること。
接続申請書（令和 9 年 3 月末）	・現行（第 2 期）セキュリティクラウドで各接続団体との接続用に用意した接続申請書を、次期（第 3 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、各接続団体の接続構成図を記

	載すること。
接続団体向け説明資料（令和 8 年 12 月末）	・接続団体向け説明会用の資料のこと。セキュリティクラウドの機能概要、設定変更等の流れ、緊急時対応等を記載し、詳細は、本県と協議を実施したうえで作成すること。 ・本資料は毎年度更新を行うこと。
各種設定一覧（令和8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を記載したもの。 ・ハードウェアを納品している場合は、ラック構成図のほか、必要な内容等を記載すること。
運用・保守体制表（令和 8 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・保守体制を記載したもの。 ・通常時の体制のほか、緊急時体制を記載すること。 ・本資料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の定期レポート、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。 ・議事録を適宜作成すること。

表　ドキュメントの詳細

11　業務詳細

（1）設計業務全体の要件

ア　基本方針

- 安定した稼動、業務の継続性を重視し、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、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た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を行うこと。
- 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の設計を行うこと。
- 本県担当者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。
- 各接続団体担当者、及び、関係する受託事業者等に、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、負担を少なくすること。
- 作成した設計書、手順書等は、作成の都度、本県に説明を行い、承認を得ること。

（２）事前調査の要件

ア　各接続団体における事前調査及びヒアリング

- 各接続団体の事前調査として、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、現状との差異を確認し、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担当者のほか、各接続団体の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、EDR等）の保守担当事業者等からヒアリングを行い、意見・要望等のほか、障害情報、機器更新等の変更予定等の情報を収集するとともに、必要な連絡体制を確認すること。
- 移行期間中の、各接続団体の既存ネットワーク及び既存システム等の設定変更時の立ち合いの可否や、設定変更等に対する作業依頼の可否を確認すること。

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の内容を確認すること。
- 既存事業者と協議を行い、詳細な内容を確認すること。
- 移行期間中の、設定変更時の立ち合いの可否や、設定変更等に対する業務依頼の可否を確認すること。

（３）サービス設計の要件

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は、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」を参照すること。

各種サービスに対して、性能要件や障害発生時の業務継続性を記載すること。

NOC及びSOCが提供する各種サービスについて、業務内容のほか提供可能なサービスレベルをSLAまたはSLOとして記載すること。

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を本県に報告し、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の要件

三重県情報ネットワークとの接続に必要な接続設計を行うこと。また、必要に応じてラック構成図を作成すること。

接続設計にあたっては、三重県情報ネットワークの受託事業者と調整を行い、可能な限りシンプルな構成とすること。

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）は本委託業務の範囲中で準備すること。（三重県情報ネットワーク機器の詳細は、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は、データセンター事業者に依頼してラック間配線を行うこと。なお、ラック間配線は、本委託業務の範囲内で行うことこと。（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データセンター事象者に依頼すること。）

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、余裕をもって発注すること。

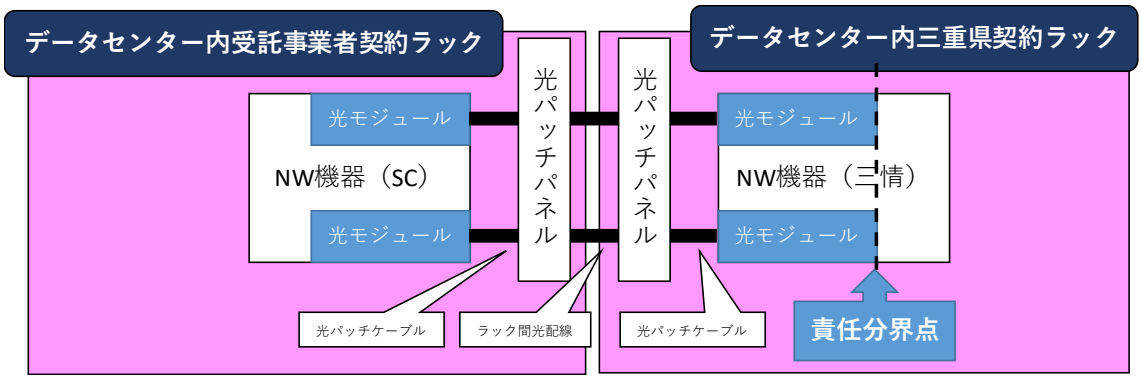

図　三重県情報ネットワークとの接続詳細

（５）構築設計

現行（第 2 期）セキュリティクラウド、各接続団体の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、既存の構成等にできるだけ影響を与えないような構築設計を行うこと。

「（3）サービス設計の要件」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、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）を記載すること。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、Zoom コミュニケーションズ社 Zoom 等）へのアクセスは、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。

本仕様書にて、各種サービスの要件のみが記載され、詳細な構成等が記載されていない場合は、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の費用等は本委託業務の範囲内とすること。

各接続団体の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 XFF（X-Forwarded-For）の設定の設計を行うこと。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の受託事業者が実施することを想定している。

次期（第３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の機能要件、性能要件等の確認が行えるよう、稼働試験及び性能試験の設計を行うこと。特に、性能試験は、各種サービス単体テスト、疎通テスト等のほか、できる限り実環境に近い構成による試験が

できるようにすること。

次期（第３期）セキュリティクラウド内に冗長部分がある場合（例えば、Active/Standby構成の機器や通信回線など）、切り替え作業の試験及び切り戻し試験の設計を行うこと。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（切り戻しの時間、通信断の時間など）の情報を取得するため、可能な限り実環境に近い試験を実施できるようにすること。

運用期間中の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の試験の設計を行うこと。

全ての構築作業及び各種試験が完了した段階で、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判断できる稼働試験の設計を行うこと。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「稼働判定基準」の作成を行うとともに、当該判定基準について、本県に説明を行い、承認を得ること。

（６）移行業務等の設計の要件

各接続団体が現行（第２期）のセキュリティクラウドから、次期（第３期）セキュリティクラウドへ移行するために移行業務の設計を行うこと。

現行（第２期）セキュリティクラウド（EDR（追加セキュリティ対策）も含む）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。

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等、さまざまな理由により予定通りの移行が進まない場合でも、移行期間内に全ての作業が完了するよう、余裕を持った設計とすること。

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、移行作業量が軽微な接続団体から優先して移行すること。

接続団体への影響が小さくなるよう、各接続団体のネットワークや各種サービスの停止時間を最小限に抑え、かつ、安全で確実に移行作業を実施すること。

障害発生等により移行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、発生する可能性のある障害等を想定し、調査方法等を手順書等として準備すること。

移行作業実施時に、各接続団体担当者及び既存ネットワークや既存システムの受託事業者による作業が必要ない設計を行うこと。やむを得ず、各接続団体担当者及び既存ネットワークや既存システムの受託事業者に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、事前リハーサルや当日の作業立会など、確実な移行作業が実施できること。

接続申請書は、各接続団体の移行後の状態を記載するよう様式を修正したうえで、各接続団体の移行設計を反映させること。

各接続団体内で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。

移行作業の詳細を設計するとともに、移行後の試験として各種サービスの稼働試験のほか、

可能な限り性能要件の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の障害に備え、バックアップ回線等の冗長化構成を有し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、各接続団体の移行作業の実施日時や各担当者名、連絡先等を網羅した各接続団体の移行計画を策定すること。

策定した移行計画を各接続団体に説明し、承認を得ること。

（7）運用・保守業務の設計の要件

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

- 運用・保守業務を行う運用・保守要員等が勤務する施設として、NOC 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 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。
- 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、少なくとも 1 拠点は 24 時間 365 日の有人運用とすること。
- セキュリティ監視等の業務を行う SOC と NOC との間で緊密な連携が取れること。なお、SOC は NOC と同一施設とする必要はない。
- 各接続団体担当者の業務負荷軽減とセキュリティ・可用性の向上を考慮すること。
- 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 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、運用・保守業務を実施すること。

イ　総合窓口

- 接続団体担当者からの問合せ、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電話及びメールのほか、柔軟な連絡手段を用意すること。
- 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

になる機能を有すること。

- セキュリティ監視等業務における、インシデント発生時の詳細情報の情報共有を行える機能を有すること。
- ポータルサイトへのアクセスは、ID パスワードに加え、クライアント証明書や 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（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ほか、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。
- 全接続団体が閲覧可能な掲示板機能を有すること。
- 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等に通知が行えること。
- 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等による通知が行えること。
- 問合せの進捗状況・ステータス及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。
- 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の進捗を管理し、完了まで責任を持って対応を行うこと。
- 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すること。

オ　稼動監視・障害対応

- 各種サービスの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、障害の一次切り分け、障害発生ポイント等の特定、暫定対応等の実施、各接続団体担当者への報告などを速やかに行えるよう、対応フロー等を整理すること。
- 監視対象として、各種サービスの提供状態のほか、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

ータス等を監視対象とすること。安定的な運用のために、監視が必要と考えられる項目を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、関係機関へ報告を行うこと。
- 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）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、軽微な障害等は、翌営業日以降の対応も可とする。
- 障害対応の進捗を管理し、完了まで責任を持った対応を行うこと。

カ　設定変更対応

- 各接続団体担当者からの依頼に基づき、各種設定変更を行うこと。なお、疑義のない設定変更依頼は、原則として翌営業日中に対応を行うこと。
- 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は、本県担当者の承認を得てから作業を実施すること。
- 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
  - Web サイトの SSL 複合除外設定
  - 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
  - プロキシの接続団体向け IP 設定
  - DNS サーバのレコード設定
  - DNS マスタ、スレーブ設定
  - 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）
  - 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
  - ポータルアカウント登録・変更・削除
- 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。
- 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。

キ　調達した機器に対するリスク管理

- 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。
- 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の適用は、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対応すること。
- 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こと。

ク　構成情報の更新対応

- 稼働監視・障害対応、設定変更対応、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のシステム構成や設定内容等に変更があった場合、更新履歴を残したうえで、各種設計書の必要な情報の更新を行うこと。
- 各種設計書は、常に最新版の情報を閲覧できるとともに、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

- 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、対面またはWEB会議での開催を原則とすること。
- 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を報告すること。なお、日程調整は受託事業者が実施すること。
- 報告会では、運用・保守の対応状況として、問合せ件数、進捗管理状況のほか、障害やインシデントの発生状況や対応状況を取りまとめ、報告書として提出すること。また、各接続団体の各種サービスの利用状況や稼働状況（負荷情報など）のほか、通信回線等のトラフィック情報等を報告すること。
- 報告内容によっては、全ての報告会での報告を求めるものではないが、本県に対しては、半年に1度以上、全ての項目の報告を行うこと。
- 後述するセキュリティ監視等業務の内容を、本報告会にて報告すること。
- 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、報告すること。

コ　セキュリティ監視等業務

- 後述する「（8）セキュリティ監視等業務の設計の要件」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、運用・保守業務の一環として、必要な対応を実施すること。なお、現地対応は、各接続団体担当者及び既存ネットワークや既存システムの受託事業者が対応を行い、また、リモートによる対応で十分な場合が大半のため、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、対応フロー等を整理すること。
- 緊急時連絡は、SOCから各接続団体担当者や関係受託事業者等に直接連絡を行

うフローを想定するが、SOCからの支援だけでは十分な支援ができない場合は、NOC 要員が SOC からの連絡を受けた後、各接続団体に報告・支援を行うフローも可とする。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業務を実施できること。

- 被害状況の確認や、既存ネットワークや既存システムの受託事業者への説明、根本的な対応策の提案や根本対応等の実施の支援まで、各接続団体からの要望に応じて対応すること。
- 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のアラート通知などの情報を SOC と情報共有すること。

サ　職員研修対応

- 接続団体のシステム管理者や新任者を対象とした県主催の研修会にて、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、障害時対応等の説明を実施すること。
- 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。なお、対面または WEB 会議での開催を原則とすること。

シ　対応時間帯

- 対応時間は、下記を目安とするが、安定的な運用・保守を行え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
システム設定変更対応	平日 8:30～17:15
システム更新（セキュリティパッチ適用）対応	平日 17:15～8:30 土日祝日
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、各接続団体担当者に対し、インシデント発生を想定した模擬訓練を実施すること。
- 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。
- 場合によっては、実施しない場合もある。

（８）セキュリティ監視等業務の設計の要件

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 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。
- 各接続団体担当者の業務負荷軽減とセキュリティ・可用性の向上を考慮した設計とすること。
- 運用期間中、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、改善し、安定的、効率的かつ高品質なサービスを提供すること。
- 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うこと。

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、または、登録見込みであること。
- SOC におけるセキュリティ監視等業務は、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。
  - 独立行政法人情報処理推進機構の認定資格「情報処理安全確保支援士」
  - (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」
  - 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 5 年以上持つこと。
- 分析結果に関する技術的な問合せに、24 時間 365 日対応できること。また、不正アクセス等の内容を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。
- 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。
- 窓口対応は、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

- 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。

- 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で能動的に見直しを行うこと。また、セキュリティ監視等の対象機器の検知精度を向上させるため、検知ポリシーは検知及び分析結果をもとに検討すること。
- 検知ポリシーの変更等は、本県担当者から照会があった場合、その運用方法等の概要を説明できること。
- 検知ポリシーの変更等は、本県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こと。
- 機器メーカーから検知シグネチャ等が提供された場合は、セキュリティ監視等の対象機器等の、正常な通信に影響を及ぼさないよう適用できること。なお、適用する検知シグネチャ等は、セキュリティクラウドの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すること。
- セキュリティ監視等の対象機器に対し、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の双方向通信を調査・解析できること。また、危険度に応じて、各接続団体担当者に報告を行うとともに、対策等の助言が実施できること。
- SOC から各接続団体に直接報告を行い、対応策等の支援が実施できること。さらに、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機器において、不正な通信を検知、遮断できること。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	・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、各接続団体担当者に報告するとともに、該当端末利用

合	者等に対する対処方法を報告すること。
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の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 は、分類可能とすること。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 ・過去に悪性と判断されたイベント
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 ・被害の痕跡が確認できたイベント

表　危険度と対応方針

・ 危険度分析において、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）と判断した場合は、不正な通信に対する調査、解析とともに、監視対象ネットワークに影響を与えない範囲で対象機器の脆弱性有

無を確認し、最終的な判断を行うこと。

- 危険度の判定で重大なセキュリティインシデントと判定した場合、60 分以内に、受託事業者の専門技術者から当該接続団体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を確実に伝達すること。
- 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端末と判断できる場合は、可能な限り端末を特定すること。端末を特定できた場合は、当該端末を隔離措置等したうえで電話やメール等の方法により報告すること。
- 接続団体側に Proxy サーバが設置されている多段 Proxy 構成で、送信元 IP アドレス情報 XFF（X-Forwarded-For）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

- 検知したイベントは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	・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	・各接続団体の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。

（9）利用サービスの詳細の要件

セキュリティクラウドで提供される各種サービスは以下の要件を満たすこと。

ア　基本要件

- クラウドサービスは、受託事業者が提供するサービスのほか、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、本委託業務の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一の内容とするが、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しないよう制限できること。

- クラウドサービスで取り扱う情報資産について、運用・保守業務の目的以外に利用しないこと。

イ　機能要件

- 各種サービスにおける詳細な機能要件は、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」を参照すること。また、令和 7 年 5 月 23 日総行サ 9 号総務大臣通知「地方公共団体サイバーセキュリティ対策事業費補助金交付要綱、地方公共団 体サイバーセキュリティ対策事業実施要領（自治体情報セキュリティクラウ ド更新事業）等の策定について（通知）」で示された「自治体情報セキュリティクラウド機能要件一覧」の必須要件を満たすこと。
- なお、各種サービスの詳細要件に記載がなくても、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な機能は、適宜、提供すること。特に、単一障害によるサービス停止を防ぐ冗長化構成等や、ウィルス対策等の対応等を実施すること。
- ブレイクアウト接続回線の通信は、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は、全ての接続団体が利用しても問題ないよう十分な処理能力を有したものとすること。
- ブレイクアウト接続回線からの通信は、通信ログの採取とレポート作成ができること。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。
- CDN は、運用期間中の設定変更（CDN の対象となるサイト数の増減、FQDN の変更等）も本委託業務の範囲内とすること。
- CDN は、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。
- 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は、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。
- 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。

ウ　性能要件

- 「2　事業概要（2）業務範囲　ウ　接続団体」の接続団体が、契約期間終了時まで利用できる十分な性能を有すること。
- 各接続団体から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は、後述する「(10) 通信回線の要件　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及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は、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。
- 選定するファイアウォールは、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。
- WAF は、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。
- 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。

(10) 通信回線の要件

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、運用期間中、利用できること。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こと。
- 後述する「ブレイクアウト接続回線」と合わせて計 5Gbps 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 2Gbps の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 の帯域確保または

帯域保証回線とすること）を用意すること。

分類	インターネット接続回線	ブレイクアウト接続回線	計	クラウド接続回線
ブレイクアウト接続回線をDC（津市内）で接続する場合	2Gbps(帯域保証)	1Gbps(帯域保証) 2Gbps(ベスト)	5Gbps	2Gbps（帯域保証）
ブレイクアウト接続回線をクラウド接続回線経由で接続する場合	2Gbps(帯域保証)	1Gbps(帯域保証) 2Gbps(ベスト)	5Gbps	3Gbps(帯域保障) 2Gbps(ベスト)

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

※　クラウド接続回線及びブレイクアウト接続回線の詳細は、後述の記載を参照すること。

※　ベスト：ベストエフォート

- インターネット接続回線は、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個以上利用できること。ただし、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。また、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。
- インターネットから接続団体のWebサーバに対するWeb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）は、Webアクセス全体の処理能力として読み替えること。
- 現行(第2期)のセキュリティクラウドにて利用中のドメイン(mie-sec-cloud.jp)を、次期(第3期)セキュリティクラウドにおいても継続利用できること。なお、継続利用するにあたり、現行（第2期）セキュリティクラウドの受託事業者からドメイン管理業務を引き継ぎ、運用期間中の管理費用（5年間）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を接続する回線として、以下の要件を満たすこと。

- 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で用意すること。
- 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、利用できること。
- 前述した「インターネット接続回線」と合わせて計 5Gbps 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 2Gbps の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 の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が不通となった場合は、インターネット接続回線等を経由する経路変更の対応や、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。
- ブレイクアウト接続回線は、インターネット接続回線とは別キャリアとすること。
- グローバル IP アドレスを 128 個以上利用できること。ただ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。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。

エ　サービスレベル要件について

- インターネット接続回線、クラウド接続回線については、サービスレベルを定めた回線とする。
- 提供業者は回線毎・月間毎の稼働率を把握・管理し、SLA 報告書として提出すること。
- 各回線の稼働率を月毎に算出し、99.9%を下回った月があった場合、下記の計算式に応じた金額を減額する。なお、減額は該当回線毎に月額で算出する。
  ただし、提供業者が独自に上記よりも厳格な SLA 項目を設定している場合は、それを適用する。

  【計算式】

  SLA 減額＝SLA 未達成の回線における該当月の通信回線サービス利用料×減額率

稼働率	減額率
99.8%以上 99.9%未満	1%
98.0%以上 99.8%未満	3%

95.0%以上 98.0%未満	10%
90.0%以上 95.0%未満	20%
90.00%未満	100%

（11）データセンターの要件

クラウドサービス提供施設として本県が別途調達してい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は「イ　設備要件」を参照すること。
- データセンターは日本の法令が適応されること。また、管轄裁判所に関しては、日本国内の裁判所を合意管轄裁判所とできること。

イ　設備要件

要件	詳細
情報セキュリティマネジメントシステム	・JIS Q 27001 または 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。
立地	・国内に設置された施設を利用し、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（耐震構造または免振構造）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がないこと。 ・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化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（第３期）セキュリティクラウドの構築の要件

次期（第３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、冗長化構成等の切り替え試験等、現行（第２期）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。

三重県が別途調達してい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。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（第２期）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、ネットワーク等への影響を与えないようにすること。

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、速やかに本県に報告を行うこと。また、速やかに構築設計を修正し、本県に説明を行い、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、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を行うこと。

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、根本解決策等を本県に報告を行うこと。

構築後、しばらくの間は現行（第２期）セキュリティクラウドの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、その結果を本県に説明し、承認を得ること。

（13）接続団体の移行の要件

全ての接続団体について、現行（第２期）セキュリティクラウドから次期（第３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。

三重県が別途調達しているデータセンターで作業を実施する際は、入館申請が必要となる。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の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担当者に連絡を行うこと。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説明を行い、承認を得ること。

各種試験の結果は、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に報告

を行うこと。

各接続団体の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、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を行うこと。

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、根本解決策等を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。

移行計画の全ての作業が完了後、本県及び当該接続団体に説明を行い、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「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、必要に応じて現地確認等も実施し、サービスレベルを低下させないこと。

（15）セキュリティ監視等業務の要件

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「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」の内容のほか、各接続団体における詳細構成等も引継ぎを実施し、要員変更によるサービスレベルを低下させないこと。

（16）契約終了時の要件

受託者は、本業務に関連し調達したハードウェアまたは記録媒体（以下、「ハードウェア等」という）を交換または撤去する場合は、ハードウェア等に記録されたデータの復元が不可能となるよう物理的な破壊を行ったうえで、適正に廃棄すること。

データの抹消作業は、三重県が指定する場所で行うこと。なお、記録されたデータの内容によっては、抹消作業に三重県の職員が立ち会うことがある。また、データの抹消作業に際し、以下のことを行うこと。

- 事前に対象となるハードウェア等の名称、型番、数量及び抹消作業の方法を三重県に説明し承認を得ること。

- データの抹消作業の前及び後にハードウェア等の数量を記録すること。
- 当該作業の結果、ハードウェア等のデータ復元が不可能な状態に破壊されたことを証する証明書を三重県に提出すること。

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。