資料２

三重県自治体情報セキュリティクラウド

（追加セキュリティ対策）構築及び運用・保守業務

に関する仕様書

令和３年12月

三重県デジタル社会推進局

スマート改革推進課

1　本仕様書について 1
（1）はじめに 1
（2）必須、提案、想定 1
2　背景と目的 1
（1）三重県自治体情報セキュリティクラウドとは 1
（2）追加セキュリティ対策とは 2
（3）本委託業務の目的 2
3　事業概要 3
（1）契約名 3
（2）業務範囲 3
4　調達スケジュール 9
5　履行場所 9
6　納品物件 10
（1）ハードウェア及びソフトウェア 10
（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 10
（3）ドキュメント 11
7　支払い 12
（1）支払条件 12
（2）内訳資料の提出 12
8　機密保持 12
9　暴力団等による不当介入に対する対応 13
10　注意事項 13
11　調達全般に関する共通要件 14
（1）プロジェクト管理に関する要件 14
（2）本県からの提供資料 15
（3）他の受託事業者との調整 15
（4）ドキュメント 16
12　業務詳細 18
（1）設計業務全体にかかる要件 18
（2）事前調査にかかる要件 19
（3）全体構成と機能要件 19
（4）構築業務等の設計にかかる要件 21
（5）導入業務等の設計にかかる要件 22
（6）セキュリティインシデント対応支援業務の設計にかかる要件 24
（7）セキュリティ監視等業務の設計にかかる要件 27
（8）データセンターにかかる要件 30
（9）追加セキュリティ対策の構築にかかる要件 31
(10) 接続団体の導入業務にかかる要件 32
(11) セキュリティインシデント発生時における対応支援業務要件 32
(12) セキュリティ監視等業務にかかる要件 33

１　本仕様書について

（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（追加セキュリティ対策）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）必須、提案、想定

本仕様書では、各項目を「必須」「提案」「想定」に分類した形で仕様書上に記載している。必須、提案、及び、想定にかかる詳細は次の通りである。なお、本文中には「必須」は記載せず（本書に記載されている要求事項は必須）、「提案」「想定」のみを記載するものとする。

分類	詳細
必須	本県が求める仕様であり記載内容通り必ず実現すること
提案	本県が受託事業者に求める提案要件であり受託事業者は必要に応じて提案を行うこと
想定	本県が提案要件に対して想定している内容であるため、必ずしも実現する必要はないが、受託事業者は提案にあたり参考にすること。

表　必須と提案

２　背景と目的

（１）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

といった機能を有しているが、令和 4 年 3 月末日をもって、運用・保守期限が到来することとなっており、さらに、令和 2 年 8 月に総務省から、次期セキュリティ

クラウドにかかる標準要件が示され、その必須要件として、

- 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）
- 可用性、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セキュリティインシデント対応

等への対応が求められたことなどから、令和3年8月6日に「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」を締結し、これらの機能を備えた次期セキュリティクラウドの構築を行っているところである。

今後、令和3年度末までに次期セキュリティクラウドの構築と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を経て、令和4年4月1日から令和9年3月31日までの運用を予定している。

（2）追加セキュリティ対策とは

令和2年5月「自治体情報セキュリティ対策の見直しのポイント」により、効率性・利便性を向上させた新たな自治体セキュリティ対策のモデルとして、従来のαモデル（三層の対策を施した構成）に対して、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）が示された。また、その際、「EDR（Endpoint Detection and Response）」の導入がβ/β’モデルへの移行にかかる必須要件として示された。

また、令和3年9月に開催された三重県自治体セキュリティクラウドにおける各接続団体（三重県、県内29市町、一部事務組合等、計33団体）間の協議において、すでにβ/β'モデルへ移行済みの団体、及び、移行を予定している団体から、EDR機能の導入を含むセキュリティ対策にかかる機能追加が提案され、協議の結果、了承された。そのため、セキュリティクラウドへの機能追加として、「追加セキュリティ対策」の実施を行うこととなった。

なお、追加セキュリティ対策として、EDR機能の追加に加えて、次期セキュリティクラウドで調達している NOC（Network Operation Center）/ SOC（Security Operation Center）の活用や、ライセンス費用について、共同調達による費用削減を実現するよう要望があった。そのため、これらの要望を可能な限り実現することを目指し、価格だけではなく、追加セキュリティ対策の内容について受託事業者から提案を受け総合的な評価が可能となる、総合評価一般競争入札による調達を行うこととした。

（3）本委託業務の目的

以上のことから、次期セキュリティクラウドに対する追加セキュリティ対策として、EDR機能を含む最も効果の高いセキュリティ対策の構築と運用を行うことを本委託業務の目的とする。

３　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（追加セキュリティ対策）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、必要な設計を行うこと。
- 全接続団体が利用できる形で、追加セキュリティ対策を提供できるようにすること。また、ライセンス等についても必要数を納入すること。
- 接続団体に対して利用開始時期についての調査を行い、それぞれの利用開始時期に応じて導入作業の支援を行うこと。
- 契約期間終了日まで、追加セキュリティ対策の安定的な運用を行うとともに、接続団体からの設定や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。
- 追加セキュリティ対策にかかる運用監視を行い、セキュリティ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、エンドポイント（業務端末）の論理抜線、ネットワークの制限、復旧までの支援等の対応を行うこと。
- 業務の詳細については、「12　業務詳細」を確認すること。

イ　接続団体

- 追加セキュリティ対策を利用できる接続団体として、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の計 33 団体（内、地方自治体は三重県の他 29 市町）とすること。

ウ　利用者数、端末数

- 全接続団体における利用者数 約 15,000 人、端末数 約 15,000 台（最大の利用者数として 30,000 アカウント、端末数として 26,500 台を想定）とすること。

エ　次期セキュリティクラウドのサービス構成

・ 次期セキュリティクラウドにかかるサービス構成については、以下のとおり。

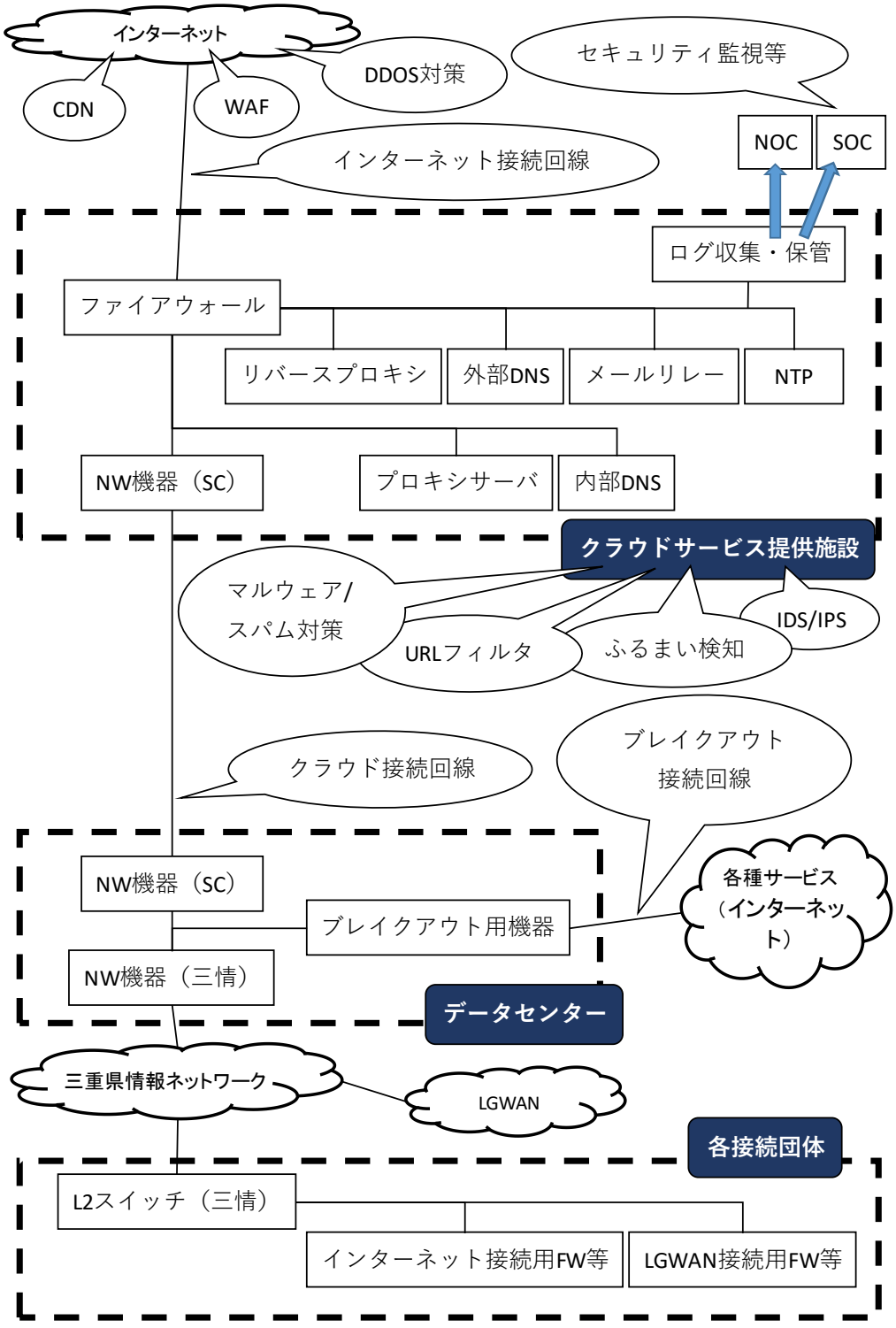

図　次期セキュリティクラウドのサービス構成

※ 上図は現在構築中の次期セキュリティクラウドについて、現時点の情報をもとにまとめたものであり、実際の構成と異なる場合があるため、注意すること。

カ　追加セキュリティ対策のサービス構成例

・　追加セキュリティ対策のサービス構成例については、以下のとおり。

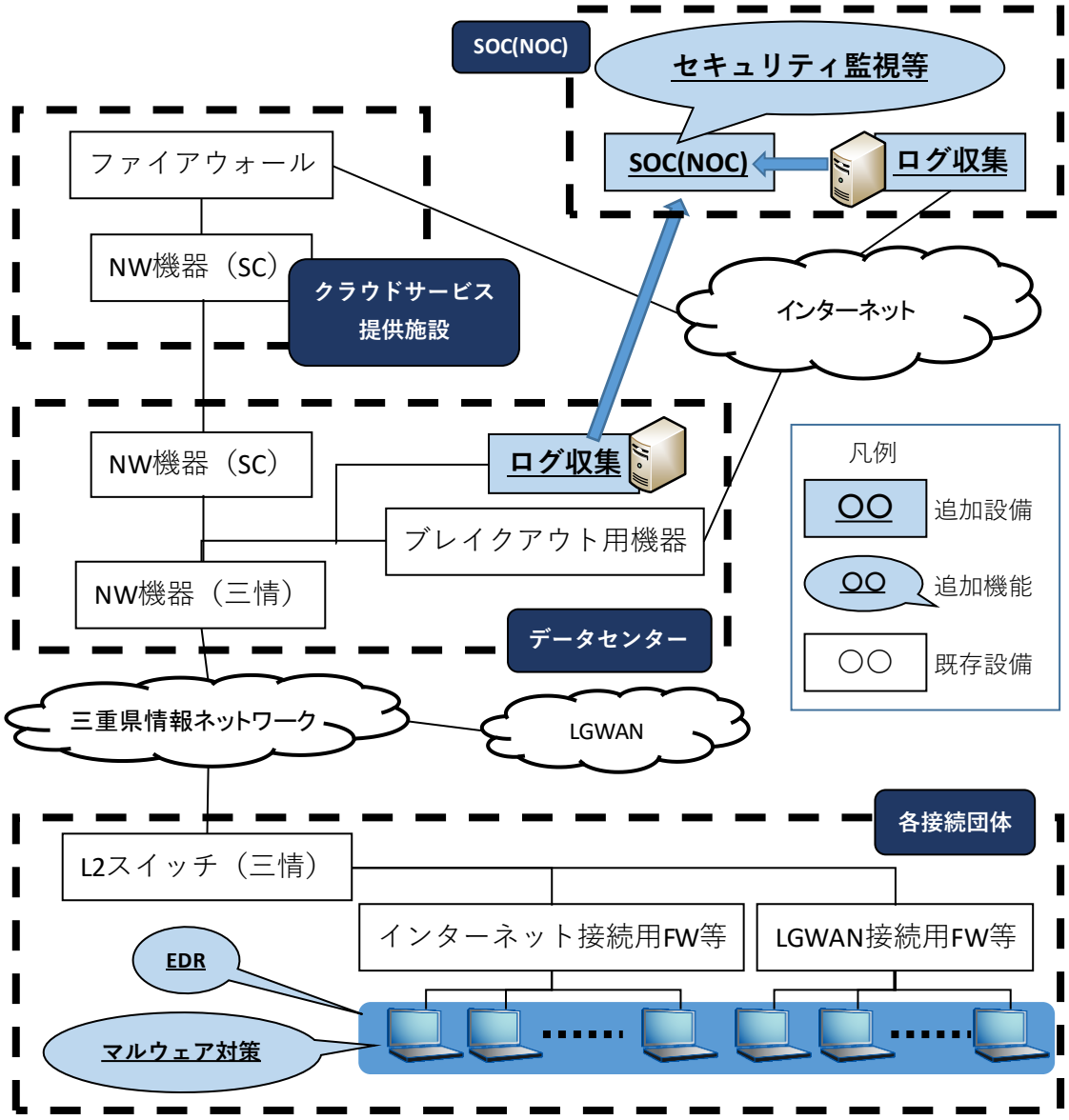

図　追加セキュリティ対策の構成例

機器・機能	内容
全体構成	・「追加セキュリティ対策」の必須機能として、「EDR」「マルウェア対策」を提供すること。また、これらの機能を実現するために必要となる「ログ収集」「SOC(NOC)」等の設備についても必要に応じて準備すること。 ・【提案】追加セキュリティ対策の全体構成について提案を行うこと。また、必須機能の詳細の他、任意機能として提供可能な各種機能についても提案を行うこと。 **【提案要素１ 追加セキュリティ対策の全体構成】**

表　追加セキュリティ対策における全体構成

機器・機能	内容
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、セキュリティ等にかかる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。 ・【提案】EDR の詳細機能について、提案を行うこと。 **【提案要素 2 追加セキュリティ対策の機能詳細】** ➢ ログの収集・分析・・・エージェントソフトウェアを導入したエンドポイントから常時、又は、必要な時にログを収集し、分析する。通常、ログを収集するための「ログ収集」設備が必要になる。 ➢ 被害の検知・・・収集したログを横断的に分析することで、エクスプロイト攻撃やファイルレス攻撃、攻撃時における特徴的なふるまい等による検知の他、感染の痕跡（IOC　Indicator Of Compromise）による検知など、従来のマルウェア対策ソフトでは対応できなかった攻撃を検知する。 ➢ 不審な通信や動作の遮断・・・C&C サーバ（Command and Control Server）との通信遮断や特定プロセスの停止等を行う。また、被害があったエンドポイントに対して、被害の拡大を防ぎつつ、迅速な対応を行うため、セキュリティインシデント対応で利用する通信（例えば、調査を行うためのリモート接続等）以外の通信を全て遮断する（論理抜線）。ファイルの削除やレジストリの復旧なども行う。なお、「不審な通信や動作の遮断」については、マルウェア対策による対応も可とする。 ➢ 侵入経路や被害範囲の調査・・・収集・分析したログ等の情報からマルウェア等の脅威がどの端末から感染し広がったのか、どれだけの端末に広がっているか、どのような被害（どのファイルがアップロードされたのか、どの管理者権限が奪取されたのかなど）があったのか、などを調査可能な状態に可視化する。
マルウェア対策	・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。 ・具体的には、パターンファイルやシグネチャ等のパターンマッチングによる検知、ふるまい検知やサンドボックス等の機械学習による検知、マルウェアの遮断（通信遮断、ファイル削除等）等の機能を提供できること。 ・【提案】マルウェア対策の詳細機能について、提案を行うこと。 **【提案要素 2 追加セキュリティ対策の機能詳細】**

表　追加セキュリティ対策における必須機能

設備	内容
ログ収集	・各エンドポイント（業務端末）のログを必要に応じて収集・保管できること。 ・データセンター内、又は、SOC(NOC)等のクラウドサービス上に設置すること。
SOC（NOC）	・SOC の機能として、収集したログの常時監視、又は、全エンドポイントに対するログ分析等を通じて、セキュリティインシデント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について支援が実施できること。 ・【提案】SOC(NOC)の詳細機能について、提案を行うこと。 **【提案要素 3 SOC（NOC）が提供するサービス内容】**

表　追加セキュリティ対策の必須機能を実現するために必要になる設備

- 【提案】追加セキュリティ対策における任意機能として、セキュリティインシデントが発生した場合の初期段階で検知することで被害を最小限に抑えるための「検知機能の強化」と、セキュリティインシデント自体を未然に防ぐための「セキュリティインシデントの未然防止策」について、提案を行うこと。なお、必須機能により、十分な対応が可能な場合は、その内容を記載すること。

  【提案要素 2 追加セキュリティ対策の機能詳細】

- 【想定】「検知機能の強化」として SIEM（Security Information and Event Management）やセキュリティインテリジェンスを想定しており、「セキュリティインシデントの未然防止策」として IT ハイジーン（IT Hygiene）を想定している。詳細は以下のとおり。

機器・機能	内容
SIEM	・SIEM（Security Information and Event Management）は、通常、さまざまな機器（ファイアウォール等）やソフトウェアのログを収集し、一元的に分析することで、セキュリティインシデントの検知を行うものであるが、EDR にて収集したログについても一元的に分析することで、検知機能が強化されると想定している。 ・なお、次期セキュリティクラウドにおいて、SIEM を導入予定のため、本委託業務における任意機能として求める SIEM は、さまざまな機器やソフトウェアのログに加えてEDRのログの分析を行うことで初めて検知機能が強化されることになると考えているため、注意すること。
セキュリティインテリジェンス	・セキュリティインテリジェンスは、サイバー攻撃やマルウェア等のさまざまな脅威に関する情報を収集し、提供を行うことを指すが、収集した情報を SIEM や EDR 等と連携させることで、侵入等の痕跡をいち早く検知できるようになるとともに、誤検知を少なくすることにつながるため、検知機能が強化されると想定している。

IT ハイジーン	・IT ハイジーンは、エンドポイントにおける「衛生管理」を意味し、各エンドポイントにおける、セキュリティパッチの適用状況や、マルウェア対策ソフトウェアにおけるパターンファイル等の更新状況を一元管理するとともに、対応が不十分なエンドポイントを把握するための機能や、それらの端末に対して、適正な状態にするための機能（アプリケーションの一斉配布、強制配布、未対応の端末に対する機能制限など）が提供されることで、セキュリティインシデントの未然防止につながると想定している。 ・IT ハイジーンは、マルウェア対策や EDR のオプション機能として提供される場合もあれば、全く別のソフトウェアとして提供される場合もあると想定している。

表　追加セキュリティ対策における任意機能の想定

キ　実績及び認証取得等

・ 【提案】本委託業務の受託事業者は、以下の各項目を満たすことが望ましい。そのため、以下の各項目を参考とし、実績や認証取得等について提案を行うこと。

【提案要素 6 実績及び認証取得等】

要件	詳細
運用実績	・受託事業者は本県または他都道府県を含め、EDR 機能の構築・運用実績があることが望ましい。
認証取得	・以下のいずれかの認証を受けていることが望ましい。 ➢ 経済産業省の情報セキュリティサービス審査登録制度の情報セキュリティサービス基準を満たす事業者であること。 ➢ 一般社団法人情報マネジメントシステム認定センターが運用する情報セキュリティマネジメントシステム適合性評価制度（ISMS）の認証を取得していること。 ➢ ISO/IEC27001 又は JIS Q 27001 に基づく認証（事業部単位で認証を受けている場合は、当該事業部が本委託業務の実施体制に参画できること。）のいずれか、またはそれらと同等であると証明可能な情報セキュリティに関する規格を、本委託業務の実施組織・部門が認証取得していること。また、ISO/IEC27017 に基づく ISMS クラウドセキュリティ認証についても取得していることが望ましい。 ➢ プライバシーマーク制度の認定事業者又はこれと同等以上の ISO Guide72:2001 に従った第三者適合性評価制度の認証取得事業者であること。 ➢ 政府情報システムのためのセキュリティ評価精度（ISMAP）による、ISMAP クラウドサービスリストに掲載されているサービスを提供できること。

SOC（NOC）	・受託事業者が提供する NOC、及び、SOC について、EDR 機能の運用・保守実績を有することが望ましい。 ・経済産業省の情報セキュリティサービス基準適合認定（セキュリティ監視・運用サービス）に登録されていることが望ましい。 ・SOC におけるセキュリティ監視等業務について、以下の資格を有する者が従事していることが望ましい。 ➢ (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 年以上持つことが望ましい。

4　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 3 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 4 月から令和 5 年 3 月 31 日までとする。 ・移行期間内に、接続団体からの移行調査結果に基づき、必要な移行作業等の支援を行うこと。
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。

5　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）、受託事業者が利用するデータセンター、SOC（NOC）とする。

SOC（NOC）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、「12　業務詳細（8）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
本庁舎	・三重県の本庁舎のこと。
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。
受託事業者が利用するデータセンター	・追加セキュリティ対策を提供するために受託事業者が契約するデータセンターのこと。
SOC（Security Operation Center）	・追加セキュリティ対策による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。
NOC（Network Operation Center）	・追加セキュリティ対策を提供するために必要となる、運用・保守要員等が勤務する施設のこと。

表　履行場所の詳細

６　納品物件

（１）ハードウェア及びソフトウェア

本委託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し、納入すること。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。

（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。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、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	ライセンス数	期間
エージェントソフトウェア	3,000 ライセンス	令和４年４月１日から 60 か月分

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。

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。（例えば、令和９年３月１日であっても、残存期間で利用可能なライセンスを追加購入可能なこと。）

三重県の追加購入後、三重県及び他の接続団体が、さらなる追加調達を行う場合には、同価格、又は、同価格以下にて購入が可能であること。また、ライセンスの追加調達に伴い、SOC(NOC)における利用費用の増大が見込まれるが、「３事業概要（２）業務範囲 ウ 利用者数、端末数」に記載の端末数をあらかじめ見込み、SOC(NOC)にかかる追加費用が発生しないよう、あらかじめ、本委託業務にかかる費用に見込んでおくこと。

【提案】エージェントソフトウェアにおける追加購入時の単価として、令和 4 年度に三重県が、9,000 ライセンスを追加購入（最大 60 か月分）する際に提供可能な価格を提案すること。

【提案】αモデルを採用している各接続団体においては、インターネット閲覧用に、VDI、SBC、画面転送等によるさまざまな方式のインターネット仮想環境を構築しているため、これらの方式を踏まえて、必要ライセンス数の考え方について提案を行うこと。

【提案】エージェントソフトウェアの追加購入について、最低購入ライセンス数や必要ライセンス数の考え方（ユーザ単位、デバイス単位）、年単位以外（〇〇か月分）の購入可否、支払い方法（先払い、部分払い）について、条件や制限等がある場合は、併せて明記すること。（記載のないものについては、契約締結後、本県との協議のうえ、決定することを想定している。）

【想定】必要ライセンス数の最大数として、例えば、インターネット仮想環境を VDI 形式で利用している場合、仮想端末が生成された総数分のライセンスが必要になると、大量のライセンスが必要になるため、各接続団体における総ユーザ数や、物理端末数に加えてインターネット仮想環境にかかる同時接続数、等を基準にするなど、過剰なライセンス数が必要にならない考え方を想定している。

【想定】エージェントソフトウェアの追加調達は、本委託業務の受託事業者からの随意契約を想定している。

【提案要素 5 必要ライセンス数とライセンス価格】

（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「11　調達全般に関する共通要件（4）ドキュメント」を参照すること。

７　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 50.0%
- 令和４年度 10.0%
- 令和５年度 10.0%
- 令和６年度 10.0%
- 令和７年度 10.0%
- 令和８年度 10.0%

（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、契約額の各年度における内訳資料（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、ライセンス費用（ライセンス単価）とその他の構築費、各団体に対する導入経費について、明確に分離した内訳資料を作成すること。

８　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。

９　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。

10　注意事項

本委託業務において、契約書、仕様書の他、受託事業者から提案された内容について、受託事業者が責任を持って実現すること。

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。

11　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（主任技術者）としてプロジェクトに参加させ、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、原則として、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。
- 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）他の受託事業者との調整

ア　接続団体関連事業者等

- 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。
- 接続団体関連事業者等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

- 次期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、当該機器を所管する受託事業者と設定変更等にかかる協議等を実施すること。
- 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、別途費用が発生する場合があると想定しているため、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、追加セキュリティ対策にかかる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、追加セキュリティ対策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、本委託業務の範囲外とする。

（4）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、構築・移行等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 4 年 3 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すること。

種別/提出時期	詳細
サービス定義書（令和４年３月末）	・追加セキュリティ対策にて提供される各機能の詳細について定義したもの。 ・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４年３月末）	・サービス定義書で定義した追加セキュリティ対策の各機能を提供するための構築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４年３月末)	・各接続団体が追加セキュリティ対策を利用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。 ・各接続団体に対して、利用開始時期をヒアリングし、その結果についても記載すること。
運用・保守設計書（令和４年３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。 ・本県と受託事業者との間で締結するSLA（Service Level Agreement）、又は、SLO（Service Level objective）についても記載すること。 ・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４年３月末）	・運用期間におけるセキュリティ等に関する業務内容について記載したもの。 ・マルウェア対策、EDR等による検知、SOCによる検知に対する一次対応の他、各接続団体に対するインシデント対応支援等の二次対応等についても記載すること。
接続団体向け説明資料（令和４年３月末）	・接続団体向け説明会用の資料のこと。内容として、追加セキュリティ対策の機能概要、利用開始までの流れ、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、必要に応じ、毎年度更新を行うこと。
各種設定一覧（令和４年３月末）	・追加セキュリティ対策の構築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４年３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、必要に応じ、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

12　業務詳細

（1）設計業務全体にかかる要件

ア　基本的な考え方

- 追加セキュリティ対策は、全接続団体が利用できることを目指して、次期セキュリティクラウドの一機能として導入するものであり、各団体がαモデル、β/β’モデル等、どのような構成であったとしても、利便性の向上やDXの推進等につながることから、可能な限り多くの団体で導入すべきと考えている。しかし、実際に各接続団体に追加セキュリティ対策を導入するためには、各エンドポイントに対して、既存のウィルス対策ソフトの入れ替えや本委託業務で調達するエージェントソフトウェアの導入の他、導入時のチューニング作業等が発生するため、導入を積極的に進めることができない団体も少なからず存在すると考えている。そのため、可能な限り、多くの団体で追加セキュリティ対策を導入することができるよう留意して、設計を行うこと。
- 一方で、追加セキュリティ対策の導入は、あくまで各接続団体の方針に従う必要があることから、導入しない方針を決定した団体に対しては、それ以降の追加セキュリティ対策における運用・保守作業等は発生しない形になるため、注意すること。
- 【想定】追加セキュリティ対策の一つであるEDRは、β/β’モデルへ移行するための必須要件であるため、少なくとも、β/β’モデルの団体、又は、β/β’モデルへの移行を目指している団体（計13団体）においては、導入を行うことになると想定している。（逆に、導入を見送る団体は5団体と想定している。）

イ　基本方針

- 追加セキュリティ対策の安定した稼動、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、原則として、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、作業の依頼等を行う場合は、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　各接続団体に対する追加セキュリティ対策の利用意向調査

- 各接続団体に対する利用意向調査を行うこと。なお、調査に先立って、追加セキュリティ対策で利用可能となる各種機能の紹介に加え、各接続団体側において利用開始までに発生する導入作業の内容等についても併せて説明を行うこと。
- 各接続団体に対する調査依頼は本県から実施するが、調査を行う内容や回答様式の作成、及び、回答のとりまとめについては、受託事業者が実施すること。また、意向調査の結果については、とりまとめ次第、本県に対して説明を行うこと。
- 意向調査の結果に基づき、必要に応じて詳細ヒアリングを実施し、追加セキュリティ対策の利用範囲や端末数、導入時期（利用を開始したい時期）、ライセンスの追加調達の有無、既存のマルウェア対策の状況、今後の機器更新の変更予定、必要な連絡体制等の詳細について、確認を行うこと。
- 【想定】現時点でβ/β’モデル、又は、EDR の導入を検討している団体は本県を含めて 13 団体となっているため、少なくとも 13 団体に対して詳細ヒアリングを実施することを想定している。
- 【想定】広域連合（3 団体）に対する調査は、主管する市町と一括で実施できると想定している。

イ　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、及び、次期セキュリティクラウド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、詳細を確認すること。
- 構築時において想定される、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）全体構成と機能要件

ア　全体構成

- 追加セキュリティ対策における全体構成については、本県に対して詳細な説明を行い、承認を得たうえで設計を行うこと。
- 追加セキュリティ対策における全体構成の設計においては、「３事業概要（２）業務範囲 カ 追加セキュリティ対策のサービス構成例」を参考とすること。
- 【提案】追加セキュリティ対策の全体構成について、提案を行うこと。

【提案要素１ 追加セキュリティ対策の全体構成】

イ　機能要件

- 追加セキュリティ対策における各機能の詳細な機能要件について、必須機能である「EDR」「マルウェア対策」の他、本委託業務で提供可能な任意機能について、本県に対して詳細な説明を行い、本県の承認を得たうえで設計を行うこと。
- 追加セキュリティ対策における必須機能の詳細な機能要件については、「別紙　追加セキュリティ対策の必須機能にかかる詳細な機能要件」を参考とすること。
- 【提案】追加セキュリティ対策における必須機能の詳細、及び、本委託業務で提供可能な任意機能の詳細について、提案を行うこと。
- 【提案】「別紙　追加セキュリティ対策の必須機能にかかる詳細な機能要件」に記載された項目について、実現できない機能が存在する場合は、その詳細を明記すること。ただし、当該機能を実現させる必要がない理由（その機能がそもそも不要な理由）がある場合は、その理由についても記載すること。（詳細、かつ、具体的な理由等が確認できない場合、減点の対象となるため、注意すること。）
- 【想定】代替案による機能実現や、複数の製品を組み合わせた機能実現も可とするため、全ての項目が実現可能と想定している。

【提案要素 2 追加セキュリティ対策の機能詳細】

- SOC（NOC）が提供する各種業務の詳細や、提供される各種業務に対する SLA（サービスレベル協定 Service Level Agreement）、又は、SLO（サービスレベル目標 Service Level objective）について、別紙「三重県自治体情報セキュリティクラウド（追加セキュリティ対策）構築及び運用・保守業務にかかるサービスレベル（案）」を参考として設計に盛り込むこと。また、毎月、本 SLA、又は、SLO にかかる実績を管理し、報告を行うこと。なお、SLA として減額ポイントを盛り込んだ場合で、かつ、減額ポイントの要件を満たした場合（SLA を満たせなかった場合）は、当該減額ポイントに基づき、運用保守費の減額を実施することになるため、注意すること。
- 【提案】SOC（NOC）が提供する業務内容の詳細とその業務に対する SLA、又は、SLO について、提案を行うこと。なお、SLO による提案を行う場合は、可能な限り、過去の実績値についても記載すること。
- 【想定】SLA と SLO の違いとして、SLA は目標を達成できない場合に減額が発生するが、SLO における目標はあくまで努力目標のため目標を達成できない場合でも減額は発生しない、と想定している。逆に、SLO は SLA と比較して、（達成できなくても減額等が発生しないため）目標が高くなると想定している。

【提案要素 3 SOC（NOC）が提供するサービス内容】

- 追加セキュリティ対策における各機能が、次期セキュリティクラウドで提供される機能と重複する場合は、その差異や、重複して構築する意図（機能の棲み分け等）の他、運用方法についても設計に盛り込むこと。

- 【想定】次期セキュリティクラウドと追加セキュリティ対策において、SOC(NOC)機能は、必要となる業務が大きく異なるため、重複して調達を行う形になると想定している。
- 追加セキュリティ対策の各機能について、障害時等における業務継続性や冗長化構成等についても設計に盛り込むこと。
- 必須機能、及び、任意機能により利用可能となる各種機能について、「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）構築業務等の設計にかかる要件

ア　構築設計

- 追加セキュリティ対策の構築業務における設計として、次期セキュリティクラウドや各接続団体における既存ネットワーク、既存システム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築設計を行うこと。
- 設計には、「（3）全体構成と機能要件」にて策定した「サービス定義書」に定義した全ての機能を提供するために必要となる構築業務について、漏れなく含めること。
- 追加セキュリティ対策の構築後、提供される各機能に対して、稼働試験が実施できるよう、試験内容についても設計を行うこと。
- 追加セキュリティ対策における各機能において、冗長化された部分がある場合（例えば、Active/Standby 構成の機器や通信経路の切り替えなど）、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。
- 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方法や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、構築された追加セキュリティ対策が、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。

イ　経路設計

- 追加セキュリティ対策は、次期セキュリティクラウドの一機能として構築することとしていることから、追加セキュリティ対策について、次期セキュリティクラウドを経由して各接続団体から利用できるようにするために必要となる経路設計を行うこと。
- 経路設計にあたっては、次期セキュリティクラウド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。

ウ　データセンターの利用にかかる詳細設計

- 追加セキュリティ対策を構築するうえで、ハードウェアを設置する必要がある場合は、三重県が別途調達しているデータセンター、又は、受託事業者が利用するデータセンターへの設置を行うことになるため、注意すること。なお、データセンターにかかる要件については、「12　業務詳細（8）データセンターにかかる要件」を参照すること。
- 三重県が別途調達しているデータセンター、又は、受託事業者が利用するデータセンターにハードウェアを設置する場合は、ラックの利用料やラック配線にかかる費用等、全ての費用については、本委託業務の範囲内で受託事業者が準備すること。
- 三重県が別途調達しているデータセンターにハードウェアを設置する場合は、次期セキュリティクラウドとの接続用に、次期セキュリティクラウド用ネットワーク機器の接続スイッチに 10/100/1000BASE-T のポートを用意するため、受託事業者がハードウェアを設置したラックから、当該ラックに対してラック間配線を行うこと。なお、ラック間配線については、データセンターの施設管理者に依頼する必要があり、また、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。
- 三重県が別途調達しているデータセンターにハードウェアを設置する場合は、ラック構成図を作成すること。
- 受託事業者が利用するデータセンターにハードウェアを設置する場合は、受託事業者が利用するデータセンターにて必要になる通信回線も、本委託業務の範囲内で受託事業者が準備すること。
- 各エンドポイントからログ収集設備に対して、ログの送信等が実施されると想定しているが、ログ送信全体にかかる通信として、大きな負荷をかける場合は、追加セキュリティ対策用にローカルブレイクアウト回線を用意すること。
- 【想定】通信容量が、おおよそ 10Mbps 未満の場合は、次期セキュリティクラウドの通信回線を利用することも可とする。

（5）導入業務等の設計にかかる要件

ア　エージェントソフトウェアの導入時における要件

- 各接続団体において、追加セキュリティ対策の導入を行うため、各エンドポイントに対して、既存のマルウェア対策にかかるエージェントソフトウェアから EDR/マルウェア対策にかかるエージェントソフトウェアへの入れ替え作業を行う必要があると想定しているが、この入れ替え作業（導入作業）にかかる導入設計を行うこと。
- 導入作業は、原則として、各接続団体が主体的に実施する形を想定しているが、各接続団体におけるセキュリティ対策の実施状況に配慮し、各接続団体におけるセキュリティ対策等への影響を最小限に抑え、かつ、安全で確実に実施可能な導入作業が実施できるよう留意すること。

- 導入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に備えて、あらかじめ、障害原因の調査方法などについて、準備しておくこと。
- 導入作業実施時には、各接続団体における業務端末や既存システムにかかるサーバ等において、設定変更等の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、可能な限り、負担が軽減されるような設計を行うこと。
- 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。
- 導入作業完了後、導入作業が完了したことを確認するための導入試験についても設計を行うこと。
- 策定した導入設計については、各接続団体に対して説明し、承認を得ること。
- 【提案】作成した導入設計をもとに、各接続団体において導入作業を実施することになるが、できるだけ接続団体の負荷が低減されるような導入設計について提案すること。

【提案要素４　移行作業にかかる提案】

- 【想定】エージェントソフトウェアにかかる入れ替え作業は、各接続団体がこれまで運用してきた配布方法（ログインバッチ、手作業、配信管理ソフトによる配信など）により実施する形を想定している。そのため、各接続団体の配布方法に合わせて、インストール用エージェントソフトウェアの用意や、導入が正常に確認したかを確認するための確認作業などが発生すると想定している。

イ　安定稼働するまでの要件

- エージェントソフトウェアの導入後、安定稼働するまでの間におけるチューニング作業について、チューニング設計を行うこと。
- チューニング作業として、EDR/マルウェア対策にかかるエージェントソフトウェアの導入後、しばらくの間に発生すると想定される、過検知や誤検知に対して、これらを低減させるために必要となる作業について、設計に含めること。
- 策定したチューニング設計については、各接続団体に対して説明し、承認を得ること。
- 【提案】作成したチューニング設計をもとに、各接続団体においてチューニング作業を実施することになるが、できるだけ接続団体の負荷が低減されるようなチューニング設計について提案すること。

【提案要素４　移行作業にかかる提案】

（６）セキュリティインシデント対応支援業務の設計にかかる要件

各接続団体におけるセキュリティインシデント発生時の対応支援業務等を行うために必要となるセキュリティインシデント対応支援設計を行うこと。

セキュリティインシデント対応支援設計にあたっては、以下の要件を満たす設計とすること。

ア　基本方針

- 追加セキュリティ対策にかかるセキュリティインシデント対応支援業務を行ううえで必要となる、セキュリティインシデント対応支援要員等が勤務する施設として、NOC を設置すること。なお、後述する SOC と同一施設とすることも可とする。
- 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いること。
- 問い合わせやセキュリティインシデント発生時の支援要請に対応するため 24 時間 365 日対応可能な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 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。
- 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。

イ　総合窓口

- 接続団体における担当職員からの問合せ、セキュリティインシデント発生時の受付及び支援等を実施す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。

ウ　管理画面（EDR）

- EDR について、ライセンスやセキュリティインシデント発生状況や支援対応状況等について、情報共有が可能な管理画面を用意すること。
- セキュリティインシデント支援対応の進捗状況・ステータス、および対応履歴が確認できること。
- 管理画面への接続は、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。
- 【想定】セキュリティインシデント発生時において、管理画面にセキュリティインシデントの詳細や進捗状況を掲載し、情報共有を行うことで、迅速な対応が可能になると想定している。

エ　運用・保守業務

- 機器障害、外部からの攻撃等によるサービス停止など、追加セキュリティ対策の各機能が提供できなくなるなどの事故・障害が発生した場合は、運用・保守業務として、24 時間 365 日の対応を行い、迅速に復旧させること。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。

- 発生した事故・障害に対して、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。
- 事故・障害等に対する原因の一次切り分けの結果、本委託業務の範囲外の要因によることが判明した場合は、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。
- 各接続団体における担当職員からの依頼に基づき、必要に応じて、追加セキュリティ対策における、対応フローの変更等の対応を行うこと。なお、疑義のない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。
- 追加セキュリティ対策自体に大きな影響を与えるような変更については、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。

オ　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。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。
- 報告会では、セキュリティインシデント対応支援業務の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。
- 年に１回以上、追加セキュリティ対策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。

カ　セキュリティ監視等業務にかかる対応業務

- 後述する「（７）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、セキュリティインシデント対応支援業務の一環として、必要な対応が実施できること。
- 【提案】以下の想定を参考とし、追加セキュリティ対策で実施するセキュリティインシデント対応支援業務の内容について、提案を行うこと。

【提案要素３SOC（NOC）が提供するサービス内容】

- 【想定】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。

- 【想定】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・支援を行う形などを想定している。このとき、NOC 要員は、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する。
- 【想定】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、対応フロー等の整理を行うことを想定している。
- 【想定】被害状況の確認、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等を実施することを想定している。
- 【想定】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、セキュリティ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 と情報共有を行うなどの対応を想定している。

キ　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、追加セキュリティ対策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。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。

ク　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
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、セキュリティインシデント発生を想定した対応模擬訓練を実施できること。
- 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、セキュリティインシデント対応支援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。

（7）セキュリティ監視等業務の設計にかかる要件

追加セキュリティ対策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

- 追加セキュリティ対策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 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、又は、一つのチームの影響によりサービスの全停止やサービスレベルの低下を招かない仕組み（濃厚接触者とならない仕組み）が構築されていること。
- 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。
- セキュリティインシデントが検知された場合、そ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。
- 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。

イ　セキュリティ監視、調査、及び、解析

- セキュリティ監視、調査、及び、解析業務として、EDR により各エンドポイントから収集したログの常時監視、又は、全エンドポイントに対するログ分析等を通じて、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できること。また、必要に応じて、さらなる調査、解析ができること。
- セキュリティ監視として、緊急度の高いアラートのみではなく、出力される全てのログを監視対象とすること。
- 【想定】SOC においてログの常時管理を行う場合は、ログ分析機能(SIEM)による 24 時間 365 日の相関分析を行うと想定している。
- 【想定】SOC において、全エンドポイントに対するログ分析を行う場合は、常時監視と比較して、被害が発生してからのタイムラグが発生すると想定している。
- 追加セキュリティ対策における検知ポリシーは、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。
- セキュリティ監視等業務における危険度の分析基準は、検知シグネチャに定義された危険度ではなく、不正な動作に対する調査、解析の結果から監視等の対象となるエンドポイントに対する影響度や不正アクセス等の成否によって 4 段階以上で定義し、危険度に応じた対応ができること。

- 危険度の分析において、重大なセキュリティインシデント（攻撃が成功した可能性が高いまたは攻撃が成功）を判断する場合は、不正な動作に対する調査、解析結果とともに、当該エンドポイントに影響を与えない範囲において対象となる機器における脆弱性の有無を確認し最終的な判断を行えるようにすること。
- 【想定】SOC において、全エンドポイントに対するログ分析等を実施する場合は、セキュリティインシデントが発生した痕跡を検知することから対応が開始されると想定しているが、重大な被害が出ているかを基準として、危険度の判定を行う形を想定している。
- 危険度の判定として、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。

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、情報漏洩、データ破壊（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

- 重大なセキュリティインシデントと判断してから 60 分以内に、受託事業者から当該接続団体の担当者に電話やメール等の方法により緊急連絡を実施し、担当者に対してセキュリティインシデントの内容等について、確実に伝達すること。
- 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)への緊急通信遮断等を実施するため、次期セキュリティクラウド側の運用担当者に対して連絡を行うこと。
- エンドポイントにおける、不正な動作やその痕跡を検知した場合、SOC からの操作により、当該エンドポイントに対する調査・解析等に必要な通信以外の通信を遮断（論理抜線）できること。

・ 不正な動作に対する調査、解析を実施し、その結果に基づいて、以下のケースに応じた対応等を実施できること。

不正な動作の種別	対応
不審な動作またはマルウェアへの感染・活動等及びその兆候や痕跡を検知した場合	・速やかに不審な動作等か否かを解析すること。 ・不審な動作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、該当エンドポイントに対する対処方法、及び、他のエンドポイントに対する対応方法等についても報告すること。

表　不正な通信を検知した際の対応方針

・ 【提案】以下の想定を参考とし、追加セキュリティ対策で実施するセキュリティ監視、調査、及び、解析業務の内容について、提案を行うこと。

【提案要素 3 SOC（NOC）が提供するサービス内容】

・ 【想定】セキュリティ監視、調査、解析は、EDR における「被害の検知」に相当し、EDR を活用した SOC(NOC)の対応が、「不審な通信や動作の遮断」「侵入経路や被害範囲の調査」に相当すると想定している。
・ 【想定】セキュリティ監視による検知以外に、マルウェア対策のパターンマッチング等により検知を行った場合も、SOC において、EDR による検知と同様の対応を行うことを想定している。
・ 【想定】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。
・ 【想定】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・支援を行う形などを想定している。このとき、NOC 要員は、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する。
・ 【想定】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、対応フロー等の整理を行うことを想定している。
・ 【想定】被害状況の確認、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等を実施することを想定している。
・ 【想定】NOC 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、セキュリティ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 NOC と情報共有を行うなどの対応を想定している。

・ 【想定】セキュリティインテリジェンスとして、脆弱性配信サービスや外部データベースの活用、独自情報等の活用、等により、網羅的な脆弱性情報を収集したうえで、セキュリティ監視業務で活用することを想定している。

ウ　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。報告内容として、全体傾向（セキュリティインシデントの発生件数や推移、危険度別件数等）と詳細情報（発生したセキュリティインシデントに対する詳細情報）を含めること。また、発生したセキュリティインシデントに対して、事前対策が可能な場合は、その対策案についても必要に応じて報告内容に含めること。

エ　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。

（8）データセンターにかかる要件

受託事業者が利用するデータセンター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システム	・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。
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

（９）追加セキュリティ対策の構築にかかる要件

追加セキュリティ対策の構築作業として、「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。

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。

次期セキュリティクラウドとの接続時には、各受託事業者と綿密な連絡を取りながら、セキュリティクラウド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。

構築作業に伴い、重大な事故・障害が発生した場合は、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、事故・障害発生状況、影響範囲、根本解決策等について本県に報告を行うこと。

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。

（10）接続団体の導入業務にかかる要件

追加セキュリティ対策の導入を決定した接続団体が、導入設計に沿って導入作業を行うが、各接続団体において、エージェントソフトウェアの導入作業と、導入後のチューニング作業がスムーズに実施できるよう、支援を行うこと。

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。

各種試験の結果については、導入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。

導入作業に伴い、重大な事故・障害が発生した場合は、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、事故・障害発生状況、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。

予定していた全ての導入作業が完了後、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。

（11）セキュリティインシデント発生時における対応支援業務要件

追加セキュリティ対策の安定的な運用を行うため、セキュリティインシデント発生時における対応支援業務を行うこと。

セキュリティインシデント発生時における対応支援業務は、先に作成した「セキュリティインシデント対応支援設計」に従い、確実に実施すること。

セキュリティインシデント発生時における対応支援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、「セキュリティインシデント対応支援設計」の内容だけでなく、各接続団体担当者への挨拶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。

（12）セキュリティ監視等業務にかかる要件

追加セキュリティ対策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。