三重県情報ネットワーク

設計・構築・運用保守業務

詳細仕様書

目次

1. はじめに

1.1. 目的

三重県情報ネットワークについて、現行ネットワークの機器更新に留まらず、信頼性・可用性、効率性・利便性を向上させるため、現行ネットワーク機器等の機器更新及び機能追加を実施する。また、機器更新に伴って必要となる、既存の関連契約との調整のほか、設計、機器調達、構築、移行、運用、保守業務を行うことを本業務の目的とする。

1.2. 本仕様書の位置づけ

本仕様書は、令和 9 年 4 月から運用開始予定の次期三重県情報ネットワーク（以下、「次期ネットワーク」という。）に係るネットワークシステム設計・構築・運用保守の仕様を記載している。なお、次期ネットワーク構築業務の全体概要については、「三重県情報ネットワーク設計・構築・運用保守業務共通仕様書」（以下、「共通仕様書」という。）を参照すること。

1.3. 仕様書の記載要件

本仕様書では、各項目を「必須」、「提案」に分類した形で仕様書上に記載している。必須及び提案に係る詳細は以下「表 1-1 必須・提案」のとおり。なお、本文中には「必須」は記載せず（本仕様書に記載している要求事項は必須）、「提案」のみ記載しているため、注意すること。

表 1-1 必須・提案

分類	詳細
必須	本県が求める要件であり、記載内容のとおり必ず実現すること。
提案	本県における各種課題に対して、その解決方法を受託事業者に求めるもの。提案にあたっては、本県が想定している実現方法とは異なる提案も可とする。 また、本県が想定している要件より優れた要件の提案も可とする。ただし、提案した内容については、本業務の範囲内として実現させること（提案内容を実現するために追加費用が発生する場合は、予め契約金額に含めた形とすること）。

2. 事業概要

2.1. 契約名

「三重県情報ネットワーク設計・構築・運用保守業務委託」

2.2. 業務概要

2.2.1. 設計・構築業務

2.2.1.1 全体管理

- 次期ネットワークの構築業務を実施するにあたり、設計・構築・移行・運用保守の全フェーズにわたって、全体スケジュールの管理、調整を主体となって行うこと。
- 次期ネットワークの構築・変更・移行等により、本県職員の業務に支障をきたさないよう全体スケジュールの調整を行うこと。
- 週に1回程度、関係者を集めた全体定例会を開催し、次期ネットワークの構築業務全体における連絡調整や各種報告等を行うこと。

2.2.1.2 各受託事業者との調整

- 関連するシステム等の各受託事業者（現行ネットワーク受託事業者、IDC、各回線受託事業者、防災行政無線工事受注事業者等）との調整を行い、役割分担の整理や作業依頼等を行うこと。
- 各受託事業者は締結済みの契約における業務の範囲内でのみ対応が可能なため、従来の業務範囲を超えて作業依頼等を行う場合は、本県の承認を得たうえで、本県と受託事業者の締結済みの契約の範囲内として依頼を行うこと。

2.2.1.3 次期ネットワークの設計

- 現行ネットワークの調査や各受託事業者との協議等を実施したうえで、次期ネットワークの全体設計を行うこと。
- 次期ネットワークの設計を行うにあたり、現行ネットワークを調査したうえで、構成変更内容及び要件を踏まえて最適な設計を行うこと。
- ＜提案＞次期ネットワークの安定した稼動、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。

- 次期ネットワークを構築するために更新する必要がある機器・サービス等のうち、本受託事業者が納入・提供を行うものについて、基本設計及び詳細設計を行うこと。
- 次期ネットワークを構築する際に、各受託事業者へ依頼する場合は、作業依頼書等の作成を行い、本県にも提出すること。
- 次期ネットワークを構成する機器・サービスについて、正常な稼働を確認するため、テスト設計を行うこと。さらに、テストを実施するためのテスト計画書や手順書についても作成すること。
- 現行ネットワークから次期ネットワークへの移行を行うための移行設計を行うこと。また、移行を実施するための移行計画書や手順書についても作成すること。
- 次期ネットワークに係る運用・保守設計を行うこと。また、運用保守を実施するための手順書についても作成すること。
- 運用・保守設計を行うにあたり、本業務で調達した機器・サービス等及び既存システム（ユーザ認証システム、マイナンバー利用事務系ネットワーク等）機器等の監視が可能な障害監視システムの設計を行うこと。
- 全ての設計内容については、本県に対してレビューを実施し、本県の承認を得たうえで次の工程に進むこと。

2.2.2. 機器・サービスの調達

- 次期ネットワークを構築するために必要となる機器・サービス等の調達を行うこと。

2.2.3. 機器・サービスの設定・構築

- 各種ネットワーク・サーバ等の導入機器について、各種設計に基づき設定を行うこと。また、クラウドサービス等についても設定作業を行うこと。
- 必要に応じて OS 及びソフトウェアのインストールを行うこと。
- 調達機器については、導入時点での最新のセキュリティパッチ等をインストールすること。
- 機器及びソフトウェア製品等の取得・納入、インストール、設定及びクラウドサービスの設定に要する場所の確保等に発生する費用は、一時的に必要となるものを含め、全て本受託事業者の負担とする。本庁舎及び IDC については本県にて用意するラックの空きを使用することは可能であるが、不足するラック分については、本受託事業者で費用を負担すること。

2.2.4. ネットワークの移行

- 現行ネットワークから次期ネットワークへの移行について、各種設計に基づいて作業を行うこと。
- 移行作業の実施にあたっては、移行設計時に作成した移行計画書や移行手順書に従って実施すること。
- 本番移行作業を実施する前に納入機器の単体テスト及び通信テスト等を実施し、移行時のリスク低減に努めること。なお、テスト内容については本県と協議し、本県の指示に従うこと。
- 本番稼働前に障害監視システムの事前テストを実施すること。
- 次期ネットワークへの移行において、段階的に移行作業を行う場合は、移行作業を行う都度、現行ネットワークにおいて設定変更が発生すると想定されるため、現行ネットワーク受託事業者と事前に調整のうえ、必要に応じて現行ネットワーク受託事業者に作業依頼すること。
- ネットワーク移行が完了し、現行機器を撤去できる状態になった際には、本県に事前に確認のうえ、現行ネットワーク受託事業者に作業依頼すること。
- 移行にあたって必要となる、各受託事業者や各市町、利用者等との連絡、調整、協議等についても主体的に実施すること。

2.2.5. 運用業務

2.2.5.1 運用管理 SE の常駐業務

本庁舎に統括業務を実施するリーダを含めた運用管理 SE を常駐させ、本業務に係る運用業務に従事させること。なお、他システムを運用するうえで必要となる各種作業のうち、本県から指示があったものについては、特段の支障がない限り対応を行うこと。またその際は、各受託事業者と連携すること。

また、運用業務として、障害対応や、定例会及び各種打ち合わせへの参加、各種問い合わせ対応を行うこと。

2.2.5.2 統括業務

リーダは次期ネットワークを円滑に稼働させるため、ヘルプデスク、各受託事業者、本県職員等と連携して業務を実施すること。また、セキュリティリスクに係る調査を定期的に実施し、本県及び関係者等へ注意喚起や技術的助言を行い、影響を最小限に留めるよう努めること。

2.2.5.3 関係者用総合窓口機能（Web ポータルサイト）

専用のポータルサイトを構築し、以下の機能及び情報を提供すること。

- 利用者等からの依頼事項や問い合わせを管理し、本受託事業者へ直接連絡できる機能を提供すること。
- インシデントの概要や注意喚起に関する情報を掲載すること。
- よくある質問と回答（FAQ）を公開可能であること。
- 最新の利用者向けドキュメント、管理者向けドキュメント、構成情報等を共有できること。
- 障害情報、是正措置・予防措置の内容は障害記録として掲載すること。また、常に活用できるようにすること。

2.2.5.4 構成管理

- ハードウェアの物理構成、論理構成等を適切に管理すること。
- ネットワークの物理回線構成（配線等）を適切に管理すること。
- 詳細設計の内容を把握し、次期ネットワークに係る全ての装置・設備を適切に操作・使用可能な体制を整えること。
- 最新の設定情報を随時更新のうえ、管理を実施し、本県職員と共有すること。
- 構成管理に必要なドキュメントは随時更新のうえ、本県職員と共有できるように本調達で構築する全庁ファイルサーバ、ポータルサイト等に保存すること。

2.2.5.5 ドキュメント管理

次期ネットワークで導入する機器等の設定や、運用業務の実施手順等をドキュメント化し、管理すること。

2.2.5.6 電源管理

ヘルプデスクと協力し、本庁舎 7 階サーバ室及び総合庁舎情報機器室内の電源管理、非常用電源の接続機器等の管理、UPS の接続機器等の管理を実施すること。

2.2.5.7 設定変更

- 機器等の各種設定作業を行うこと。また、それに係る検証作業、手順書の作成も行うこと。
- 物理回線構成（配線）の構成変更作業を行うこと。
- システムの運用に必要な設計や設定変更を実施すること。ただし、本県の要求

仕様変更により基本設計が大幅に変更となる場合は別途協議とする。

2.2.5.8 セキュリティパッチ対応

- 本受託事業者が納入した機器及び本受託事業者の保守対象となった機器等について、必要に応じてファームウェア等のバージョンアップ作業を行うこと。また、それに係る検証作業、手順書の作成も行うこと。
- 本受託事業者が納入したハードウェア、ソフトウェアのサポートが終了する場合、本受託事業者の責任において、速やかに代替機器の調整、ソフトウェアのバージョンアップ等を行い、継続してサポートが受けられるように対応を行うこと。

2.2.5.9 引継ぎ業務

- 運用設計を行う段階で、現行ネットワーク受託事業者から、「2.2.5.11 既存システムの運用」に記載のシステムについて、引継ぎを受けること。引継ぎの内容やスケジュールについては本県職員と協議のうえで実施すること。
- 運用中のシステム状況や運用に必要な手順等、現行ネットワーク受託事業者からの情報共有を適宜実施すること。

2.2.5.10 職員等研修

次期ネットワークに係る全体把握のため、本県からの依頼に応じて本県職員等に対する研修を実施すること。

2.2.5.11 既存システムの運用

本受託事業者が納入した機器等以外において、三重県情報ネットワークに関連する以下の既存システムについて、設計時に確認し、各受託事業者と役割を整理のうえで運用を実施すること。詳細は「10.12 既存システムの運用」を参照すること。

- ユーザ認証システム
- 三重県 DX 推進基盤

2.2.5.12 サーバのバックアップ及びリストア

サーババックアップ計画に基づいた定期的なバックアップの実施と障害時対応等によるリストア作業を行うこと。バックアップデータは適切な世代管理を行うこと。

2.2.5.13 停電対応

本庁舎の停電時にネットワーク機器やサーバ等の停止、再起動及び動作確認を行うこと。

2.2.5.14 技術支援

本県の指示により、自治体中間サーバ団体用 VPN 装置の設定支援、三重県行政 WAN・情報ネットワーク内の不具合等の原因解析及び対処方法の検討、無線 LAN 導入拠点のレイアウト変更や電波不達等への対応を実施すること。

2.2.5.15 問い合わせ対応

本県や各受託事業者等からの次期ネットワークに関する各種問い合わせへの対応を行うこと。また、機器ベンダや各受託事業者へ問い合わせや作業依頼等を行うこと。

2.2.5.16 インシデント・問い合わせ管理

本業務で発生した障害や実施した作業、問い合わせ等の内容を発生・受付から復旧・解決まで記録し、管理すること。また、関係者に対応状況や作業依頼等の情報を公開すること。

2.2.6. 情報セキュリティ対策

2.2.6.1 アクセス制御・権限管理

次期ネットワークを利用するアカウントについて、適切なアクセス権限を付与すること。

2.2.6.2 ログの取得・管理

次期ネットワークで導入する機器等のログを収集し、適切に管理すること。

2.2.6.3 ソフトウェアに関する脆弱性対策

次期ネットワークで導入するソフトウェア等の脆弱性情報を定期的に収集し、適切なセキュリティ対策を講じること。

2.2.6.4　不正プログラム対策

庁内への不正プログラムの侵入を防ぐため、次期ネットワークで導入する機器等を用いて不正プログラムの検知及び防御を実施すること。

2.2.6.5　セキュリティインシデントへの対応

セキュリティインシデント発生時に迅速に対応するため、適切な体制や手順を定めること。

2.2.7.　監視業務

2.2.7.1　監視対象システム

監視対象システムは以下とするが、設計時に監視対象を確認のうえ、本県の承認を得ること。なお、次期ネットワーク以外のシステムにおいては、各受託事業者と役割を整理のうえで一部の監視を実施することになるため、詳細は「12.2 障害監視」を参照すること。

- 次期ネットワーク（本調達構築範囲）
- ユーザ認証システム
- マイナンバー利用事務系ネットワーク

2.2.7.2　障害監視

監視業務を実施するため、有人の監視センターを設置し、「2.2.7.1 監視対象システム」で指定されたシステムを 24 時間 365 日監視すること。

2.2.7.3　性能監視

各種リソース情報の収集・分析を行い、適正な性能範囲であるか定期的に監視すること。

2.2.7.4　セキュリティ監視

情報セキュリティ対策を適切に維持するため、セキュリティに関するログやアラート・通知を常時監視すること。

2.2.7.5　障害発生時における切り分け

障害発生時には、一次切り分けを行い、関係者へ連絡を行うこと。

2.2.8.　保守業務

2.2.8.1　保守受付

原則 24 時間 365 日、電話及びインターネットメール、ビジネスチャット等による保守受付に応じること。

2.2.8.2　障害対応

- 障害原因が本調達で導入したハードウェアにある場合は、速やかに代替機器の調整を行い、交換を行うこと。
- 障害原因が本調達で導入したソフトウェアにある場合は、ファームウェアバージョンアップ、セキュリティパッチの適用、アプリケーション設定等の適切な調整を行い、正常状態へと復旧させること。

2.2.8.3　その他

本業務で必要な保守物品・消耗品について、本調達に含めること。

2.2.9.　機器撤去

本業務終了時、本受託事業者が納入したハードウェア等については、本県が指示するものを除き、本受託事業者でデータの完全な消去等を行ったうえ、撤去し、処分すること。クラウドサービスについては、データの完全な消去を行うこと。

2.3.　調達範囲

本業務の調達範囲については、関連文書「共通仕様書」中の項番「3.1.調達概要」、「3.2.次期ネットワークの調達範囲」を参照すること。

2.4.　履行場所

本業務における主な履行場所は以下のとおり。

- IDC（所在地は別途開示予定）

・　本庁舎（三重県津市広明町 13 番地）

その他の履行場所については、「【別紙 1】ネットワーク設計構築拠点一覧」を参照すること。

2.5.　本県からの提供資料

現行ネットワーク構成等の詳細については、三重県電子調達システム（物件等）利用登録申請が承認され、守秘義務の遵守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。

・　現行ネットワークの設計構成情報、ハードウェア・ソフトウェア構成に係る情報
・　現行ネットワークの監視・運用・保守に係る情報
・　三重県 DX 推進基盤の構成・計画に係る情報
・　セキュリティクラウドの構成に係る情報
・　EDR の構成に係る情報
・　マイナンバー利用事務系ネットワークの構成に係る情報
・　ユーザ認証システムの構成に係る情報
・　本庁舎・総合庁舎・単独地域機関フロア図

2.6.　責任分界点

本業務に係る関連契約の各受託事業者との責任分界点は以下のとおり。

2.6.1.　主回線受託事業者

主回線受託事業者との責任分界点については、「図 2-1 主回線受託事業者との責任分界点」に示したとおり、主回線受託事業者にて調達する回線側機器の接続インターフェースを責任分界点とする。そのため、責任分界点までの一切の機器の準備及び配線を本受託事業者の責任で行うこと。

現行ネットワークから次期ネットワークへの移行において、主回線側の機器等に設定変更が必要となる場合は、本受託事業者の業務範囲として主回線受託事業者と調整し、必要な対応を行うこと。なお、主回線受託事業者へ作業依頼を行う際に費用負担を求められた場合は本受託事業者が負担すること。

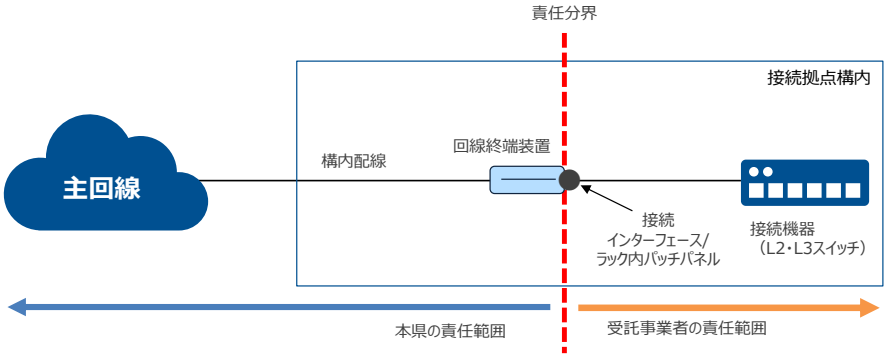

図 2-1 主回線受託事業者との責任分界点

2.6.2. 単独地域機関回線受託事業者

単独地域機関回線受託事業者との責任分界点については、「図 2-2 単独地域機関回線受託事業者との責任分界点」に示したとおり、単独地域機関回線受託事業者にて調達する回線側機器の接続インターフェースを責任分界点とする。そのため、責任分界点までの一切の機器の準備及び配線を本受託事業者の責任で行うこと。

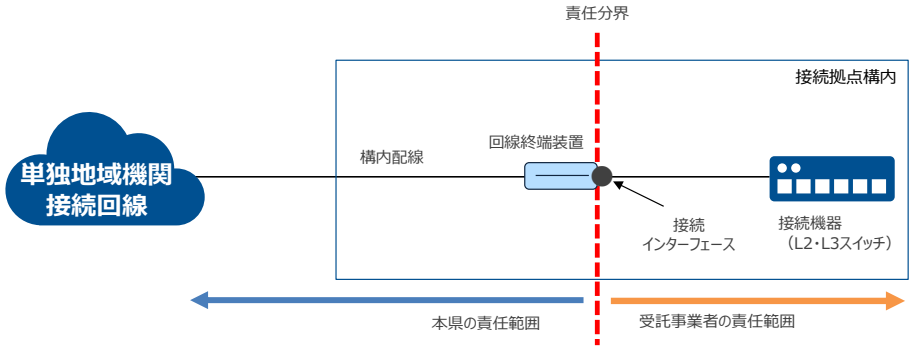

図 2-2 単独地域機関回線受託事業者との責任分界点

2.6.3. バックアップ回線受託事業者

バックアップ回線受託事業者との責任分界点については、「図 2-3 バックアップ回線受託事業者との責任分界点」に示したとおり、バックアップ回線受託事業者にて調達する回線側機器の接続インターフェースを責任分界点とする。そのため、責任分界点までの一切の機器の準備及び配線を本受託事業者の責任で行うこと。

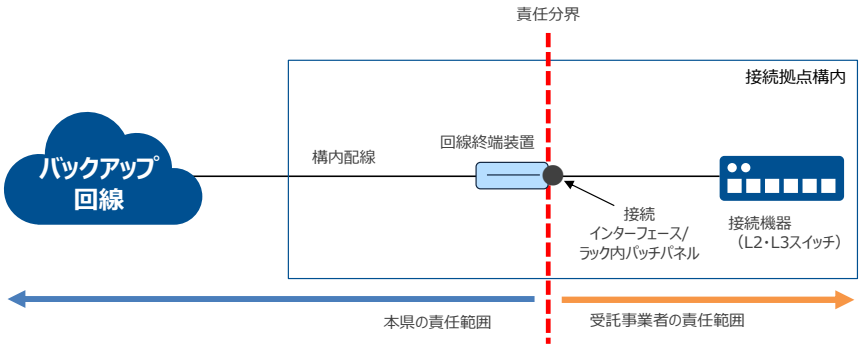

図 2-3 バックアップ回線受託事業者との責任分界点

2.6.4. 現行ネットワーク受託事業者

現行ネットワーク受託事業者との責任分界点については、「図 2-4 現行ネットワーク受託事業者との責任分界点」に示したとおり、現行ネットワーク調達機器の接続インターフェースを責任分界点とする。そのため、責任分界点までの一切の機器の準備及び配線を本受託事業者の責任で行うこと。

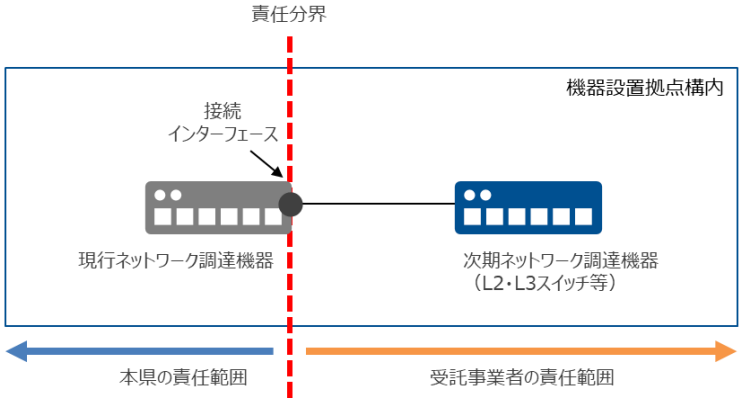

図 2-4 現行ネットワーク受託事業者との責任分界点

2.6.5. 各受託事業者

セキュリティクラウド等の各受託事業者との責任分界点については、「図 2-5 各受託事業者との責任分界点」に示したとおり、各受託事業者の調達機器の接続インターフェースを責任分界点とする。そのため、責任分界点までの一切の機器の準備及び配線を本受託事業者の責任で行うこと。

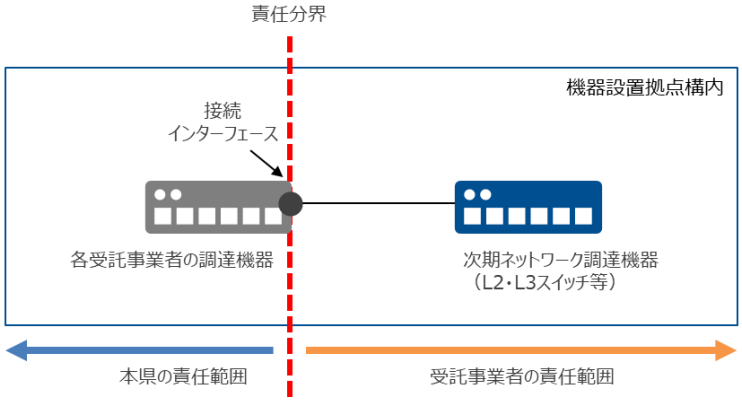

図 2-5 各受託事業者との責任分界点

3. 契約期間

3.1. 契約期間

契約期間は、令和 7 年度（2025 年度）の契約締結の日から令和 14 年（2032 年）3 月 31 日までとする。ただし、次期ネットワークへの移行において、全庁ファイルサーバについては令和 8 年（2026 年）9 月 30 日までに、その他の機器等については令和 9 年（2027 年）3 月 31 日までに完了すること。なお、次期ネットワークの保守・運用については、移行等が完了した部分から順次開始すること。

3.2. 想定スケジュール

本業務の想定スケジュールは、「図 3-1 本調達の想定スケジュール」のとおり。次期ネットワークの構成要素のうち、全庁ファイルサーバについては、現行環境の保守サポート期間に制約があるため、次期ネットワークの切り替え時期である令和 9 年（2027 年）4 月より前のタイミングで切り替えることを想定している。また、仮契約、本契約、詳細設計、構築、移行期間中に各種回線の敷設や切り替えを予定しているため、別途本県を含め、現行ネットワーク受託事業者、各回線受託事業者と十分に協議のうえ、確定すること。

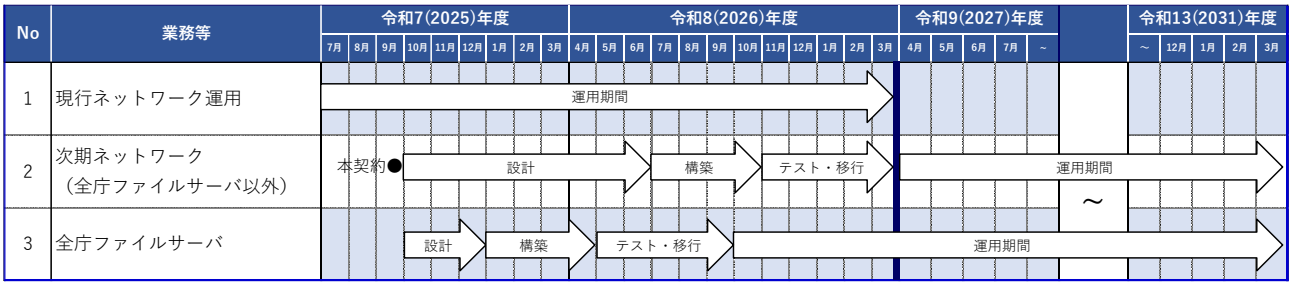

図 3-1 本調達の想定スケジュール

4. 支払条件等

4.1. 支払条件

本業務の利用に係る費用の支払条件は以下のとおり。

- 設計構築等（①設計、②構築、③テスト稼働、④移行）に係る費用は、各年度において、①から④のそれぞれ完了した分の完了検査を行い、相当分を支払うこととする。
- 運用保守等（⑤運用保守、⑥監視、⑦クラウドサービス利用等）に係る費用は、年度毎に完了検査を行い、相当分を支払うこととする。運用保守費用については、運用費用、保守費用、IDC 費用、回線費用等が含まれるものとする。
- 年度の途中で消費税率が改正された場合は、当該年度の費用を改正前後の期間で按分した支払いを可能とする。
- 消費税法が改正され本業務が経過措置の対象とならない場合、該当する期間の費用について改正後の税率を適用する。
- 業務未完了分を前倒しで支払うことはできない。

4.2. 各年度の支払い上限額

各年度の支払い上限額は以下のとおりとする。

※調達公告時に記載予定

4.3. 内訳資料の提出

上記支払条件を踏まえて契約額の内訳資料を作成し、契約締結前までに提出すること。特に、設計、機器、ソフトウェア等の納入、設置、構築、テスト、移行、運用、保守、監視、クラウドサービス利用料については明確に分割することとし、また、年度毎でも分割すること。

内訳項目の細目とその金額が明確な内訳資料を作成し、提出すること。

5. 納品成果物

5.1. ハードウェア・ソフトウェア・サービス

本業務に必要な全てのハードウェア・ソフトウェア・サービスを納入すること。

5.2. 文書成果物

本受託事業者は、以下の文書成果物を指定された提出期限までに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うこと。

5.2.1. 業務計画書

本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に取りかかること。なお、業務計画書の内容は以下のとおりとする。

また、現行ネットワークの調査の結果、納入予定物品等に変更がある場合は速やかに修正すること。

- 業務スケジュール
- 本事業の進め方に係る基本方針・ルール等
- 業務遂行体制・業務従事者名簿
- 機器構成、納品予定物品一覧

5.2.2. 各種設計書、完成図書及び報告書

本受託事業者は、各工程の計画、成果を示すドキュメントを作成すること。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、本県と十分に協議すること。また、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。レビュー会については本県における確認期間、本県からの指摘を受けて修正する期間等を考慮し、指定成果物の提出期限を踏まえて、十分余裕をもった時期に実施すること。なお、次期ネットワークの構成要素のうち、全庁ファイルサーバについては、切り替え時期が異なるため、以下の分類とする。

- Ａ：全庁ファイルサーバ
- Ｂ：全庁ファイルサーバ以外

表 5-1 設計・構築に係る成果物の概要及び一覧

No.	成果物	内容	提出期限
1	プロジェクト管理資料	進捗管理、課題管理、リスク管理等、プロジェクト管理に必要な資料	適宜
2	基本設計書	本県の要求事項を整理し、物理的なネットワーク構成、機器構成等を定めた成果物	A：令和 7 年 12 月末 B：令和 8 年 6 月末
3	詳細設計書	基本設計書に基づき、各機器へ設定するパラメータの設定根拠及び設定ルール等を示す成果物	A：令和 8 年 4 月末 B：令和 8 年 10 月末
4	移行計画書	移行スケジュール及び移行手順等、安全かつ円滑に移行するために必要な移行計画を示す成果物	A：令和 8 年 4 月末 B：令和 8 年 10 月末
5	移行手順書	次期ネットワークへの移行における移行手順、タイムテーブル等を示す成果物	A：令和 8 年 5 月末 B：令和 8 年 11 月末
6	テスト計画書	テストの実施スケジュール、実施内容、進捗の予定等、テストの計画を示す成果物	A：令和 8 年 5 月末 B：令和 8 年 11 月末
7	テスト手順書	単体テスト、結合テスト、総合テスト等の手順を示す成果物	A：令和 8 年 5 月末 B：令和 8 年 11 月末
8	テスト結果報告書	テストの実績、実施結果等、テストの結果を報告する成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
9	導入機器一覧	本受託事業者が納入する機器の一覧を示す成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
10	システム俯瞰図	次期ネットワークの構築によって、関連するシステムを含めた、全体を俯瞰できる成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
11	通信フロー	次期ネットワークの通信フローを示す成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
12	通信制御一覧	ファイアウォールやプロキシ等による通信制御に関する情報を示す成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
13	物理構成図	次期ネットワークの物理的な配線形状、機器構成等を示す成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
14	論理構成図	次期ネットワークの IP アドレスや VLAN 情報等の論理的な構成を示す成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
15	機器設置図	次期ネットワークで設置する機器等の設置箇所を示す成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
16	機器設定シート	各機器への設定パラメータの値を示す成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末
17	施工写真	各拠点の施工前、施工中、施工後の施工状況を示す写真等の成果物	A：令和 8 年 9 月末 B：令和 9 年 3 月末

表 5-2 運用・保守に係る成果物の概要及び一覧

No.	成果物	内容	提出期限
1	運用体制図	次期ネットワークにおける運用体制を示す成果物	A：令和 8 年 3 月末 B：令和 8 年 9 月末
2	保守設計書	次期ネットワークを継続的・安定的に提供するための保守の実施手順等を定めた成果物	A：令和 8 年 6 月末 B：令和 8 年 12 月末
3	保守体制図	次期ネットワークにおける保守体制及び保守窓口を示す成果物	A：令和 8 年 3 月末 B：令和 8 年 9 月末
4	運用設計書	次期ネットワークの運用管理方法、各種手順等を定めた成果物	A：令和 8 年 6 月末 B：令和 8 年 12 月末
5	運用手順書	全庁ファイルサーバ利用ルール、ファイル授受サービス利用ルール等の手順を定めた成果物	A：令和 8 年 8 月末 B：令和 9 年 2 月末
6	操作マニュアル	導入するシステムの操作・設定方法に関するマニュアル	A：令和 8 年 8 月末 B：令和 9 年 2 月末
7	運用業務フロー	定例業務、非定例業務の内容や担当、業務の流れを示すフロー	A：令和 8 年 8 月末 B：令和 9 年 2 月末
8	保守業務フロー	機器故障や障害等が発生した場合の切り分け手順、復旧方法を示すフロー	A：令和 8 年 8 月末 B：令和 9 年 2 月末
9	インシデント対応手順	重大なインシデントが発生した場合の連絡・対応手順	A：令和 8 年 8 月末 B：令和 9 年 2 月末
10	構成管理台帳	最新の構成情報と機器やサービスの設定変更の情報が記載されている台帳	随時
11	システム俯瞰図	次期ネットワークの運用開始後、ネットワーク、システム構成に変更があった場合、全体を俯瞰できる最新の成果物	随時
12	通信フロー	次期ネットワークの運用開始後、通信フローに変更があった場合、最新の通信フローを示す成果物	随時
13	通信制御一覧	次期ネットワークの運用開始後、通信制御に変更があった場合、最新のファイアウォールやプロキシ等による通信制御を示す成果物	随時
14	月次報告書	本業務における運用状況、作業報告等の月次結果を報告するもの	月末
15	年次報告書	本業務における運用状況、作業報告等の年次結果を報告するもの	年度末
16	障害報告書	本業務における障害状況、障害対応等の結果を報告するもの	随時

No.	成果物	内容	提出期限
17	運用保守実施報告書	期間内に実施した運用実績・保守実績 期間内に発生した障害事象・対応 SLA 報告	サービス提供期間中 半期毎
18	データ消去作業完了証明書	データ消去実施後の作業完了を証明するもの	データ消去終了時
19	業務完了報告	本契約の業務完了についての報告書	契約終了時

5.2.3. 打ち合わせ議事録

本業務の遂行に伴う打ち合わせの議事録は、本受託事業者がその都度速やかに（概ね 3 営業日以内）作成し、本県に提出すること。

回線受託事業者等、各受託事業者との協議においても同様に議事録を作成し、本県に提出すること。

6. 全体管理

本章では、本業務を遂行するにあたり、円滑かつ手戻りの少ない進行や工程管理を行うために必要となる各受託事業者との調整及びスケジュール管理等に関する要求事項を記載する。

6.1. 業務計画書

本受託事業者は、契約後速やかに本業務に関する「業務計画書」及び「工程表」を作成し、本県に提出して承認を得ること。業務計画書には、全体の体制及び役割と作業工程、スケジュール及び納入予定物品一覧等の概要を記載すること。

＜提案＞各フェーズにおいて想定する作業体制、役割、作業工程及びスケジュール等を提示すること。

6.2. プロジェクト管理

本業務における調達、設計、構築、移行といった運用開始までに必要な各種業務について問題なく遂行できるよう、現行ネットワーク受託事業者、主回線、単独地域機関回線、バックアップ回線等の各受託事業者と調整を行ったうえ、主体的にプロジェクト全体を管理するため、以下の業務を実施すること。

6.2.1. 進捗管理

- 本受託事業者は、業務計画書に基づき WBS（Work Breakdown Structure）を作成し、作業工程の状況及び計画との差異を把握するために進捗管理を行うこと。
- 計画から遅れが生じた場合は、原因を調査のうえ、本県に改善策を速やかに提示し、承認を得たうえで対策を実施すること。

6.2.2. 課題管理

- 本受託事業者は、課題管理を行う際、課題、問題事項等の概要・対応策・解決状況等を管理し、「課題管理表」に記録すること。
- 定期的に実施する定例会議において、本業務における課題、問題事項等の発生状況及び解決状況について本県に報告すること。
- 本業務を遂行するうえで発生した課題、問題事項のうち、複数の受託事業者に関係するものについては、各受託事業者と協働し、本受託事業者側で対応可能なものは速やかに対応すること。また、各受託事業者側で対応が必要となる事項については、各受託事業者に作業依頼を行うこと。なお、作業依頼を行う際に費用負担を求められた場合は本受託事業者が負担すること。

6.2.3. リスク管理

- 本受託事業者は、業務の進捗に影響を及ぼし得る未発生の課題、問題事項等をリスクとして捉え、「リスク管理表」を作成のうえ、適切な管理を行うこと。
- 定期的に実施する定例会議において、課題、問題事項等の報告とあわせて、未発生の課題、問題事項等をリスクとして本県に報告すること。
- リスク管理を行い、想定されるリスクの内容と発生した際の対策案を予め検討し、リスクを回避又は低減できるよう、必要な措置を講じること。また、発生した場合は速やかに対応できるよう準備すること。
- リスクが顕在化した際、対策案を検討し、本県に提案すること。また、本県の承認後に対策案を実施し、その結果を本県に報告すること。なお、緊急の場合は本県への提案前に対策を実施し、事後報告とすることも可とする。

6.3. 関係者との調整

- 本業務を問題なく遂行できるよう、設計・構築・移行・運用保守全てのフェーズにおいて、現行ネットワーク受託事業者及び IDC、主回線、単独地域機関回線、バックアップ回線、防災行政無線等の各受託事業者との調整を主体的に行うこと。また、各市町担当者、各庁舎管理者等との連絡、調整についても主体的に行うこと。
- 関係者等との調整において発生した課題等について管理し、課題解決に向けて協議等を実施すること。

6.4. 会議体

本受託事業者は、本業務の遂行にあたり、「表 6-1 会議体一覧」に示す会議を開催すること。原則として、会議終了後 3 日以内に「打ち合わせ議事録」を作成のうえ、本県に提出すること。当該議事録には、開催日時、開催場所、出席者、配布資料、受領資料、決定事項、宿題又は課題事項、議事詳細、次回会議予定を簡潔に記述すること。

表 6-1 会議体一覧

会議体	概要	頻度
キックオフ会議	業務計画書の内容について、本受託事業者が本県へ説明するため開催する会議として、契約後速やかに開催すること。	契約締結後 2 週間以内
進捗会議	本県に対し、進捗報告を兼ねた進捗会議を開催すること。進捗会議の中で、作業の進捗状況、課題管理の状況、個別事案等について報告すること。	設計・構築期間中 週次を想定

会議体	概要	頻度
設計・構築検討会議	設計・構築を実施するうえで詳細な内容を個別に協議するための設計・構築検討会議を開催すること。検討するテーマによって、本県と調整のうえ、適宜開催すること。	設計・構築期間中 適宜
運用月次報告会議	本県に対し、運用業務の実績報告を行う運用月次報告会議を開催すること。会議の際には定められた月次報告の内容に沿って、報告すること。また、SLA の集計期間翌月（年度末は 3 月度）の報告会議においては、遵守結果報告を行い、遵守できなかったものに関しては、原因、改善策、対応結果について報告すること。	運用期間中 月次を想定
運用年次報告会議	本県に対し、運用業務の実績報告を行う運用年次報告会議を開催すること。会議の際には定められた年次報告の内容に沿って、報告すること。	運用期間中 年次を想定
SLM 会議	SLA の時点修正について協議し、本県及び本受託事業者双方で合意するための SLM 会議を開催すること。	運用期間中 年次を想定
その他会議	上記以外の会議が必要となった場合、本県と調整のうえ、適宜開催すること。	契約期間中 適宜

7. 設計・構築業務

本章では、本業務における設計・構築業務に係る、本県が要求する事項を記載する。

7.1. 設計業務に関する基本要件

設計業務に関する基本要件は以下のとおり。

7.1.1. 設計業務に関する共通要件

設計業務について、以下の要件を満たすこと。

- 設計業務を実施する際は、現行ネットワーク及び関連システムの設定、及び、構成を理解したうえで各種設計を行うこと。
- 設計業務は、契約開始後より「表 5-1 設計・構築に係る成果物の概要及び一覧」で定める期限までに実施し、実施した設計毎にそれぞれの設計書を成果物として作成すること。また、作成した設計書は、本県に対しレビューを実施し、本県の承認後、提出すること。
- 設計として、基本設計、詳細設計、構築設計、移行設計、テスト設計、運用保守設計等、必要な設計を行うこと。
- 設計時において、最適な設計を実施できるよう、機器やソフトウェア等の製造元のエンジニアへ技術問い合わせが行える体制、又はそれに準じる体制を確保すること。
- ＜提案＞次期ネットワークを設計・構築するにあたり、現行のネットワーク状況等の調査方法を具体的に記載すること。

7.1.2. 基本設計、詳細設計に係る詳細要件

基本設計・詳細設計として、以下の要件を満たすこと。

- 次期ネットワークの全体構成や納品する機器、及び、ソフトウェア一覧、構築期間、移行期間、運用保守期間における業務内容等、本業務を実施するうえで必要となる基本的な内容等について基本設計を行うこと。
- 本業務で利用可能となるクラウドサービス等についてどのような形で構築し、利用できるようにするかについても、基本設計に含めること。
- 本業務で導入する機器やソフトウェア等について、利用方法等に係る詳細な検討を行ったうえで、各種設定を行うために必要となる詳細設計を行うこと。
- 各ネットワーク、システムに係る個別の要件は「7.2 システム別設計・構築要件」に示す。

7.1.3. 構築設計に係る詳細要件

構築設計として、以下の要件を満たすこと。

- 本業務で導入する機器等について、構築作業を行うために必要となる構築設計を行うこと。
- 各機器の搬入、設置、必要な OS のインストール、ソフトウェアのインストール・設定作業は原則として全て本受託事業者が実施すること。
- 設置場所への納入、設置作業、配線作業並びに回線等への接続作業の実施においては、本県、又は関係者と事前に協議を行い設計に反映させること。
- 機器の納入、取り付けにあたっては、耐震固定のアンカーボルトを装着する等により、必要な耐震措置をとること。
- ネットワークの停止を伴う作業は原則認めないため注意すること。ただし、避けられない場合は閉庁日もしくは夜間の限られた時間での実施となる。なお、ネットワークの停止を伴わない場合は、平日、日中時間帯での作業を可とする。
- 各受託事業者に作業を依頼する必要がある場合は、作業指示書等を作成したうえで本県に提出し、承認を得ること。
- 各機器のシステムログを取得・保存できるようにすること。また、各機器において時刻同期を行うことで、ログの出力時刻が適切に記録されるようにすること。
- 本調達において工事業務が発生する際は、石綿（アスベスト）含有の事前調査および対策等、必要な安全対策を実施すること。

7.2. システム別設計・構築要件

本章では、次期ネットワークで導入する各システムにおける要求事項を記載する。

原則、現行ネットワークの基本構成等を踏襲したうえで、以下の各種条件等を実現させるための設計を行うこと。なお、更新対象機器及び現行ネットワークの構成概要については、「【別紙 2】更新機器一覧」を参照すること。

IDC、本庁舎のシステム構成については、「【別紙 4】次期ネットワーク構成概要図」を参照すること。

7.2.1. システム分類

本業務は広範囲にわたるため、各種調達物品を用途により「表 7-1 システム分類」のとおり、12 のシステムに分類して記載を行う。システム分類は以下のとおりとする。なお、本分類に回線は含まない。調達物品の詳細な要件は「9 構成要素の仕様」に記載する。

表 7-1 システム分類

システム名	対象
有線ネットワーク（スイッチ、ルータ）	基幹コア L3 スイッチ(IDC) 基幹コア L3 スイッチ(本庁舎) 拠点コア L3 スイッチ(総合庁舎 10 拠点 + 吉田山会館) 拠点コア L3 スイッチ(アスト津/シングル構成) 拠点コア L3 スイッチ(教育センター/シングル構成) サーバ接続用スイッチ(IDC/10G) サーバ接続用スイッチ(IDC/1G) サーバ接続用スイッチ(本庁舎/1G) ファイアウォール接続用スイッチ(24 ポート) VPN 集約ルータ(IDC 設置ルータ) ルータ集約スイッチ(IDC) 市町等利用機関接続用スイッチ L2 スイッチ(48 ポート) L2 スイッチ(24 ポート) 単独地域機関接続用ルータ Web 会議回線接続用ルータ
無線 LAN	無線 LAN アクセスポイント(本庁舎：既設+一部増設) 無線 LAN アクセスポイント(総合庁舎、吉田山会館：既設) 無線 LAN アクセスポイント(単独地域機関 19 拠点：新設) 無線 LAN コントローラ 無線 LAN 監視装置
基幹ファイアウォール	基幹ファイアウォール
ネットワーク(その他)	Syslog サーバ Radius サーバ セキュリティログ保存サーバ(Syslog 二次バックアップ) セキュリティログ保存サーバ(Radius ログバックアップ) ネットワーク管理サーバ プロキシサーバ
ロードバランサ	プロキシ・メールサーバ用ロードバランサ クラウド接続用ロードバランサ
メール/DNS	メールセキュリティ対策サーバ 内部メールサーバ 外部メールサーバ 外部 DNS サーバ 内部 DNS サーバ
全庁ファイルサーバ	全庁ファイルサーバ（インターネット接続系） 全庁ファイルサーバ（LGWAN 接続系）
ファイル授受システム	ファイル交換システム(外部共有) LGWAN ファイル転送システム(INT-LGWAN) ファイル無害化システム
LGWAN 接続システム	LGWAN 接続システム

システム名	対象
防災ネットワーク	災害時用ルータ 災害時用プロキシサーバ 災害時用ファイアウォール 災害時用 Radius サーバ
ネットワーク可視化	ネットワーク可視化システム
その他	OS 関連 無停電電源装置（UPS）

7.2.2. 共通要件

7.2.2.1 全般

次期ネットワークの設計にあたっては、現行ネットワークの論理設計を踏襲することを原則とする。現行ネットワークの論理構成は「図 7-1 三重県行政 WAN 論理構成図」のとおり。

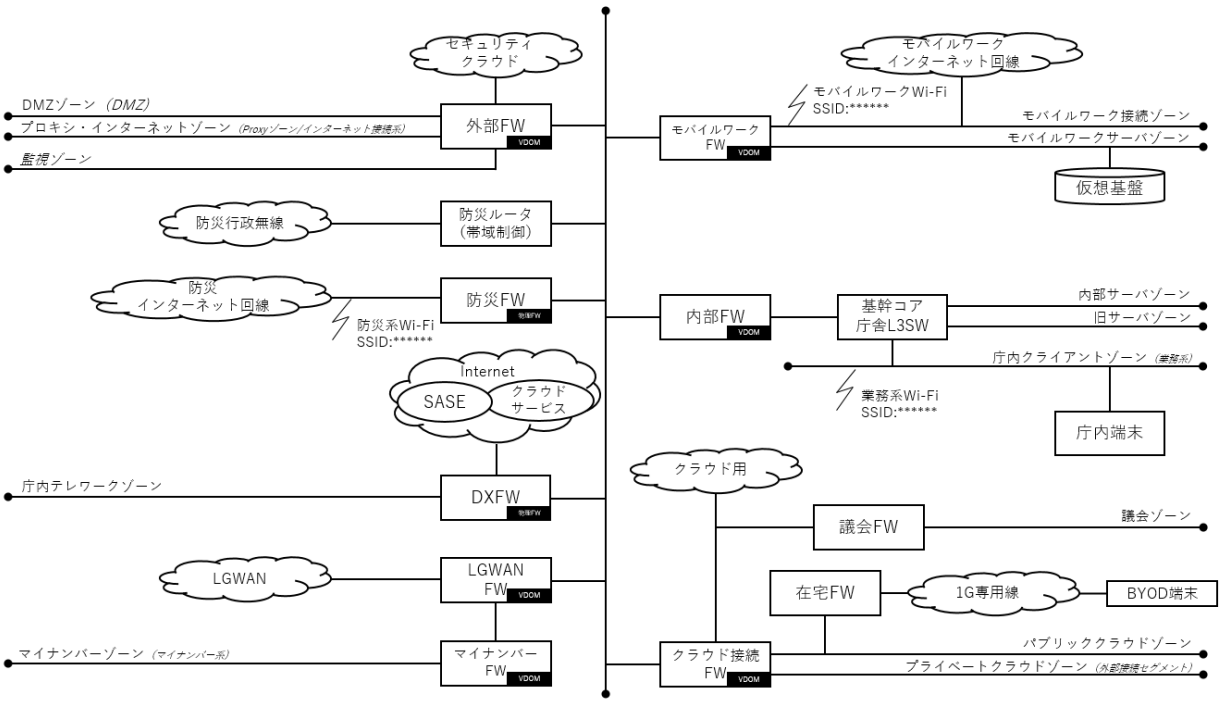

図 7-1 三重県行政 WAN 論理構成図

以下については、本県が提示する課題解決のために必要な機器やシステムの調達と再設計を行い、検討結果や解決方針について合意を得たうえで設計すること。再設計時には、既存で提供しているサービスが継続して提供可能な構成とすること。

(機器/システムの増設要件)

- 市町等利用機関が主回線と接続するスイッチの冗長化対象及びバックアップ回線収容対象拠点
- 基幹ファイアウォールの物理分割
- 本庁舎の無線 LAN アクセスポイント増設
- 大規模単独地域機関拠点及び単独地域機関への無線 LAN アクセスポイント展開

(機器/システムの削減要件)

- フロアスイッチの機器集約及びポートの削減
- L3 機能が不要な機器の L2 スイッチへの変更
- 通信制御装置及びプロキシの構成
- 外部メールサーバの機能集約による削減
- その他重要な機器について、効果的な機能分割及び機器集約・削減ができる場合は提示すること。

(論理/システム構成の再検討)

- 基幹ファイアウォールの論理統合
- メール通信フローの見直し
- 全庁ファイルサーバ構成
- LGWAN 接続システム構成
- ネットワーク可視化
- 防災衛星回線の活用（防災衛星回線自体の設計は除く）

(その他の要件)

- 保守、運用、監視設計の運用設計とドキュメント整備

・ 現行ネットワークに係る基本構成や詳細設定及び IDC、各種回線、インターネットメールシステム、ユーザ認証システム等に係る詳細構成については、各種ドキュメント等の確認や各受託事業者への確認を通じて調査を実施し、全体把握を行うこと。
・ ドキュメントの不備や各受託事業者への確認を行ったうえで詳細が把握できない場合は、機器に対する設定情報を確認する等により、可能な限り詳細な把握を行うこと。
・ 上記の内容を踏まえ、次期ネットワークに必要な設計を行い、本県の承認を得ること。

7.2.2.2 IP アドレス体系

・ 次期ネットワークにおいて使用する IP アドレスは、原則として IPv4 のプライベートアドレスとする。
・ IP アドレス体系については、原則として既存ポリシーを踏襲すること。ネット

ワーク構成の見直し等により、追加や変更が必要な場合は本県と協議のうえで利用するアドレス及びセグメントを決定すること。

- 次期ネットワークのアドレス設計にあたり、既存システムとの接続や、採用する移行方法等により、既存の IP アドレス体系を利用する際は、既存システムへの影響を極小化するよう検討したうえで、現行ネットワーク受託事業者等へ利用可否を確認し、本県と協議のうえ、承認を得てから利用すること。

7.2.2.3 時刻同期

- 本業務において導入するネットワーク機器は、NTP・SNTP で時刻同期を行うこと。
- 時刻同期先のサーバは LGWAN 接続系のサーバとするが、アクセス制限等により、時刻同期が困難な場合は、本県と協議し、代替案により時刻同期を行うこと。
- 時刻同期先のサーバ負荷を考慮し、ネットワークトポロジにあわせた、マスタ/スレーブ構成の時刻同期とすること。

7.2.2.4 共通ドキュメントの整備

現行ネットワーク導入後、在宅勤務システム等の導入、β’モデルへの移行といった各種システム導入のための再設計/設定変更が発生している。特にコロナ禍の際は緊急対応に迫られたこともあり、実施された変更がドキュメント化されていない場合が散見される。

また、セキュリティクラウドや三重県 DX 推進基盤等、ネットワークに関して複数の契約や受託事業者が関係しており、それぞれの契約範囲のみ個別に構成管理される等、ネットワークの全体構成の把握や管理が困難な状態となっており、通信経路の見直しの際等に支障をきたしている。

＜提案＞これらを踏まえ、本調達では現行ネットワークの更新にあわせて設計内容を再確認したうえで、ネットワーク構成図や通信フロー等を共通のドキュメントとして整備すること。また、整備したドキュメント類は随時管理し、設計変更、設定変更の都度更新すること。主な要素としては以下を想定しているが、最終的な成果物は本県と協議のうえで決定すること。また、以下に記載されていないもので、ネットワーク構成の明確化のため、整備すべき項目があれば提案すること。

- 本調達で導入する各システム全てが記載されたシステム俯瞰図
- 本県職員が利用する各種端末から本調達で導入する各システムまでの通信フロー
- 本調達で導入する各システムが他システム（AD や外部のサービス）と連携する場合の通信フロー
- PBR、プロキシ（PAC）といった通信制御に関する情報の一覧化

- 制御ポイント（制御している機器のホスト名等）
- 用途
- 送信元及び宛先

・ ファイアウォールにおける以下情報の一覧化
- オブジェクト/オブジェクトグループの対象情報
- ポリシーの用途及び送信元、宛先

7.2.2.5 サーバ構築に係る要件

本業務において、必要なサービス機能を提供するため、サーバを構築する場合、個別の項目にて特段指定がない場合は、専用サーバ（専用アプライアンス含む）を用意して構築する他、本県が保有する共通機能基盤上に構築することも可とする。ただし、本業務において使用可能な共通機能基盤のリソースには限りがあるため、「7.2.2.5.1 共通機能基盤リソース」を参照すること。

サーバの構成に関する共通の要件を以下に記載する。

・ 本県が保有する共通機能基盤上、もしくは専用サーバ（専用アプライアンス含む）を用意して導入を行うこと。
・ 専用サーバでも共通機能基盤と同等の耐障害性を確保すること。
・ 本県が保有する共通機能基盤上に構築する場合、以下の本県が保有するものを利用可能とする。利用可能なリソース上限値は、「7.2.2.5.1 共通機能基盤リソース」に記載のとおり。
  - サーバ OS：Windows Server 2022 DataCenter
  - セキュリティ（ウイルス対策ソフト）：Microsoft Defender/ServerProtect for Linux
  - バックアップシステム：Veeam Backup&Replication
・ ただし、セキュリティ（ウイルス対策ソフト）については、共通機能基盤上に構築しない場合でも利用可能（専用 OS は除く）である。
・ バックアップシステムの世代数やバックアップ手法は共通機能基盤側の運用に準拠する。

7.2.2.5.1 共通機能基盤リソース

本業務で利用可能な共通機能基盤のリソースは以下とする。

- コア数：144vCPU
- メモリ：300GB
- ディスク：13,020GB

上記リソースを超えないのであれば、仮想マシンは本県と協議のうえで、何台構築しても問題ない。リソースが不足する場合は、不足リソース分の物理サーバを別途用意す

ること。

7.2.3. 有線ネットワーク

本県の有線ネットワークは主に以下の拠点により構成している。

- IDC
- 本庁舎
- 総合庁舎：10 拠点
- 吉田山会館、勤労者福祉会館、栄町庁舎、合同ビル
- 大規模単独地域機関：2 拠点
- 単独地域機関（インターネット VPN 接続）：156 拠点
- 単独地域機関（閉域網接続）：10 拠点
- 市町等利用機関：33 拠点（市町向け回線を収容するスイッチのみ）

本章では、従来のネットワークの設計を踏襲しつつも、長期的なシステム更新を考慮した新しいネットワーク構成の導入やコストの効率化を行うための要件を記載する。なお、本章の記載は有線ネットワーク全般に係る設計及び構築要件であり、導入機器個別の要件については「9 構成要素の仕様」に記載する。

- 導入機器において重要度の高いものは冗長構成とすること。また、機能の分割を行うこと。拠点毎における各機器の方針は「7.3 拠点別構築要件」を参照すること。
- 既存機器の不要機能の削除やポートの集約を検討すること。なお、以下項目を特に重要視している。
  - L3 機能が不要な機器を L2 スイッチに変更
  - フロアスイッチの機器集約及びポートの削減

IDC 以外の拠点へ機器を導入する際は、各設置場所の電源について調査し、必要に応じて本県に確認のうえ、電源の増設等を行うこと。

重要機器の機能分割や不要機能の削除、ポート削減等に伴う作業が発生する場合は、その費用を本調達に含めること。例として、電源増設や再配線等の工事業務を指す。

7.2.4. 無線 LAN

本県は本庁舎及び総合庁舎、吉田山会館及びその配下の拠点（勤労者福祉会館、合同ビル、栄町庁舎）に居室内の行政端末が無線接続をするための無線 LAN 環境を導入しており、端末更新や新システムの導入に伴い、無線 LAN の需要がさらに高まっている。そのため、本調達では無線 LAN の拡張として、本庁舎への無線 LAN アクセスポイントの追加、新規拠点（別途指定する単独地域機関）への無線 LAN 導入、既設アクセスポイントの機器更新を行う。

無線 LAN の拡張における要件を記載する。なお、導入機器個別の要件については「9 構成要

素の仕様」に記載する。

- 既存の無線 LAN 環境では通信速度が一時的に低下する現象を確認している。システムの更新時に速度低下の原因調査を行い、速度低下が可能な限り発生しない構成とすること。その際、構成の変更や再設計が必要となった場合、その背景と手法を本県に説明したうえで協議を行い決定すること。
- ＜提案＞将来的に職員数、端末数が増加した際、大きな設定変更を伴わず、機器の追加及び配線工事等で無線 LAN アクセスポイントの増設が可能な拡張性を有する設計を行うこと。
- ＜提案＞現行ネットワークでは、無線 LAN の認証について、SSID の用途毎に異なる認証方法や認証機関を利用している。セキュリティ対策強化のため、最新の認証方法の導入のうえ、認証方法を統一し、運用すること。ただし、後述する防災用 SSID 及び StarLink 用 SSID についてはこの限りではない。

7.2.4.1 無線 LAN アクセスポイント

無線 LAN アクセスポイントは、本庁舎や総合庁舎、一部の単独地域機関において、居室内の行政端末が無線接続をするためのアクセスポイントである。

本庁舎においては、現在、約 1,400 台の業務端末等が無線 LAN アクセスポイントに接続しており、今後、約 700 台の業務端末増加が見込まれる。また、一部の会議室においては、電波が到達しないことを確認している。そのため、次期ネットワークにおいては、約 30 台のアクセスポイントを増設することを予定している。

単独地域機関については一部を除き、新規に無線 LAN 環境の構築が必要となる。

無線 LAN 拡張によるアクセスポイント増加分を含めた各拠点の設置想定台数は以下のとおり。

- 本庁舎　：168 台
- 総合庁舎（10 拠点）　：282 台
- 吉田山会館及び栄町庁舎・勤労福祉会館・合同ビル　：　56 台
- 単独地域機関（19 拠点）　：120 台

なお、無線 LAN アクセスポイントの追加台数については、後述する要件に従い、適切な台数を算出する必要がある。

各拠点の無線 LAN アクセスポイント数は「【別紙 1】ネットワーク設計構築拠点一覧」を参照すること。

要件は以下のとおり。

- 現行の無線 LAN 環境の設計を踏襲し、同じ SSID で同一の利用方法を可能にすること。各 SSID は IDC 設置の Radius サーバにて認証を行うこと。
- 外来波等の外的要因によらず、安定的に無線 LAN 環境が利用できるよう設計及び構築を行うこと。

- 保守作業や無線 LAN アクセスポイントの追加用に、展開機器とは別に 10 台を追加で調達に含めること。
- 既存システムの導入から年数が経過しているため、認証方式及び暗号化方式が適切かを再検討し、必要に応じて最適な方式に再設計を行うこと。なお、現行の無線 LAN 環境では以下の認証方式を使用している。
  - MAC アドレス認証+WPA2 PSK
  - MAC アドレス認証+WPA2 Enterprise(EAP-TLS)
- 災害発生時に庁内での無線利用を可能とするため、防災用 SSID 及び StarLink 専用 SSID を設定すること。
- 防災用 SSID についてのみ、本庁舎内に構築する災害時用 Radius サーバにて認証を行うこと。
- 新規導入拠点及び増設拠点については事前にサイトサーベイを実施し、無線 LAN アクセスポイントの設置位置を決定すること。ただし、既設拠点については、無線 LAN コントローラやネットワーク管理サーバが類似の機能を有する場合は、手法を本県に説明のうえで代替手法とすることを可とする。

7.2.4.2 無線 LAN コントローラ

無線 LAN コントローラは、無線 LAN アクセスポイントのチャネルや電波の自動制御を実施するとともに、複数の SSID 毎にネットワーク接続認証やアクセス制限を実施する装置である。

要件は以下のとおり。

- クラウド管理型の無線 LAN コントローラを構築すること。
- 本調達で導入する全拠点に点在する 700 台以上の無線 LAN アクセスポイントの一元管理を行うこと。
- クラウド上の無線 LAN コントローラと無線 LAN アクセスポイント間の接続が切断された場合でも無線 LAN アクセスポイントがローカルで動作を継続可能な設計とすること。
- 既存環境では本庁舎のみ無線 LAN コントローラでの集中管理となっており、他拠点はコントローラアクセスポイントによる管理となっている。今後の運用を踏まえ、次期ネットワーク構成では全拠点のアクセスポイントを集中管理可能な構成とすること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、本県に説明のうえで協議を行うこと。

7.2.4.3 無線 LAN 監視装置

無線 LAN 監視装置は、本庁舎、総合庁舎、単独地域機関等に設置する無線 LAN アクセスポイントを集中管理する機能を有し、電波の状況や無線 LAN クライアントの接続品質等を確認する装置である。

要件は以下のとおり。

- 本調達で導入する全ての無線 LAN アクセスポイントを集中管理し、電波状況、無線 LAN クライアントの接続品質等を確認すること。
- アクセスログの取得と分析を実施し、監査証跡として一定期間保管が可能な構成とすること。
- 機器に求める機能要件については「9.3.3 無線 LAN 監視装置」へ記載する。なお、無線 LAN 監視装置へ求める機能が無線 LAN アクセスポイント及び無線 LAN コントローラ、その他本調達で導入する機器に含まれる場合、それらの機器へ統合することを可とする。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。
- 「7.2.4.2 無線 LAN コントローラ」において、上記の機能を有している場合は個別に無線 LAN 監視装置を構築せず、コントローラにて管理することも可とする。

7.2.5. 基幹ファイアウォール

基幹ファイアウォールは、各ゾーンの境界に設置し、それぞれのセキュリティルールにあわせた通信制御を行う。

要件は以下のとおり。

- ネットワークを各ゾーンに分割し、仮想ファイアウォールで制御を行う現行のセキュリティポリシーを踏襲すること。
- 外部系通信を制御するファイアウォールと内部系通信を制御するファイアウォールを物理的に筐体分割し、それぞれ 2 台ずつのファイアウォールで冗長構成にすること。外部系通信及び内部系通信の内訳は以下のとおり。

（内部系通信）

- 庁内クライアントゾーン
- 庁内テレワークゾーン
- 旧サーバゾーン
- 内部サーバゾーン
- LGWAN ゾーン

- マイナンバーゾーン

（外部系通信）

- DMZ ゾーン
- プロキシゾーン
- 監視ゾーン
- パブリッククラウドゾーン
- プライベートクラウドゾーン
- モバイルワークゾーン

・ 耐障害性向上のため、現行は 2 台（HA による 1 セット構成）で稼働しているファイアウォールを 4 台（HA による 2 セット構成）に分割すること。
・ 新規システムの導入や構成変更についても原則としてセキュリティポリシーを踏襲しつつ、必要な設計変更は本県と協議のうえで実施すること。
・ 現行ネットワークにおいて、複数の仮想ファイアウォールが乱立している状態にあるため、削減可能なファイアウォールについては集約を検討している。なかでも、現行ネットワーク構築時に運用していた、モバイルワークシステム用の仮想ファイアウォール（モバイルワークファイアウォール）について、現在の通信状況を確認し、他の通信経路への振り分けを行った後、廃止すること。また、その他の仮想ファイアウォールについても既存ネットワーク調査時に通信状況を確認し、集約について検討すること。
・ 一部のファイアウォール等において、一部のクラウドサービスへの接続を、ポリシーベースルーティングで通信させているため、通信経路を見直し、ポリシーベースルーティングを行わないルーティング設計とすること。
・ 現行ネットワークにおいて、IDC のファイアウォール経由で、現行ネットワークと LGWAN アクセス回線を接続しているため、継続して利用できるようにすること。
・ 現行ネットワークにおいて、IDC 内のセキュリティクラウド用機器と、構内配線にて接続しているため、継続して利用できるようにすること。なお、セキュリティクラウドは同時期に更改を予定しているため、セキュリティクラウド受託事業者と調整し、必要な接続設計を行うこと。
・ ファイアウォールについて、通信を遮断した全てのログ及び、本県が指定する通信を許可したログを保存できること。ログには日時、送信元/宛先 IP アドレス及びポート、許可・拒否の種別等を記録できること。
・ 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
・ 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.6. ネットワーク（その他）

本県では各システムの管理を行うために主に以下のコンポーネントを導入している。なお、導入機器個別の要件については「9 構成要素の仕様」に記載する。

- ログ保存用の Syslog サーバ及び認証装置専用のログ保管サーバ
- 上記ログのバックアップ保管サーバ
- 認証用サーバ（AD とは異なる無線 LAN の認証用サーバ）
- ネットワーク管理サーバ
- セキュリティクラウド/インターネット/LGWAN 等への接続用プロキシサーバ

既存環境では上記サーバが個別に存在するが、新規システム導入時に機能を兼任する構成を提案する場合は機能集約を検討してもよい。なお、機能集約により、「9 構成要素の仕様」に記載の要件から変更となる場合は、事前に本県に説明し、承認を得ること。

各コンポーネントの設計・構築に関する要件を以下に記載する。

7.2.6.1 Syslog サーバ

Syslog サーバは、本調達で導入する機器のログを一括して取得・保存するサーバである。

要件は以下のとおり。

- 導入台数は 1 台以上とすること。
- 本業務で導入する機器の各種ログを保存するための Syslog サーバを構築し、各種ログを収集、保存すること。
  - ログの分類と保管先は本県と協議のうえで決定すること。
  - ログをホスト単位でファイルに保存が可能なこと、又はホスト単位でログの検索が可能であること。
  - 特定のサイズ、又は特定の期間でログローテーションが可能なこと。また、別機器にログを保存することも可とする。
- ネットワーク機器の設定情報を自動的に保存しておくこと。
- ログの種類に応じて二次バックアップ先を作成し、長期保管が可能な構成とすること。二次バックアップ先については後述の「7.2.6.3 セキュリティログ保存サーバ（Syslog 二次バックアップサーバ）」、「7.2.6.4 セキュリティログ保存サーバ（Radius ログバックアップサーバ）」を参照し、構築すること。
- ログの保存期間は運用期間中とすること。なお、一定期間経過後のログは安価なストレージにアーカイブする等、ログの肥大化によるストレージ容量の圧迫を軽減できるよう設計すること。
- アーカイブしたログは Syslog サーバ等にインポートすることで、簡単なオペレーションにて確認できるようにすること。また、バックアップしたログデータはテキストや CSV 等、汎用的に読み取りが可能な形式とすること。
- Syslog サーバの障害時におけるバックアップ等の対応を考慮して設計すること。仮想サーバで導入する場合、複数の物理サーバ間で HA 構成を組むこと。

・ 本業務終了時に各サーバ/システムにて保持している全てのログデータをテキストや CSV 等、汎用的に読み取ることができる形式にて出力すること。なお、その際、個別のファイルは圧縮されていてもよい。
・ 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
・ 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.6.2 Radius サーバ

Radius サーバは、無線 LAN アクセスポイントと連携し、三重県行政 WAN に無線で接続する行政端末の認証を行うことで、機器毎の通信可否を制御する。

要件は以下のとおり。

・ 無線 LAN の認証で利用する認証サーバを構築すること。
・ 導入台数は 2 台以上とし、マスタ/スレーブの冗長構成とすること。
・ 冗長構成をとる際に必要な機器等が存在する場合、調達に含めること。
・ 端末の更新時期を考慮し、同時に 10,000 台が認証できるよう、ライセンスを含めて準備すること。
・ 証明書による認証を実施する場合、証明書の配布方法は問わないが、本受託事業者が実施すること。
・ 最終承認日から一定期間認証していないアカウントや有効期限が切れたアカウントが自動無効・削除されるよう設計すること。有効期間については本県と協議のうえで決定すること。
・ Radius サーバについて、行政端末等の認証を行ったログを保存すること。ログには日時、ユーザ ID、クライアント IP アドレス、認証結果等を記録すること。
・ 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
・ 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.6.3 セキュリティログ保存サーバ（Syslog 二次バックアップサーバ）

セキュリティログ保存サーバ（Syslog 二次バックアップ）は、本調達に含まれる Syslog サーバのログを長期間保管するためのサーバとして利用する。認証等の重要度の高いログについては後述の「7.2.6.4 セキュリティログ保存サーバ（Radius ログバックアップサーバ)」に保存することを予定している。

要件は以下のとおり。

・ 導入台数は 1 台とすること。

- Syslog サーバとは異なる仮想基盤上、もしくは専用サーバ（専用アプライアンス含む）を用意して導入を行うこと。
- 動作に必要な OS やソフトウェアを必要数分用意すること。
- ログの保存期間は運用期間中とすること。なお、一定期間経過後のログは安価なストレージにアーカイブする等、ログの肥大化によるストレージ容量の圧迫を軽減すること。
- 取得するログの分類と保管先は本県と協議のうえで決定すること。
- アーカイブしたログは Syslog サーバ等にインポートすることで、簡単なオペレーションにて確認できるようにすること。また、バックアップしたログデータはテキストや CSV 等、汎用的に読み取りが可能な形式とすること。
- ログをホスト単位でファイルに保存が可能なこと、又はホスト単位でログの検索が可能であること。
- 本業務終了時に各サーバ/システムにて保持している全てのログデータをテキストや CSV 等、汎用的に読み取ることができる形式にて出力すること。なお、その際、個別のファイルは圧縮されていてもよい。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.6.4 セキュリティログ保存サーバ（Radius ログバックアップサーバ）

セキュリティログ保存サーバ（Radius ログバックアップ）は、認証等の重要度の高いログの二次保管先として利用する。

要件は以下のとおり。

- 導入台数は 1 台とすること。
- Radius サーバとは異なる仮想基盤上、もしくは専用サーバ（専用アプライアンス含む）を用意して導入を行うこと。
- 動作に必要な OS やソフトウェアを必要数分用意すること。
- ログの保存期間は運用期間中とすること。なお、一定期間経過後のログは安価なストレージにアーカイブする等、ログの肥大化によるストレージ容量の圧迫を軽減すること。
- 取得するログの分類と保管先は本県と協議のうえで決定すること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.6.5　ネットワーク管理サーバ

本調達で導入する機器及びシステムの監視及び管理をするため、ネットワーク管理サーバを構築する。ネットワーク管理サーバは本業務の監視業務において、主に以下の 3 つの用途で利用する。なお、監視業務の内容については別途「12 監視業務」に記載する。

- ネットワーク機器の一元管理
- 機器やシステムの死活、サービス状態、リソース状態、トラフィック等の監視
- ネットワークトポロジの可視化

要件は以下のとおり。

- 導入台数は 2 台以上とすること。
- 監視対象ノードは本受託事業者が納入した機器及び既存システムの監視対象機器とすること。加えて、本県と協議のうえで、本調達以外のシステム監視を行うこと。
- 障害監視システムとして、以下の監視を実施すること。
  - ネットワーク障害
  - トラフィック監視
  - サービス稼働
  - OS パフォーマンス
  - ログ
  - バックアップ状況
- 障害監視システムの設置場所は、三重県情報ネットワーク内もしくは、外部施設、クラウド上からリモートで監視を行ってもよいこととする。ただし、障害監視システムを設置するための設備・回線等、一切の環境を、本受託事業者の負担にて準備すること。また、障害監視システムを三重県情報ネットワーク内に設置する場合は、IDC 内の監視セグメントに設置することとし、ファイアウォールにて監視に必要な最小限のポート番号のみ通信を許可する等、セキュリティを考慮すること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.6.6　プロキシサーバ

プロキシサーバは、本県が管理する各種端末がインターネット接続系や LGWAN 接続系に接続する際のアクセスログの取得やフィルタリング機能を実装するためのサーバである。

今回の調達範囲とするプロキシは複数台存在し、端末種別により利用方法が異なる点について以下に記載する。なお、情報セキュリティ基盤で導入されている SWG（Secure Web

Gateway）は本調達の対象外とする。

現在、本県は端末移行の過渡期であり、端末種別により利用するプロキシサーバが異なる場合がある。端末種別は大きく以下の 3 つに分類される。

① 情報セキュリティ基盤（本県が構築、運用）のサービスが利用可能な端末（NK 端末）

② ①が利用できない、かつインターネット接続系に属する端末（DK 端末）

③ LGWAN 接続系又はマイナンバー利用事務系に属する端末（LK 端末、MK 端末）

また、3 種類の端末は、主に以下の 5 つの用途で導入されたプロキシを経由している。

① セキュリティクラウドを主なインターネット通信経路として利用する端末のデフォルトプロキシサーバ（「7.2.7.2 クラウド接続用ロードバランサ」を指す）でプロキシ①とする。

② セキュリティクラウド向けプロキシサーバ（情報セキュリティ基盤を利用する端末も一部通信で利用する）でプロキシ②とする。

③ プロキシ②経由では通信不可となる接続を特定通信として管理するためのプロキシサーバ、及びβ’構成移行済みの端末が特定通信として LGWAN 接続系のシステムを利用する際に管理を行うプロキシサーバでプロキシ③とする。

④ LGWAN 接続系システムを利用する際に経由するプロキシサーバでプロキシ④とする。

⑤ マイナンバー利用事務系システムを利用する際に経由するプロキシサーバでプロキシ⑤とする

これらを踏まえ、導入するプロキシサーバの構成は以下とすること。

- プロキシ①
  - 本調達の「9.6.2 クラウド接続用ロードバランサ」で実装すること。また、要件についても「9.6.2 クラウド接続用ロードバランサ」に準じること。
- プロキシ②
  - 機器要件については「9.5.6.1 セキュリティクラウド用プロキシサーバ」へ記載する。
- プロキシ③
  - LGWAN 接続系及び Internet 接続系それぞれで用意をすること。機器要件については「9.5.6.2 特定通信用プロキシサーバ（LGWAN 接続系向け）」、及び「9.5.6.3 特定通信用プロキシサーバ（Internet 接続系向け）」へ記載する。
- プロキシ④、⑤
  - 機器要件についてはそれぞれ「9.5.6.4 LGWAN 接続系プロキシサーバ」、「9.5.6.5 マイナンバー利用事務系プロキシサーバ」へ記載する。

なお、上に記載した各プロキシサーバを通じた経路制御全体のフロー図は「【別紙 5】現行プロキシ構成図」に記載する。

各プロキシサーバの設計に係る要件は以下のとおり。

- 本県が保有する共通機能基盤上、もしくは専用サーバ（専用アプライアンス含む）を用意し、プロキシサーバを導入すること。
- 特定通信用プロキシサーバ（プロキシ③）はシングル構成とすること。
- ②、④及び⑤のプロキシサーバは原則として冗長構成とすること。なお、上記構成で 1 台以上と記載したプロキシは冗長構成でなくともよい。
- 冗長構成をとる際に必要な機器等が存在する場合、調達に含めること。
- 動作に必要な OS やソフトウェアを必要数分用意すること。
- 本県職員がアクセスするにあたりストレスなく通信できるようにサイジングを行うこと。
- AD と連携し、利用者を特定することを目的としてユーザ認証（kerberos 認証等）を実施すること。また、AD のセキュリティグループを用いたフィルタリング制御を実施すること。
- 通信の復号化処理を実施できること。また、ホワイトリスト登録等により、FQDN や、ドメイン単位で復号化除外対象を指定できること。
- プロキシとして利用しているため PAC 等の調査も行い、最適な経路選択及び PAC ファイルとなるよう端末の通信経路の見直しを行うこと。
- プロキシサーバについて、Web 閲覧を行ったログを保存すること。ログには日時、ユーザ ID、クライアント IP アドレス、宛先 URL、カテゴリ、閲覧可否結果、ダウンロード/アップロードサイズ等を記録すること。また、Web 閲覧のログについて、ユーザ別、カテゴリ別等のヒット数を集計したうえで集計結果について、任意のユーザにメールにて送付できること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.7. ロードバランサ

7.2.7.1 プロキシ・メールサーバ用ロードバランサ

本調達で導入するプロキシサーバやメールサーバ等への負荷分散及び冗長構成を提供するため、ロードバランサを導入する。

要件は以下のとおり。

- 導入台数は 2 台以上とすること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえ

で協議を行うこと。

7.2.7.2 クラウド接続用ロードバランサ

クラウド接続を利用するシステムについて、ローカルブレイクアウトによる負荷分散を提供するため、ロードバランサを導入する。

要件は以下のとおり。

- 導入台数は2台とし、冗長構成とすること。
- 冗長構成をとる際に必要な機器等が存在する場合、調達に含めること。
- 設置場所はIDCとし、専用機器を用意して導入を行うこと。
- ロードバランサにより、以下の通信制御を行うこと。
  - 特定のクラウドサービス向けのトラフィックについては、セキュリティクラウド経由のインターネットを使わず、IDCから直接アクセスするネットワーク構成とすること。
  - 通信内容を識別し、予め登録されたクラウドサービスであれば指定の回線や情報セキュリティ基盤を利用できること。
  - 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
  - プロキシとして利用しているためPAC等の調査も行い、最適な経路選択及びPACファイルとなるよう端末の通信経路の見直しを行うこと。
  - 現在実装されている仕組みの変更や削除を行う場合、本県に説明のうえで協議を行うこと。

7.2.8. メール/DNS

メールサーバは、IDCに設置され、メール誤送信の防止機能、添付ファイルの分離機能、ウイルスチェック機能を提供するサーバである。

本県のメール/DNSは主に以下の要素で構成している。

- メールサーバ
  - 誤送信対策システムサーバ
  - 添付ファイル分離システムサーバ
  - メール用ウイルスチェックシステムサーバ
  - 内部メールサーバ
  - 外部メールサーバ
  - メールリレーサーバ
- DNSサーバ
  - 外部DNSサーバ
  - 内部DNSサーバ

本調達では、クラウドメールシステム（Exchange Online）に適したメールセキュリティの検討及び複雑化しているメール経路を整理し、障害ポイントの少ないメール経路の実現を想定している。また、DNS は名前解決環境が複雑化しており、各 DNS サーバの関係性の整理、統合を検討している。

メールセキュリティの検討及びメール経路の整理における要件を記載する。導入機器個別の要件については「9 構成要素の仕様」に記載する。

- 外部メールサーバと外部 DNS サーバが 1 つのサーバで稼働しているため、機能毎にサーバを用意し、構築すること。
- 現行のメールサーバにおける、送受信ルール等の制御設定について確認・整理し、必要な送受信ルールのみ移行すること。また、整理した条件をまとめた資料を整備すること。
- 過去の慣習により残存しているイレギュラーなメール運用として、旧ドメイン（pref.mie.jp）での外部からのメール送受信を行っており、将来的には廃止を予定しているため、本県と協議のうえ、方向性を決定すること。
- ＜提案＞可用性の向上及び構成簡素化の観点から、各メールサーバ機能の集約を検討しているため、最適な構成とすること。最終的な方針は本県と協議のうえで決定すること。ただし、上記の外部メールサーバと外部 DNS サーバは機能分割させること。現行のメール経路については「【別紙 6】現行メール構成図」を参照すること。
- インターネット及び LGWAN からのメール送受信を行うためにメール誤送信の防止機能、添付ファイルの分離機能、ウイルスチェック機能を提供するメールサーバの構築を行うこと。
- メール用ウイルスチェックサーバ、誤送信対策システムサーバ、添付ファイル分離サーバ、及びクラウドサービス間の配送方法は、SMTP スタティック配送を利用すること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。
- ウイルス検出の状況のログを保存すること。ログには日時、該当 URL、ウイルス名、処理結果等を記録すること。
- メールサーバについて、メール転送を行ったログを保存すること。ログには日時、送信元アドレス、宛先アドレス、転送先メールサーバ、ファイルサイズ、転送結果等を記録すること。

7.2.8.1 内部メールサーバ

内部メールサーバは、IDC に設置され、Exchange Online では対応できない仕組みを利用し、共用アドレスや庁内システムの送受信用のメールサーバを提供する。

要件は以下のとおり。

- 導入台数は 2 台以上とすること。

・ 認証ありのメールサーバ、認証なしのメールサーバの 2 種類をそれぞれ 1 台ずつ構築すること。
・ 認証ありのメールサーバについては、送信元ドメイン制限を実施すること。
・ 認証ありのメールサーバについては、LGPKI SSL 証明書を利用すること。
・ 利用端末から送信されたメールを受け付け、外部宛のメールはウイルスチェックサーバに転送し、内部宛のメールは該当のメールボックスに格納する。また、メール用ウイルスチェックサーバから転送された本県宛のメールを該当のメールボックスに格納し、利用端末からの POP アクセスにより各利用端末へ配送すること。
・ メール配送には、SMTP スタティック配送方法を利用すること。
・ ウイルスチェックサーバのメンテナンス等に備えて、外部へ送信するメール 1 週間分程度をローカルディスク、又は共有ディスクに保持できること。
・ 各利用端末から内部メールサーバへのメール配送は、認証付きの SMTP が利用できること。
・ システム等からのメールを処理するため、認証なしの SMTP が利用できること。ただし、送信元 IP アドレスにより、接続の制限が行えること。

7.2.8.2 外部メールサーバ

外部メールサーバは、IDC に設置され、セキュリティクラウド上のメールサーバから転送された本県宛のメール及び外部から転送された本県宛のメールの中継、インターネット宛メールをセキュリティクラウドメールサーバへ中継する役割を提供している。

本サーバは、機能集約し削減を検討しているものの、導入が必要な場合の要件は以下のとおり。

・ 導入台数は 2 台以上とすること。
・ インターネット/LGWAN から本県宛のメールを、メール用ウイルスチェックサーバへ転送すること。また、本県から外部宛のメールをメール誤送信対策サーバから受け取り、インターネット/LGWAN へ送信すること。
・ メールの配送方法は冗長性等を考慮し、最適な設定とすること。現状、インターネットからのメール配送はスタティック配送、LGWAN からのメール配送は MX 配送を利用している
・ メールボックスは保持しないこと。
・ RFC 非準拠のメールに対しても送受信できるよう設計すること。
・ 宛先に応じて転送先をインターネットと LGWAN に振り分けている。現状、LGWAN へメールを送信する場合、特殊なメール運用を行っているため、本県と協議のうえ、振り分けに関する設定を決定すること。
・ 後方錯乱メール（Backscatter）対策のため、添付メールの件名に特定の文字列を含むメールを破棄できること。

7.2.8.3 DNS サーバ

DNS の整理における要件を記載する。なお、導入機器個別の要件については「9 構成要素の仕様」に記載する。

内部/外部 DNS サーバはそれぞれ以下の機能を提供している。

- 外部 DNS は主に外部からの名前解決応答用として、pref.mie.lg.jp 及び pref.mie.jp のゾーン管理を行う。

内部 DNS は、主に三重県行政 WAN 内部で使用しているドメイン（mieken.jp、lgwan.local 等）のゾーン管理を行う。

要件は以下のとおり。

- 設計にあたり、各 DNS サーバの役割と機能を明確化すること。また、フォワーダ設定については通信フローと業務内容の関係性を整理した後、実装すること。
- 導入台数は外部 DNS サーバ及び内部 DNS サーバ各 2 台以上とすること。
- セキュリティクラウドの DNS と連携するためのマスタサーバとして、外部 DNS サーバを構築すること。なお、本業務で導入する外部 DNS サーバをマスタとして、セキュリティクラウドで導入する外部 DNS サーバにゾーン情報等を転送し、外部からの名前解決に応答しているため、現行と同様の機能を担保すること。なお、セキュリティクラウドで導入する外部 DNS サーバについても同時期に更改を予定しているため、次期セキュリティクラウド受託事業者と主体的に連絡、調整し、円滑に移行作業を実施すること。現行の DNS 構成については「【別紙 7】現行 DNS 構成図」を参照すること。
- 三重県行政 WAN 内部からの要求に対して名前解決を行うキャッシュサーバとして内部 DNS サーバを構築すること。
- 各 DNS サーバはマスタ/スレーブの設定等により冗長性等を確保すること。
- 外部 DNS サーバはメールサーバの分離を検討し、本県と協議のうえで方針を決めること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.9. 全庁ファイルサーバ

本県の全庁ファイルサーバは以下の要素で構成している。

- 全庁ファイルサーバ（インターネット接続系）
- 全庁ファイルサーバ（LGWAN 接続系）

本調達における全庁ファイルサーバ（インターネット接続系）は、各部局で個々に調達・管理しているNASやストレージ等を可能な限り一元的に集約し、統合管理によるセキュリティ強化及びバックアップによる耐障害性の向上を図るため、導入するものである。また、β’モデルに移行したことにより、全庁ファイルサーバ（LGWAN接続系）は、現行の容量では過剰のため、実際の運用にあわせた容量を導入すること。

全庁ファイルサーバにおける要件を記載する。なお、導入機器個別の要件については「9 構成要素の仕様」に記載する。

- ファイルサーバを整備し、統制された適切な場所にデータを保存できるようにすること。また、ファイル授受システムでファイルの交換ができるようにすること。
- オンプレミス型ファイルサーバは、ランサムウェアへの対策等のセキュリティ対策を検討すること。
- 全庁ファイルサーバの構成や設定により、業務継続性を担保すること。
- データのバックアップは筐体内バックアップで実装すること。ただしRAID構成やホットスペアを用いることで耐障害性の確保した構成とすること。

7.2.9.1 全庁ファイルサーバ（インターネット接続系）

全庁ファイルサーバ（インターネット接続系）は、本県職員が庁内でファイル保管を行うファイルサーバであり、各所属のフォルダを提供するシステムである。

要件は以下のとおり。

- 導入台数は1台以上とすること。
- オンプレミス型ファイルサーバとして導入する場合は、IDCに設置すること。
- オンプレミスで構築する場合は、筐体内バックアップ構成とすること。
- 全庁ファイルサーバは、原課NASやストレージ等を可能な限り一元的に集約し、統合管理によるセキュリティ強化及びバックアップによる耐障害性の向上を実現するものである。実現方法について移行及び運用の観点を含めて設計と構築を行うこと。
- 現行機器からのデータ移行設計を実施したうえで、データ移行作業を実施すること。ただし、移行時に容量不足の見込みがある場合は、本県と協議のうえで、設計時に割り当てる容量を見直しすること。
- 全庁ファイルサーバは、三重県行政WANの全拠点から、共有ファイルが読み書きされることを想定し、適切な性能・セキュリティ設計を実施すること。
- 1日あたり複数回のバックアップ取得を行うこと。取得回数及び時間については本県と協議のうえ、決定すること。夜間にバックアップを実施する等、ネットワーク機器・回線への負荷が、業務やバッチ処理に影響を与えないよう考慮すること。
- ストレージ容量が不足した際、ディスクの増設のみで実行容量500TBまで追加することが可能な設計とすること。

・ 各フォルダは、必要なアクセス権限やセキュリティポリシーの適用を行うこと。アクセス設計については本県と協議のうえで決定すること。
・ アクセス制限については庁内 AD と連携し、運用部分も含めて設計を行うこと。
・ 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
・ 現在実装されている仕組みの変更や削除を行う場合、本県に説明のうえで協議を行うこと。

7.2.9.2 全庁ファイルサーバ（LGWAN 接続系）

全庁ファイルサーバ（LGWAN 接続系）は、本県職員が庁内の LGWAN 接続系にて、ファイル保管を行うファイルサーバである。

要件は以下のとおり。

・ 導入台数は 1 台以上とすること。
・ オンプレミス型ファイルサーバとすること。
・ 全庁ファイルサーバ（LGWAN 接続系）は、本庁舎に設置すること。
・ オンプレミスでの筐体内バックアップ構成とすること。
・ LGWAN 接続環境にて、共有ファイルの読み書きを想定し、適切な性能・セキュリティ設計を実施すること。
・ 現行機器からのデータ移行設計を実施したうえで、データ移行作業を実施すること。ただし、移行時に容量不足の見込みがある場合は、本県と協議のうえで、設計時に割り当てる容量を見直しすること。
・ 1 日あたり複数回のバックアップ取得を行うこと。取得回数及び時間については本県と協議のうえ、決定すること。夜間にバックアップを実施する等、ネットワーク機器・回線への負荷が、業務やバッチ処理に影響を与えないよう考慮すること。
・ ストレージ容量が不足した際、ディスクの増設のみで実行容量 500TB まで追加することが可能な設計とすること。
・ 各フォルダは、必要なアクセス権限やセキュリティポリシーの適用を行うこと。アクセス設計については本県と協議のうえで決定すること。
・ アクセス制限については庁内 AD と連携し、運用部分も含めて設計を行うこと。
・ 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
・ 現在実装されている仕組みの変更や削除を行う場合、本県に説明のうえで協議を行うこと。

7.2.10. ファイル授受システム

外部及び庁内における安全なファイル授受を実現するため、ファイル授受システムを実装している。本県のファイル授受システムは以下のサブシステムで構成している。

- ファイル交換システム（外部共有）
- LGWAN 用ファイル転送システム（INT-LGWAN）
- ファイル無害化システム

ファイル授受システムの設計及び構築に関する要件を記載する。導入機器個別の要件については「9 構成要素の仕様」に記載する。

7.2.10.1 ファイル交換システム（外部共有）

ファイル交換システム（外部共有）は、本県職員と外部関係者（各受託事業者や県民等）が安全に大容量のファイルを交換するためのシステムである。

要件は以下のとおり。

- 導入台数は 1 台以上とすること。
- 県庁外のユーザ（事業者や県民等）と大容量のファイルをやり取りするためのシステムを構築すること。
- ファイル交換システムの利用者総数は、7,500 ユーザとし、1 ユーザの利用容量を 10GB として 1,000 ユーザが同時利用可能であること。
- 想定する送信方法は以下のとおり。
  ① 本県職員がファイル交換システム上にファイルをアップロードし、その URL を取得する。
  ② URL をメール等にて外部関係者に送付し、外部関係者がその URL からファイルをダウンロードする。
- 想定する受信方法は以下のとおり。
  ① 本県職員がファイル交換システム上にフォルダ等のファイルの保存場所を作成し、その URL を取得する。
  ② URL をメール等で外部関係者に送付し、外部関係者がファイルをアップロードする。
  ③ アップロード後に、本県職員にメール等で速やかに通知され、ファイルをダウンロードする。
- ファイルのアップロード時に、ファイルにパスワードの入力を必要とする設定が可能であること。
- ファイル交換システムの利用状況の可視化や監視の仕組みを提供すること。
- ファイルの保存期間を設定できること。また、1 週間以上保存できること。
- 本システムを単体として構築する場合、後述のファイル無害化システムと連携して、ファイルの安全性をチェックできる構成とすること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。

・ 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.10.2 LGWAN ファイル転送システム（INT-LGWAN）

LGWAN ファイル転送システム（INT-LGWAN）は、インターネット接続系と LGWAN 接続系の間のファイル交換を実現するためのシステムである。

要件は以下のとおり。

・ 導入台数は 1 台以上とすること。
・ 自治体分離におけるインターネット接続系と LGWAN 接続系でファイル交換を行うシステムを構築すること。
・ 後述のファイル無害化システムと連携し、ファイル無害化及びマルチスキャン後にファイル交換を行う構成とすること。
・ 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
・ 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.10.3 ファイル無害化システム

ファイル無害化システムは、本県職員が外部関係者（各受託事業者や県民等）とファイルの受け渡しをする際及び庁内のインターネット接続系と LGWAN 接続系間でファイルを受け渡しする際に、ファイルの無害化及びマルチスキャンを行うシステムである。

要件は以下のとおり。

・ 導入台数は 1 台以上とすること。
・ ファイルの安全性をチェックし、危険なファイルは無害化もしくは危険と判断して、ブロックするためのシステムを構築すること。前述のファイル交換システム及び LGWAN ファイル転送システムと連携が可能なこと。
・ 現状の設定内容を精査し、既存で提供しているサービスが継続して、提供可能な構成とすること。
・ 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.11. LGWAN 接続システム

現行ネットワークでは、仮想基盤に構築された RDSH（SBC）方式及び一部 VDI 方式により、インターネット接続系及びテレワーク系と LGWAN 接続系を仮想的に分離している。次期ネットワークでは上記の分離方式から、セキュアコンテナにより、インターネット接続系端末内に隔

離領域を構築し、端末内でインターネット接続系と LGWAN 接続系を分離させる方式へ移行する。LGWAN 接続系ネットワーク上に、LGWAN への接続を中継させるゲートウェイサーバを構築し、セキュアコンテナ方式による隔離領域からのみアクセス可能となるようアクセス制御を行う。なお、導入機器個別の要件については「9 構成要素の仕様」に記載する。

LGWAN 接続システム環境は、インターネット接続系の職員端末から LGWAN 接続系の環境を安全に利用するための環境である。

要件は以下のとおり。

- 同時接続数は 200 とし、それに必要なコンポーネントを導入すること。
- ゲートウェイサーバは専用サーバ（専用アプライアンス含む）を用意して導入を行うこと。
- サンドボックス型セキュリティソフトウェアにより、安全にファイルを閲覧、編集するための隔離領域を作成すること。
- 自治体分離のβ’モデル構成において LGWAN 接続系のブラウジングやファイルサーバへのアクセス、ファイルサーバ上のファイル編集等を行うこと。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して、提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。
- 同時接続数の追加が可能な拡張性を有すること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して提供可能な構成とすること。
- LGWAN 接続システムを利用するにあたって、インターネット接続系の職員端末へ必要なアプリケーション等を展開すること。

7.2.12. 防災ネットワーク

7.2.12.1 防災ネットワーク及び接続サービスの概要

本県では、大規模災害等の発生により主回線を経由したインターネット接続ができなくなった場合に備え、防災関連システム等の許可された一部のインターネットサービスに対して本庁舎から直接接続可能な環境を整備している。

防災ネットワークで提供している機能は以下のとおり。

- 本庁舎、各総合庁舎等の県内防災拠点を、有線系、地上系（無線）、衛星系の 3 系統の回線で接続させている。
- 本庁舎から、4 経路のインターネット回線（法人向けインターネット接続回線、固定光回線(B フレッツ)、携帯電話回線(LTE)、衛星回線(PLANET-BB)）が接続され、防災ネットワーク全体のインターネット接続口として利用している。特定の業務端末がインターネットへ接続可能となるよう、災害時プロキシサーバを

使用している。

・ インターネット接続時、災害時ファイアウォールを使用し、簡単な Web 通信に対するセキュリティ対策（アンチウイルス、IPS 機能を利用する等）を実施している。なお、防災ネットワークの概要は「図 7-2 防災ネットワーク構成概要」のとおり。

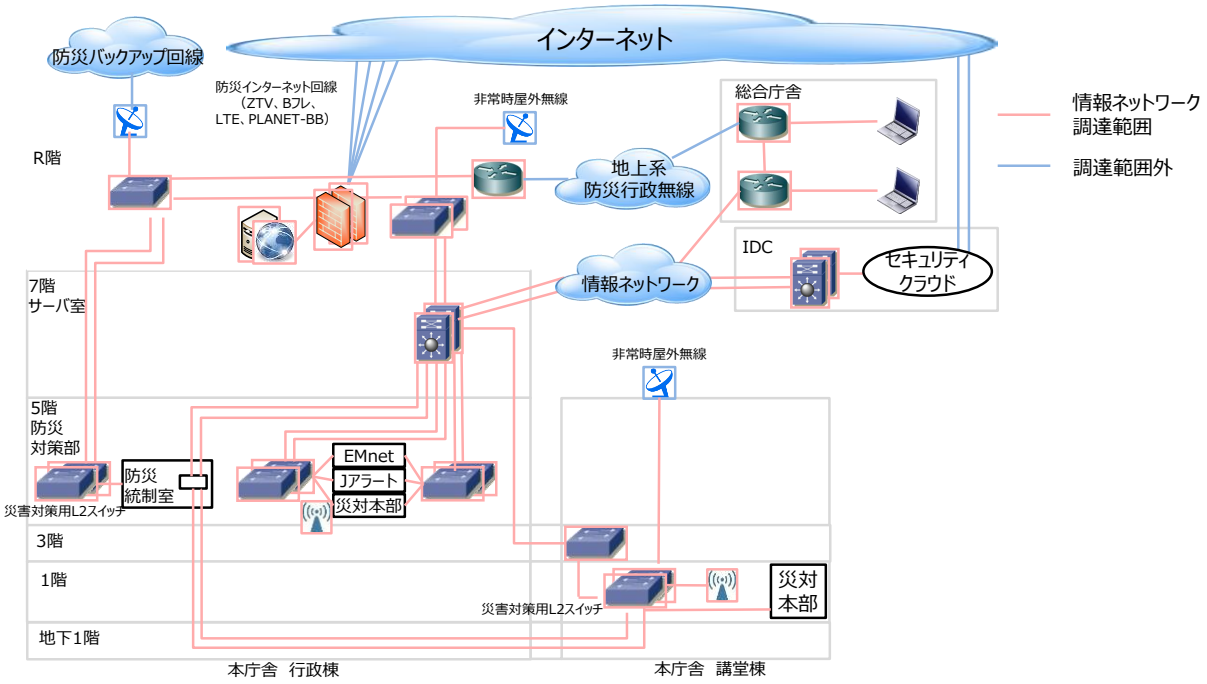

図 7-2 防災ネットワーク構成概要

7.2.12.2 防災用インターネット接続

災害発生時には、防災情報システム（クラウドサービス）の情報更新を職員がインターネット経由で行う等、インターネット接続が必須となるが、災害等の影響により、主回線、IDC 及びインターネット回線が損傷を受けた場合、インターネットへのアクセスが不能となるリスクが存在する。

このリスクを軽減するため、別調達にて導入している、本庁舎の防災ネットワーク内にあるインターネット回線（以下、「防災用インターネット回線」という。）を利用し、災害時に本庁舎からインターネットへ接続可能な構成としている。なお、防災用インターネット接続の概要は「図 7-3 防災用インターネット接続フロー」のとおり。

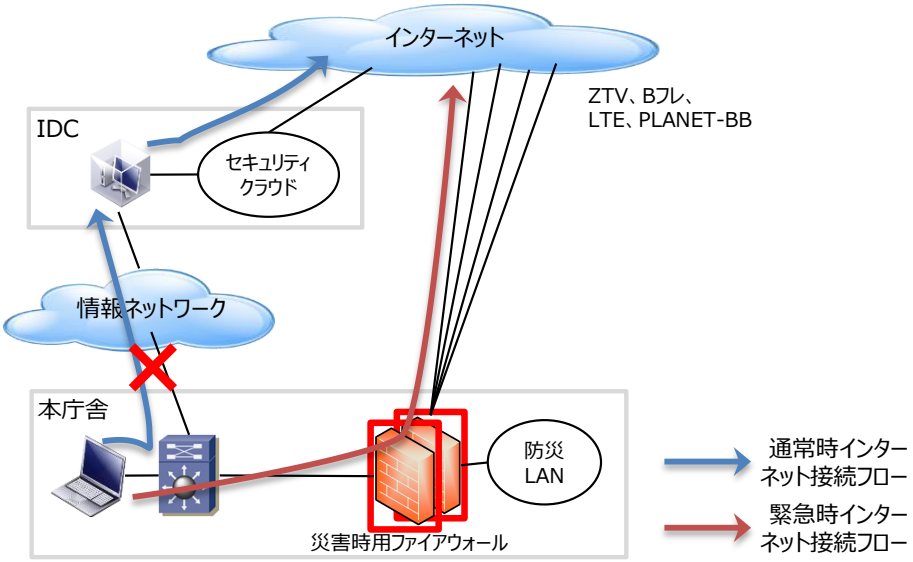

図 7-3 防災用インターネット接続フロー

要件は以下のとおり。

- 災害発生時、防災用インターネット回線を通じ、インターネットへ接続可能な構成とすること。
- インターネット接続時は、後述の災害時用プロキシサーバ及び災害時用ファイアウォールを経由するよう設計すること。

7.2.12.3 災害対策本部通信の多重化

大規模災害等の発生時、本庁舎 5 階防災対策部又は講堂棟 1 階において、三重県災害対策本部が設置される。災害対策本部は、本県内外との災害等に関する情報収集・発信の場となることから、様々なケースを想定し、本庁舎 5 階及び講堂棟 1 階のネットワークの可用性を高め、通信経路の多重化を行っている。

通信経路の多重化に係る要件は以下のとおり。

- 本庁舎基幹コア L3 スイッチから講堂棟内災害対策本部間は、以下に記載する 3 系統のルートによる経路冗長化を実施すること。
  - ➢ 行政棟 7 階サーバ室から講堂棟 3 階を直接接続するルート
  - ➢ 行政棟 5 階防災統制室、地下 1 階を経由して講堂棟 1 階へ接続するルート
  - ➢ 行政棟から講堂棟間の非常時用屋外無線 LAN を利用するルート
- 他の既存ネットワーク設計に可能な限り影響を与えることなく、3 系統のルートの優先順位及び切り替え方式を設計し、それぞれのルートが個別に切断されても他のルートで講堂棟災害対策本部向けの通信が途絶しないようにすること。

7.2.12.4 防災行政無線（本庁舎と総合庁舎間の接続）

災害発生時、主回線が損傷し拠点間の疎通が不可能となった場合、防災行政無線を利用し、本庁舎と総合庁舎間で必要最低限の通信が可能な設計としている。なお、防災行政無線による通信バックアップの概要は「図 7-4 防災行政無線接続フロー」のとおり。

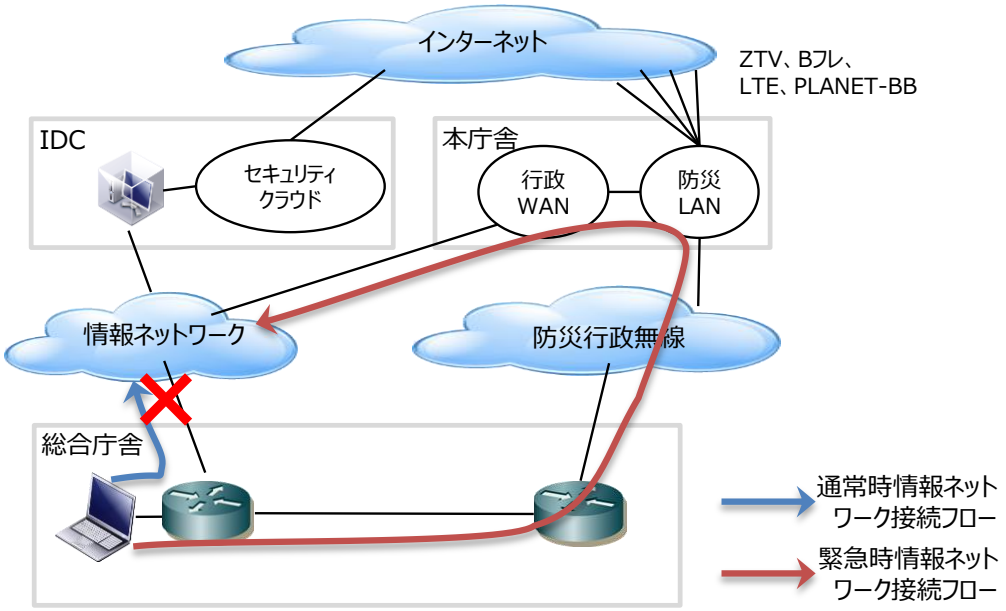

図 7-4 防災行政無線接続フロー

要件は以下のとおり。

- 本庁舎及び総合庁舎において、主回線、バックアップ回線ともに障害が発生し、通信ができなくなった際は、防災行政無線を利用し、三重県行政 WAN 内から継続して通信が可能となるよう、本県及び防災行政無線工事受事業者と調整し、必要な設計・設定情報の開示等の各種調整を行うこと。
- 本庁舎及び総合庁舎内において、三重県行政 WAN と防災行政無線の境界線に災害時用ルータを設置すること。
- 災害時用ルータについては、本庁舎及び総合庁舎内の行政端末が、防災行政無線経由でインターネットへ接続可能となるよう、ルーティング及び帯域制御機能を提供するよう設計すること。
- 防災行政無線を利用して通信を行う場合、不要なトラフィックが防災行政無線のネットワーク帯域を占有するおそれがある。そのため、本県及び防災行政無線工事受注事業者と調整のうえ、適切な帯域制御設定を設計し、必要最小限の通信のみが防災行政無線上を流れるようにすること。

7.2.12.5 災害時用プロキシサーバ

災害時用プロキシサーバは、災害時に、許可された一部のインターネットサービスに対して、本庁舎から直接接続する際に利用されるプロキシサーバである。

要件は以下のとおり。

- 導入台数は 2 台とすること。
- 設置場所は本庁舎サーバ室とし、専用の物理サーバ（専用アプライアンス含む）を用意して導入を行うこと。
- 防災関連ネットワーク利用時、インターネット通信時に利用するプロキシサーバを構築すること。
- 災害時用プロキシサーバの利用数は 1,000 とすること。
- プロキシとして利用しているため PAC 等の調査も行い、最適な経路選択及び PAC ファイルとなるよう端末の通信経路の見直しを行うこと。
- 本サーバの電源は同ラック内に設置する UPS へ収容し、停電時に非常用電源へ切り替わるまでの約 10 分間電源断が起こらないよう構成すること。
- 本サーバの筐体上に災害時用 Radius サーバをあわせて構築すること。
- 業務端末のプロキシ接続先を容易（ボタン等）に通常時から災害時用プロキシに切り替えが可能な仕組みを実装すること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して、提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.12.6 災害時用ファイアウォール

災害時用ファイアウォールは、災害時に、許可された一部のインターネットサービスに対して、本庁舎から直接接続する際に利用されるファイアウォールである。

要件は以下のとおり。

- 導入台数は 2 台とし、冗長構成とすること。
- 設置場所は本庁舎 R 階無線機器室とし、専用機器を導入すること。
- 防災関連ネットワーク利用時、インターネット通信時の通信制御を行うこと。
- 新規システムの導入や構成変更についても原則としてセキュリティポリシーを踏襲しつつ、必要な設計変更は本県と協議のうえで実施すること。
- 現状の設定内容を精査し、既存で提供しているサービスが継続して、提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.12.7 災害時用 Radius サーバ

災害時用 Radius サーバは、災害時に使用する防災用 SSID の認証を行う Radius サーバである。

要件は以下のとおり。

- 導入台数は 2 台とすること。
- 災害時用プロキシサーバと同一の物理サーバ上に構築すること。
- 主回線を経由したインターネット接続が切断された際、防災 SSID の認証が可能なように構築すること。
- 認証方式は PSK 認証のみとし、常時ステルスで有効化状態とする構成で設計、構築、テストを実施すること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.2.12.8 災害時バックアップ回線（衛星回線）

災害時バックアップ回線は、災害が発生し通常の回線が切断された際に利用する回線である。回線そのものについては、別調達にて可搬型の衛星回線（StarLink）を調達済みである。衛星回線接続用機器は本庁舎及び総合庁舎に各 1 基ずつ配備されるため、本調達では StarLink を利用しインターネットに接続可能な環境を構築する必要がある。

要件は以下のとおり。

別調達で導入する StarLink を利用し、インターネット接続が可能な環境を構築すること。

設計、構築の範囲は、庁内ネットワークから StarLink を収容するスイッチまでとする。

- StarLink を収容するスイッチについては、契約後本県と協議し決定すること。
- StarLink は有線で利用せず、無線での利用を予定している。StarLink 利用時の専用 SSID を新たに作成すること。
- 専用 SSID の認証は PSK 認証のみとし、常時ステルスで有効化状態とする構成で設計、構築、テストを実施すること。
- 専用 SSID が利用可能なエリア、及び専用 SSID を使用する対象の無線 LAN アクセスポイントについては、設計時に本県と協議のうえ、決定すること。
- 専用 SSID を使用する無線 LAN アクセスポイントの管理通信は主回線側を利用すること。
- 災害により、無線 LAN アクセスポイントと無線 LAN コントローラ間の疎通がとれない状態でも利用が可能な設計、環境を構築すること。
- 新規のインターネット接続環境となるため、既存通信に影響が発生しないようにネットワーク設計を行うこと。必要に応じて新規 VLAN の作成、ルーティングテーブルの分割等を行うこと。

7.2.13. ネットワーク可視化

ネットワーク障害時の早急な原因切り分けや、機器やシステムの死活、サービス状態、リソース状態、トラフィック監視を行うため、新たにネットワークを可視化する環境を整備する。

- 以下の拠点へ導入することを想定している。
  - IDC
  - 本庁舎
  - 総合庁舎
  - 単独地域機関
- LAN/WAN を問わず、通信経路上の機器及び経路間のトラフィックを GUI で確認でき、ネットワークのボトルネック箇所が特定できるシステムを導入すること。
- プロキシを境界として内部/外部問わずネットワーク可視化を実行できる構成すること。必要に応じて専用のコンポーネントを設置すること。
- 業務端末にエージェントソフトをインストールする場合は、適切な監視範囲を検討し、必要な端末にインストールすること。
- 障害ポイントの即時発見、障害切り分けのための情報収集に利用が可能となるよう、管理者へのアラート・通知機能を設定すること。
- 設計及び運用方針は本県と協議のうえで決定すること。

7.2.14. その他

本項目では各システムの導入において必要となる UPS 及び OS についての要件を記載する。

OS は構成により種類や数量が異なるため、「9 構成要素の仕様」を確認のうえ、準備を行うこと。本県が提供可能なリソースは、共通仕様書の「4. 本県所有のライセンスに関して」を参照すること。

UPS は本庁舎や総合庁舎等において、重要なネットワーク機器やサーバの電源を一時的に供給する装置である。

要件は以下のとおり。

- 導入機器に応じて、以下要件を満たすものを選定すること。
- 稼働期間は以下とする。
  - 開始：既存機器を撤去し、本調達で導入した機器がサービス提供を行うタイミング
  - 終了：次期調達で本機器が撤去されたタイミング（令和 14 年 1 月から 3 月頃を予定）
- 稼働時間として、商用電源からの電力提供がなくなってから 10 分以上の稼働を担保すること。
- UPS の対象は以下とする。各 UPS は対象機器の消費電力に合わせ、電源容量に過不足

が無いよう構築すること。

- 基幹コア L3 スイッチ(本庁舎)
- 拠点コア L3 スイッチ(総合庁舎 10 拠点 + 吉田山会館)
- 拠点コア L3 スイッチ(アスト津/シングル構成)
- 拠点コア L3 スイッチ(教育センター/シングル構成)
- サーバ接続用スイッチ(本庁舎/1G)
- 全庁ファイルサーバ（LGWAN 接続系）の本庁舎設置分
- 災害時用ルータ（本庁舎）
- 災害時用プロキシサーバ
- 災害時用ファイアウォール

・ その他要件は「9.13 その他」を参照すること。

7.3. 拠点別構築要件

回線との接続、機器の冗長化有無等、拠点毎に異なる構築要件について、以下に記載する。

7.3.1. IDC

7.3.1.1 機器及びネットワーク構成

有線ネットワークを構築するうえで各コンポーネントの構成に求める要件は以下のとおり。

- 基幹コア L3 スイッチ
  - 2 台以上のスイッチで冗長構成とすること。
  - 主回線、バックアップ回線を収容すること。
- サーバ接続用スイッチ（10G）
  - 2 台以上のスイッチで冗長構成とすること。
  - 基幹コア L3 スイッチへ接続すること。
- サーバ接続用スイッチ(1G)
  - 2 台以上のスイッチで冗長構成とすること。
  - 基幹コア L3 スイッチへ接続すること。
- 基幹ファイアウォール
  - 2 台×2 以上の機器で冗長構成とすること。
  - 基幹コア L3 スイッチ又はファイアウォール接続用スイッチ（24 ポート）へ接続すること。
- ファイアウォール接続用スイッチ（24 ポート）
  - ファイアウォールを収容する基幹スイッチのため、3 台以上の機器で冗長構成とすること。
  - 基幹コア L3 スイッチへ接続すること。

・ 基幹ファイアウォールを接続すること。

- Web 会議回線接続用ルータ
  - ・ Web 会議システム等の通信をブレイクアウトしている Web 会議用回線を収容し、ルータ集約スイッチへ接続すること。ルータ本体の機器仕様については「9.2.16 単独地域機関接続用ルータ」に従うこと。
- VPN 集約ルータ
  - ・ 3 台以上のルータで冗長構成とすること。
  - ・ 単独地域機関向けのインターネット VPN 回線、閉域網回線を収容すること。
  - ・ ルータ接続スイッチを介して基幹コア L3 スイッチへ接続すること。
- ルータ集約スイッチ
  - ・ Web 会議回線接続用ルータ及び VPN 集約ルータへ接続させること。
  - ・ 基幹コア L3 スイッチへ接続すること。

・ 機器の接続に関しては、高い信頼性や可用性を確保すること。調査のうえで現行ネットワークから構成の変更や削除を行う場合、背景を本県に説明のうえで協議を行い決定すること。

・ 必要に応じて本県が保有する共通機能基盤上へのシステム（仮想マシン）の設計と構築を行うこと。

・ 機器は本県の指定する IDC 内のラックを使用すること。設置に関する要件は以下のとおり。

- ラックの規格は H2,000mm×W600mm×D900mm(35U)である。現状の空きユニット数については「2.5 本県からの提供資料」で開示する資料を参照すること。
- 利用できる電源容量は、1 ラックあたり 100V、20A までとする。
- 移行時に並行稼働ができるよう、必要に応じて追加のラックスペースや電源容量を確保すること。その際に必要となる費用については、受託事業者の負担とする。安定稼働が確認できた場合、並行稼働は不要とするため、移行手順を踏まえ、必要な期間の費用を見込むこと。
- ラック間の配線は、IDC 事業者が実施するため、作業費用については、受託事業者が負担すること。
- ラック間の配線は、申請から実施まで 1 カ月程度を要するため、余裕をもって設置計画を立てること。

7.3.1.2 各種インターネット上流回線との接続

・ 現行ネットワークにおいて接続している各種インターネット接続回線を継続して、利用できるようにすること。

・ 回線構成や用途は多岐にわたるため、既存図書や機器の設定内容を十分に調査

し、更新後に他システムへの影響が出ないように更新を行うこと。
・ 新規導入するシステムでインターネット接続が必要となるシステムが問題なく稼働できる構成とするため、必要に応じて再設計や構成の変更を行うこと。

7.3.1.3 主回線との接続

・ 現行ネットワークにおいて接続している主回線（5Gbps×2 回線）を、継続して利用できるようにすること。
・ 主回線に対して冗長化した接続とすること。
・ 主回線を利用した通信については、タグ VLAN、拡張タグ VLAN 等を利用しているため、継続して利用できるようにすること。バックアップ回線への切り替わりについてもこの点を考慮して設計すること。

7.3.1.4 バックアップ回線との接続

・ 主回線に係る障害が発生し、他の拠点と通信ができなくなった際、主回線からバックアップ回線に切り替え、継続して通信が可能となるようにすること。
・ バックアップ回線で利用する VLAN については、本県と協議のうえで決定すること。
・ 主回線からバックアップ回線への切り替えは自動で行われるようにすること。また、切り替わり、切り戻しともに 5 分以内となるようにすること。

7.3.1.5 単独地域機関の接続

・ 現行ネットワークにおける単独地域機関との通信については、IDC に設置している VPN 集約ルータを用い、インターネット経由での暗号化通信により接続している。本構成を継続して利用できること。
・ 単独地域機関のうち、インターネット VPN で接続する拠点との接続には、十分に安全と考えられる暗号化方式等を利用することにより、現行と同等以上のセキュリティを確保すること。
・ 単独地域機関のうち、インターネット VPN で接続する拠点との接続を収容する VPN 集約ルータは、IDC に 3 台以上設置し、1 台の機器に障害が発生した際も、別の機器で接続が継続できるようにすること。
・ 今後全ての単独地域機関へ無線 LAN アクセスポイントを展開できるよう、回線仕様によらず、複数の VLAN が利用可能な構成とすること。
・ LGWAN 接続系やマイナンバー利用事務系を利用する可能性があるため、拠点間で共通の VLAN を利用することは禁止とする。必ず拠点毎に個別の VLAN を使用し、LGWAN 接続系やマイナンバー利用事務系が論理的に分割可能な設計とするこ

と。構成の例を以下の「図 7-5 拠点間 VLAN 論理分割例」へ記載する。設計時にポート数の不足が懸念される場合は、本県の用意する HUB を利用すること。

・ なお、単独地域機関とルータ間の接続要件の詳細については「7.3.1.5 単独地域機関の接続」を参照すること。

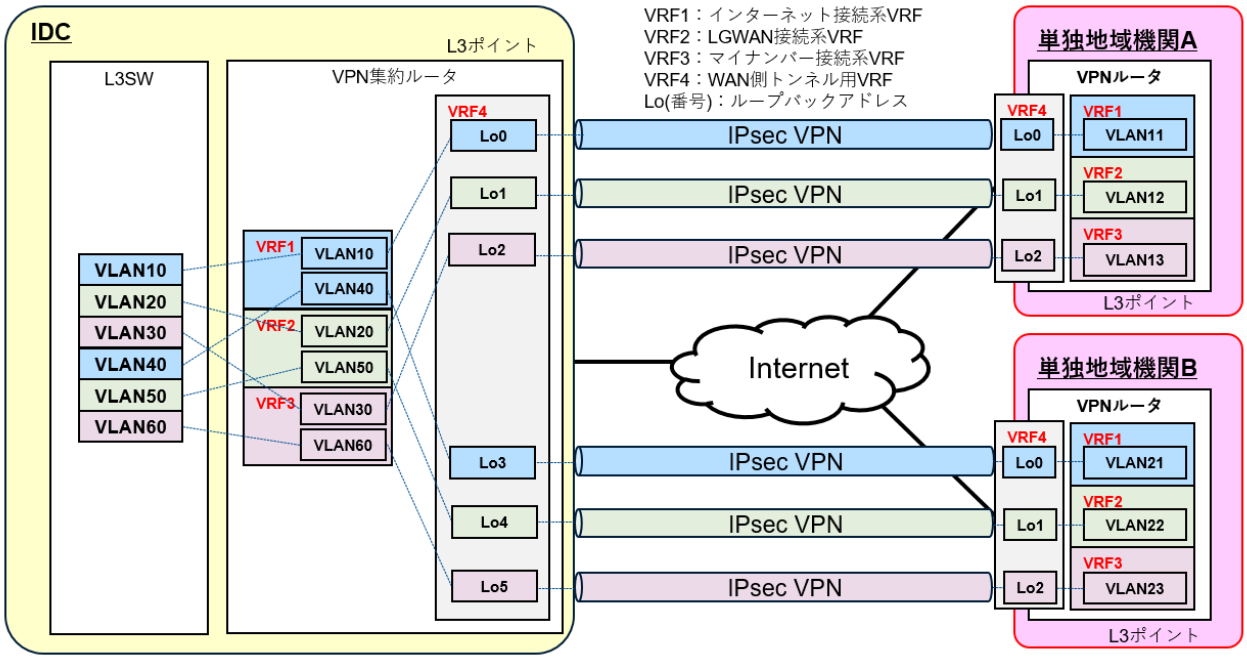

図 7-5 拠点間 VLAN 論理分割例

7.3.2. 本庁舎

7.3.2.1 機器及びネットワーク構成

有線ネットワークを構築するうえで各コンポーネントの構成に求める要件は以下のとおり。

- 基幹コア L3 スイッチ
  - 2 台以上のスイッチで冗長構成とすること。
  - 主回線、バックアップ回線を収容すること。
- サーバ接続用スイッチ(1G)
  - 2 台以上のスイッチで冗長構成とすること。
  - 基幹コア L3 スイッチへ接続すること。
- フロア L2 スイッチ（24/48 ポート）
  - 冗長化は行わずシングル構成とすること。
  - 基幹コア L3 スイッチへ接続すること。

機器の接続に関しては、高い信頼性や可用性を確保すること。調査のうえで構成の変更

や削除を行う場合、背景を本県に説明のうえで協議を行い、決定すること。

7.3.2.2 主回線との接続

- 現行ネットワークにおいて接続している主回線（5Gbps×2 回線）を、継続して利用できるようにすること。
- 主回線に対して冗長化した接続とすること。
- 主回線を利用した通信については、タグ VLAN、拡張タグ VLAN 等を利用しているため、継続して利用できるようにすること。バックアップ回線への切り替わりについてもこの点を考慮して設計すること。
- 現行の光ケーブルを利用し、本庁舎の基幹コア L3 スイッチと吉田山会館の拠点コア L3 スイッチを接続すること。

7.3.2.3 バックアップ回線との接続

- 主回線に係る障害が発生し、他の拠点と通信ができなくなった際、主回線からバックアップ回線に切り替わり、継続して通信が可能となるようにすること。
- バックアップ回線で利用する VLAN については、本県と協議のうえで決定すること。
- 主回線からバックアップ回線への切り替えは自動で行われるようにすること。また、切り替わり、切り戻しともに 5 分以内となるようにすること。

7.3.2.4 防災対策用 L2 スイッチの接続

防災ネットワークを構築するうえで、防災対策用の役割を持った L2 スイッチを複数設置する必要がある。各防災対策用 L2 スイッチに求める要件は以下のとおり。なお、機器要件については全て「9.2.14 L2 スイッチ（48 ポート)」に従うこと。

- ➢ 講堂棟災害対策本部用 L2 スイッチ
- 災害発生時に災害対策本部が設置される講堂棟までの通信を確保するため、本庁舎講講堂棟 1 階に設置すること。
- 3 台以上のスイッチにより冗長構成とすること。
- 本庁舎講堂棟 3 階設置のフロアスイッチを経由して基幹コア L3 スイッチと接続すること。

- ➢ 行政 WAN-防災 LAN 間 L2SW
- 7 階サーバ室の行政 WAN と R 階内防災ネットワークとを接続するため、本庁舎行政棟 R 階無線機器室に設置すること。
- 2 台以上のスイッチで冗長構成とすること。
- 災害時用ファイアウォール、基幹コア L3 スイッチ、非常時用屋外無線 LAN を本

スイッチへ接続すること。

- ➢ 防災対策本部 L2SW
- ・ 本庁舎行政棟 5 階防災統制室へ設置すること。
- ・ 2 台以上の冗長構成とすること。
- ・ 基幹コア L3 スイッチへ接続すること。

7.3.2.5 防災行政無線との接続

- ・ 防災行政無線の収容機器と災害時用ルータを接続すること。
- ・ 災害時用ルータと基幹コア L3 スイッチを接続すること。

7.3.2.6 災害時バックアップ回線（衛星回線）との接続

- ・ 災害時バックアップ回線の衛星回線接続用機器を本調達で導入する機器へ接続すること。
- ・ 現状の設定内容を精査し、災害発生時に災害時バックアップ回線を通じて既存で提供しているサービスが継続して提供可能な構成とすること。
- ・ 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.3.3. 総合庁舎

7.3.3.1 機器及びネットワーク構成

有線ネットワークを構築するうえで各コンポーネントの構成に求める要件は以下のとおり。

- ➢ 拠点コア L3 スイッチ
  - ・ 2 台以上のスイッチで冗長構成とすること。
  - ・ 主回線、バックアップ回線を収容すること。
- ➢ フロア L2 スイッチ（24/48 ポート）
  - ・ 冗長化は行わずシングル構成とすること。
  - ・ 拠点コア L3 スイッチへ接続すること。
- ・ 機器の接続に関しては、高い信頼性や可用性を確保すること。調査のうえで構成の変更や削除を行う場合、背景を本県に説明のうえで協議を行い決定すること。

7.3.3.2 主回線との接続

- 現行ネットワークにおいて接続している主回線を、継続して利用できるようにすること。
- 主回線を利用した通信については、タグ VLAN、拡張タグ VLAN 等を利用しているため、継続して利用できるようにすること。バックアップ回線への切り替わりについてもこの点を考慮して設計すること。

7.3.3.3 バックアップ回線との接続

- 主回線に係る障害が発生し、他の拠点と通信ができなくなった際、主回線からバックアップ回線に切り替え、継続して通信が可能となるようにすること。
- バックアップ回線で利用する VLAN については、本県と協議のうえで決定すること。
- 主回線からバックアップ回線への切り替えは自動で行われるようにすること。また、切り替わり、切り戻しともに 5 分以内となるようにすること。

7.3.3.4 防災行政無線との接続

- 防災行政無線の収容機器と災害時用ルータを接続すること。
- 災害時用ルータと基幹コア L3 スイッチを接続すること。

7.3.3.5 災害時バックアップ回線（衛星回線）との接続

- 災害時バックアップ回線の衛星回線接続用機器を本調達で導入する機器へ接続すること。
- 現状の設定内容を精査し、災害発生時に災害時バックアップ回線を通じて既存で提供しているサービスが継続して提供可能な構成とすること。
- 現在実装されている仕組みの変更や削除を行う場合、背景を本県に説明のうえで協議を行うこと。

7.3.4. 大規模単独地域機関

7.3.4.1 機器及びネットワーク構成

有線ネットワークを構築するうえで各コンポーネントの構成に求める要件は以下のとおり。

- 拠点コア L3 スイッチ

・　冗長化は行わずシングル構成とすること。
・　主回線を収容すること。

➢ フロア L2 スイッチ（24/48 ポート）
・　冗長化は行わずシングル構成とすること。
・　拠点コア L3 スイッチへ接続すること。

・ 機器の接続に関しては、高い信頼性や可用性を確保すること。調査のうえで構成の変更や削除を行う場合、背景を本県に説明のうえで協議を行い決定すること。

7.3.4.2 主回線との接続

・ 現行ネットワークにおいて接続している主回線を、継続して利用できるようにすること。
・ 主回線に対して冗長化した接続とすること。
・ 主回線を利用した通信については、タグ VLAN、拡張タグ VLAN 等を利用しているため、継続して利用できるようにすること。バックアップ回線への切り替わりについてもこの点を考慮して設計すること。

7.3.5. 単独地域機関

7.3.5.1 VPN 集約ルータ（IDC）との接続

単独地域機関については、単独地域機関接続ルータを用いて IDC 設置の VPN 集約ルータと VPN 接続を行っている。なお、単独地域機関と IDC 間はインターネット回線により接続しているが、マイナンバー利用事務系ネットワークを利用する一部の単独地域機関については、閉域網接続を行っている。また、次期ネットワークの運用開始にあわせて、一部の拠点について、インターネット回線による接続から閉域網接続への切り替えを予定している。

単独地域機関接続ルータは各単独地域機関に 1 台のルータで構成すること。

また、県立学校（高等学校、特別支援学校）については、学校情報ネットワーク、GIGA スクールネットワークに係る通信が単独地域機関-IDC 間の回線及びセキュアな通信トンネルを利用する形で構成されている。単独地域機関接続ルータ及び VPN 集約ルータの設計を行う際は、既存構成を把握したうえで県立学校の通信に影響が出ないよう考慮すること。

7.3.5.2 新規無線 LAN 導入に伴う L2 スイッチの配備

現行ネットワークにおいて単独地域機関は無線 LAN 環境が導入されていない。そのため、無線 LAN 環境を新規に導入する単独地域機関については、無線 LAN アクセスポイント

接続用の L2 スイッチを構築すること。

導入する L2 スイッチは「9.2.14 L2 スイッチ（48 ポート）」、「9.2.15 L2 スイッチ（24 ポート）」を参照すること。なお、必要なポート数については調査のうえ、導入すること。

7.3.6. 市町等利用機関

7.3.6.1 市町等利用機関接続用スイッチ

市町等利用機関接続用スイッチは、市町等利用機関に設置し、主に主回線及びバックアップ回線を収容するスイッチである。

全 33 拠点のうち、筐体の冗長化が必要な 13 拠点については 2 台以上のスイッチで冗長構成とすること。その他の拠点についてはシングル構成とする。対象拠点については本県と協議のうえで決定すること。

7.3.6.2 主回線との接続

- 現行ネットワークにおいて接続している主回線を、継続して利用できるようにすること。
- 主回線を利用した通信については、タグ VLAN、拡張タグ VLAN 等を利用しているため、継続して利用できるようにすること。バックアップ回線を利用する拠点については、主回線からバックアップ回線への切り替えについてもこの点を考慮して設計すること。

7.3.6.3 バックアップ回線との接続

- 市町等利用機関接続用スイッチを冗長化する 13 拠点のうち、11 拠点はバックアップ回線を新規で接続すること。対象拠点については本県と協議のうえで決定すること。また、接続にかかる調整を本県、市町等利用機関、市町受託事業者及びバックアップ回線受託事業者との間で実施すること。
- 主回線に係る障害が発生し、他の拠点と通信ができなくなった際、主回線からバックアップ回線に切り替え、継続して通信が可能となるようにすること。
- バックアップ回線で利用する VLAN については、本県と協議のうえで決定すること。また、必要な場合は新規に専用の VLAN を設計すること。
- 主回線からバックアップ回線への切り替えは自動で行われるようにすること。また、切り替わり、切り戻しともに 5 分以内となるようにすること。

7.4. 移行設計要件

本業務について、移行業務を行うために必要となる移行設計を行うこと。
移行設計にあたっては、以下の要件を満たす設計とすること。

- 現行ネットワークから次期ネットワークへの移行について、本県職員の業務に支障をきたさないように留意した移行設計を行うこと。
- 移行設計を実施する際は、各受託事業者と十分な協議を行い、役割分担等について十分な確認を行うこと。
- その他詳細な要件については「8.1.2 移行に係る要求事項」を参照すること。

7.5. 運用設計要件

本業務について、運用・保守業務を行うために必要となる運用設計を行うこと。
運用設計にあたっては、以下の要件を満たす設計とすること。

- 運用設計を行うにあたり、現行ネットワーク、ユーザ認証システム、三重県 DX 推進基盤等の調査を行うこと。なお、必要に応じて、各受託事業者と協議、調整を行うこと。
- 定型業務・非定型業務の定義、運用プロセス、役割等を整理し、運用設計を行うこと。
- 導入するシステムの操作・設定方法に関する管理者向けマニュアル及び利用者向けマニュアルを作成すること。
- 運用設計においては、ITIL 等で推奨されるプロセスを参考とし、運用業務の効率化を図ること。なお、運用設計に際しては本県と定期的な会議を開催し、要件整理、合意を得たうえで必要な成果物を納品すること。
- 定型業務の設計として以下を含めること。
  - 各運用業務・システムの定常運用業務フロー及び手順
  - 各システムの申請・問い合せ（随時業務）のフロー及び手順
  - その他、サービス提供するために本県と共有すべき内容
- 非定型業務の設計として以下を含めること。
  - 本県との連絡調整窓口、及び連絡フロー設計
  - 各システムの監視設計及び障害時の保守手順
  - 想定されるサービス障害発生時に定めておくべきフローの設計
- セキュリティインシデント発生時の運用設計として以下を含めること。
  - 本県との連絡調整窓口、セキュリティ監視運用業務との連絡フロー設計
- ＜提案＞業務フローや手順については作成後、レビューを実施のうえ、本県の承認を得ること。業務の実施結果を「15 サービスレベル要件」と同様に定期的に評価・分析して本県に改善策を提示する等、業務改善に努めること。また、改善内容に応じて業務フローや手順を更新すること。
- 本業務において必要なドキュメント管理や、問い合わせが可能な Web ポータルサイトを導入すること。

7.6. 監視設計要件

本業務について、監視業務を行うために必要となる監視設計を行うこと。

監視設計を行うにあたり、監視対象、監視方法、適切な閾値、ログの保存内容及び保存先等について検討を行ったうえで、本県に承認を得ること。

障害発生時の一時切り分けやその後の対応（機器等の再起動等）マニュアル、手順書を作成し、本県に承認を得ること。

本県や各受託事業者との役割分担についても関係者間で協議し、決定すること。関係者間の協議については、本受託事業者が主体的に調整すること。

7.7. 保守設計要件

本業務について、保守業務を行うために必要となる保守設計を行うこと。

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。

- 保守業務に係る体制、対応フローについて検討し、本県に承認を得ること。
- 本県や各受託事業者との役割分担についても関係者間で協議し、決定すること。関係者間の協議については、本受託事業者が主体的に調整すること。

8. 移行業務

本章では、本業務における次期ネットワークの移行に関する要求事項を記載する。

8.1. 移行

8.1.1. 移行の基本方針

- 作成したテスト設計、移行設計に応じて、テスト及び移行作業等を実施すること。
- テスト設計、移行設計の作成にあたっては、「8.1.2 移行に係る要求事項」に記載の要件を満たすこと。

8.1.2. 移行に係る要求事項

- 本受託事業者が納入する機器について、テスト設計に基づき、テストを実施すること。
- 移行設計の結果を移行計画書及び移行手順書等に整理のうえ、本県に対し、レビューを実施したうえで、承認を得ること。
- 移行計画書及び移行手順書には、大まかな時間の流れや担当者の他、テスト項目についても記載すること。
- ネットワークの停止を伴う作業は原則認めないため注意すること。ただし、避けられない場合は閉庁日もしくは夜間での限られた時間での実施となる。なお、ネットワークの停止を伴わない場合は、平日、日中時間帯での作業を可とする。
- 各受託事業者に作業を依頼する必要がある場合は、作業指示書等を作成したうえで、本県に提出し、承認を得ること。
- 移行対象となるそれぞれの機器、システムにおいて、移行作業に必要となる作業の詳細（具体的な移行日時や作業の役割分担等）を明らかにした移行計画を策定すること。
- 移行作業完了時において、拠点又は機器、システム単位で移行作業の内容や懸案事項等をまとめた移行完了報告書を速やかに提出できるよう予め様式等について準備を行うこと。
- 重要機器については、障害発生時の影響を低減するため、切り戻しが可能かつ段階的な移行を行うこと。動作確認はある程度の網羅性（拠点単位、システム単位等）を持って実施すること。具体的な実施内容は移行設計時に本県と協議のうえで決定すること。また、移行時に異常が発生した場合に迅速な検知が可能な体制を検討すること。
- ＜提案＞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、様々な理由により予定どおりの移行が進まないと想定されるが、移行計画

については、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、移行計画とすること。

- ＜提案＞主回線に接続する市町等利用機関と事前に十分協議し、移行に係る影響を可能な限り軽減可能な計画とすること。
- 移行作業により、現行ネットワークの通信に影響があった場合に備え、切り戻しが可能な計画とすること。
- 移行作業において、切り戻し作業が発生した場合、移行計画等の見直しを実施し、本県に対し、レビューを実施したうえで、承認を得ること。
- 1 拠点毎の移行が可能な移行計画とすること。
- テスト環境を用意し、移行業務に係るリハーサルを実施すること。
- 移行期間中に必要となる電源増設や再配線等の工事業務について、本県に承認を得たうえで実施すること。また、各受託事業者や本県担当者（庁舎管理者等)、市町担当者等との連絡・調整・協議等についても主体的に実施すること。

8.2. テスト

8.2.1. テストの基本方針

- 各システムを導入するにあたり、テスト設計及び計画書を作成すること。
- 単体、結合、総合、障害、運用テストを実施すること。
- 実施する具体的なテスト内容は本受託事業者にて作成し、本県と協議のうえ、決定すること。

8.2.2. テストに係る要求事項

- 本受託事業者が納入する機器について、機器不良がないことを確認可能なテスト設計を行うこと。
- テスト設計の結果をテスト計画書及びテスト手順書等に整理のうえ、本県に対し、レビューを実施したうえで、承認を得ること。
- ＜提案＞テスト計画書の作成にあたっては、各機器、機能等について、実際の利用シーンを想定したうえで、ユーザ数、データ量数等を設定し、性能を確認できるようにすること。
- ＜提案＞テスト実施の際は、可能な限り本番環境に近いテスト環境を用意することとし、動作確認及び移行時の業務への影響について確認できるようにすること。
- テスト結果から、納入する機器が仕様等を満たさないことが判明した場合、速やかに機器の再選定や再設計等を実施すること。
- テスト結果については、本県に報告を行い、承認を得たうえで、次の工程に進むこと。

9. 構成要素の仕様

本章では、本受託事業者が納入する機器等の構成要素に関する要求事項を記載する。

全ての機器は「7 設計・構築業務」に記載した各種設計要件を実現することが可能な機器を選定すること。

本章に記載された要件と「7 設計・構築業務」に記載された要件に不明な点や矛盾がある場合は、調達時に質問し、明らかにしておくこと。

契約締結後、「7 設計・構築業務」と本章の記載内容の齟齬を理由として、「7 設計・構築業務」に記載した要件が満たせない、追加費用が発生する等は認められないため、注意すること。

＜提案＞導入する機器については、構成要素毎にリスクのない処理能力を有し、運用期間中において極力障害等が発生しないよう、信頼性、保守性、可用性の高い製品等を選定すること。また、将来的なネットワーク構成の変更、通信量や拠点、端末数等の増加にも対応するため、可能な限りコストを抑えた、構成変更及び拡張等の実現が可能な機器を選定すること。

9.1. 機器台数一覧

拠点毎の現行の機器台数については、「【別紙 1】ネットワーク設計構築拠点一覧」のとおり。

9.2. 有線ネットワーク要件

9.2.1. スイッチ・ルータ共通要件

スイッチ及びルータの共通要件は以下のとおり。

9.2.1.1 スイッチ共通要件

- 本調達で導入するネットワーク機器と通信ケーブルの接続について、SFP 等のモジュールが必要な場合、ケーブル/コネクタ種別に応じたモジュールを必要数用意すること。コネクタ形状の変更が必要な場合、該当作業は本業務に含むものとする。なお、現行ネットワークで使用しているモジュールの数量については、「【別紙 2】更新機器一覧」に記載しているため、参考とすること。
- 各機器の要件に記載している必要ポート数や機能は本県の想定である。実際に導入する機器は「7.2.3 有線ネットワーク」に記載のとおり、必要に応じて本県に確認を行い、適切な機器を選定すること。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- IPv4 のハードウェアスイッチングに対応可能な L2/L3 スイッチ製品であること。

- IPv4 の Static ルーティング、RIPv1/v2、OSPF、PBR 機能を有していること（L2 スイッチ除く）。
- DHCP サーバ機能（サーバ及びリレー等）を有していること（L2 スイッチ除く）。
- VRF 機能を有していること（L2 スイッチ除く）。
- VRF 上で DHCP 機能（サーバ及びリレー等）及びアクセスリスト機能を有効にできること（L2 スイッチ除く）。
- IPv6 の Static ルーティング、RIPng、OSPFv3 機能を有していること（L2 スイッチ除く）。
- SNMPv1/v2/v3、SNMP Trap、Syslog、コンソール、SSH 管理機能を有していること。
- NetFlow や sFlow を利用したフロー情報を取得し、全トラフィックのフローの可視化及び解析ができること。
- 優先制御機能（IEEE 802.1p CoS、DSCP のマーキング等）を有していること。
- IEEE 802.1Q をサポートしていること。
- 4,000 個以上の VLAN ID が利用可能なこと。
- IEEE 802.3ad に準拠したリンクアグリゲーション機能を有していること。
- 筐体をまたいだリンクアグリゲーション機能を有していること。
- IEEE 802.1D、IEEE 802.1w、IEEE 802.1s に準拠したスパニングツリー機能を有すること。
- アクセスリストによる L3/4 レベルでのアクセス制御に対応していること。
- PIM-Sparse Mode、PIM-Source Specific Multicast に対応していること。
- ユニキャスト・マルチキャスト・ブロードキャストストーム検知・防御に対応していること。
- 隣接機器検出プロトコル（LLDP 等）に対応していること。
- 9,000byte 以上のジャンボフレームに対応していること
- NTP による時刻同期機能を有すること。
- AC100V 電源に対応していること。
- 不具合対応・機器サポートが受けられること。
- メーカの技術支援が受けられること。

9.2.1.2 ルータ共通要件

- 本調達で導入するネットワーク機器と通信ケーブルの接続について、SFP 等のモジュールが必要な場合、ケーブル/コネクタ種別に応じたモジュールを必要数用意すること。コネクタ形状の変更が必要な場合、該当作業は本業務に含むものとする。
- IPv4 の Static ルーティング、RIPv1/v2、OSPF、BGP、PBR 機能を有しているこ

と。
- DHCP サーバ機能（サーバ及びリレー等）を有していること。
- IPv6 の Static ルーティング、RIPng、OSPFv3 機能を有していること。
- SNMPv1/v2/v3、SNMP Trap、Syslog、コンソール、SSH 管理機能を有していること。

優先制御機能（IEEE 802.1p CoS、DSCP のマーキング等）を有していること。
- 通信の暗号化機能として IPsec、GRE、GRE over IPsec に対応していること。また、ハードウェアにて暗号化処理できること。
- 暗号化方式については DES、3DES、AES 128、AES 192、AES 256 に対応していること。また、VPN トンネル設定可能数は 20 以上であること。
- IEEE 802.1D、IEEE 802.1w、IEEE 802.1s に準拠したスパニングツリー機能を有すること。
- ユニキャスト・マルチキャスト・ブロードキャストストーム検知・防御に対応していること。
- 隣接機器検出プロトコル（LLDP 等）に対応していること。
- NTP による時刻同期機能を有すること。
- AC100V 電源に対応していること。
- 不具合対応・機器サポートが受けられること。
- メーカの技術支援が受けられること。

9.2.2. 基幹コア L3 スイッチ（IDC）

要件は以下のとおり。
- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 1G/10G/25GBE 対応 SFP/SFP+ポートを 48 ポート、100GBE 対応 QSFP を 4 ポート実装していること（SFP は別途必要）。
- 2 台以上のスイッチが 1 組の論理スイッチとして管理できること。
- 2 台以上のスイッチを接続するケーブルが 1G/10G/40GBE 対応 SFP/SFP+/QSFP ポート又はバックプレーンを接続する専用ケーブルで構成できること。
- 筐体あたりの消費電力が 1,000W 以下であること。
- 筐体単位で電源の冗長化が可能なこと。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 3.2Tbit/s 以上であること。
- スイッチバッファ容量が 36Mbyte 以上であること。
- スイッチ仮想インターフェースを 1,000 個以上利用可能であること。
- VRRP 等のゲートウェイ冗長プロトコル機能を有すること。
- IGMP Filtering、IGMP snooping 機能を有すること。

・ その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L3 スイッチであること。

9.2.3. 基幹コア L3 スイッチ（本庁舎）

要件は以下のとおり。

・ 形状は 19 インチラックマウント可能であり、1RU 以下であること。
・ 1G/10G/25GBE 対応 SFP/SFP+ポートを 48 ポート、100GBE 対応 QSFP ポートを 4 ポート実装していること（SFP は別途必要）。
・ 2 台以上のスイッチが 1 組の論理スイッチとして管理できること。
・ 2 台以上のスイッチを接続するケーブルが 1G/10G/40GBE 対応 SFP/SFP+/QSFP ポート又はバックプレーンを接続する専用ケーブルで構成できること。
・ 筐体あたりの消費電力が 1,000W 以下であること。
・ 筐体単位で電源の冗長化が可能なこと。
・ 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
・ スイッチング容量が 3.2Tbit/s 以上であること。
・ スイッチバッファ容量が 36Mbyte 以上であること。
・ スイッチ仮想インターフェースを 1,000 個以上利用可能であること。
・ VRRP 等のゲートウェイ冗長プロトコル機能を有すること。
・ IGMP Filtering、IGMP snooping 機能を有すること。
・ その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L3 スイッチであること。

9.2.4. 拠点コア L3 スイッチ（総合庁舎 10 拠点+吉田山会館）

要件は以下のとおり。

・ 形状は 19 インチラックマウント可能であり、1RU 以下であること。
・ 10/100/1000BASE-T ポートを 24 ポート、1G/10GBE 対応 SFP/SFP+ポートを 4 ポート実装していること（SFP は別途必要）。
・ 2 台以上のスイッチが 1 組の論理スイッチとして管理できること。
・ 2 台以上のスイッチを接続するケーブルが 1G/10G/40GBE 対応 SFP/SFP+/QSFP ポート又はバックプレーンを接続する専用ケーブルで構成できること。
・ 筐体あたりの消費電力が 350W 以下であること。
・ 筐体単位で電源の冗長化が可能なこと。
・ 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
・ スイッチング容量が 200Gbit/s 以上であること。

- スイッチバッファ容量が 16Mbyte 以上であること。
- スイッチ仮想インターフェースを 1,000 個以上利用可能であること。
- VRRP 等のゲートウェイ冗長プロトコル機能を有すること。
- IGMP Filtering、IGMP snooping 機能を有すること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L3 スイッチであること。

9.2.5. 拠点コア L3 スイッチ（アスト津/シングル構成）

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T ポートを 24 ポート、1G/10GBE 対応 SFP/SFP+ポートを 4 ポート実装していること（SFP は別途必要）。
- 筐体あたりの消費電力が 350W 以下であること。
- 筐体単位で電源の冗長化が可能なこと。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 200Gbit/s 以上であること。
- スイッチバッファ容量が 16Mbyte 以上であること。
- スイッチ仮想インターフェースを 1,000 個以上利用可能であること。
- VRRP 等のゲートウェイ冗長プロトコル機能を有すること。
- IGMP Filtering、IGMP snooping 機能を有すること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L3 スイッチであること。

9.2.6. 拠点コア L3 スイッチ（教育センター/シングル構成）

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T ポートを 24 ポート、1G/10GBE 対応 SFP/SFP+ポートを 4 ポート実装していること（SFP は別途必要）。
- 筐体あたりの消費電力が 350W 以下であること。
- 筐体単位で電源の冗長化が可能なこと。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 200Gbit/s 以上であること。
- スイッチバッファ容量が 16Mbyte 以上であること。
- スイッチ仮想インターフェースを 1,000 個以上利用可能であること。

- VRRP 等のゲートウェイ冗長プロトコル機能を有すること。
- IGMP Filtering、IGMP snooping 機能を有すること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L3 スイッチであること。

9.2.7. サーバ接続用スイッチ（IDC/10G）

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 1G/10G/25GBE 対応 SFP/SFP+ポートを 24 ポート、100GBE 対応 QSFP ポートを 4 ポート実装していること（SFP は別途必要。RJ45 コネクタの接続が必要になった際 SFP モジュールで接続可能なこと）。
- 2 台以上のスイッチが 1 組の論理スイッチとして管理できること。
- 2 台以上のスイッチを接続するケーブルが 1G/10G/40GBE 対応 SFP/SFP+/QSFP ポート又はバックプレーンを接続する専用ケーブルで構成できること。
- 筐体あたりの消費電力が 1,000W 以下であること。
- 筐体単位で電源の冗長化が可能なこと。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 2.0Tbit/s 以上であること。
- スイッチバッファ容量が 36Mbyte 以上であること。
- スイッチ仮想インターフェースを 1,000 個以上利用可能であること。
- VRRP 等のゲートウェイ冗長プロトコル機能を有すること。
- IGMP Filtering、IGMP snooping 機能を有すること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L3 スイッチであること。

9.2.8. サーバ接続用スイッチ（IDC/1G）

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T を 24 ポート、1GBE 対応 SFP ポートを 4 ポート実装していること（SFP は別途必要）。
- 2 台以上のスイッチが 1 組の論理スイッチとして管理できること。
- 2 台以上のスイッチを接続するケーブルが 1G/10G/40GBE 対応 SFP/SFP+/QSFP ポート又はバックプレーンを接続する専用ケーブルで構成できること。
- 筐体あたりの消費電力が 125W 以下であること
- 筐体単位で電源の冗長化が可能なこと。

- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 128Gbit/s 以上であること。
- スイッチバッファ容量が 6Mbyte 以上であること。
- スイッチ仮想インターフェースを 500 個以上利用可能であること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L2 スイッチであること。

9.2.9. サーバ接続用スイッチ（本庁舎/1G）

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T を 48 ポート、1GBE 対応 SFP ポートを 4 ポート実装していること（SFP は別途必要）。
- 2 台以上のスイッチが 1 組の論理スイッチとして管理できること。
- 2 台以上のスイッチを接続するケーブルが 1G/10G/40GBE 対応 SFP/SFP+/QSFP ポート又はバックプレーンを接続する専用ケーブルで構成できること。
- 筐体あたりの消費電力が 125W 以下であること。
- 筐体単位で電源の冗長化が可能なこと。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 176Gbit/s 以上であること。
- スイッチバッファ容量が 6Mbyte 以上であること。
- スイッチ仮想インターフェースを 500 個以上利用可能であること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L2 スイッチであること。

9.2.10. ファイアウォール接続用スイッチ（24 ポート）

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T ポートを 24 ポート、1G/10GBE 対応 SFP/SFP+ポートを 4 ポート実装していること（SFP は別途必要）。
- 構成する 3 台以上の機器のうち 1 台をホットスタンバイして構成すること。
- 3 台以上のスイッチが 1 組の論理スイッチとして管理できること。
- 3 台以上のスイッチを接続するケーブルが 1G/10G/40GBE 対応 SFP/SFP+/QSFP ポート又はバックプレーンを接続する専用ケーブルで構成できること。
- 筐体あたりの消費電力が 350W 以下であること。

- 筐体単位で電源の冗長化が可能なこと。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 200Gbit/s 以上であること。
- スイッチバッファ容量が 16Mbyte 以上であること
- スイッチ仮想インターフェースを 1,000 個以上利用可能であること。
- VRRP 等のゲートウェイ冗長プロトコル機能を有すること。
- IGMP Filtering、IGMP snooping 機能を有すること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L3 スイッチであること。

9.2.11. VPN 集約ルータ（IDC 設置ルータ）

要件は以下のとおり。

- ルータ側での複数の機能や詳細な設定変更が発生することを考慮し、クラウド管理型機器以外を選定すること。
- 形状は 19 インチラックに実装可能で、1U/筐体であること。
- 3 台以上のルータで冗長構成とすること。
- IPsec 使用時において 1.9Gbps 以上の速度で通信可能であること。
- 最大スループットは 19.7Gbps 以上であること。
- 10/100/1000BASE-T を 8 ポート以上/筐体を有すること。
- 筐体内で冗長化された電源モジュールを有すること。
- IPv4、IPv6 に対応していること。
- VXLAN に対応していること。
- VRRP 等のゲートウェイ冗長プロトコル機能を有すること。
- カプセル化機能として GRE、802.1q VLAN をサポートしていること。
- 動作に必要なライセンス等を調達に含めること。
- その他機能要件について、「9.2.1.2 ルータ共通要件」に準拠したルータであること。

9.2.12. ルータ集約スイッチ

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T を 24 ポート、1GBE 対応 SFP ポートを 4 ポート実装していること（SFP は別途必要）。
- 筐体単位の消費電力が 100W 以下(PoE 給電時を除く)であること。
- 筐体単位で 370W 以上の PoE 給電能力を有すること。

- 搭載する 10/100/1000BASE-T 全ポートで以下の機能を有すること。
  - 802.3af/802.at に対応していること。
  - ポート毎の最大給電容量が制御可能なこと。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 128Gbit/s 以上であること。
- スイッチバッファ容量が 1.5 Mbyte 以上であること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L2 スイッチであること。

9.2.13. 市町等利用機関接続用スイッチ

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T を 24 ポート、1GBE 対応 SFP/SFP+ポートを 4 ポート実装していること（SFP は別途必要)。
- 2 台以上のスイッチが 1 組の論理スイッチとして管理できること。
- 2 台以上のスイッチを接続するケーブルが 10GBE 対応 SFP/SFP+ポート又はバックプレーンを接続する専用ケーブルで構成できること。
- 筐体単位の消費電力が 100W 以下であること。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 128Gbit/s 以上であること。
- スイッチバッファ容量が 1.5Mbyte 以上であること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L2 スイッチであること。

9.2.14. L2 スイッチ（48 ポート）

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T を 48 ポート、1GBE 対応 SFP ポートを 4 ポート実装していること（SFP は別途必要)。
- 筐体単位の消費電力が 100W 以下(PoE 給電時を除く)であること。
- 筐体単位で 370W 以上の PoE 給電能力を有すること。
- 搭載する 10/100/1000BASE-T 全ポートで以下の機能を有すること。
  - 802.3af/802.at に対応していること。
  - ポート毎の最大給電容量が制御可能なこと。

- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 176Gbit/s 以上であること。
- スイッチバッファ容量が 3Mbyte 以上であること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L2 スイッチであること。

9.2.15. L2 スイッチ（24 ポート）

要件は以下のとおり。

- 形状は 19 インチラックマウント可能であり、1RU 以下であること。
- 10/100/1000BASE-T を 24 ポート、1GBE 対応 SFP ポートを 4 ポート実装していること（SFP は別途必要）。
- 筐体単位の消費電力が 100W 以下(PoE 給電時を除く)であること。
- 筐体単位で 370W 以上の PoE 給電能力を有すること。
- 搭載する 10/100/1000BASE-T 全ポートで以下の機能を有すること。
  - 802.3af/802.at に対応していること。
  - ポート毎の最大給電容量が制御可能なこと。
- 筐体に搭載するネットワークインターフェースの全てが規格上のスピードで通信を行った場合においても処理可能なバックプレーン容量を有すること。
- スイッチング容量が 128Gbit/s 以上であること。
- スイッチバッファ容量が 1.5 Mbyte 以上であること。
- その他機能要件について、「9.2.1.1 スイッチ共通要件」に準拠した L2 スイッチであること。

9.2.16. 単独地域機関接続用ルータ

要件は以下のとおり。

- ルータ側での複数の機能や詳細な設定変更が発生することを考慮し、クラウド管理型機器以外を選定すること。
- 形状は 19 インチラックに実装可能であり、1U/筐体であること。
- IPsec 使用時において 150Mbps 以上の速度で通信可能であること。
- WAN 専用ポートとして 10/100/1000BASE-T ポートを 1 ポート以上/筐体、LAN 専用ポートとして 10/100/1000BASE-T ポートを 8 ポート以上/筐体を有すること。
- PPPoE のマルチセッションに対応していること。
- IPv4、IPv6 に対応していること。
- カプセル化機能として GRE、802.1q VLAN をサポートしていること。
- 動作に必要なライセンス等を調達に含めること。

- VXLAN に対応していること。
- その他機能要件について、「9.2.1.2 ルータ共通要件」に準拠したルータであること。

9.3. 無線 LAN 要件

9.3.1. 無線 LAN アクセスポイント

要件は以下のとおり。

- 居室内天井及び壁等に取り付け可能なこと。
- 動作温度は 0～50℃、動作湿度は 5～95%の環境で動作をすること。
- アンテナ内蔵タイプのアクセスポイントであること。
- 状態確認用の LED を有し、点滅/色で動作状態が判別可能なこと。
- 100/1000/2500BASE-T の有線ポートを有すること。
- 設定・管理用のコンソールポートを有すること。
- 電源アダプタでの電源受電が可能なこと。
- IEEE 802.3af/802.3at に基づく PoE 電源受電に対応をしていること。
- 受電電力の状況によって、稼働機能を縮退することでアクセスポイントの動作を継続させる機能を有すること。
- 無線の規格として IEEE 802.11a/b/g/n/ac/ax に対応していること。
- 5GHzRadio において W52//W53//W56 に対応すること。また、6GHzRadio の利用が可能なこと。
- Wi-Fi Alliance の認定を取得していること。
- 2.4GHz 帯及び 5GHz 帯、6GHz 帯を同時利用できる機能を有すること
- 利用可能な 3 つの周波数帯（2.4GHz、5GHz、6GHz）のうち、任意の 2 つの周波数帯にチューニングできること。
- 2.4GHzRadio において 2 x 2 : 2 MIMO に対応していること。
- 5GHzRadio において 2 x 2 : 2 MIMO に対応していること。
- 6GHzRadio において 2 x 2 : 2 MIMO に対応していること。
- 6GHzRadio において 160MHz のチャンネルボンディングに対応をしていること。
- 最大端末 Association 数は Radio あたり 512 台以上であること。
- 無線 LAN コントローラによって制御可能なものであること。
- 仮想コントローラ機能を内蔵していること。
- 無線 LAN アクセスポイントのファームウェアを一括、グループ単位、個別等の単位でバージョンアップする機能を有すること。
- ＜提案＞無線 LAN コントローラとの連携又は個別で無線周波数を検出し、干渉源周囲のワイヤレス電波到達範囲を最適化する自動調整機能を有すること。
- 不具合対応・機器サポートが受けられること。

・ メーカの技術支援が受けられること。

9.3.2. 無線 LAN コントローラ

要件は以下のとおり。

・ 無線 LAN コントローラはクラウド管理型とすること。
・ クラウド稼働率の SLA が 99.9%以上であること。
・ クラウドが完全にダウンしても、ローカルで機器設定やモニタリングができること。
・ ユーザのアクセス権限（参照のみ可、参照更新とも可、個人情報は不可等）を定めることが可能なこと。
・ 役割・責任者及び権限に応じたアクセス区分の設定ができる機能を備えること。
・ 複数のテナントを一元的に管理してサービスを提供する機能（MSP）を有すること。
・ データセンタが国内にあること。
・ 日本語の GUI に対応していること。
・ ウィザード形式（対話型形式）で簡単に無線 LAN の設定ができること。
・ グループ単位で複数デバイスを同時に設定できること。また、デバイス単位でも設定が可能なこと。グループは拠点毎に加え、拠点をまたがった特定のデバイスのみを同時に設定できること。
・ 管理機器とクラウドの疎通が完全に途絶えても、ローカルで CLI や UI で設定できること。管理機器へのアクセスは SSH とコンソールアクセスに対応していること。
・ テンプレートを使った設定に対応し、CLI で設定できる詳細な設定もクラウド経由で実現できること。
・ ネットワーク機器をインターネットとの通信可能なネットワークへ接続するのみでクラウド管理が可能となるゼロタッチプロビジョニングに対応可能なこと。
・ ネットワーク機器の設定を変更した際に、機器への適用タイミングを自動か手動か選択できること。
・ ラベルを設定し管理できること。
・ 管理しているデバイスの再起動ができること。
・ GUI ベースの設定においてホスト名の設定を変更できること。
・ GUI ベースの設定において管理ユーザ名、パスワード、SNMP、NTP の設定ができること。
・ テンプレートベースの設定において、CLI ベースのコンフィグレーションをクラウドで管理可能なこと。また、変数を用いたパラメータの個別設定に対応可能なこと。
・ 管理しているデバイスがクラウドと通信ができないとき、又はクラウドの契約が終了した場合は単体の機器として継続利用可能なこと。
・ 本調達で導入する全ての無線 LAN アクセスポイントを一元管理できること。
・ 不具合対応が受けられること。

・ メーカの技術支援が受けられること。

9.3.3. 無線 LAN 監視装置

要件は以下のとおり。

・ 無線 LAN 監視装置はクラウド管理型とすること。
・ クラウド稼働率の SLA が 99.9%以上であること。
・ クラウドが完全にダウンしても、ローカルで機器設定やモニタリングができること。
・ 無線 LAN コントローラと同一のメーカであること。
・ ユーザのアクセス権限（参照のみ可、参照更新とも可、個人情報は不可等）を定めることが可能なこと。
・ 役割・責任者及び権限に応じたアクセス区分の設定ができる機能を備えること。
・ 複数のテナントを一元的に管理してサービスを提供する機能（MSP）を有すること。
・ データセンタが国内にあること。
・ Web ブラウザベースの GUI ではダッシュボードとして、無線 LAN アクセスポイント、トラフィック量とクライアント数のグラフ表示、トラフィック量の多い上位 5 つの無線 LAN アクセスポイントとクライアント、無線クライアントのアプリケーションの利用状況を表示可能なこと。
・ 拠点毎の管理機器のステータス、高メモリ使用のデバイス数、高 CPU 使用のデバイス数、高チャネル使用率、高ノイズの無線 LAN アクセスポイント数を一覧で確認できること。
・ クライアントのトラフィック利用状況、利用アプリケーションの概要が確認できること。
・ 管理機器のステータスを一覧で確認することができること。拠点毎と拠点をまたがった特定グループ毎に確認できること。
・ 端末の一覧を確認できること。拠点毎と拠点をまたがった特定グループ毎に確認できること。
・ 端末が利用しているアプリケーションの利用率を一覧で確認できること。拠点毎と拠点をまたがった特定グループ毎に確認できること。
・ ユーザと位置の過去データを提供する機能を有すること。
・ 物理的な設置場所をサイトとして定義し、マップを使って管理できること。
・ 無線 LAN のヒートマップの表示機能に対応していること。無線 LAN アクセスポイントが出力している電波のヒートマップと接続端末、不正アクセスポイントの位置情報も表示することができること。また、電波のカバーエリアを正確に表示するため、MAP 状に壁を入力し、電波の減衰もシミュレートしたうえで表示ができること。減衰値は複数パターン設定できること。
・ 管理機器の相互接続状況を把握するためのトポロジ表示に対応していること。

- クライアント端末が無線に接続した際に、接続成功・認証失敗・ローミング失敗の日時、デバイス MAC アドレス、接続していた BSSID を記録する機能を有すること。また、保存期間は 30 日以上有すること。
- AI 等を用いて、再起動の多いアクセスポイントを検知し、その詳細を確認できること。
- AI 等を用いて、チャネル変更の回数が多いアクセスポイントを検知し、その詳細を確認できること。
- AI 等を用いて、クライアントが 802.1x 認証に失敗する数が通常より多いことを検知し、その詳細を確認できること。
- AI 等を用いて、クライアントが MAC 認証に失敗する数が通常より多いことを検知し、その詳細を確認できること。
- AI 等を用いて、クライアントが Web 認証に失敗する数が通常より多いことを検知し、その詳細を確認できること。
- AI 等を用いて、2.4GHz チャンネルの使用率が高いアクセスポイントを検知し、その詳細を確認できること。
- AI 等を用いて、アクセスポイントの送信出力が頻繁に変更されたことを検知し、その詳細を確認できること。
- AI 等を用いて、5GHz チャンネルの使用率が高いアクセスポイントを検知し、その詳細を確認できること。
- AI 等を用いて、クライアントがローミングする際、大きな遅延が発生したことを検知し、その詳細を確認できること。
- アラートの送信は特定のメールアドレス宛と Webhook に対応していること。
- 管理ユーザが追加・削除・変更された時にアラートが送信できること。
- 新しい管理機器が追加・削除された時にアラートが送信できること。
- アクセスポイントへの電力供給が足りなくなった時にアラートが送信できること。
- 不正アクセスポイントが検出された時にアラートが送信できること。
- 管理機器の CPU 使用率が一定期間設定値を上回った時にアラートが送信できること。閾値毎に、アラートのシビリティが設定できること。
- 管理機器のメモリ使用率が一定期間設定値を上回った時にアラートが送信できること。閾値毎に、アラートのシビリティが設定できること。
- 無線 LAN アクセスポイントのチャネル使用率が一定期間設定値を上回った時にアラートが送信できること。閾値毎に、アラートのシビリティが設定できること。
- 無線 LAN アクセスポイントのノイズフロアの値が一定期間設定値を上回った時にアラートが送信できること。閾値毎に、アラートのシビリティが設定できること。
- 無線 LAN アクセスポイントの接続端末数が、一定期間設定値を上回った時にアラートが送信できること。閾値毎に、アラートのシビリティが設定できること。
- DNS の遅延やエラーが発生した際にアラートが送信できること。
- 認証の遅延やエラーが発生した際にアラートが送信できること。

- 無線アソシエーションの遅延やエラーが発生した際にアラートが送信できること。
- DHCP の遅延やエラーが発生した際にアラートが送信できること。
- 不具合対応が受けられること。
- メーカの技術支援が受けられること。

9.4. 基幹ファイアウォール

要件は以下のとおり。

- 1U/筐体であること。
- 分割したファイアウォールはそれぞれ別メーカ製品を選定してもよい。
- ファイアウォールスループットが 70Gbps 以上（64byte UDP）であること。
- 同時セッションが 7,800,000 以上であること。
- 新規セッション/秒が 500,000 以上であること。
- 設定可能ルール数が 10,000 以上であること。
- 1G/10GBE 対応 SFP/SFP+ポート 4 ポート以上/筐体、1GBE 対応 SFP ポート 8 ポート以上を有すること。
- 10/100/1000BASE-T を 16 ポート以上/筐体を有すること。
- 仮想ファイアウォール機能を有しており、10 台以上の仮想ファイアウォールを構築できること。
- Web 管理コンソールからのオブジェクト・ルール編集作業が可能であること。
- 不正侵入検知/防御機能を有していること。
- アンチウイルス機能を実装していること。
- IPS 機能を有すること。
- IPS スループットが 12Gbps 以上であること。
- アンチウイルススループットが 10Gbps 以上であること。
- ログ管理や管理コンソール設定を行うことができること。
- アクティブースタンバイのステートフルフェールオーバ機能に対応可能なこと。
- DHCP サーバ機能（サーバ及びリレー等）を有していること。
- マスタ/スレーブの冗長構成とすること。
- マスタからスレーブに対して設定情報の同期が可能であること。
- 筐体内で冗長電源であること。
- 不具合対応・機器サポートが受けられること。
- メーカの技術支援が受けられること。

9.5. ネットワーク（その他）要件

9.5.1. Syslog サーバ

要件は以下のとおり。

- 動作に必要な OS やソフトウェアを必要数分用意すること。
- ログの保存が必要な機器からのログを全て保存できること。
- ログをホスト単位でファイルに保存が可能なこと。
- Web GUI でログを表示できること。
- ホスト名、ホスト IP アドレス、プライオリティ、メッセージテキストキーワード、日次でフィルタリングが可能であること。
- 任意のタイミング、あるいは定期的に、Zip ファイルや暗号化ファイル等のログファイルを自動でアーカイブが可能であること。
- 不具合対応・機器サポートが受けられること。
- メーカの技術支援が受けられること。

9.5.2. Radius サーバ

要件は以下のとおり。

- Web ブラウザ、MAC アドレス、IEEE 802.1x 認証機能に対応していること。
- 動作に必要な OS やソフトウェアを必要数分用意すること。
- MAC アドレスの区切り文字に関わらず認証成功できる機能を有すること。
- 認証端末の MAC アドレスを収集する機能を有すること。
- サーバ・クライアント証明書の発行が可能なこと。
- クライアント証明書の一括発行、失効、ダウンロードが可能であること。
- 下位認証局（中間認証局）として動作すること。
- アカウント情報を登録、編集、削除できること。
- 設定情報を外部のサーバに自動的にバックアップできる機能を有すること。
- 最終承認日から一定期間認証していないアカウントや有効期限が切れたアカウントを自動無効・削除できること。
- マスタからスレーブに対して設定情報の同期が可能であること。
- 不具合対応・機器サポートが受けられること。
- メーカの技術支援が受けられること。

9.5.3. セキュリティログ保存サーバ（Syslog 二次バックアップ）

要件は以下のとおり。

- Syslog サーバからのログを全て保存できること。
- ログをホスト単位でファイルに保存が可能なこと。
- Web GUI でログを表示できること。
- 任意のタイミング、あるいは定期的に、Zip ファイルや暗号化ファイル等のログファイルを自動でアーカイブが可能であること。

・ 不具合対応・機器サポートが受けられること。
・ メーカの技術支援が受けられること。

9.5.4. セキュリティログ保存サーバ（Radius ログバックアップ）

要件は以下のとおり。

・ Radius サーバからのログを全て保存できること。
・ ログをホスト単位でファイルに保存が可能なこと。
・ Web GUI でログを表示できること。
・ 任意のタイミング、あるいは定期的に、Zip ファイルや暗号化ファイル等のログファイルを自動でアーカイブが可能であること。
・ 不具合対応・機器サポートが受けられること。
・ メーカの技術支援が受けられること。

9.5.5. ネットワーク管理サーバ

要件は以下のとおり。

・ 障害発生時の有人によるログ解析等を含む、監視サービスが 24 時間 365 日可能なこと。
・ リアルタイムで障害の検知が可能なこと。
・ 機器の CPU 使用率、HDD 使用率、メモリ使用率等の監視が可能なこと。
・ ファン、電源、湿度等の異常の検知が可能なこと。
・ ネットワーク機器、サーバ機器については、Critical 以上（Critical、Alerts、Emergencies）のログの検知が可能なこと。
・ SNMP Trap を受信し、異常の検知が可能なこと。
・ 障害の発生を複数の宛先にメール通知できること。
・ サーバ・ネットワーク機器の性能及びトラフィック監視を行い、設定した基準値を下回った場合に、複数の宛先にメール通知できること。
・ SNMP 等により、エージェントレス監視に対応が可能なこと。
・ SNMP ポーリング等により、ネットワーク機器に対するトラフィック量の監視が可能なこと。監視データのログは、1 年以上閲覧可能であること。
・ 監視データは、グラフ表示等によって見やすく表示が可能なこと。
・ ネットワークトポロジの可視化ができること。
・ ネットワーク機器を自動検出で登録できること。
・ ネットワーク機器のコンフィグの一元管理ができること。
・ コンフィグの変更履歴を確認できること。
・ ネットワーク機器の OS バージョンの一元管理ができること。
・ OS バージョンの古い機器を自動検出できること。

- OS の一括バージョンアップができること。
- 変更前、変更後のコンフィグの差分チェックができること。
- ネットワーク機器のログの一元管理ができること。
- ネットワーク管理サーバは冗長構成ができること。
- レポートの出力機能を有すること。
- 不具合対応・機器サポートが受けられること。
- メーカの技術支援が受けられること。

9.5.6. プロキシサーバ

9.5.6.1 セキュリティクラウド用プロキシサーバ

要件は以下のとおり。

- プロキシ/キャッシュ機能、コンテンツフィルタリング機能を有すること。
- キャッシュ機能として以下に対応していること。
  - Web コンテンツ蓄積による代理応答
  - アップロード/ダウンロード容量制限
  - 動画閲覧対応
  - 接続先 URL によるキャッシュ利用有無制御
  - XFF（X-Forwarded-for）ヘッダ追加可能
- コンテンツフィルタリング機能として以下に対応していること。
  - 70 種類以上の URL カテゴリ分類分け、自動更新
  - カテゴリ別「閲覧許可」「閲覧規制」「書き込み規制」制御
  - 手動による URL の任意カテゴリ登録
  - 日本語・英語・中国語・韓国語等に対応したカテゴリ分類
  - 任意の Web ページ閲覧ユーザ特定
  - 特定ホスト・ネットワークに対する閲覧可否制御
  - AD サーバ等からユーザ情報の同期
- Web コンテンツのマルウェア検知機能として以下に対応していること。
  - ホームページの改ざんやマルウェア感染の疑いがある場合に通知を行うサービスが利用可能なこと。
  - ファイルの拡張子をリスク別にダウンロード制限が可能であり、Web サイトにアクセスしただけでマルウェアに感染してしまう攻撃への対策ができること。
- アクセスログの内容を解析・検索する、汎用 DB を利用しないレポーティングソフトにより、リスクの高い Web サービスを利用しているユーザ、送信量の多いユーザの確認が可能なこと。なお、レポーティングソフトはプロキシとは別で構築してもよい。その際も本県の共通機能基盤は利用可能とする。

- 管理画面にて同時接続数の状態及び、管理者毎に管理対象グループのカテゴリ毎アクセス件数、メーカからの重要なお知らせが確認可能なこと。
- 設定情報の同期が可能であること。
- 不具合対応・機器サポートが受けられること。
- メーカの技術支援が受けられること。

9.5.6.2 特定通信用プロキシサーバ（LGWAN 接続系向け）

要件は以下のとおり。

- プロキシ/キャッシュ機能を有すること。
- RFC に則った標準的な通信の制御と管理が可能なこと。
- 不具合対応・機器サポートが受けられること。
- 製品メーカもしくは OS サポートとしての技術支援が受けられること。

9.5.6.3 特定通信用プロキシサーバ（Internet 接続系向け）

要件は以下のとおり。

- プロキシ/キャッシュ機能を有すること。
- RFC に則った標準的な通信の制御と管理が可能なこと。
- 不具合対応・機器サポートが受けられること。
- 製品メーカもしくは OS サポートとしての技術支援が受けられること。

9.5.6.4 LGWAN 接続系プロキシサーバ

要件は以下のとおり。

- プロキシ/キャッシュ機能を有すること。
- RFC に則った標準的な通信の制御と管理が可能なこと。
- 冗長構成とすること。
- 不具合対応・機器サポートが受けられること。
- 製品メーカもしくは OS サポートとしての技術支援が受けられること。

9.5.6.5 マイナンバー利用事務系プロキシサーバ

要件は以下のとおり。

- プロキシ/キャッシュ機能を有すること。
- RFC に則った標準的な通信の制御と管理が可能なこと。
- 冗長構成とすること。
- 不具合対応・機器サポートが受けられること。

・ 製品メーカもしくはOSサポートとしての技術支援が受けられること。

9.6. ロードバランサ要件

9.6.1. プロキシ・メールサーバ用ロードバランサ

要件は以下のとおり。

・ 負荷分散機能として、以下のロードバランシング方式を備えること。
  - Round Robin(均等)
  - Ratio(比率)
  - Least Connections(最小接続)
  - Fastest(最速)
  - Least Sessions(最小セッション)
  - Weighted Least Connection(重み付け最小接続)
  - Observed(監視)
  - Predictive(予測)
  - Dynamic Ratio(動的比率)
・ ヘルスチェック機能として、以下のモニタリング方法をサポートすること。
  - ICMP、TCP、UDP、Diameter、RADIUS、HTTP、HTTPS、FTP、IMAP、LDAP、MSSQL、MySQL、NNTP、Oracle、POP3、PostgreSQL、Real Server、SASP、RPC、SIP、SMB、SOAP、WAP、WMI、Firepass、DNS
・ ICMP、YCP、UDP、HTTP、HTTPS等のさまざまな方式により障害検知が可能なこと。

9.6.2. クラウド接続用ロードバランサ

要件は以下のとおり。

・ 19インチラックに収容でき、1Uに収まること。
・ Gigabitカッパーポートを5ポート以上有すること。
・ SFP+を使用することにより、10Gigabit Fiberポートを4ポート以上搭載可能なこと。
・ 記憶装置としてSSD（ソリッドステートドライブ）を搭載していること。
・ L4/L7でそれぞれ20Gbps/20Gbps以上のアプリケーションスループットを有すること。
・ L4 CPSが500,000以上であること。
・ L7 CPSが180,000以上であること。
・ SSL CPSがSSLの鍵長2048bitでRSAの場合で最大15,000以上、ECDSAで8,000以上であること。

- TCL 等のスクリプト言語で負荷分散方法を記述できること。
- ラウンドロビン、最小コネクション数、重み付きラウンドロビン、重み付き最小コネクション数、最速応答時間でのロードバランシング方式に対応していること。
- ソース IP、クッキーによるパーシスタンス機能に対応していること。
- スクリプト等の機能により Microsoft 365 で使用する URL 一覧を取得できる機能を有していること。また取得した URL を条件としてトラフィックをロードバランス・別装置への転送・破棄することが可能なこと。
- 本装置を非透過 HTTP プロキシとして端末に設定が可能なこと。
- 任意の HTTP ヘッダを挿入できる機能を有していること。
- Radius、LDAP、Windows AD と連携し認証プロキシの機能を提供できること。
- SSL アクセラレーションにおいて PFS/ATS 高速処理をするための専用チップを搭載していること。
- グローバル・サーバー負荷分散機能を提供できること。
- ステートフル L4 ネットワークファイアウォール機能を有していること。
- SSL 可視化でミラー・インライン・ICAP 構成に対応できる機能を有していること。
- SSL 可視化の機能において Dynamic Port Intercept（SSL 通信であれば TCP ポート番号・上位プロトコルにかかわらず動的に復号化）する機能を有していること。
- SSL 可視化の機能において接続先サーバとの SSL ハンドシェイクに失敗した場合、自動的にバイパスする機能を有していること。
- SSL 可視化の機能において指定の Web サイトにて、サーバが SSL クライアント認証を要求した場合は自動的にバイパスし認証を継続する機能を有していること。
- DDoS 防御機能を有していること。
- 外部デバイスと ICAP 連携する機能を有していること。
- リバースプロキシ機能を有していること。
- IPv6 環境、もしくは IPv6、IPv4 混在環境での負荷分散機能を有していること。
- 回線負荷分散機能を有していること。
- クラウドアクセス負荷分散機能において明示/透過の両方に対応する機能を有していること。
- Web ベースの GUI で設定が可能で、日本語を含めた多言語に対応していること。また、CLI でも設定が可能なこと。
- マルチテナント構成が可能なこと。
- SSL 可視化の設定においてウィザード形式（対話型形式）で設定が可能なこと。

9.7. メール/DNS 要件

9.7.1. メールセキュリティ対策サーバ

各機能共通の要件は以下のとおり。

- メールアドレスにおいて、「@」の直前にピリオドがある場合等、RFC（2821/2822）非準拠のメールであっても配送を行う機能を有すること。
- 以下の性能要件を満たすこと。
  - システム利用者（インターネットメールを利用する職員）：約 8,000 名
  - アカウント数：8,000 アカウント
  - メールアドレス数：8,500 アカウント
  - ピーク時/1 か月 ：約 28 万通
  - 平均/1 か月 ：約 24 万通
  - ピーク時/1 分：300 通

メールサーバに必要となる各機能の要件は後述に記載する。

9.7.1.1 誤送信対策システム

要件は以下のとおり。

- メールフィルタリングソフト、もしくはメールフィルタリングサービスであること。
- 外部からの攻撃メールを受信された場合、本県へそのリスク情報を通知する無償のサービスを提供していること。
- 動作環境として、Windows Server と Red Hat Enterprise Linux のいずれにも対応していること。
- メール通信プロトコルは SMTP のみでなく POP3 にも対応しており、メール暗号化方式として STARTTLS にも対応していること。
- Bcc 強制変換等のメールフィルタリング機能が備わっていること。
- メールが一時的に保留される仕組みを有し、保留時間が設定できること。
- ポリシーグループの設定ができ、組織毎に誤送信対策ポリシーを設定できること。
- 更改時に設定情報をスムーズに移行可能であること。

9.7.1.2 添付ファイル分離システム

要件は以下のとおり。

- メールフィルタリングソフト、もしくはメールフィルタリングサービスであること。

・ 外部からの攻撃メールを受信された場合、本県へそのリスク情報を通知する無償のサービスを提供していること。
・ 動作環境として、Windows Server と Red Hat Enterprise Linux のいずれにも対応していること。
・ メール通信プロトコルは SMTP のみでなく POP3 にも対応しており、メール暗号化方式として STARTTLS にも対応していること。
・ 添付ファイルが Zip パスワードロックされている場合でもファイルの危険因子の判定が可能なこと。
・ ＜提案＞メール本文の無害化処理（添付ファイル削除、URL 含めたリンクの無効化、HTML メールやリッチテキストメールの本文テキスト化等）を実施したうえでメール配送が可能なこと。
・ 更改時に設定情報をスムーズに移行可能であること。

9.7.1.3 メール用ウイルスチェックシステム

要件は以下のとおり。

・ メールフィルタリングソフト、もしくはメールフィルタリングサービスであること。
・ 動作環境として、Windows Server と Red Hat Enterprise Linux のいずれにも対応していること。
・ メール通信プロトコルは SMTP のみでなく POP3 にも対応しており、メール暗号化方式として STARTTLS にも対応していること。
・ SPF 認証の技術と独自のロジックをベースに送信元アドレスの偽装を判定可能なこと。
・ 安全な差出人の「IP アドレス」と「ドメイン」をデータベースとして有し、データベースを利用して安全なメールのみを受信可能な機能を有すること。また、データベースに存在しない「IP アドレス」と「ドメイン」を収集し、精査したうえでデータベースとして配信できること。
・ 更改時に設定情報をスムーズに移行可能であること。

9.7.2. 内部メールサーバ

要件は以下のとおり。

・ 内部メールサーバ 1:1、1:N のエイリアス設定が可能なこと。
・ ソフトウェアは現行のソフトウェア（Postfix、Dovecot）からの移行が容易で、設定・運用が容易かつセキュリティが高いものを使用すること。
・ メールボックスを保持できること。
・ RFC 非準拠のメールに対しても送受信ができること。

- メール送受信を行ったユーザや端末を IP アドレス等で識別・特定できるログを取得できること。
- メール送受信の成否を追跡できるログを取得できること。
- メール送受信サイズは 1 メールあたりメールヘッダを含め、制限できること。
- 各ユーザのメールボックス容量を制限なしと設定できること。
- 各ユーザのメールボックス使用量を一括で確認できる仕組みがあること。
- ユーザ認証において、暗号化パスワードでの認証機能を有すること。

9.7.3. 外部メールサーバ

「9.7.1 メールセキュリティ対策サーバ」で機能集約ができる場合は、本サーバは不要とする。導入する場合の要件は以下のとおり。

- ソフトウェアは現行のソフトウェア（Postfix）からの移行が容易で、設定・運用が容易かつ、セキュリティが高いものを使用すること。
- RFC 非準拠のメールに対しても送受信ができること。
- メール送受信を行ったユーザや端末を IP アドレス等で識別・特定できるログを取得できること。
- メール送受信の成否を追跡できるログを取得できること。
- メール送受信サイズは 1 メールあたりメールヘッダを含め、制限できること。

9.7.4. 外部 DNS サーバ

要件は以下のとおり。

- 以下の性能要件を満たすこと。
  - DNS クエリ：500 件/1 分間
- インターネットからのドメインの問い合わせ対応及びインターネットへの接続に対応するために設置する外部 DNS 機能を有していること。ただし、対象は現行管理しているドメインのみとする。
- セキュリティクラウド上の DNS サーバに対して、ゾーン転送ができる機能を有すること。
- 指定サーバ以外からの再帰問い合わせを受け付けない機能を有すること。
- ソースポートランダマイゼーション機能を有効化すること。
- DNS クエリの分析や、クエリレスポンスやその他 DNS に関する統計情報からサイトのサービスレベルの状態確認について、別サーバでの対応も含め実施できる機能を有すること。

9.7.5. 内部 DNS サーバ

要件は以下のとおり。

- 製品の操作は日本語・英語で表記された Web 管理画面で提供されていること。
- 製品の操作マニュアル、リリースノート、その他の関連文書は日本語で提供されていること。
- Web 管理画面へのアクセスが不能になった場合でも、コンソールからの状態復旧が可能であること。
- ネットワークインターフェースを 2 つ以上有すること。
- DNS（Domain Name System）サーバ機能を有すること。
- 正引きゾーンと逆引きゾーンを登録できること。
- ゾーン数の最大は 1,000 以上であること。
- レコード数の最大はプライマリ、セカンダリともに 50,000 以上であること。
- 正引きゾーンには、A、AAAA、CNAME、MX、NS、SRV、TXT、DS、SPF レコードを設定できること。
- 逆引きゾーンには、PTR、NS、CNAME、DS レコードを設定できること。
- 上位 DNS や委任ゾーンからの応答の正当性を、付与されているレコード署名を使用して検証できること。
- DNSSEC（DNS Security Extensions）情報を要求する名前解決要求に対して、署名情報を付与して応答できること。
- プライマリ、セカンダリ方式により冗長構成ができること。
- 問い合わせ要求を許可・拒否するネットワーク、又は IP アドレスを指定できること。
- DNS サービスを監視し、停止している場合にはサービスを自動起動できること。
- 設定のバックアップを Web 管理画面から行えること。また、バックアップは、手動の他、自動バックアップにも対応すること。
- 機能の追加やセキュリティアップデートを、Web 管理画面から行えること。
- コンソールから、ネットワーク設定の変更、設定の初期化、システムの停止又は再起動ができること。
- Web 管理画面からネットワークコマンドを実行できること。対応するコマンドとして ping、traceroute、nslookup、dig、packet capture に対応すること。
- Web 管理画面を使用する際の通信は暗号化されていること。
- Web 管理画面へのアクセスを、管理用コンピュータの IP アドレスやネットワークアドレスで制限できること。
- Web 管理画面で操作を行わなかった場合、自動的にログオフすること。また、自動的にログオフするまでの時間は任意に指定できること。

9.8. 全庁ファイルサーバ要件

9.8.1. 全庁ファイルサーバ（インターネット接続系）

要件は以下のとおり。

- EIA 規格 19 インチラックに搭載可能なラックマウント型筐体とすること。
- ファイルサーバ部分とディスクストレージが一体型の NAS 装置で構成されること。
- 実効容量として、100TB 以上のストレージ容量を構成すること。
- 10GbE 対応 SFP+ポートを 2 ポート以上/筐体を有すること。
- CIFS（SMB1、2)、NFS、FTP、HTTP それぞれのプロトコルをサポート可能であること。
- 各フォルダに対して、容量制限を行うクォータ機能を有すること。指定されたユーザやグループ、サブフォルダに対して、容量を制限できること。
- 本県職員の個人用フォルダと所属毎の共有ファイルサーバ（以下「所属ファイルサーバ」という。）を筐体内で論理的に分離して、構成できること。ネットワーク分離に対応できること。
- 個人用フォルダについては、本県職員 7,500 人に対して作成し、必要なアクセス権限やセキュリティポリシーの適用を行うこと。アクセス設計については本県と協議のうえで決定すること。各フォルダに対して、クォータを設定できること。
- 所属ファイルサーバについては、各所属（約 400 所属）に対して、フォルダを作成し、必要なアクセス権限やセキュリティポリシーの適用を行うこと。アクセス設計については本県と協議のうえで決定すること。各フォルダに対して、クォータを設定できること。
- アクセス制限については庁内 AD と連携し、運用部分も含めて設計を行うこと。
- 動作に必要な OS やソフトウェアを必要数分用意すること。
- スナップショット領域含む論理容量を備え、管理・運用を簡便化するために、それぞれの論理ボリュームにおいて、その全領域を 1 個のファイルシステムで構成可能であること。
- ファイルアクセスのログについては、集計データ（ファイルアクセス及びアクセス権限の変更ログ等）を取得できること。
- SNMPv1/v2/v3、SNMP Trap、Syslog、コンソール、SSH 管理機能を有していること。

9.8.2. 全庁ファイルサーバ（LGWAN 接続系）

要件は以下のとおり。

- EIA 規格 19 インチラックに搭載可能なラックマウント型筐体とすること。
- ファイルサーバ部分とディスクストレージが一体型の NAS 装置で構成されること。
- 実効容量として、30TB 以上のストレージ容量を構成すること。
- 10GbE 対応 SFP+ポートを 2 ポート以上/筐体を有すること。
- CIFS（SMB1、2)、NFS、FTP、HTTP それぞれのプロトコルをサポート可能であること。
- 各フォルダに対して、容量制限を行うクォータ機能を有すること。指定されたユー

ザやグループ、サブフォルダに対して、容量を制限できること。

- 本県職員の個人用フォルダと所属毎の共有ファイルサーバ（以下「所属ファイルサーバ」という。）を筐体内で論理的に分離して、構成できること。ネットワーク分離に対応できること。
- 個人用フォルダ及び所属ファイルサーバとは別で、実行容量 30TB のうち 10TB を防災用領域として利用する共有ファイルサーバを構成すること。
- 動作に必要な OS やソフトウェアを必要数分用意すること。
- スナップショット領域含む論理容量を備え、管理・運用を簡便化するために、それぞれの論理ボリュームにおいて、その全領域を 1 個のファイルシステムで構成可能であること。
- ファイルアクセスのログについては、集計データ（ファイルアクセス及びアクセス権限の変更ログ等）を取得できること。
- SNMPv1/v2/v3、SNMP Trap、Syslog、コンソール、SSH 管理機能を有していること。

9.9. ファイル授受システム要件

9.9.1. ファイル無害化システム

要件は以下のとおり。

- ファイルの無害化を行う対象ストレージとして、以下のストレージ内のファイル検査が行えること。
  - クラウドストレージ（BOX/AWS S3/Microsoft OneDrive 等）
  - オンプレミスストレージ（DELL-EMC/HPE 等）
  - ファイルサーバ（Windows SMB ファイルサーバ等）
- ストレージ内のファイル検査については、ファイルが格納されたら検査する、スケジューラで指定して一斉検査を行う等柔軟な検査タイミングの設定（月/日の単位で任意の期間指定）が可能なこと。
- マルウェア検査でマルウェア判定された際に以下の処理が行えること。
  - マルウェア判定されたファイルは別領域に保存する。
  - マルウェア判定されたファイルは削除する。
- 無害化処理後のファイルについて、以下の処理が行えること。
  - 無害化されたファイルは別領域に保存する。
  - 無害化されたファイルは無害化前の元ファイルを上書きする。
- LGWAN ファイル転送システム（INT-LGWAN）を経由して、インターネット接続系ネットワークからファイルを LGWAN 接続系端末へ取込む場合にはスクリプトやマクロや OLE オブジェクト等リスクの高い因子について総務省ガイドラインの無害化処理要件を満たしたうえで取り込めること。
- 無害化エンジンのソースファイルの拡張子は 100 種類以上に対応すること。また、

その情報は一般に公開されていること。

- 無害化後のファイルの操作性（編集・加工）やアプリケーションの適合性を保持するため、無害化処理前と処理後で 75%以上はファイル拡張子が変わらないこと。なお、無害化処理についてはファイル構造を解析して、内部構造に含まれるファイル要素も無害化処理して再構成する処理プロセスを要件とし、この処理においてファイル拡張子が維持されること。
- 無害化に対応していないファイルについては、マルチスキャン処理（複数のマルウェア検査エンジンによるウイルスチェック）を行い、安全判定となった場合に無害化処理はせずにファイルのダウンロードを可能とする制御ができること。なお、無害化に対応しないファイルについて、危険因子のないことを確認するため、マルチスキャンエンジンについては、4 つ以上のマルウェアエンジンで検査できること。
- ファイルの拡張子のみでなく、ファイルシグネチャーやファイル構造等からファイルタイプを識別できること。また、ファイル構造が正規の仕様と異なる場合はこれを遮断もしくは正規のファイル形式への修正ができること。
- 無害化に対応していない拡張子や拡張子を改ざんした不正なファイルの転送を遮断、又は許可できること。
- 無害化処理のポリシー設定については、アプリケーション単位にポリシー設定が可能であること。(例：Microsoft Office の場合、Word/Excel/PowerPoint 等の単位)。
- 無害化結果は、そのファイルが有する要素（Office ファイルの場合、埋め込みオブジェクトやマクロ、ハイパーリンク等）毎に確認が可能であること。
- 以下のファイルを無害化処理できること。

  ＜文書ファイル＞

  - Word（doc、docx、docm）
  - Excel（xls、xlsx、xlsm）
  - PowerPoint（ppt、pptm、pptx、ppsm）
  - Word Viewer（rtf）
  - Visio（vsdx）
  - 一太郎文書（jtd、jtdc）

  ＜画像ファイル＞

  - JPEG（jpg/jpeg）、PNG（png）、TIFF（tiff）、GIF（gif）、BMP（bmp）、Windows Metafile（wmf/emf）

  ＜動画ファイル＞

  - WMV（wmv）、MPEG（mpeg）、WAV（wav）、MP3（mp3）、MP4（mp4）、MOV（mov）、AVI（avi）、WEBM（webm）

  ＜圧縮ファイル＞

  - ZIP（zip）、RAR（rar）、7Z（7z）、GZIP（gz）、XZ（xz）、LZH（lzh）

  ＜CAD＞

- AutoCAD（dwg)、AutoCAD Drawing Template（dwt)、AutoCAD Drawing Standards（dws)
- SXF Feature Comment（sfc)、STEP Data Model（p21)、JW CAD（jww)、Drawing Interchange Format（dxf)
- Design Web Format（dwf)、3D Studio（3ds)

・ 無害化対象とする拡張子は、各拡張子に有効・無効が設定可能であること。
・ アクセス管理においてADと連携が可能であること。
・ ログ情報をSyslogサーバに転送可能であること。
・ 無害化装置の保守サポートにあたっては国内に製品担当技術者・サポートセンターがあり、日本語での問い合わせの対応が実施できること。
・ 利用者の端末に専用モジュールをインストールせずに機能を提供すること。
・ VMWare等の仮想サーバ上でも物理・ベアメタルリソース上と同様の動作が可能であること。
・ 利用ユーザ数の増減によって、ライセンス費用が変化しないこと。
・ マルチスキャンの搭載エンジンがエンジンメーカより提供終了となった場合、追加費用が不要でエンジンが補填されること。

9.9.2. LGWAN ファイル転送システム（INT-LGWAN）

要件は以下のとおり。

・ ADと連携し、本県職員のユーザアカウントをファイル転送システムの利用者アカウントとして登録すること。
・ 異なるネットワーク間でデータファイルを受け渡しが可能で、ネットワーク間のやり取りは片方向、双方向に制限可能な機能を有すること。
・ データファイルを受け取る前に任意のユーザによる承認機能を有すること。
・ 承認を行うネットワークを設定することが可能な機能を有すること。
・ 特定のファイルタイプのみ受け渡し可能なデータの拡張子を制限可能な機能を有すること。
・ インターネット接続系からLGWAN接続系にファイルを送信する際、「9.9.1 ファイル無害化システム」に記載のファイル無害化システムと連携して、受け渡しの際にファイルを無害化できること。
・ 受け渡しの際に、アップロードファイルを自動的にZip暗号化する機能を有すること。
・ ファイルの受け取り方法を運用によって、変更できる機能を有すること。
・ データベースを別途インストールしなくても動作すること。
・ AD/LDAP連携に標準対応していること。
・ CSVからユーザのインポート/エクスポート可能な機能を有していること。
・ 利用履歴と証跡を一元的に保存する機能を有していること。

・ アップロードされたファイルに自動的に保管期間が設定可能であること。
・ 画面上の全ての文言を自由に変更する機能を有すること。
・ ファイルの受け渡しは双方向ともに Web ブラウザを用いた方式に加え Windows のネットワーク共有フォルダを用いてエクスプローラーから行えること。
・ 暗号化 Zip ファイルであってもパスワードを入力する仕組みを別途用意することでエクスプローラーから受け渡しすることができること。

9.9.3. ファイル交換システム（外部共有）

要件は以下のとおり。

・ AD と連携し、本県職員のユーザアカウントをファイル交換システムの利用者アカウントとして登録すること。
・ 一時 URL を経由して、利用者アカウントを持たない他人に対して、ファイルを送信することができること。
・ 一時 URL を経由して、利用者アカウントを持たない他人からファイルを受信することができること。
・ 外部ユーザからファイルを受信する際、「9.9.1 ファイル無害化システム」に記載のファイル無害化システムと連携して、受け渡しの際にファイルを無害化できること。
・ 利用者アカウントを有する複数の利用者でアクセス可能な領域を作成し、ファイルを共有できること。
・ 利用者が Web ブラウザでファイル操作が可能な Web インターフェースを有すること。
・ データファイルを受け渡す、受け取る前に任意のユーザによる承認機能を有すること。
・ 特定のファイルタイプのみ受け渡し可能なデータの拡張子を制限可能な機能を有すること。
・ データベースを別途インストールしなくても動作すること。
・ AD/LDAP 連携に標準対応していること。
・ CSV からユーザのインポート/エクスポート可能な機能を有していること。
・ 利用履歴と証跡を一元的に保存する機能を有していること。
・ アップロードされたファイルに自動的に保管期間が設定可能であること。
・ 画面上の全ての文言を自由に変更する機能を有すること。

9.10. LGWAN 接続システム要件

9.10.1. LGWAN 接続システム環境

要件は以下のとおり。

- 隔離領域内で実行されたアプリケーションが行うファイルの書き換え（保存）やレジストリ値の変更が、隔離領域外の環境には影響を与えないように制御し、コンピュータの環境を保護できること。
- 隔離領域内で実行されたアプリケーションの TCP/IP 通信が制御可能なこと。
- 隔離領域内で実行されたアプリケーションと、OS や隔離領域外で実行された他のアプリケーション間とのデータ通信（COM 経由によるデータ通信）を禁止できること。
- 隔離領域内で表示するファイル種類は管理者によって拡張子で指定ができること。
- 隔離領域内で実行されたアプリケーションから取得したクリップボードデータを、隔離領域外で実行された他のアプリケーションにコピーすることを制御可能なこと。
- 隔離領域内で実行されたアプリケーションから取得したクリップボードデータを、テキストデータ（Web リンク等の書式を含む）のみ隔離領域外で実行された他のアプリケーションにコピーすることを制御可能なこと。
- 隔離領域外で実行されているアプリケーションから取得したクリップボードデータを、テキストデータ（Web リンク等の書式を含む）のみ隔離領域内にペーストすることを制御可能なこと。
- 隔離領域内で実行されたアプリケーションからの印刷処理を制御可能なこと。
- 隔離領域内の Zip 形式（パスワード付含む）のファイルを解凍できること。
- 隔離領域内のファイルを Zip 形式（パスワード付含む）にて圧縮できること。
- 隔離領域外のファイルを、隔離領域内から参照することを制御可能なこと。
- 隔離領域内にファイルが存在するかを、利用者が容易に確認できること。
- 隔離領域内で動作しているアプリケーションを、利用者が容易に確認できること。
- 隔離領域は、サンドボックス型セキュリティソフトウェアの終了時に削除されること。
- サンドボックス型セキュリティソフトウェアには、隔離領域内で Web 参照を可能とする専用のセキュリティブラウザが内包されていること。
- セキュリティブラウザを利用して Web 参照する際は、参照先 Web サーバとコンピュータとで直接通信させることなく、専用のセキュリティゲートウェイを経由した通信経路に限定することが可能なこと。
- 隔離領域外のアプリケーションから、隔離領域内のデータへアクセスすることを禁止できること。
- セキュリティブラウザによりダウンロードしたファイルを、隔離領域内に保持することが可能なこと。また、そのファイルを編集可能なアプリケーションを、隔離領域内において実行可能な場合は、編集後のファイルも隔離領域内に保持することが可能なこと。
- 隔離領域内のダウンロードファイルや編集後のファイルを、セキュリティファイルゲートウェイと連携することにより、予め指定した Windows ファイル共有サーバに

アップロードすることが可能なこと。

- 前項要件のアップロードを、ドラッグ＆ドロップによる操作によって可能なこと。
- 隔離領域内のダウンロードファイルや編集済みファイル、セキュリティブラウザのキャッシュや閲覧履歴等のデータは、サンドボックス型セキュリティソフトウェアの終了時に削除され、コンピュータ上に残さない設定が可能なこと。
- 隔離領域内のダウンロードファイルや編集済みファイルを、コンピュータ上に保持する設定の場合、サンドボックス型セキュリティソフトウェアの終了後も該当データが保護されること。
- 隔離領域内で Windows のリモートデスクトップクライアントを実行し、セキュリティゲートウェイを経由して、別の Windows 端末へリモートデスクトップ接続できるよう制御できること。
- 隔離領域内で、リモートデスクトップの接続先設定情報を管理する機能を有すること。
- ユーザは、リモートデスクトップの接続先毎に、リモートデスクトップクライアントの動作設定を保存できること。
- 前項要件の設定情報について、サンドボックス型セキュリティソフトウェアへの次回ログイン時も使用することを制御可能なこと。
- リモートデスクトップの接続先毎に、リモートデスクトップ接続に使用する認証情報を保持することを制御可能なこと。認証情報を保持する場合は、サンドボックス型セキュリティソフトウェアにログイン中は、同じ接続先へのリモートデスクトップ接続時に、その認証情報を使用して自動で認証できること。
- 前項要件の認証情報については、サンドボックス型セキュリティソフトウェアへの次回ログイン時も使用することを制御可能なこと。次回ログイン時も使用する場合は、同じ接続先へのリモートデスクトップ接続時に、その認証情報を使用して自動で認証できること。
- サンドボックス型セキュリティソフトウェアが動作している端末のカメラ(ビデオキャプチャーデバイス)・マイク・スマートカードリーダーを、リモートデスクトップ接続先端末で利用することを制御可能なこと。
- 隔離領域内で実行された Windows のリモートデスクトップクライアントからの印刷処理を制御可能なこと。
- 隔離領域内で実行された Windows のリモートデスクトップクライアントから取得したクリップボードデータを、隔離領域外で実行された他のアプリケーションにコピーすることを制御可能なこと。
- 隔離領域内で実行された Windows のリモートデスクトップクライアントから取得したクリップボードデータを、テキストデータ（Web リンク等の書式を含む）のみ隔離領域外で実行された他のアプリケーションにコピーすることを制御可能なこと。
- 隔離領域外で実行されているアプリケーションから取得したクリップボードデータを、テキストデータ（Web リンク等の書式を含む）のみ隔離領域内で実行された

Windows のリモートデスクトップクライアントにペーストすることを制御可能なこと。

- サンドボックス型セキュリティソフトウェアが起動前の状態から、隔離領域外のショートカットアイコンをクリックすることで、隔離領域内で実行された Windows のリモートデスクトップクライアントからショートカットに指定した接続先へリモートデスクトップ接続が実行可能なこと。
- 隔離領域内で実行された Windows のリモートデスクトップクライアントから別の Windows 端末へリモートデスクトップ接続する際は、リモートデスクトップ接続先端末においては、サンドボックス型セキュリティソフトウェア独自のエージェントソフトウェアは使用せずに、Windows のリモートデスクトップ接続機能で実現可能なこと。
- 隔離領域内で Windows のリモートデスクトップクライアントを複数起動し、複数の接続先端末に同時にリモートデスクトップ接続が可能なこと。
- 仮想環境でファイルサーバをネットワークドライブとしてマウントできること。
- マウントしたネットワークドライブ上のファイルを編集、保存できること。

9.11. 防災関連ネットワーク

9.11.1. 災害時用ルータ

詳細要件は「9.2.16 単独地域機関接続用ルータ」と同じとする。

9.11.2. 災害時用プロキシサーバ

要件は以下のとおり。

- 冗長構成をとる際に必要な機器等が存在する場合、調達に含めること。
- 動作に必要な OS やソフトウェアを必要数分用意すること。
- 本県職員がアクセスするにあたり、ストレスなく通信できるようにサイジングを行うこと。
- プロキシ/キャッシュ機能、コンテンツフィルタリング機能を有すること。
- キャッシュ機能として、以下に対応していること。
  - Web コンテンツ蓄積による代理応答
  - アップロード/ダウンロード容量制限
  - 動画閲覧対応
  - 接続先 URL によるキャッシュ利用有無制御
  - XFF（X-Forwarded-for）ヘッダ追加可能
- コンテンツフィルタリング機能として、以下に対応していること。
  - 70 種類以上の URL カテゴリ分類分け、自動更新

- カテゴリ別「閲覧許可」「閲覧規制」「書き込み規制」制御
- 手動による URL の任意カテゴリ登録
- 日本語・英語・中国語・韓国語等に対応したカテゴリ分類
- 任意の Web ページ閲覧ユーザ特定
- 特定ホスト・ネットワークに対する閲覧可否制御

・ アクセスログの内容を解析・検索する、汎用 DB を利用しないレポーティングソフトにより、リスクの高い Web サービスを利用しているユーザ、送信量の多いユーザの確認が可能なこと。
・ 管理画面にて同時接続数の状態及び、管理者毎に管理対象グループのカテゴリ毎アクセス件数、メーカからの重要なお知らせが確認可能なこと。
・ AD と連携し、利用者を特定することを目的としてユーザ認証（kerberos 認証等）を実施すること。また、AD のセキュリティグループを用いたフィルタリング制御を実施すること。
・ 設定情報の同期が可能であること。
・ 不具合対応・機器サポートが受けられること。
・ メーカの技術支援が受けられること。

9.11.3. 災害時用ファイアウォール

要件は以下のとおり。

・ 形状は 19 インチラックに実装可能で、1U/筐体であること。
・ ファイアウォールスループットが 10Gbps 以上（64byte UDP）であること。
・ IPS スループットが 2.6Gbps 以上であること。
・ アンチウイルススループットが 1.6Gbps 以上であること。
・ 同時セッションが 1,500,000 以上であること。
・ 新規セッション/秒が 56,000 以上であること。
・ 設定可能ルール数が 10,000 以上であること。
・ 10/100/1000BASE-T ポートを 8 ポート以上/筐体を有すること。
・ 仮想ファイアウォール機能を有しており、10 台以上の仮想ファイアウォールを構築できること。
・ Web 管理コンソールからのオブジェクト・ルール編集作業が可能であること。
・ 不正侵入検知/防御機能を有していること。
・ アンチウイルス機能を実装していること。
・ ログ管理や管理コンソール設定を行うことができること。
・ アクティブースタンバイのステートフルフェールオーバ機能に対応可能なこと。
・ DHCP サーバ機能（サーバ及びリレー等）を有していること。
・ マスタ/スレーブの冗長構成とすること。
・ マスタからスレーブに対して、設定情報の同期が可能であること。

- 冗長電源であること。
- 不具合対応・機器サポートが受けられること。
- メーカの技術支援が受けられること。

9.11.4. 災害時用 Radius サーバ

要件は以下のとおり。

- 災害時用プロキシサーバと同一の物理サーバ上で動作可能なこと。
- 外部認証として利用する際、MAC アドレス認証や PSK に対応していること。
- サーバ・クライアント証明書の発行が可能なこと。
- 下位認証局（中間認証局）として動作すること。
- アカウント情報を登録、編集、削除できること。
- 設定情報を外部のサーバに自動的にバックアップできる機能を有すること。

9.12. ネットワーク可視化

9.12.1. ネットワーク可視化システム

要件は以下のとおり。

- 機器やシステムの死活、サービス状態、リソース状態、トラフィック等の可視化が可能なこと。
- GUI から可視化状況の確認が可能なこと。
- 本装置により収集した情報を過去 30 日以上遡り確認が可能なこと。また、データの保存及びレポートとして出力が可能なこと。
- ネットワークトポロジ図の可視化が可能なこと。
- 任意に設定したルールに従い、アラートの表示、管理者へ通知する機能を有すること。
- LAN/WAN 問わず、ネットワークボトルネック個所が特定できる機能を有すること。

9.13. その他

9.13.1. 無停電電源装置（UPS）

要件は以下のとおり。

- 電源収容対象の機器に対し、10 分以上の稼働が確保できる電源容量であること。
- ラックマウント型であること。
- 契約期間中におけるバッテリ経年劣化等の交換対応が可能であること。
- 不具合対応・機器サポートが受けられること。

・　メーカの技術支援が受けられること。

10.運用業務

本章では、次期ネットワークの運用業務を遂行するにあたり、本県が要求する事項を記載する。
＜提案＞本章の要件において、本県担当職員の負荷軽減につながる提案があれば記載すること。

10.1. 管理体制・連絡体制

- 次期ネットワークにおいて導入するサーバ類の管理、ネットワーク管理及び、その他次期ネットワークに関連するネットワーク全体の監視・運用統括業務を行い、ヘルプデスク、各受託事業者と連携して迅速な対応が可能な体制を整えること。
- 本章の業務を実施するために必要な SE を運用管理 SE として本庁舎に常駐させること。要員数は「10.19 想定業務量」を参考にすること。また、運用管理 SE のうち 1 名をリーダとして、運用業務を統括させること。
- リーダは本県と同等規模の都道府県、政令指定都市、省庁において、運用業務の経験を 5 年以上有し、複数の受託事業者を統括する業務を経験していること。
- リーダは、既存システムの運用業務を含む業務全体を管理・統括すること。
- 以下に示す資格要件を満たす者、もしくは同等の業務経験・技術スキルを有する者を本業務に参画させること。同等の実績を挙げる場合は実績に関する証明書を添付し、同等の経験・スキルを保有していることを示すこと。
  - ネットワークスペシャリスト
  - 情報セキュリティスペシャリスト（情報処理安全確保支援士）
  - IT サービスマネージャ
  - ITIL スペシャリスト
- 毎日、簡単な業務報告を行うこと。報告内容については、本県と協議すること。
- 本業務の作業内容に関する月次及び年次の報告書を提出すること。報告内容については本県と協議すること。
- 契約後速やかに運用管理 SE の名簿を提出すること。運用管理 SE に変更・追加が発生した場合も同様とする。
- 当該業務に従事する者は、予め身分を証明する書類を本県へ提出すること。また、業務遂行中は本県の発行する許可証を必ず着用すること。
- 当該業務に従事する者を変更する場合は、現行従事者との十分な引継ぎを行い運用業務に支障をきたさないようにすること。
- 病気等で運用管理 SE に欠員が生じた場合は、速やかに補員し、業務遂行体制を維持すること。複数名の欠員は原則認めないが、やむを得ない場合は本県と協議のうえ、業務遂行体制を維持すること。
- 月末までに翌月の運用管理 SE の業務従事スケジュールを提出すること。
- 本県からの障害連絡及び障害監視システムからの自動通知メールを 24 時間受けられるように、スマートフォン・携帯電話を受信できるようにしておくこと。

・ 緊急時の連絡体制を整えること。

10.2. 業務時間

・ 運用管理 SE は原則として本県の休日を定める条例第 1 条 1 項に規定する休日以外の日（以下、「平日」という。）の 7 時 30 分から 20 時 00 分まで業務に従事すること。昼間時間帯（8 時 30 分から 17 時 15 分まで）は複数名が業務に従事すること。ただし、年末年始期間（12 月 29 日から 1 月 3 日まで）は除く。
・ 緊急障害対応等は、本県の休日を定める条例第 1 条 1 項に規定する日（以下、「休日」という。）と時間外についても必要に応じて業務に従事すること。主に以下のような業務を指示することがある。
  ➢ 各種設定変更作業：時間外作業を月数回程度、休日作業を年数回程度
  ➢ 計画停電対応：休日・時間外作業を年数回程度
  ➢ セキュリティパッチ対応：時間外作業を月数回程度
  ➢ 選挙開票作業待機：休日待機を国政、県政選挙の度
  ➢ 単独地域機関新設・廃止対応：休日・時間外作業を年数回程度
  ➢ 人事異動・組織改編対応：休日・時間外作業を数日程度
  ➢ 年度末移行作業：年度末、年度始めの休日・時間外作業を数日程度
  ただし、緊急障害対応等は、上記に関わらず責任をもって対応すること。

10.3. 統括業務

・ リーダは次期ネットワークを円滑に稼働させるため、定期的に連携が必要な以下の関係者等との調整を行う。
  ➢ ヘルプデスク
  ➢ 各受託事業者の NOC 及び SOC
  ➢ 各システムベンダ
  ➢ 本県担当職員
  ➢ 本県原課職員（業務システム担当者）
・ 次期ネットワーク及び関連するシステム等の状況を把握し、定期的に本県へ報告すること。
・ 定期的に各システムやネットワーク機器の脆弱性情報を調査し、リスクが高いと判断した場合、リスクを最小限に留めるため、本県に報告するとともに関係者等へ注意喚起や、必要に応じて技術的助言を行い、影響を最小限に留めること。
・ ヘルプデスクに、サーバ、ネットワーク機器の簡易な作業（コマンド投入、バックアップ、ウイルス対策ソフトのパターンファイルの更新等）を指示すること。
・ 統括業務の遂行にあたり問題が生じた場合は原因を調査のうえ、本県に改善策を速やかに提示し、本県の承認を得たうえで対策を講じること。

10.4. 関係者用総合窓口機能（Web ポータルサイト）

次期ネットワークで発生した障害や実施した作業、問い合わせ等の内容を発生・受付から復旧・解決まで記録し、管理・閲覧する仕組みとして、専用のポータルサイトを構築し、提供すること。

なお、ポータルサイトの構築にあたっては、本県が所有する Microsoft 365 ライセンスも利用可能とする。

ポータルサイトの要件は以下のとおり。

- ネットワーク担当職員、ヘルプデスク、各受託事業者、及び、各情報システム担当職員からの依頼事項や問い合わせを運用管理 SE へ直接連絡できる機能（ポータル機能）及び問い合わせ等を管理することができる機能を有すること。必要とするポータル及び問い合わせ管理機能の詳細は以下のとおり。
  - 利用者が「問い合わせ・依頼」を登録できる Web フォームを用意し、Web ポータルサイトにリンクを掲載すること。
  - 利用者が Web フォームより登録を行う際に、氏名や所属・連絡先等が自動反映されること。
  - 利用者が Web フォームより登録を行った内容をインシデント管理データとして管理できること。
  - 利用者が登録を行った際にチケット（管理）番号を自動発番できること。
  - インシデント情報の登録・更新時に関係者へメール通知等ができること。
  - インシデント管理データは、運用期間中のデータを保管できること。
  - インシデント管理データの利活用ができること。
  - インシデント管理データは、管理番号・日時・起票者・依頼者・ステータス等の条件で検索できること。
  - 検索条件を指定してレポート集計ができること。
  - いつ、誰が何を更新したのか、登録内容の更新履歴が確認できること。
- ポータルサイトの利用者は、運用管理 SE、ネットワーク担当職員、ヘルプデスク、各受託事業者、及び各情報システム担当職員とし、それぞれのユーザ管理が実施できること。また、ネットワーク担当職員、及び運用管理 SE には、ポータル機能における管理者権限等の付与ができること。
- ネットワーク担当職員、及び運用管理 SE は、全ての作業依頼等の内容を閲覧できること。
- ネットワーク担当職員、及び運用管理 SE からヘルプデスク、各受託事業者、及び各情報システム担当職員に対して、掲示板機能等により周知が可能なこと。
- 必要な情報が掲載された場合、ユーザ単位でメール等による通知が可能なこと。
- 各種設定、パラメータシート等を安全にやり取りするための機能として、ファイル交換等の機能が利用できること。

・ Web ポータルサイトによくある質問と回答（FAQ）を公開可能であること。
・ 次期ネットワークでの利用及び運用が可能であれば、オンプレミスでもクラウドサービス利用でも可とするが、当該ポータルサイトを稼働させるために必要となる費用については、本業務の範囲内に含めること。
・ 次期ネットワークの構成情報、ドキュメント、コンフィグ、ナレッジ等を利用者に対して、共有できること。また、利用者や共有内容に応じて適切にアクセス制御を行うこと。
・ ＜提案＞Web ポータルサイトの画面遷移図や問い合わせ対応フロー等、Web ポータルサイトを用いた運用イメージについて提案すること。

10.5. 構成管理

・ 次期ネットワークを構成する IDC、本庁舎、総合庁舎、単独地域機関、市町等利用機関、吉田山会館、勤労者福祉会館、栄町庁舎、合同ビルにおけるネットワーク機器等の物理構成、論理構成を定期的に確認し、管理すること。
・ IDC、本庁舎、総合庁舎における本県が指定するサーバの物理構成、ハードウェア構成を定期的に確認し、管理すること。
・ ネットワークの物理回線構成（配線）を管理すること。
・ ネットワークのルーティング構成、IP アドレス構成、VLAN 構成等の論理構成を管理し、各種情報の追加、更新、削除を行うこと。
・ IP アドレスの払い出し、削除に伴い、アドレスの重複等がないように管理すること。
・ 機器の名称を管理し、機器の追加、削除に伴い、名称の重複等がないように管理すること。
・ IDC の機器構成については、実機との照合を 1 年に 1 回以上実施し、最新化とともに履歴管理を行うこと。
・ 本調達以外の構成管理業務を依頼することがあるため対応すること。業務内容の例としては以下のとおり。
  ➢ ユーザ認証システムにおいて、AD にユーザアカウントや端末情報を登録しているため、運用上必要な登録や削除、変更を行うこと。
  ➢ 三重県 DX 推進基盤において、インターネットメールアカウントを登録しているため、運用上必要な登録や削除、変更を行うこと。
・ ファイルサーバやメール等のアクセス権管理のため、定期的に棚卸を実施し、適切なアクセス権の割り当てがされているか確認すること。
・ 運用業務により、構成情報の更新が発生した場合には変更履歴の記録及び版数管理を行ったうえで速やかに各種構成情報を更新すること。
・ 各種構成情報は「10.18 インシデント・問い合わせ管理」の Web ポータルサイトで共有できること。
・ 一部の構成情報については今後、管理台帳のひな形としても利用することを想定してい

るため、各受託事業者の構成情報の統合を意識した記載内容とすること。なお、記載項目や構成については本県と協議のうえ、決定すること。

10.6. ドキュメント管理

- 次期ネットワークでは、運用管理手順を可視化し、工数削減・運用品質向上を図るため、運用業務におけるルールや作業手順をとりまとめた運用手順書を策定すること。
- 契約後提示するセキュリティポリシーに則り、セキュリティに関する運用手順書を策定すること。
- 本業務上作成した各種管理表、図面及び資料等を提出すること。また、これら資料等は、履歴管理を行ったうえで更新の都度提出すること。
- 機器の構成・仕様・設定等をドキュメント化し、管理すること。
- 運用業務の実施手順、ルールを標準化し、マニュアルとして整備すること。
- 運用業務により、ドキュメント等の修正が発生した場合には履歴管理を行ったうえで速やかに各種ドキュメントを修正すること。なお、ドキュメントの修正にあたっては本県へ説明を行ったうえで、承認を得ること。
- 「7.2.2.4 共通ドキュメントの整備」で作成したドキュメント等の修正が発生した場合には履歴管理を行ったうえで速やかに各種ドキュメントを修正すること。なお、ドキュメントの修正にあたっては本県へ説明を行ったうえで、承認を得ること。
- 作成したドキュメントは随時更新のうえで、本県職員と共有できるように本調達で構築する全庁ファイルサーバに保存すること。なお、ファイルサーバのアクセス権やフォルダの階層設計等を含めて、適切に実施すること。

10.7. 電源管理

- ヘルプデスクと協力し、本庁舎 7 階サーバ室及び総合庁舎情報機器室内の電源管理（どのブレーカーからどの機器につながっているか等）を行うこと。
- 非常用電源に接続されている機器等を一覧表で管理すること。なお、各庁舎における電源等の構成については契約後別途開示する。
- UPS に接続している機器等を一覧表で管理すること。
- 機器等の増減が生じた場合は、都度更新すること。

10.8. 設定変更

- 事前に承認されたネットワーク環境の変更に伴い、ネットワーク機器の設定変更が必要な場合は、本県に承認を得たうえで各種設定作業を行うこと。なお、設定作業を実施するにあたっては、それに係る検証を行ったうえで、手順書を作成し、作業を実施すること。変更作業後は結果を確認し、本県へ報告すること。

・ 問題が生じた場合は、設定変更作業を中止し、切り戻しを実施すること。
・ 本県の指示により、ケーブルの繋ぎ換え、配線等の構成変更作業を行うこと。
・ 必要に応じて、設定変更作業前後で、システム領域のフルバックアップ又はスナップショットを取得すること。ネットワーク機器の場合は、コンフィグファイル等の設定データを取得すること。設定変更がシステム領域以外の領域に及ぶ場合は、影響を及ぼす範囲のバックアップを取得すること。
・ 設定変更に伴い「10.5 構成管理」の構成情報を更新すること。
・ 次期ネットワークの運用期間中、以下の既存システムの追加・更改等を予定しているため、追加、更改等に伴うネットワーク接続の各種設定作業を行うこと。なお、設計変更が伴う作業が発生する場合は、本県と協議のうえで対応すること。
  ➢ セキュリティクラウド
  ➢ 三重県 DX 推進基盤
  ➢ 共通機能基盤
  ➢ EDR
・ 次期ネットワークの運用期間中、新規で業務システムのガバメントクラウドへの移行が想定されている。移行が発生した際は、IP アドレスの払出、接続に係るファイアウォール等への設定作業等を行うこと。また、移行システム側の受託事業者と協議し、必要な設定等について調整すること。なお、接続構成は「図 10-1 ガバメントクラウドの構成概要」のとおり。

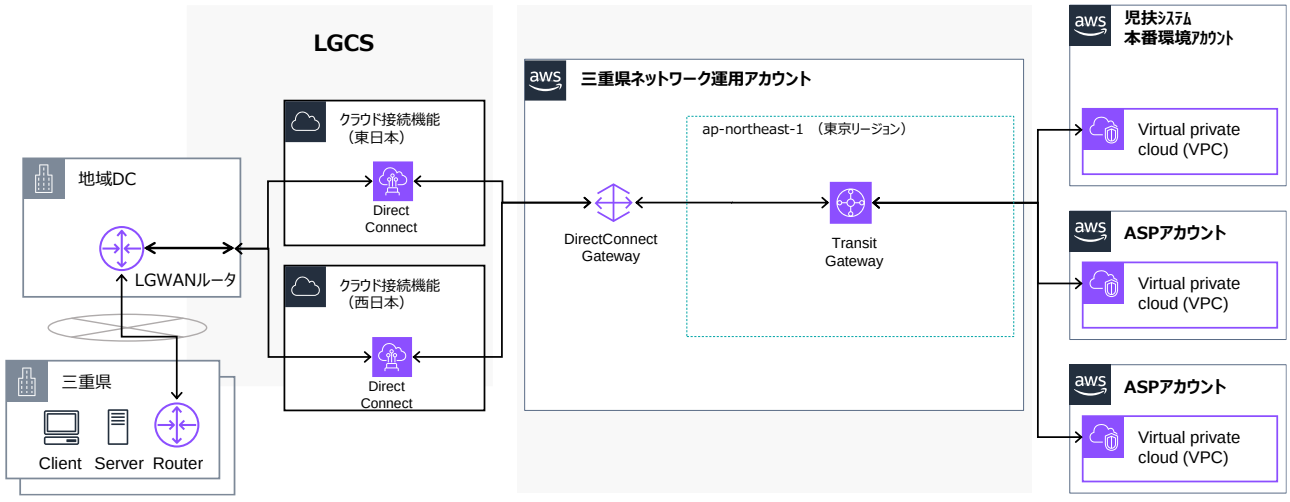

図 10-1 ガバメントクラウドの構成概要

10.9. セキュリティパッチ対応

・ 必要に応じて、本受託事業者が納入した機器及び既存システムの運用対象機器に係るファームウェア、セキュリティパッチの適用等のメンテナンスを行うこと。実施するタイミングとしては、セキュリティパッチリリース時、脆弱性の公開時、インシデント発生

時、共通機能基盤の OS アップデート等を想定すること。
・ ファームウェア、セキュリティパッチの適用においては、事前評価したうえで作業すること。

10.10. 引継ぎ業務

10.10.1. 現行ネットワーク受託事業者等からの引継ぎ

・ 次期ネットワーク移行までに、本県立ち会いのもと、運用業務を行うにあたり必要な引継ぎを現行ネットワーク受託事業者及び既存システム受託事業者から受けること。引継ぎの内容やスケジュールについては本県職員と協議のうえで実施すること。
・ 運用業務中のシステム状況や運用に必要な手順等、現行ネットワーク受託事業者及び既存システム受託事業者からの情報共有を適宜実施すること。
・ 本県からは引継ぎを行わないため、各受託事業者から業務の一切を引継ぐこと。
・ 現行ネットワークの運用期間中にガバメントクラウドへの接続等を実施する。ガバメントクラウド上のネットワーク運用管理は、別途調達する運用管理補助者が実施するが、ガバメントクラウド上の CIDR 設計・管理や、ガバメントクラウド接続のための次期ネットワーク内の各種設定作業については本受託事業者が実施する。現時点では未構築だが、本作業についても引継ぎを行うこと。

10.10.2. 本県が指定する受託事業者への引継ぎ

・ 本業務終了に伴い、本県が指定する受託事業者へ運用業務の一切をもれなく引継ぐこと。また、移行等のネットワーク変更が生じる場合は必要に応じて技術的なサポートを行うこと。

10.11. 職員等研修

次期ネットワークに係る全体把握のため、本県からの依頼に応じて本県職員等に対する研修を実施すること。現在想定している開催頻度及び対象者は以下のとおり。また、研修に必要な説明書類・マニュアル等を作成すること。

・ 次期ネットワーク導入時、年度始めにヘルプデスク（15 名程度）及び本県ネットワーク担当職員（デジタル改革推進課情報基盤班：10 名程度）向けの説明会を実施
・ 次期ネットワーク導入時、本県システム担当職員（50 名程度）向けの説明会を実施

10.12. 既存システムの運用

既存システムを構成するハードウェア、ソフトウェアに対する保守業務は既存システム受託事業者にて遂行されるため本業務には含まないが、一部の運用業務については本業務に含まれるものとし、各受託事業者から説明を受けたうえで、運用管理 SE が実施するものとする。詳細については「2.5 本県からの提供資料」で開示する資料を参照すること。

なお、現在運用を行っている既存システムは以下のとおり。実施する運用業務の詳細については本県と協議のうえ、業務内容を確定すること。

- ユーザ認証システム
- 三重県 DX 推進基盤

10.12.1. 各既存システムに係る運用業務の概要

各既存システムに係る運用業務について、以下に主要な業務を示す。詳細な業務内容及び現在の作業手順書については契約後別途提示する。

なお、各既存システムについては、次期ネットワーク運用期間中において更改を予定しているため、各受託事業者から示される手順書に基づき、運用業務を行うこと。

10.12.1.1 ユーザ認証システム

ユーザ認証システムにおいて、AD、WSUS、資産管理ソフトを導入している。本業務においては以下の運用業務を行うこと。

- AD の運用
  - 本県からの依頼に応じて、ユーザオブジェクトの新規登録、登録内容の変更、削除、パスワード初期化対応等を行うこと。
  - 本県からの依頼に応じて、コンピュータオブジェクトの新規登録、登録内容の変更、削除対応等を行うこと。
  - 本県からの依頼に応じて、OU の新規登録、登録内容の変更、削除対応、オブジェクトの登録、移動等を行うこと。
  - グループポリシーの設定や適用を行うこと。
  - 各オブジェクト、OU、グループポリシー等の構成管理を行うこと。
  - ユーザ認証システムで導入している内部 DNS において、三重県行政 WAN 内部のサーバ、端末等の名前解決を行っているため、レコードの加除等、必要な設定や構成管理を行うこと。
  - AD サーバを一部の無線 LAN の認証局としても利用しているため、証明書の配布、削除、更新等必要な対応をすること。

なお、上記の設定作業については、本県が別途調達する職員アカウント集中管理システムにて各オブジェクトの登録等を依頼し、同システムから出力される CSV ファイルをバッチ処理にて AD にインポートすることで対応している。

特に年度末において、組織変更や大規模な人事異動が行われるため、毎年度3月31日の時間外に、一括処理等により上記の設定作業を行うこと。

- WSUSの運用
  - セキュリティパッチの配信を行うためのWSUSサーバを運用している。
  - WSUSサーバに対して、各セキュリティパッチ等のダウンロード許可を行うこと。
  - 本業務において導入するサーバ類及びユーザ認証システムへの配信（セキュリティパッチ等の適用）作業を行うこと。

- 資産管理ソフトの運用
  - 本県からの依頼に応じて資産管理ソフトを用いて、ウイルス対策ソフトやEDR等のソフトウェア、WSUSにて配信できないアップデートファイル等の配信を実施すること。
  - 各種実行ファイルの配信を行うこと。
  - クライアント端末の監視を行うこと。

10.12.1.2 三重県DX推進基盤

ユーザ認証システムで導入したADの拡張属性を用いて、三重県DX推進基盤で導入しているEntra IDやMicrosoft 365、Slack等への連携を行っている。連携にあたっては三重県DX推進基盤で導入したEntra ID Connect用の連携サーバ（Entra ID Connectサーバ）を中継している。また、Entra ID Connectサーバにてメールボックスの作成や、各種権限設定を行っている。

主な業務要件は以下のとおり。

- ADのユーザオブジェクトにおいて、拡張属性値を設定し、Entra IDやMicrosoft 365、Slack等への連携を行うこと。
- インターネットメールアカウントの登録や削除等について、運用マニュアルに基づき設定作業を行うこと。
- 本県からの依頼に応じて、メールボックスの作成、削除等を行うこと。
- 本県からの依頼に応じて、Outlookにおけるメールや予定表の参照、送受信、代理登録等の権限設定を行うこと。
- 必要に応じて、Entra ID Connectサーバ等との同期処理を行うこと。
- SherePoint Online上のグループウェアにおいて、職員情報を一覧化のうえ、検索可能な電子職員録アプリをPowerAppsで作成し、職員向けに公開しているため、電子職員録アプリへのユーザ情報登録、変更、削除処理を行うこと。

10.13. サーバのバックアップ及びリストア

- サーバのデータバックアップを行うこと。また、システム障害時には、必要に応じて、バックアップデータからのリストア作業を行うこと。
- サーババックアップ計画の作成及びバックアップデータの管理を行うこと。
- 共通機能基盤上に仮想サーバを構築する場合は、共通機能基盤の受託事業者側でバックアップ管理を実施するが、システム状況や運用に必要な手順等、本受託事業者からの情報共有を適時実施すること。
- ファイルサーバのデータバックアップを行うこと。また、本県からの依頼に応じてファイルやフォルダ単位でリストア作業を行うこと。

10.14. 停電対応

- 本庁舎の停電時にネットワーク機器やサーバ等の停止、再起動及び動作確認を行うこと。
- 停電の実施にあたって、監視抑止等、監視業務に関する調整を行うこと。

10.15. 必要物品

- 問い合わせ・障害対応用に、電話を運用管理 SE の常駐拠点である本庁舎及び IDC に用意すること。なお、設置工事費、基本料金及び通話料金は本受託事業者の負担とする。
- コピー機、プリンタ、作業机は、本県の備品を使用可能とする。
- 本庁舎内線専用の PHS を 1 台、本県より貸与可能であるが、故意又は過失により貸与した PHS が故障もしくは紛失した場合は、本受託事業者が費用負担を行うものとする。
- 管理用 PC 等、上記以外で業務を遂行するにあたり必要となる物品について、全て本受託事業者にて用意すること。ただし、本県が不足と判断した場合には、管理用 PC 等の端末の増設や、本県が求める性能の端末の用意すること。
- 本庁舎の運用管理 SE は、他の拠点で障害対応を行う際に車で移動できるようにしておくこと。また、本県の指示により可能な範囲で機器の運搬を行うこと。
- 本県が貸付した物品や修理依頼された物品、管理を委託された物品等について、情報漏えいや紛失等が起こらないよう適切に管理すること。

10.16. 技術支援

- 運用管理全般に係る技術支援を行うこと。
- 自治体中間サーバ団体用 VPN 装置の設定について、本県の要請により技術支援を行うこと。
- 障害監視サーバの性能監視による通知や、本県職員からの申告等で、三重県行政 WAN・情

報ネットワーク内に性能劣化等の不具合が発覚した場合、性能劣化の原因解析及び対処方法の検討を行い、担当職員へ報告すること。また、担当職員の指示により、設定・構成変更等の対処を行うこと。

- 無線 LAN 導入拠点において、年度末等、フロアのレイアウト変更が発生した際、電波不達の場所が発生した場合には、予備機を利用し、無線 LAN アクセスポイントを増設すること。作業にあたっては石綿（アスベスト）含有の事前調査および対策等、必要な安全対策を実施すること。なお、無線 LAN アクセスポイント設置個所までの配線工事については本県にて実施することを想定している。

10.17. 問い合わせ対応

- 本県からの次期ネットワークに関する各種問い合わせに対応すること。
- 本県からの指示により、必要なデータを抽出及び作成すること。
- 本県職員からの問い合わせは、別途調達するヘルプデスクが一次受付を行う。本業務においては、一次受付後、ヘルプデスクからエスカレーションした内容を受けて、機器ベンダや各受託事業者へ問い合わせや作業依頼等を行う、運用統括業務を実施すること。
- 原課が個別に調達しているシステムの担当職員及びベンダからの各種問い合わせにも対応し、必要な技術支援を行うこと。

10.18. インシデント・問い合わせ管理

次期ネットワークで発生した障害や実施した作業、問い合わせ等の内容を発生・受付から復旧・解決まで記録し、管理・閲覧する仕組みを提供すること。なお、本県が所有する Microsoft 365 ライセンスも利用可能とする。

- 本県及び関係者からの次期ネットワークに関する各種問い合わせに対応すること。
- 対応する問い合わせは、本県ネットワーク担当職員、ヘルプデスク、各受託事業者、及び各情報システム担当職員からの問い合わせを想定している。
- 次期ネットワークのサポート用 Web ポータルサイトを作成可能であること。
- Web ポータルサイトによくある質問と回答（FAQ）を公開可能であること。
- Web ポータルサイトに「問い合わせ・依頼」のリンクを作成し、インシデント管理システムへ誘導可能であること。
- 利用者が「問い合わせ・依頼」を登録できる Web フォームを用意すること。
- 利用者が Web フォームより登録を行う際に、氏名や所属・連絡先等が自動反映されること。
- 利用者が登録を行った際にチケット（管理）番号を自動発番できること。
- インシデント情報の登録・更新時に関係者へメール通知等ができること。
- インシデント管理データは、運用期間中のデータを保管できること。
- インシデント管理データを FAQ やナレッジ等に利活用ができること。

- インシデント管理データは、管理番号・日時・起票者・依頼者・ステータス等の条件で検索できること。
- 検索条件を指定して、レポート集計ができること。
- いつ、誰が何を更新したのか、登録内容の更新履歴が確認できること。
- 次期ネットワークの構成情報、ドキュメント、コンフィグ、ナレッジ等を利用者に対して、共有できること。また、利用者や共有内容に応じて適切にアクセス制御を行うこと。
- 次期ネットワークでの利用及び運用が可能であれば、オンプレミスでもクラウドサービス利用でも可とする。

10.19. 想定業務量

運用業務の想定業務量を、「表 10-1 想定業務量」示す。想定業務量は目安であり、状況により変動する。なお、現行ネットワークでは以下の業務を 4 人の運用管理 SE で実施している。

表 10-1 想定業務量

No	項目	想定業務量
1	運用統括業務	随時：1 回/日
2	構成管理	随時：1 回/週
3	ドキュメント管理	随時：1 回/月
4	電源管理	随時：1 回/年
5	設定変更	随時：1 回/月
6	セキュリティパッチ対応	随時：12 回/年（案件毎）
7	引継ぎ業務	契約開始時及び完了時：5 日間
8	既存システムの運用	随時：1 回/日
9	サーバのバックアップ及びリストア	定期：1 回/月
10	庁舎停電対応	定期：1 回/年
11	技術支援	随時：3 回/月
12	問い合わせ対応	随時：3 回/日
13	稼働確認・日時報告	随時：1 回/日

11.情報セキュリティ対策

本章では、次期ネットワークの情報セキュリティ対策を遂行するにあたり、本県が要求する事項を記載する。

11.1. 方針

- セキュリティ対策は、「地方公共団体における情報セキュリティポリシーに関するガイドライン」、「三重県電子情報安全対策基準（三重県情報セキュリティポリシー）」、「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」、「三重県個人情報の保護に関する法律施行条例」等に示されるセキュリティ対策事項を参考に実施すること。
- ＜提案＞セキュリティインシデントの状況を正確に把握できるよう、適切に分類し、報告を行うこと。
- ＜提案＞情報漏えいが疑われる、又は発生した場合、流出経路の特定等の調査を行い、対策を講じられるようにすること。
- 不要な通信は抑制すること。

11.2. アクセス制御・権限管理

- アカウントはサービスにおける作業者の役割毎（各種システム操作を含む）に作成し、作業に必要な権限のみの付与等、目的に応じた適切なアクセス制限、権限管理及び設定を行うこと。
- アクセス制御は拒否を前提とし、必要な通信のみを許可する方針とすること。管理者権限を持つアカウントを利用する場合には、管理者としての業務遂行時に限定して利用すること。
- 運用管理者が変更になった場合やシステム変更等の理由で不要となった運用管理者等のアカウントは、即時アカウントを削除又はアクセス権を削除し、使い回すことのないようにすること。
- サーバやデータへのアクセスについてはアクセス権限を適切に設定すること。ただし、業務データ等を含まない場合はこの限りではない。
- ユーザ情報を持つ場合は、人事異動及び組織改編に伴うユーザの一括登録、削除が行えること。ただし、IDaaS 等、外部の認証基盤と同期する場合はこの限りではない。

11.3. ログの取得・管理

- 本業務で提供するサービスの証跡ログを収集すること。
- 内部からの不正操作、誤操作等による情報セキュリティ上の脅威に対応するため、管理

者権限操作を含めた証跡ログを取得すること。
- 不正行為の追跡や情報セキュリティ侵害時において証跡の解析等を容易にするため、正確な時刻に同期する機能を備えること。
- 特に指定のない限り、証跡ログの保存期間は全ての機能において、1 年以上とし、直近 30 日分はすぐに分析できる状態とすること。

11.4. ソフトウェアに関する脆弱性対策

- 本業務において導入する全てのファームウェア、ソフトウェア等に関連するセキュリティホール情報は公開され次第、入手できるよう体制を整えること。脆弱性に関する情報が公開された場合、当該脆弱性がもたらすリスクを確認したうえで本県へ報告すること。
- セキュリティホール対策の実施に際しては、事前に影響を検討のうえ、検証作業等を実施し、それらの結果を踏まえて本県との協議により対応を決定すること。ただし、クラウドサービスにおいては、その限りではない。
- 機器やソフトウェアはアカウント、パスワード等を初期設定値の状態で運用しないこと。また、推察されやすい安易なユーザアカウント、パスワード等を設定しないこと。
- 利用者への提供及び運用に用いるものを除く、不要なプロセス、サービス等は原則停止すること。ただし、クラウドサービスにおいては、その限りではない。

11.4.1. セキュリティ管理

- 本調達で導入した機器等で使用するソフトウェア製品に関するバグフィックス、セキュリティパッチ等がリリースされた場合、速やかにその内容の調査を行い、本調達で導入した機器等に対する影響の調査、適用の可否を本県に報告すること。
- ＜提案＞迅速な脆弱性情報の収集方法や新たな脅威への対応方法について具体的な提案があれば記載すること。
- 本調達で導入した機器等に影響を及ぼすおそれのあるセキュリティパッチ等の提供がある場合、本受託事業者が影響の有無を確認したうえで、可能な限り影響が少なくなる手順を提案すること。また、システムベンダ等が該当セキュリティパッチの適用を行う場合は適宜立ち会い等を行うこと。
- 脆弱性情報に基づくインシデントの未然防止を行うこと。
- 脆弱性情報については、JVN（Japan Vulnerability Notes）やメーカ/ベンダのサポートサイト、メール通知等で情報収集を実施すること。報告要否の定義等については、本県と協議のうえで決定すること。
- 重大な脆弱性を検出した際は速やかに一次報告したうえで、影響範囲の調査や対応策の検討等を行うこと。
- ＜提案＞本県が別途契約するシステム等についても、機器やインストールされてい

るソフトウェア等の情報から該当有無を判定し、本県又は各受託事業者に通知すること。

11.5. 不正プログラム対策

- 本業務において導入する機器等について、不正プログラムの検知及びその実行の防止の機能を有する対策ソフトウェアを導入すること。ただし、当該機器で動作可能な不正プログラム対策ソフトウェアが存在しない場合を除く。
- 本業務において導入する機器等について、不正プログラム対策は、別途契約済みの EPP（Windows Defender 等）を利用すること。

11.6. セキュリティインシデントへの対応

- ＜提案＞セキュリティインシデントが発生した場合に備え、連絡体制・対応手順等を明示して、本県の承認を得ること。
- セキュリティインシデントが発生した場合又はそのおそれがある場合には、速やかに本県へ報告すること。また、各受託事業者やベンダへのエスカレーション、原因解析、ワークアラウンド対策の検討、設定変更等の作業を実施すること。
- セキュリティインシデントに関する問い合わせについて、24 時間 365 日受付可能とすること。
- 重大セキュリティインシデント以外のセキュリティインシデントについては、別途定める運用業務の時間内において、対応すること。ただし、業務時間内に確認されたインシデントに関しては、重大セキュリティインシデントの判断がつくまで対応すること。
- 重大セキュリティインシデントの具体的な定義については、本県と協議のうえ、決定すること。
- 業務端末への侵入検知と対応は、別途契約済みの EDR を利用すること。

12.監視業務

本章では、次期ネットワークの監視業務を遂行するにあたり、本県が要求する事項を記載する。
監視設計時に、以下の詳細要件を実現できるよう設計を行うこと。

12.1. 監視体制

監視業務を確実に実施するため、監視専用の障害監視センターを設置すること。

12.1.1. 障害監視センター

- 監視センターでは、次期ネットワークにおいて導入する機器類及び既存システム（ユーザ認証システム、マイナンバー利用事務系ネットワーク）のうち、本県が指定する機器等及び各種サービスについて 24 時間 365 日の有人監視を行うこと。また、必要に応じて本県職員や各受託事業者からの電話による問い合わせに対応すること。
- 本業務で提供する各種サービスが提供できなくなる等の重大な事案（機器障害、外部からの攻撃等によるサービス停止等）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。
- 監視センターと次期ネットワークを専用線にてセキュリティを保ったうえで接続すること。専用線の整備についても本契約に含まれるものとする。
- 監視センターでは、機器へのログイン、設定変更、再起動等が可能であること。これは、平日日中等の運用管理 SE の勤務時間については、運用管理 SE が作業を行うことを想定しているが、夜間等で運用管理 SE の不在時に監視センターでの機器へのログイン、設定変更、再起動等の緊急対応を想定している。
- 監視センターからリモートアクセスで次期ネットワークを監視するために必要な機器や回線は本受託事業者が用意すること。また、アクセス制御や ID 認証を確実に行う等、十分なセキュリティ対策を講じること。
- 必要であれば、監視センターから本県職員等に直接電話等で連絡すること。連絡が必要な基準は契約後に本県と協議し、決定すること。

12.2. 障害監視

- 障害監視システムにより、次期ネットワーク、ユーザ認証システム、マイナンバー利用事務系ネットワークを 24 時間 365 日、本受託事業者が準備する外部の監視拠点等から有人にて監視すること。
- 外部の監視拠点からリモートアクセスで次期ネットワークを監視するために必要な機器や回線は本受託事業者が用意すること。また、アクセス制御や ID 認証を確実に行う等、

十分なセキュリティ対策を講じること。
- 各種ログについて異常がないかチェックし、異常がある場合は本県に報告すること。
- 障害発生から初期対応を開始するまでの時間を、30 分以内とすること。ただし、大規模災害発生時はこの限りではないが、可能な限り対応すること。なお、初期対応とは、障害発生箇所・原因の確認作業への着手、本県や関係者への連絡等を指す。
- 監視対象、監視方法、閾値等の管理を行うこと。なお、本県からの監視内容、設定及び閾値等の変更要望についても検討し、調整を行うこと。

12.3. 性能監視

- 本業務で導入する機器について、CPU 使用率、HDD 使用率、メモリ使用率等、各種リソース情報の収集・分析を行い、適正な性能の範囲であるか定期的に監視すること。監視内容の詳細として、方法（死活監視、サービス監視、プロセス監視、http 監視等）や閾値、時間間隔等について、本県と協議のうえ、定めること。
- 異常（閾値を超えた状況等）が検知された場合、本県並びに本県が指定する所定の連絡先に通報すること。
- 適正な範囲外の状態が継続する場合は、対策案を報告し、本県の承認のうえ、対策を講じること。
- トラフィック情報の監視を行い、トラフィックの解析を行うこと。
- トラフィック情報の監視方法の詳細や時間間隔等について、本県と協議のうえ、定めること。

12.4. セキュリティ監視

- 本業務で導入する機器について、「11 情報セキュリティ対策」に記載の管理や対策のための監視を常時実施すること。監視対象、アラート・通知レベル等については、本県と協議のうえ、定めること。

12.5. 障害発生時における対応

- 「12.2 障害監視」で監視対象としている機器等について、障害発生時に、予め作成した手順書等に基づき、障害箇所の一次切り分けを行うこと。ここでいう一次切り分けとは、本業務において導入される機器、サービスにおいては機器、サービス単位で障害箇所を特定すること、既存システム、回線等においては障害箇所が次期ネットワーク側か、既存システム、回線側によるものかを切り分けることを指す。
- 障害検知した際は速やかに本県へ報告すること。
- 障害箇所特定のため、必要に応じて、関係者への協力依頼を行うこと。
- 一次切り分けの結果、障害原因が回線にある場合は、速やかにそれぞれの回線受託事業

者等と連絡を取り、対応を行うこと。

・　障害により業務への影響が考えられる場合、速やかに関係者へ連絡を行うこと。

13.保守業務

本章では、次期ネットワークの保守業務を遂行するにあたり、本県が要求する事項を記載する。
保守設計時に、以下の詳細要件を実現できるよう設計を行うこと。

13.1. 保守受付

13.1.1. 管理・連絡体制

- 緊急時に本県と確実に連絡がとれるよう、連絡体制を整えること。
- 障害対応等の連絡窓口は、平日の 7 時 30 分から 20 時 00 分は運用管理 SE とし、休日・夜間帯については障害監視センター等の単一窓口にて受け付けること。

13.1.2. 保守受付時間

- 保守受付時間は、24 時間 365 日とすること。

13.2. 障害対応

13.2.1. 保守対応時間

- 保守対応時間は、IDC、本庁舎、総合庁舎、吉田山会館、勤労者福祉会館、栄町庁舎、合同ビル、市町等利用機関においては、24 時間 365 日を原則とする。ただし、それ以外の拠点については、平日の 8 時 30 分から 17 時 15 分までの対応を原則とする。
- 保守対応時間外に障害が発生した場合は、可能な範囲で保守対応を行うこと。

13.2.2. 障害時の対応

- ＜提案＞「12.2 障害監視」の結果、本受託事業者が納入した機器等が障害原因であると判明した場合、又は切り分けが困難で障害原因が特定できない場合は、障害発生拠点へ駆け付け、不良部位の切り分け及び修理・修正・交換等を行うこと。オンサイトでの保守対応が不可能な部位がある場合については、予備品の保有等により迅速な復旧を実現すること。
- ＜提案＞IDC、本庁舎で障害が発生した場合、物品交換が必要と判断してから、駆け付け完了までの時間を 1 時間以内とすること。その他拠点においては、駆け付け完了までの時間を 2 時間以内とすること。また、尾鷲・熊野地域においては、駆け付け完了までの時間を 4 時間以内とする。ただし、大規模災害発生時はこの限りでは

ないが、可能な限り速やかに対応すること。駆け付け 4 時間以内とする拠点の詳細については、本県と協議とする。なお、平日夜間や休日の対応については、本県と協議すること。

- 障害により業務への影響が考えられる場合は速やかに関係者（本県が指定する所定の連絡先）へ連絡を行うこと。
- 障害発生時の対応記録を時系列に沿って記録し、本県職員へ共有すること。
- 復旧方法が明らかになり、かつ復旧作業が必要な場所へ到着してから、復旧するまでを 2 時間以内とすること。ただし、2 時間以内の復旧が困難と判明した場合は、2 時間以内に復旧見込み時間と対応スケジュールを報告すること。大規模災害発生時はこの限りではないが、可能な限り速やかに対応すること。
- 障害原因がハードウェアにある場合は速やかに代替機器の調整を行い、交換作業を行うこと。
- 障害原因がソフトウェアにある場合は、OS のバージョンアップ、ファームウェアのバージョンアップ、アプリケーション設定等の適切な調整を行い、対応すること。
- OS のバージョンアップ等においては、事前評価したうえ、作業すること。
- 障害によりソフトウェア、データが破損した場合、バックアップデータ等より速やかに復旧作業を行うこと。
- 性能監視において、異常（閾値を超えた状況等）が検知された場合は、調査のうえ、故障の予兆とみられる場合は、予備機に交換する等、予防措置を講じること。
- 常時保守部品（付属品、ソフトウェア等を含む）を適切に管理し、迅速な対応を可能とすること。

13.2.3. 障害事後対応

- ＜提案＞本受託事業者が納入した機器に起因する障害に限らず、次期ネットワークで発生した全ての障害に対する障害事後対策として、収集した障害情報を分析し、同様の障害が発生しないように機器の予防交換等の是正措置・予防措置を講じること。直ちに障害原因が判明しない場合は、本県の承認を得たうえで、継続して調査を行い、障害原因の特定に努めること。また、業務への影響を最小限にするための対策を講じること。
- 障害情報、是正措置・予防措置の内容は障害記録として体系的に記録のうえ、障害報告書として随時提出し、ポータルサイトに掲載すること。また、常に活用できるように保存すること。

13.3. その他

13.3.1. 保守物品・消耗品

本業務を実施するうえで必要な保守部品（付属品、ソフトウェアを含む）を常時保有するとともに、契約期間における供給が可能なこと。なお、製造中止等に伴いこれらの対応ができなくなったときは次期ネットワークに影響がないと本県が判断した場合に限り、代替品による提供も可とする。

- 製造会社のサポートやサービスの終了（EOL：End of Life）等により前項の対応ができなくなった場合は、同等以上の機能及び性能を有する代替品等による提供も可とする。その場合、それぞれの機器が EOL を迎える前に、代替品について本県の承認を得ること。
- 運用業務で必要な消耗品や備品等については、契約期間内において必要な量を見積り、納入すること。

13.3.2. 本庁舎・吉田山会館の光回線

- 障害発生時に屋外無線での通信に切り替える等、正常な動作をするよう、本県と協議したうえで可能な範囲で障害対応を行うこと。

13.3.3. 無停電電源装置

- 本調達にて設置する全ての UPS のバッテリについて適切な状態を保つこと。
- バッテリの耐用年数を経過した場合は新しいバッテリと交換のうえ、古いバッテリは撤去すること。

13.3.4. 問い合わせ

- 本県からの各種問い合わせに対応すること。また、対応方法を検討し、対応までに要する時間も含めて回答すること。

14.契約終了時の措置

本章では、本業務における契約終了時の措置に関する要求事項を記載する。

14.1. 撤去及びデータ消去業務の管理

本業務終了時、本受託事業者が納入したハードウェア等については、本県が指示するものを除き、本受託事業者でデータの完全な消去等を行ったうえ、撤去すること。クラウドサービスについては、データの完全な消去を行うこと。

① データ消去作業計画書

- データの消去にあたっては、事前にデータ消去作業計画書を作成し、本県の承認を得ること。
- データ消去作業計画書には、作業体制、役割、作業工程及びスケジュール等を記載すること。
- 契約締結後本県より開示する、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）に則り、適切に対応すること。

② 作業体制

- 本県との窓口となり、撤去及びデータ消去作業計画についての進捗管理及び課題管理、問題解決を行う作業責任者を配置すること。
- 作業責任者は、本業務の内容、進捗状況、課題等を把握し、本県と円滑な調整を実施すること。
- 本業務を滞りなく遂行できる人数の作業担当者を配置すること。
- 撤去及びデータ消去作業の期間中、作業者や第三者及び県の資産等全ての安全について責任を持って管理すること。

14.1.1. 機器の撤去

① 撤去の範囲

- 撤去範囲については、原則、本業務において本受託事業者が納入する機器等一式とする。本庁舎、IDC 等の全ての拠点を対象とする。残置については、本県と本受託事業者が協議のうえ、決定すること。

② 撤去の時期

- 次々期情報ネットワークへの更新の際には、次期ネットワークの機器の撤去を開始し、令和 14 年 3 月末までに完了すること。

③ 撤去の方法

・ ラックに搭載されている機器を取り外すこと。
・ 天井や壁に取り付けた機器を取り外すこと。
・ 本受託事業者が用意したラックがある場合は、ラックと架台を撤去すること。
・ ラックと架台を撤去する際、耐震固定のアンカーボルト跡及びフリーアクセスパネルについて、補修すること。
・ 本受託事業者が用意したLANケーブル等の配線を撤去すること。

14.1.2. 機器のデータ消去・破壊

① データ消去・破壊の範囲
・ 本業務において本受託事業者が納入する機器等一式とする。ネットワーク機器のコンフィグやログ、サーバ機器のハードディスク等の記憶媒体に保存されている内容を対象とする。

② データ消去・破壊の時期
・ 令和14年3月末までの別途指示する期間に機器のデータ消去・破壊等を実施すること。

③ データ消去・破壊の方法
・ ハードディスク等の記憶媒体に保存されているデータの消去・物理的破壊等を実施すること。
・ データ消去・破壊等の作業を実施した後、作業完了を証明する「データ消去作業完了証明書」を作成し、本県に提出すること。なお、破壊を実施した際には当該証明書に証拠写真を添付すること。
・ 作業完了を証明する書類には、消去を実施した機器の管理名称、機種、シリアル番号等の情報を含めること。

④ データ消去・破壊の方法
・ 本庁舎及び各拠点にはデータ消去・破壊等の作業場所が確保できないため、本受託事業者の責により、一時保管場所（作業場所）を確保すること。
・ 一時保管場所は、部外者の侵入等を防止する設備・体制の整った場所とすること。本受託事業者は、一時保管場所について本県の承認を得ること。

14.2. 次々期情報ネットワーク受託事業者への引継ぎ

14.2.1. 期間

・ 次々期情報ネットワークへの更新の際には、本県からの依頼に基づき質疑応答、業

務の引継ぎ及び移行に伴う情報ネットワークにおける各システムの設定作業を行うこと。

14.2.2. 対応内容

現時点で想定される引継ぎ作業等を以下に示す。記載された作業の引継ぎ元は、本受託事業者を前提とする。なお、引継ぎの対応時期は想定であり、変更する場合があるため、注意すること。

表 14-1 想定される引継ぎ作業

対応時期	引継ぎ先	対応内容
次々期情報ネットワークの仕様策定時 （令和 11 年度）	次々期情報ネットワーク調達支援事業者	・ 設計・構築及び運用・保守に係る資料・情報の提供
次々期情報ネットワークの調達時 （令和 11 年度）	次々期情報ネットワーク調達支援事業者	・ 設計・構築及び運用・保守に係る資料・情報の提供 ・ 引継ぎ資料の提供 ・ 残課題の提供 ・ 改善提案の提供
次々期情報ネットワークの設計・構築時 （令和 12 年度）	次々期情報ネットワーク受託事業者	・ 設計・構築及び運用・保守に係る資料・情報の提供 ・ 引継ぎ資料の提供 ・ 残課題の提供 ・ 改善提案等の提供
次々期情報ネットワークへの移行時 （令和 13 年度）	次々期情報ネットワーク受託事業者	・ 情報ネットワークに格納された各種データ類の提供 ・ 移行に伴う情報ネットワークの設定作業等

- 令和 12 年度に決定が予定される次々期情報ネットワークに係る各受託事業者からの質疑応答や情報・データ提供依頼には協力を行うこと。
- 上述の引継ぎ時期以外においても、本県の要求に応じて情報提供等を行えるように本受託事業者は引継ぎ内容を常に整理しておくこと。なお、次々期情報ネットワークの更改時や他のシステム等へのデータ移行が必要となる場合、情報ネットワークからデータを抽出し、本県に提供すること。

14.2.3. 次々期情報ネットワークへの移行に伴う作業

- 次々期情報ネットワークへの移行の際には、本県からの依頼に基づき、移行に必要な情報ネットワークにおける各システムの設定作業を行うこと。

15.サービスレベル要件

次期ネットワークについて、24 時間 365 日稼動できる体制を整えること。SLA は次期ネットワークの保守・運用業務開始時点から適用する。なお、保守・運用業務開始の時期は、本県と本受託事業者との協議において判断する。

サービスレベル基準値を下回った場合、減額基準に基づき、運用・監視・保守管理業務に係る費用を減額する。また、減額にかかわらず、再発を防止することを目的として速やかに改善策を提示すること。

15.1. 指標の設定

運用・監視・保守管理業務品質の維持・向上を図るため、本受託事業者は本県と SLA を締結すること。なお、本県が想定しているサービスレベル設定基準は「【別紙 3】サービスレベル設定基準（ネットワーク）」に示す。

＜提案＞提供するサービスレベルについて、基本的方針・考え方を示し、提案を行うこと。また、「【別紙 3】サービスレベル設定基準（ネットワーク）」で定めているサービス内容/サービスレベル基準値/遵守率より厳格な提案があれば記載すること。

15.2. SLA のモニタリング

本受託事業者は SLA の履行状況について毎月報告すること。

15.3. 減額基準

15.3.1. 減額ポイントの集計方法

本受託事業者が達成しなければならないサービスレベルを満たさなかった場合は、次に定める計算式により減額ポイントを集計する。項目別減額ポイントは「【別紙 3】サービスレベル設定基準（ネットワーク）」の減額ポイント欄に定める。

また、減額対象の判断については、測定時期単位毎にサービスレベルの測定を行い、本受託事業者と本県の協議のうえ判断する。半期毎に集計を行い本受託事業者と本県の協議のうえ、決定することを想定する。

（計算式）

ｓ＝ｐ × ｃ

ｓ：項目別減額ポイント

ｐ：減額ポイント

c：発生回数（測定時期単位ごとに各項目単位でカウントする。また、遵守率 100%かつ、回数で基準値を設けている項目は、基準値を超過する度にカウントする。）

集計後減額ポイント = Σ s

15.3.2. 集計後減額ポイントの累積

集計後減額ポイントは、次の規定により消滅するまでは、次期の集計に繰り越し累積するものとする。

15.3.3. 集計後減額ポイントの消滅

集計後減額ポイント（累積されているものを含む。以下同じ。）は、当該集計後減額ポイントに基づき本県が次のペナルティ基準によりペナルティを課した場合、又は測定時期より 1 か年を経過した場合に消滅する。

15.3.4. ペナルティ基準

本県が、集計後減額ポイントに基づき、本受託事業者に対して課すペナルティは次のとおりとする。

- 対象項目における集計後減額ポイントの合計が 60 ポイント以上となった場合は、当該半期分運用保守費用の 10%を減ずる。

15.4. 改善

- 本受託事業者は SLA が遵守できているか運用の中で評価し、評価した結果を受けてサービスレベルの改善を本県の承認のうえで継続して行うこと。
- SLA が遵守できない場合は原因を特定し、報告するとともに、改善策・対応結果について報告すること。
- 改善に関する費用は本受託事業者が負担すること。

15.5. SLA 適用除外条件

以下のいずれかに該当する場合は、上記 SLA の適用外とする。

- 本庁舎や総合庁舎の計画停電
- 公共交通機関の停止、災害による電源供給の停止や通信障害の場合
- 本県又は他の事業者の過失及び故意による障害の場合
- 本受託事業者の瑕疵によらず障害復旧が行えない場合

・　本受託事業者の瑕疵によらず障害監視が行えない場合
・　本受託事業者の瑕疵によらず障害通知の受信ができない場合
・　本県及び本受託事業者双方の協議のうえ、計測の除外とした場合

15.6.　クラウドサービスの利用

クラウドサービスの稼働率等は各サービスの SLA に準ずるものとする。なお、各クラウドサービスの SLA を事前に提示し、本県の承認を得ること。

16.その他

16.1. 各受託事業者との協議・調整

- 各受託事業者が納入した機器等について、本業務を実施するうえで設定変更等が必要となる場合は、本県の承認のもと、それらの機器を所管する各受託事業者と協議等を実施したうえで、設定変更に必要な支援を行うこと。
- 実際の設定変更作業は各受託事業者との契約の範囲内で本県を通じて依頼が可能である。そのため、契約の範囲を越えないように注意すること。
- なお、契約の範囲を超えても本県に対して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場合は、別途協議を行うこととする。
- 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、問い合わせ対応等の運用保守業務を想定している。ただし、作業時の立ち会いにおいては、各受託事業者により対応が分かれるため、注意すること。

16.2. 追加提案

＜提案＞次期ネットワークが本県の業務遂行にとって非常に重要な位置付けであることを踏まえ、これまでの項目に係る提案とは別に、以下の項目について、追加提案が可能であれば記載すること。追加提案要素の実装は設計時に本県と協議のうえで決定する。

ただし、追加提案要素の実現に係る費用については本受託事業者が負担すること。

- 既存システムで提供している機能やサービス内容を損なうことなく、性能・効率・耐障害性等の向上が可能な設計・構成や、目指す姿に向けて有効と考えられる追加機能について提案を行うこと。
- 運用・保守業務等、運用期間中の業務において、本県の想定を超える効果が期待でき、かつ確実に実施できる取り組みやサービスについて提案を行うこと。

17.別紙

【別紙1】ネットワーク設計構築拠点一覧
【別紙2】更新機器一覧
【別紙3】サービスレベル設定基準（ネットワーク）
【別紙4】次期ネットワーク構成概要図
【別紙5】現行プロキシ構成図
【別紙6】現行メール構成図
【別紙7】現行 DNS 構成図

以上