

別紙4-1 現行ネットワークにおける主な構成要素

| No | 契約名 | 契約期間 | 構成要素 | 概要 |
|----|------------------------------------|-----------------------|--------------------------|---|
| 1 | 三重県情報ネットワーク構築及び運用保守業務委託 | 令和元年10月31日～令和7年12月31日 | ネットワーク機器 | コアSW、FW等 機器構成については別紙4-2「現行ネットワークにおけるネットワーク機器一覧」を参照 |
| | | | 無線LANシステム | 無線管理システム、コントローラー、本庁（全フロア）及び総合庁舎の一部を対象とした無線LANアクセスポイント（約150） |
| | | | ファイル交換システム | 職員が庁外関係者と大容量ファイルを安全に送受信するためのファイル交換システム |
| | | | ファイルサーバ （全庁ファイル共有サーバ） | 本庁舎及びデータセンターに職員同士でファイルを共有するためのファイルストレージ（640TB×2）を構築 |
| | | | モバイルワークシステム | 専用のモバイルワーク端末を利用することにより、外部からのリモート接続を可能にするシステム（R4年度末に廃止済み） |
| | | | 防災対策 | 大規模災害時において、拠点間通信が不通となった場合でも、本庁及び総合庁舎から別途構築済みの防災行政無線を経由しインターネット接続が可能となる仕組み |
| | | | 障害監視システム （障害監視センター） | ネットワーク機器等の死活監視、流量監視を行うシステム 障害監視センターにて24時間365日の監視を実施 |
| 2 | 三重県DX推進基盤整備及び運用保守業務（庁内ネットワークの構成変更） | 令和4年10月19日～令和7年12月31日 | 三層モデルの変更（αモデル→β'モデルへの変更） | 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において、業務端末をLGWAN接続系ネットワークに設置するαモデルからインターネット接続系ネットワークへ設置するβ'モデルへの変更を実施 LGWAN接続系ネットワークの新規構築、ActiveDirectoryやWSUS、マルウェア対策システム、プロキシサーバ等、ネットワークを運用するうえで必要となる機能を構築 |
| | | | LGWAN接続環境 | β'モデルへの移行後、インターネット接続系ネットワーク内の業務端末からLGWAN接続系ネットワーク、及び、LGWAN上のウェブサイト等へアクセスするための仮想環境（VMware Horizonにより構築） ※現行ネットワーク構築時にモバイルワークシステムにおける仮想環境（庁外から専用端末にて仮想環境にアクセス後、庁内環境へ接続）として導入され、令和4年度にLGWAN接続環境として再構成を行った |
| 3 | 三重県行政WAN無線LANシステム拡張設計・構築業務委託 | 令和3年9月6日～令和5年3月31日 | 無線LANシステム | No1「三重県情報ネットワーク構築及び運用保守業務委託」において、本庁（全フロア）及び総合庁舎の一部を対象に無線LANアクセスポイントを敷設したが、令和4年度において本庁及び周辺4庁舎、総合庁舎（全フロア）を対象とするよう無線LANアクセスポイントを拡張敷設（約300） |
| 4 | 三重県情報ネットワークにかかる主回線の利用契約 | 長期継続契約 | 拠点間接続回線 | 三重県内における広域ネットワークサービス（SMIX）を活用した、データセンター、本庁、各総合庁舎及び各市町等を接続する回線 |
| 5 | 三重県情報ネットワークバックアップ回線提供契約 | 長期継続契約 | 拠点間接続回線 | 主回線が不通となった場合のバックアップ回線 データセンター、本庁、総合庁舎間を接続 |

| No | 契約名 | 契約期間 | 構成要素 | 概要 |
|----|--|------------------------------|---------------|--|
| 6 | 三重県行政WAN単独地域機関アクセス回線の利用（インターネット回線） 三重県行政WAN単独地域機関アクセス回線の利用（閉域網） | 長期継続契約 | 単独地域機関用アクセス回線 | 約200か所の単独地域機関とデータセンター間を接続する単独地域機関用インターネット回線 一部拠点は閉域網により接続 |
| 7 | 三重県情報ネットワークにおけるインターネットデータセンターの使用の契約 | 単年度契約（契約期間は毎年度4月1日から翌年3月31日） | データセンター、上流回線 | 基幹ネットワーク機器、サーバ群を設置しているデータセンター DX推進基盤用上流回線 |

※No1「三重県情報ネットワーク構築及び運用保守業務委託」以外については、必要な場合のみ別途調達を実施する

※No2「三重県DX推進基盤整備及び運用保守業務（庁内ネットワークの構成変更）」,No3「三重県行政WAN無線LANシステム拡張設計・構築業務委託」はNo1「三重県情報ネットワーク構築及び運用保守業務委託」の拡張、構成変更

別紙4-2 現行ネットワークにおけるネットワーク機器一覧

| 設置場所 | 機器 | 数量 | 備考 |
|-------------|----------------------|-----|----------------------|
| データセンター | 基幹コアL3 スイッチ | 2 | |
| | VPN 集約ルータ | 3 | 単独地域機関集約用 |
| | ルータ集約用スイッチ | 1 | |
| | サーバ接続用スイッチ (10G 接続用) | 2 | |
| | サーバ接続用スイッチ(1G 接続用) | 3 | |
| | ファイアウォール接続用スイッチ | 3 | |
| | 外部FW兼システム境界FW | 2 | 内部FW,外部FW等の仮想FW用物理FW |
| 本庁 (議事堂を含む) | 基幹コアL3 スイッチ | 2 | |
| | サーバ接続用スイッチ | 2 | |
| | フロアL2 スイッチ | 40 | |
| | 防災行政無線接続用ルータ | 1 | |
| | 防災用L2スイッチ | 6 | |
| | 災害用FW | 2 | |
| | 無線LANアクセスポイント | 142 | |
| | 行政WAN-防災LAN間SW | 2 | |
| 桑名庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 3 | |
| | 無線LANアクセスポイント | 20 | |
| | 防災行政無線接続用ルータ | 1 | |
| 四日市庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 6 | |
| | 無線LANアクセスポイント | 33 | |
| | 防災行政無線接続用ルータ | 1 | |
| 鈴鹿庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 4 | |
| | 無線LANアクセスポイント | 23 | |
| | 防災行政無線接続用ルータ | 1 | |
| 津庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 9 | |
| | 無線LANアクセスポイント | 38 | |
| | 防災行政無線接続用ルータ | 1 | |
| 伊賀庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 7 | |
| | 無線LANアクセスポイント | 31 | |
| | 防災行政無線接続用ルータ | 1 | |
| 松阪庁舎 | 拠点コアL3 スイッチ | 2 | |

| 設置場所 | 機器 | 数量 | 備考 |
|-------------------------|----------------------|-----|---------------|
| | フロアL2 スイッチ | 7 | |
| | 無線LANアクセスポイント | 34 | |
| | 防災行政無線接続用ルータ | 1 | |
| 伊勢庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 5 | |
| | 無線LANアクセスポイント | 31 | |
| | 防災行政無線接続用ルータ | 1 | |
| 志摩庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 3 | |
| | 無線LANアクセスポイント | 18 | |
| | 防災行政無線接続用ルータ | 1 | |
| 尾鷲庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 6 | |
| | 無線LANアクセスポイント | 32 | |
| | 防災行政無線接続用ルータ | 1 | |
| 熊野庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 6 | |
| | 無線LANアクセスポイント | 21 | |
| | 防災行政無線接続用ルータ | 1 | |
| 大規模単独地域機関 | 拠点コアL3 スイッチ | 2 | アスト津、総合教育センター |
| 吉田山会館、勤労者福祉会館、合同ビル、栄町庁舎 | 拠点コアL3 スイッチ | 2 | |
| | フロアL2 スイッチ | 11 | |
| | サーバ接続用スイッチ | 2 | |
| | 防災用L2スイッチ | 1 | |
| | 無線LANアクセスポイント | 49 | |
| 単独地域機関 | 単独地域ルータ | 171 | |
| | フロアL2 スイッチ | 7 | |
| 市町等 | セキュリティクラウド接続スイッチ(L2) | 33 | |

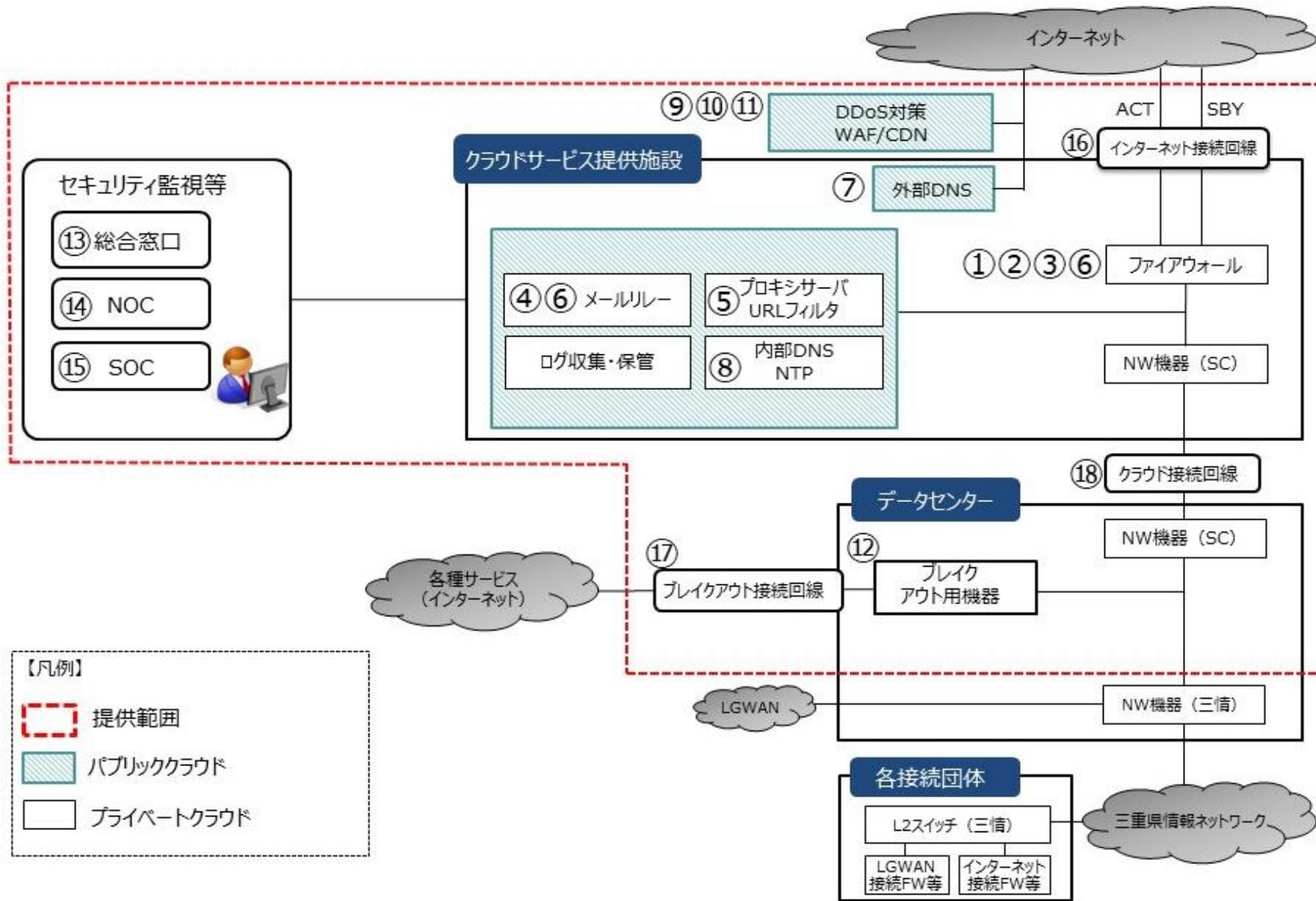
※モジュール、UPS等周辺機器は含めない。

別紙4-3 現行ネットワークに対する主な関連契約

| No | 契約名 | 契約期間 | 構成要素 | 概要 |
|----|---|--|---|--|
| 1 | 三重県統合認証管理基盤システム設計・機器調達・構築・運用保守業務 | 令和4年3月10日～令和9年7月31日 | ActiveDirectory、資産管理、クラウド認証基盤 | AD:オンプレミスAD (WindowsServer2019) 資産管理ソフト:SKY社製SKYSEA クラウド認証:Soliton社製Onegate |
| 2 | 三重県共通機能基盤再構築及び運用保守業務委託 | 平成30年10月17日～令和8年3月31日 | 統合サーバ、リモート保守環境 | 統合サーバ:中小規模のシステムを仮想化したうえで統合するためのサーバ(令和5年10月現在、44システム、165サーバが稼働) リモート保守環境:遠隔地からインターネット経由で三重県情報ネットワーク上のシステムを運用保守するためのリモート環境 |
| 3 | 三重県自治体セキュリティクラウド(令和3年度)構築及び運用・保守業務 | 令和3年8月6日～令和9年3月31日 | FW、メールリレー、WAF、NOC、上流回線等 | 三重県及び県内市町等が利用するセキュリティクラウド 構成は別紙4-4 三重県自治体情報セキュリティクラウドにおける機能及び構成概要図を参照 |
| 4 | 三重県自治体セキュリティクラウド(追加セキュリティ対策)構築及び運用・保守業務 | 令和4年1月26日～令和9年3月31日 | EPP、EDR、SOC | 三重県自治体情報セキュリティクラウドにおける拡張機能として構築された、EPP、EDR及びそれらを対象とするSOCサービス |
| 5 | 在宅勤務システム運用保守業務 | 単年度契約(契約期間は毎年度4月1日から翌年3月31日) | テレワーク環境(RDP) | 自宅等から庁内環境の業務端末へリモート接続する環境 Splashtop Streamer、Soliton社製Secure Desktop等で構成 |
| 6 | 三重県DX推進基盤整備及び運用保守業務 | 令和4年9月26日～令和10年3月31日 | コミュニケーション基盤:メールリレー、Web会議/チャット、GW、ストレージ セキュリティ基盤:SASE、NGFW、SOC、上流回線 | コミュニケーション基盤:Microsoft365、Slackを利用した庁内コミュニケーションツール セキュリティ基盤:ゼロトラストセキュリティ実現のためのセキュリティ基盤 |
| 7 | 個人番号利用事務系ネットワークにおけるセキュリティ対策業務委託(再構築) | 令和4年7月20日～令和9年10月29日 | ActiveDirectory、多要素認証、セキュリティ対策 | AD:オンプレミスAD (WindowsServer2019) 資産管理ソフト:ハンモック社製AssetView |
| 8 | インターネットメールシステム再構築及び運用保守業務委託 | 平成30年10月1日～令和6年3月31日(令和6年4月以降一部保守延長予定) | メールサーバ、誤送信対策、メールリレー、ウイルスチェック | 三重県が外部(インターネット、LGWAN)へメール送受信するためのメールシステム 現在はDX推進基盤の導入に伴いExchange Onlineを利用しているが、誤送信対策(強制BCC化)及びウイルスチェック等のため、リレーサーバ等を経由しExchange Online等へメールリレーを実施している |

別紙4-4 三重県自治体情報セキュリティクラウドにおける機能及び構成概要図

(1) 構成概要図



(2) 機能概要

| NO | 機能 | 説明 |
|----|-----------------|--|
| ① | ファイアウォール | ・三重県SCとインターネットの境界にあり、プロトコル単位で通信を制御する機能 |
| ② | IDS/IPS | ・インターネットとの通信において、不正に侵入しようとする異常な通信を検知及び遮断する機能 |
| ③ | ふるまい検知 | ・インターネットとの通信に含まれるファイルなどを隔離した疑似空間において動作を確認し、不正か否かを検知する機能 |
| ④ | メールリレー | ・インターネットを経由して送信・受信するメールを接続団体のメールサーバへリレーする機能 |
| ⑤ | プロキシサーバ/URLフィルタ | ・URLフィルタ機能(共通ブラックリスト) ・インターネット閲覧(ブラウジング通信)において、端末の代理としてインターネットとの通信をする機能 |
| ⑥ | マルウェア/スパム対策 | ・ブラウジング通信とメールに対するマルウェア対策をする機能 ・メールに対するスパム対策をする機能 |
| ⑦ | 外部DNS | ・接続団体のDNS情報(URLとグローバルIPの変換情報)を集約したDNS機能 |
| ⑧ | 内部DNS/NTP | ・再帰検索を行いドメイン情報の解決要求を行う機能 ・インターネット上の信頼できる機器と時刻同期を行い、接続団体の各機器へ時刻同期を行う機能 |
| ⑨ | DDoS対策 | ・公開WEBサーバに対するDDoS攻撃トラフィックをクラウドサービス側で緩和する機能 |
| ⑩ | WAF | ・WEBアプリケーションの脆弱性を狙った不正な通信の検知・防御する機能 |
| ⑪ | CDN | ・Web配信の「遅い」「中断する」「アクセスできない」を防止 ・災害時や感染症等によるアクセス数集中時にも安定的配信 |
| ⑫ | ブレイクアウト | ・特定のクラウドサービス向け通信を「ブレイクアウト接続回線」へ振り分ける機能 |
| ⑬ | 総合窓口 | ・接続団体における担当職員からの問合せ、障害申告の受付及びインシデント登録、対応等を受け付ける窓口 |
| ⑭ | NOC | ・セキュリティクラウドにかかる 運用・保守業務を行ううえで必要となる、運用・保守要員等が勤務する施設 |
| ⑮ | SOC | ・セキュリティクラウドにかかるセキュリティ監視等を実施していくうえで必要となる、セキュリティ監視要員等が勤務する施設 |
| ⑯ | インターネット接続回線 | ・クラウドサービス提供施設とインターネットを接続するための回線 |
| ⑰ | ブレイクアウト接続回線 | ・データセンターとインターネットを接続する回線 |
| ⑱ | クラウド接続回線 | ・データセンターとクラウドサービス提供施設を接続する回線 |