三重県 DX 推進基盤
整備及び運用保守業務
調達仕様書（案）

令和 4 年 月

目次

1. はじめに

1-1. 業務名

三重県 DX 推進基盤整備及び運用保守業務

1-2. 本仕様書の位置付け

本仕様書は三重県 DX 推進基盤整備及び運用保守業務（以下、「本業務」という。）に関する調達内容を記載している。

なお、三重県 DX 推進基盤の整備に関する全体概要については、「三重県 DX 推進基盤　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」、「想定」に分類して記載している。その詳細は以下のとおりである。

なお、本仕様書に記載の要件は、全て記載内容のとおりに実現する必要があるため、文中に「必須」は明示せず、**提案**及び**想定**のみ明示している。

項目	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	本県が求める要件であり、必ず実現すること。 なお、実現方法については、受託事業者の提案に委ねる。
想定	「提案」項目に対して、本県が想定する実現方法の一例を記載したものであり、記載のとおり実現する必要はない。

2. 本業務の概要

2-1. 目的

三重県 DX 推進基盤（以下、「DX 推進基盤」という。）は、行政 DX の推進に不可欠となる高いレベルの信頼性、可用性、保守性、保全性、安全性を維持しつつ、職員の業務効率化とさらなる生産性の向上、住民目線の行政サービス創出を目的に整備する情報基盤である。

具体的には、①クラウドサービスの利用を前提とした、メール・グループウェア等現行システムの移行・刷新、チャット等新たなツールの導入を推進するコミュニケーション基盤、②デジタルデータによる政策立案等を推進するデータ活用基盤、③情報セキュリティ対策の強化、テレワーク環境の充実を図る情報セキュリティ基盤の「3 つの基盤（サブ基盤）」の整備に取り組む。

なお、DX 推進基盤は、令和 4 年度に設計・構築・テストを完了し、令和 5 年 4 月にデータ移行、令和 5 年 5 月から令和 10 年 3 月末まで運用を行う予定である。

2-2. 本業務の内容

本業務の内容は以下のとおりである。

業務	主な業務内容
プロジェクト管理	・ DX 推進基盤の整備に向けた、業務計画書、作業体制、進捗管理、課題管理、リスク管理、会議体などのプロジェクト管理 （本仕様書「4 プロジェクト管理」に記載）
設計・構築等業務	・ DX 推進基盤の設計、構築、テスト、移行等 （本仕様書「5 設計・構築等業務」に記載） ・ 各構成要素の仕様 （本仕様書「6 構成要素の仕様（共通事項）」に記載） （本仕様書「7 構成要素の仕様（コミュニケーション基盤）」に記載） （本仕様書「8 構成要素の仕様（データ活用基盤）」に記載） （本仕様書「9 構成要素の仕様（情報セキュリティ基盤）」に記載）
研修業務	・ DX 推進基盤の研修 （本仕様書「10 研修等支援業務」に記載）
運用保守業務	・ DX 推進基盤の運用・監視・保守 （本仕様書「11 運用・監視・保守業務」に記載）

2-3. 本業務の構成要素

本業務の構成要素（サブ基盤）と概要を以下に示す。
共通事項の仕様は「6 構成要素の仕様（共通事項)」に記載。

2-3-1. コミュニケーション基盤

コミュニケーション基盤の仕様は「7 構成要素の仕様（コミュニケーション基盤)」に記載。

構成要素	概要
メールシステム・ メールリレーシステム	・ 現行のメール環境（庁内メール・インターネットメール・LGWAN メール）をクラウドサービスに移行する。 ・ インターネットメールの送信及び LGWAN メールの送受信において、既存のシステムを活用したメールリレーシステムを整備する。
Web コミュニケーション	・ 現行のグループウェア環境（予定表・施設予約・電子職員録・掲示板等）をクラウドサービスに移行・刷新する。 ・ 現行機能（予定表・施設予約・電子職員録・掲示板等）に加えて、チャットや Web 会議等のコミュニケーションツールがシームレスに利用できる環境を整備する。
ストレージサービス	・ 職員向けのファイルサーバ機能や、職員間または必要に応じて外部とのファイル（機密情報を除く。）交換・共有を行うことができる環境を整備する。
業務効率化ツール	・ 職員自身が、最小限のプログラミング知識で、素早くアプリケーションを内製できる業務効率化ツール（ノーコード／ローコードツール）を導入する。

2-3-2. データ活用基盤

データ活用基盤の仕様は「8 構成要素の仕様（データ活用基盤）」に記載。

構成要素	概要
データ活用基盤	・ 本県保有データの活用のみに留まらず、市町・企業等の保有データとの連携など、データの活用を可能とするデータ活用基盤を整備する。 ・ 本県保有データの調査及びデータ活用方針の策定･運用を行う。 ・ データ活用を行う課題テーマを定め、データ連携や分析、API 開発、データの可視化に取り組む。 ・ 職員（市町含む）にデータ活用に関する説明、操作研修等を行い、職員のデータ利活用を支援する。

構成要素	概要
	・ 設定した課題テーマに基づき、一定期間（令和 5 年度から令和 7 年度を想定）の実証を行う。

2-3-3. 情報セキュリティ基盤

情報セキュリティ基盤の仕様は「9 構成要素の仕様（情報セキュリティ基盤）」に記載。

構成要素	概要
クラウド・ネットワークセキュリティ	・ クラウドサービスの活用及び業務端末の持ち出しにより、現在のデータセンターを中心とした境界内（三重県行政 WAN）は安全とする考え方（境界型防御）から端末単体やユーザが信用できない前提として、暗号化や情報資産保護等のセキュリティ対策を徹底する「ゼロトラストセキュリティ」へ転換する。 ・ 情報セキュリティ基盤では、「ゼロトラストセキュリティ」への転換に必要となる機能を導入する。 【基本要件】 ・ 情報セキュリティ基盤をクラウドサービスとして提供する。 【セキュアウェブゲートウェイ（SWG)】 ・ 新 DK 端末からの Web アクセスに対する、ウイルス、マルウェア等の脅威検出を行う。 【クラウドアクセスセキュリティブローカー（CASB)】 ・ クラウドサービス毎に利用状況を可視化する。 ・ ポリシーに基づきクラウドサービスへのアクセスを制御する。 【ゼロトラストネットワークアクセス（ZTNA)】 ・ 新 DK 端末から、情報セキュリティ基盤を経由して、三重県行政 WAN 内部の業務システムへ安全にアクセスできる機能を提供する。 【セキュリティオペレーションセンター(SOC)】 ・ 日本国内に SOC（Security Operation Center）を設置し運用する。
エンドポイントセキュリティ	【端末ネットワーク】 ・ 新 DK 端末の通信制限を行う。 【ログオン認証】 ・ 新 DK 端末へのログオンを多要素認証とする。

構成要素	概要
	【データセキュリティ】 ・ 新 DK 端末の内蔵ストレージを暗号化する。 【端末管理】 ・ 新 DK 端末の EPP の更新状況を把握する。 ・ 新 DK 端末について、管理者が設定したポリシーに違反した端末を情報セキュリティ基盤と連携し、接続を不可とする。 ・ 新 DK 端末のリモートワイプを行う。

2-4. 履行場所

本業務における主な履行場所は次のとおりである。
三重県本庁舎（三重県津市広明町 13 番地）
データセンター（別途開示予定）
※その他の履行場所については、本仕様書に記載の各業務における履行場所とする。

2-5. 契約期間

契約期間は、令和 4 年度の契約締結日から令和 10 年 3 月 31 日までとする。

2-6. 支払

2-6-1. 支払条件

本業務における費用は、各年度末に当該年度分の費用を支払うこととする。
消費税法が改正された場合は、当該期間の費用について改正後の税率を適用する。
各年度の支払額（税込み）は、以下の割合を目安とし契約時に協議するものとする。
なお、本契約に係る予算額（税込み）は、2,442,069 千円である。

・ 令和 4 年度　　22.4065%
・ 令和 5 年度から令和 9 年度　　15.5187%／年

2-6-2. 内訳資料の提出

上記支払条件を踏まえて、契約締結後、速やかに、契約額の内訳資料（税抜き及び税込み金額を明記すること）を作成し提出すること。

特に初期費用の内、提供する構成要素単位で、設計、構築、設定、テスト、移行、研修、運用、保守費用等について、明確に分離した内訳資料を作成すること。

2-7. 全体スケジュール

本業務の全体スケジュールを以下に示す。

全体スケジュール

は受託事業者の業務

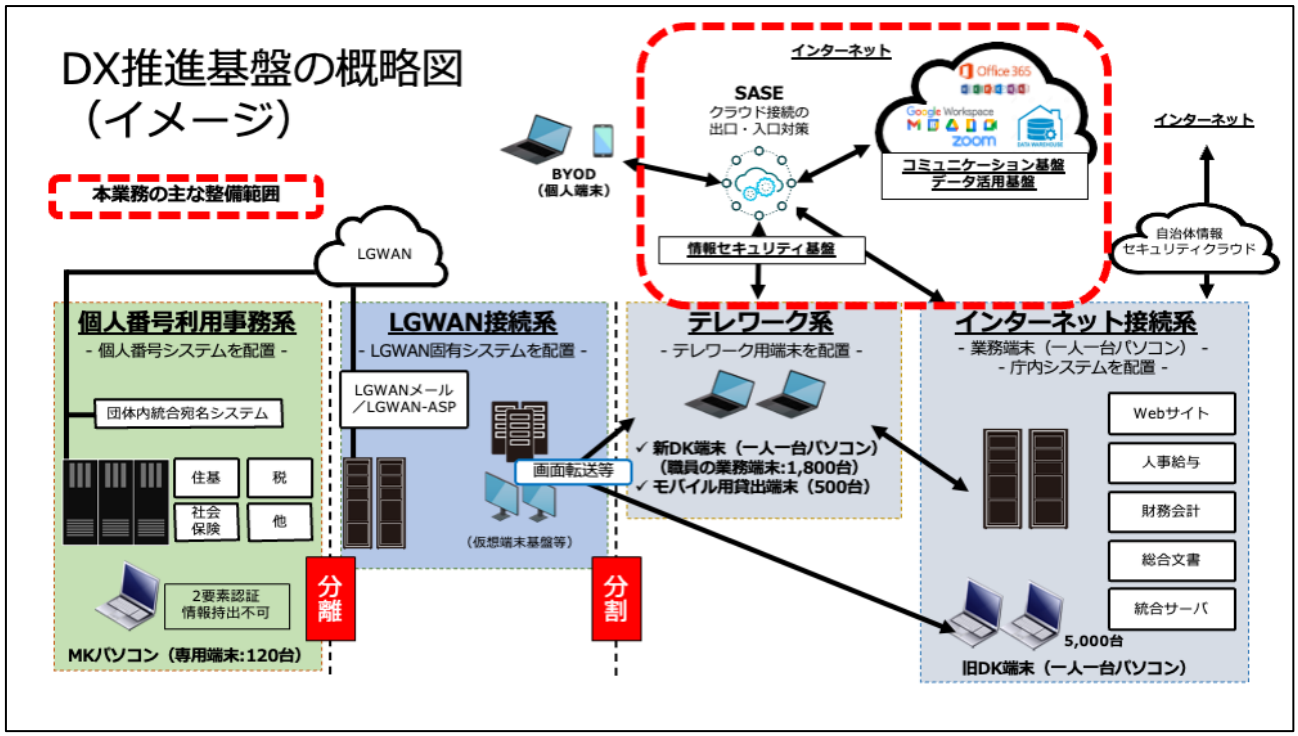
NO	項目	令和4年度				令和5年度				令和6～9年度			
		1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	R6	R7	R8	R9
1	調達・契約・運用（全体）		調達（7-9）	設計・構築（10-3）		運用（R5-R9）							
1-1	コミュニケーション基盤			研修（12-3）		移行（R5.4）・運用（R5.5-R9）							
1-2	データ活用基盤			調査・計画策定（10-3）		実証実験（R5-R7）				運用			
				オープンデータ整備									
1-3	情報セキュリティ基盤			構成変更		運用（R5-R9）							
				※庁内ネットワーク環境構成変更は別調達（外部監査を含む）		移行 ※新DK端末移行（～R6.3.31）							

2-8. 概略図と責任分界

2-8-1. 概略図

DX 推進基盤の概略図及び本業務の範囲を以下に示す。

なお、「三層の対策」については、αモデルからβ'モデルへの変更を行うこととして、その構成は以下を想定している。詳細は、「9-2 クラウド・ネットワークセキュリティ」を参照すること。



2-8-2. 責任分界

(1)　「2-8-1 概略図」で示したとおり、本業務の主な範囲はインターネット領域における新基盤（コミュニケーション基盤・データ活用基盤・情報セキュリティ基盤）の整備であり（破線囲み部分）、当該基盤が従来システムとの主な責任分界となる。

(2)　上記新基盤のほか、新基盤を利用するために必要となる DK 端末等の設定業務や、別途新設するメールリレーシステムに係る業務等についてもその範囲となる。

2-9. 利用者数及び端末台数

DX 推進基盤の利用数及び端末台数は以下のとおりとする。

項目	想定する数量等
利用者数	7,500 人以上
端末台数	8,000 台以上

2-10. 成果物

2-10-1. ハードウェア・ソフトウェア

本業務に必要なハードウェア・ソフトウェアを納入すること。

2-10-2. 業務計画書

受託事業者は、契約締結後速やかに工程表を含め業務計画書を本県に提出して承認を得ること。業務計画書には、全体及び各工程の体制、役割のほか、作業工程、業務スケジュール等を定義すること。

2-10-3. 各種設計書、完成図書及び報告書

受託事業者は、各工程の計画、成果を示すドキュメントを作成すること。想定するドキュメントは以下のとおりであるが、必要に応じて別途追加すること。また、各工程に着手する前に、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。

ただし、データ活用基盤におけるオープンデータの整備及び課題テーマへの対応に係る成果物等については、本県と別途協議し、提出期限を含め決定すること。

なお、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。

No.	成果物	内容	提出期限（予定）
1	基本設計書	本県の要求事項を整理し、DX 推進基盤の各システムにおける物理的なネットワーク構成及び機器構成、ソフトウェア等を定めた	令和 4 年 10 月末

No.	成果物	内容	提出期限（予定）
		もの 「5-4-2 基本設計書・詳細設計書の作成」を参照すること	
2	詳細設計書	基本設計書に基づき、DX 推進基盤の各システムにおける物理的なネットワーク構成及び機器構成、ソフトウェア等の具体的な設定内容、ルール等を定めたもの 「5-4-2 基本設計書・詳細設計書の作成」を参照すること	令和 4 年 12 月末
3	テスト計画書	テストの内容、スケジュール等を詳細に記載したもの 「5-6 テストに関する事項」を参照すること	令和 4 年 12 月末
4	テスト手順書	テスト計画書に基づき、テストの手順を定めたもの	令和 4 年 12 月末
5	テスト結果報告書	テスト手順書に基づき実施したテスト結果報告	令和 5 年 3 月末
6	移行計画書	現行システムとの一時的な並行運用、業務システムとの連携、業務端末の変更点等も考慮した計画について定めたもの 「5-7 移行に関する事項」を参照すること	令和 4 年 12 月末
7	移行手順書	移行計画書に基づき、移行の手順を定めたもの	令和 4 年 12 月末
8	移行結果報告書	移行手順書に基づき実施した移行結果報告	移行完了時
9	導入機器一覧、機器設定シート	本業務で導入する機器の一覧及び各機器への設定パラメータの値を定めたもの	令和 5 年 3 月末
10	論理構成図	DX 推進基盤の論理構成を示したもの	令和 5 年 3 月末
11	運用・保守設計書	運用や監視、保守業務の実現方法について設計したもの 「5-4-3 運用・保守設計書の作成」を参照すること	令和 4 年 12 月末
12	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
13	年次報告書	本業務における運用状況、作業報告等の年	年度末

No.	成果物	内容	提出期限（予定）
		次結果を報告するもの	
14	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
15	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・対応状況 SLA 報告	半年毎
16	データ活用方針	オープンデータの充実や課題テーマの解決に取り組むためのデータ活用方針 「8 構成要素の仕様（データ活用基盤)」を参照すること	令和 5 年 3 月末
17	研修計画書	職員等が本基盤の各種ツール等の操作方法を理解し、円滑に利用できるようにするための計画を定めたもの 「10 研修等支援業務」を参照すること	令和 4 年 11 月末
18	利用者マニュアル	利用者が本基盤の各種ツール等を操作する上で必要となる操作方法等について記載れたもの 「10-3 ドキュメント等の整理」を参照すること	令和 4 年 11 月末
19	管理者マニュアル	管理者が本基盤の各種ツール等を操作する上で必要となる操作方法等について記載されたもの 「10-3 ドキュメント等の整理」を参照すること	令和 4 年 11 月末

2-10-4. 納品

電子媒体（PDF 形式及び Microsoft Office Word、Excel、PowerPoint 等のファイル形式）で提出すること。本契約に関して用いる言語は、原則として日本語とする。

2-10-5. 納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、本県が納品場所を別途指示する場合はこの限りではない。

〒514-8570
三重県津市広明町 13 番地
デジタル社会推進局　デジタル改革推進課　情報基盤班

3. 現行システムの概要

3-1. 三重県情報ネットワーク

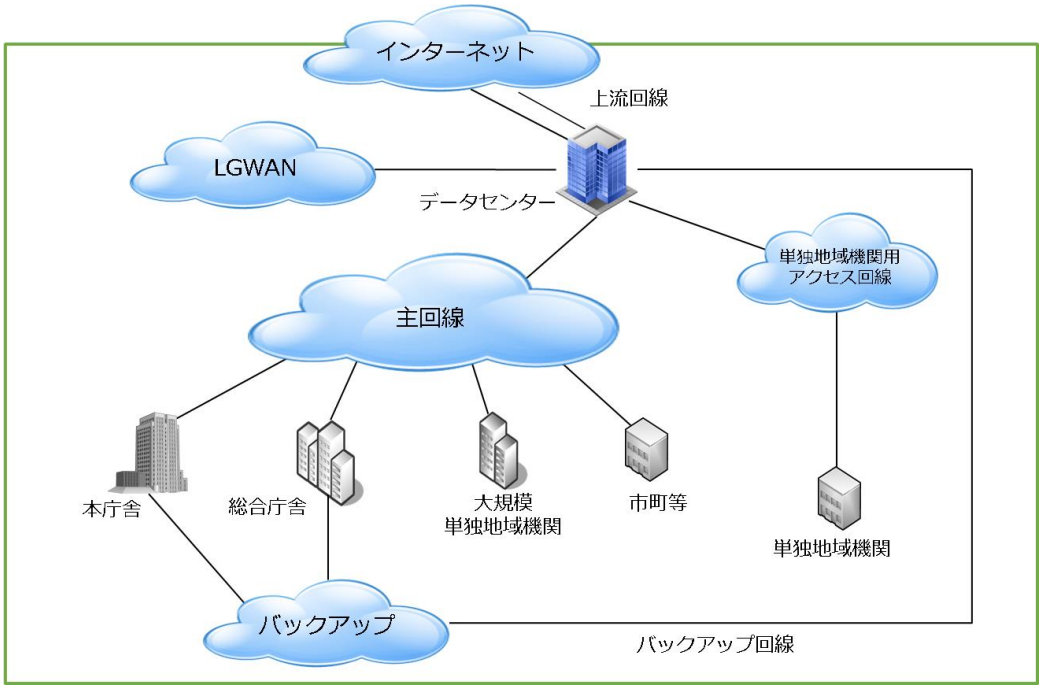
3-1-1. 全体構成

(1) 概要

- 三重県情報ネットワークは、庁内情報ネットワークである三重県行政 WAN や全国の自治体、国を接続する LGWAN、県内市町との共同運用である自治体情報セキュリティクラウドなど、本県のみならず、県内市町の業務を根幹から支える重要な基盤となっている。
- 令和 2 年度に再構築した三重県情報ネットワーク（以下、「現行ネットワーク」）は、ネットワーク機器の更新にとどまらず、費用対効果や信頼性・可用性のさらなる向上に向けて、防災対策の充実や働き方改革の推進など、これまでにない新たな視点を取り入れた情報基盤として構築した。
- 現行ネットワークが提供するサービスは以下のとおりである。

提供サービス名	サービス概要	サービス利用者
三重県行政 WAN	住民へのサービス向上を目指し、行政事務の迅速化・簡素化・高度化を進める為に整備されたネットワーク	県職員
県利用 L2 ネットワーク	県の組織が運用管理するネットワークに対して、論理分割することによりネットワーク環境を提供するサービス	県の組織、県職員
市町利用 L2 ネットワーク	知事が承認した国及び地方公共団体の管理するネットワークに対して、論理分割することによりネットワーク環境を提供するサービス	市町職員等

・ 現行ネットワークの全体構成概要は以下のとおりである。



・ 本庁舎、データセンター、総合庁舎、大規模単独地域機関、市町等は閉域網である主回線に接続されている。
・ 本庁舎、データセンター、総合庁舎は主回線とは異なる閉域網及び防災行政無線によりバックアップルートが確保されている。
・ 単独地域機関は、単独地域機関用アクセス回線(インターネット VPN または閉域網)を通じて、データセンターに接続されている。
・ データセンターは、上流回線を通じてインターネット及び LGWAN に接続されている。

(2) 機器等の構成

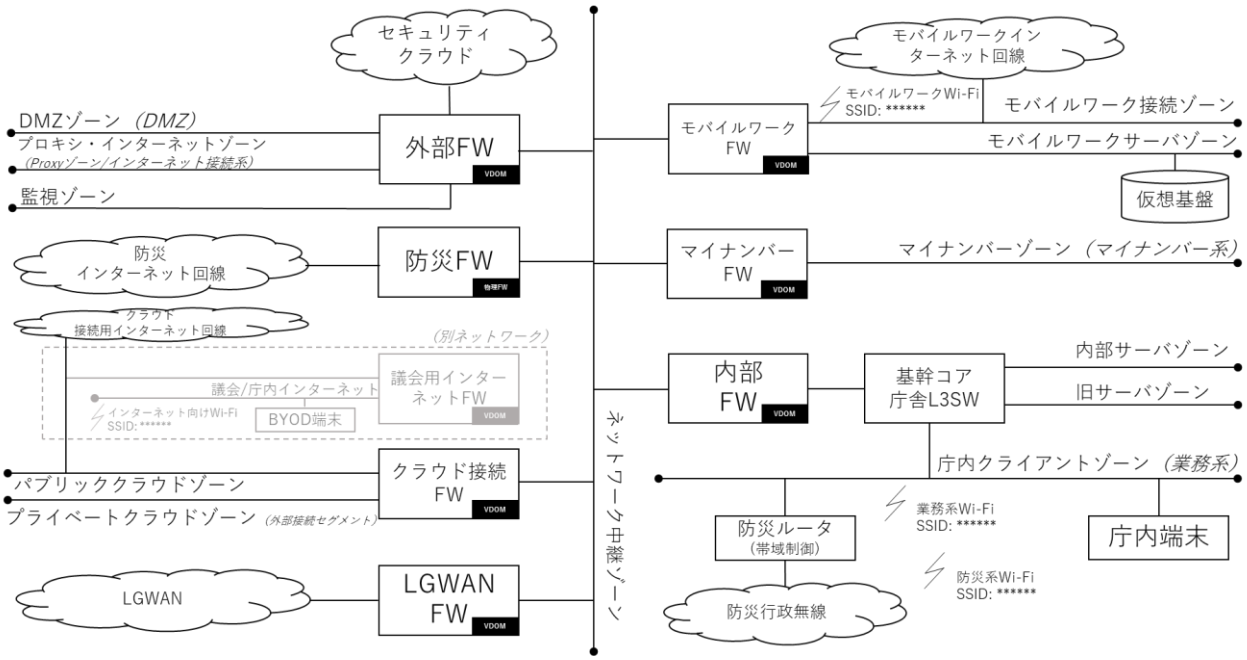
・ 本庁舎には、L3 スイッチが設置され、主回線に 10Gbps（確保帯域 10Gbps）で接続されている。また、L3 スイッチからは、各フロアに設置されたフロア L2 スイッチへ光ケーブルで接続され、業務端末は、フロア L2 スイッチへ接続されている。
・ 各総合庁舎（志摩庁舎を除く）には、L3 スイッチが設置され、主回線に 1Gbps（確保帯域 800Mbps）で接続されている。また、L3 スイッチからは、各フロアに設置されたフロア L2 スイッチへ光ケーブルで接続され、業務端末は、フロア L2 スイッチへ接続されている。
・ 総合庁舎（志摩庁舎）には、L3 スイッチが設置され、主回線に 800Mbps（確保帯域 800Mbps）で接続されている。また、L3 スイッチからは、各フロアに設置されたフロア L2 スイッチへ光ケーブルで接続され、業務端末は、フロア L2 スイッチへ接続されている。
・ 大規模単独地域機関（総合教育センター）には、L3 スイッチが設置され、主回線に 1Gbps（確保帯域 800Mbps）で接続されている。また、L3 スイッチから館内の HUB へ UTP ケーブルで接続されている。

- 大規模単独地域機関（アスト津）には、L3 スイッチが設置され、主回線に 800Mbps（確保帯域 800Mbps）で接続されている。また、L3 スイッチから館内の HUB へ UTP ケーブルで接続されている。
- データセンターには、L3 スイッチが設置され、主回線に 10Gbps（確保帯域 10Gbps）で接続されている。また、L3 スイッチからデータセンター内ラックに設置された L2 スイッチ（サーバスイッチ）に接続され、サーバスイッチには各業務システムが接続されている。さらに、各ネットワークセグメントのファイアウォールが設置され、うち、外部ファイアウォールには、インターネット回線（セキュリティクラウド）が接続されている。
- 単独地域機関（VPN 拠点）には、インターネット回線が敷設され、VPN ルータを通じてデータセンターへ接続されている。また、VPN ルータから館内の HUB へ UTP ケーブルで接続されている。
- 単独地域機関（閉域網拠点）には、閉域網が敷設され、ルータを通じてデータセンターへ接続されている。また、ルータから館内の HUB へ UTP ケーブルで接続されている。

3-1-2. システム設計・設定内容

(1) 三重県行政 WAN の論理構成

- 三重県行政 WAN は、ネットワークセグメントの整理や、一定のルールによるセキュリティレベル分けを行い、ゾーンとして定義している。また、各ゾーンは境界ファイアウォールにより制御されている。
- 各ゾーンの定義と境界ファイアウォールは以下のとおり。



境界 FW	ゾーン名	定義
外部 FW	DMZ ゾーン	インターネットに公開する Web サーバ等が接続されているゾーン。
	監視ゾーン	監視サーバ等が接続されているゾーン。
	プロキシ・インターネットゾーン	インターネット接続のためのプロキシサーバ及び仮想端末基盤（インターネット接続環境）が接続されているゾーン。
クラウド接続 FW	プライベートクラウドゾーン	プライベートクラウドサービス等と接続するためのゾーン。
	パブリッククラウドゾーン	パブリッククラウドサービス等、外部と接続するゾーン。
LGWAN FW	LGWAN ゾーン	LGWAN との接続を行うためのゾーン。
モバイルワーク FW	モバイルワーク接続ゾーン	モバイルワーク端末を接続するためのゾーン。
	モバイルワークサーバゾーン	モバイルワークのための仮想端末基盤（モバイルワーク環境）が接続されているゾーン
マイナンバー FW	マイナンバーゾーン	個人番号事務系端末及びサーバが接続されているゾーン
内部 FW	内部サーバゾーン	庁内システムサーバが接続されているゾーン
	旧サーバゾーン	更新前の庁内システムサーバが接続されているゾーン
	クライアントゾーン	業務端末が接続されているゾーン
－	ネットワーク中継ゾーン	境界 FW を相互接続するためのゾーン

(2)　「三層の対策」における強靱化モデル

- 現在の三重県行政 WAN は、「三層の対策」における強靱化のαモデルで運用している。
- 業務端末及び庁内業務システムは LGWAN 接続系に配置されている。
- インターネット接続は、インターネット接続系に配置されたインターネット接続環境（仮想端末基盤）及びセキュリティクラウドを通じて行っている。

- LGWAN へは、業務端末から直接アクセスを行っている。
- インターネットからダウンロードされたファイルは、LGWAN 接続系へファイル転送システムにより無害化されて転送される。
- 個人番号利用事務は、個人番号利用事務系に接続された業務システム及び専用端末により行っている。
- 三重県行政 WAN におけるαモデルの構成は「共通仕様書」を参照すること。

3-2. 三重県統合認証管理基盤

3-2-1. 概要

- Microsoft Windows Server の ActiveDirectory ドメインを利用し、ユーザ認証及びリソース管理を行うオンプレミス認証基盤を運用している。
- オンプレミス認証基盤では、グループポリシーを庁内端末に適用することにより、セキュリティ対策等を行っている。また、庁内業務システムと LDAP 等で連携することにより、シングルサインオンを実現している。
- クラウドサービスなどに対し、認証機能やシングルサインオンなどの ID 連携機能等を提供するクラウド認証基盤(Soliton OneGate)を運用している。
- 庁内端末の資産管理、セキュリティパッチ適用等を管理するための統合管理システム（SKYSEA Client View）を運用している。

3-2-2. 機器等の構成

- オンプレミス認証基盤は、7 台の Microsoft Windows Server で構成され、4 台は物理サーバ、3 台は、庁内の共通機能基盤で運用されている。ただし、令和 4 年度中に再構築を予定している。
- クラウド認証基盤は、IDaaS として Soliton OneGate をクラウド上で令和 4 年度中に運用を開始する予定である。
- 統合管理システムは、2 台のサーバで構成されているが、令和 4 年度中に再構築を予定しており、サーバ台数も変更される予定である。

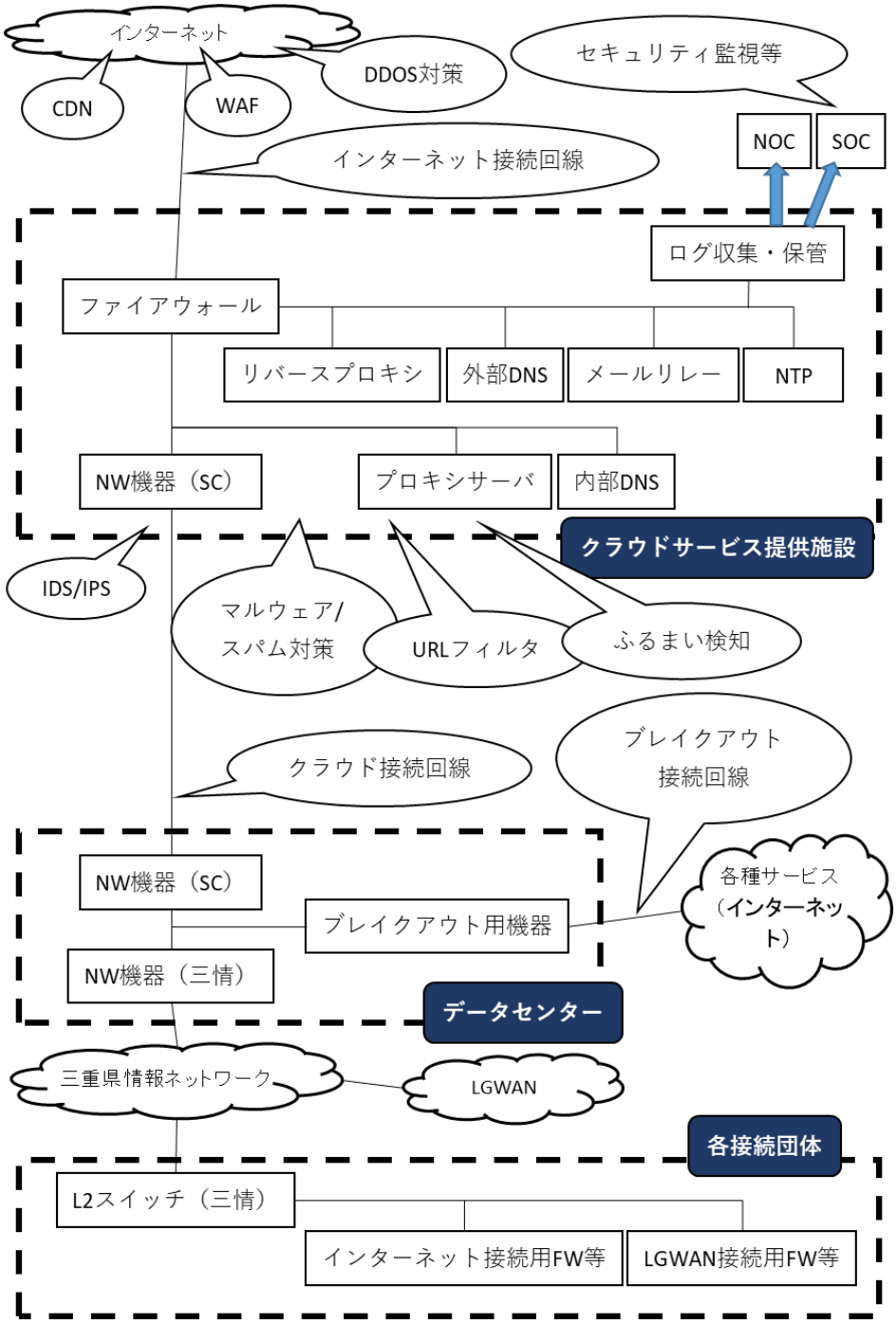
3-3. 三重県自治体情報セキュリティクラウド

3-3-1. 概要

- 三重県自治体情報セキュリティクラウドは、複数の団体からのインターネット接続を一つに集約し、高度なセキュリティ監視を行うことでセキュリティ対策を行うものであり、現在、本県や県内市町（29 市町)、広域連合（3 団体）の計 33 団体が利用している。
- 参加団体に対し、CDN、WAF、DDoS 対策、マルウェア/スパム対策、URL フィルタ、ふるまい検知、IDS/IPS 機能を提供している。
- セキュリティ監視等を行うため、SOC 及び NOC を運用している。
- 上記セキュリティ監視の SOC とは別に、EDR に係る SOC を運用している。

3-3-2. 機器等の構成

- 三重県自治体情報セキュリティクラウドの各機能は、クラウドサービスとして提供されている。
- クラウドサービスは、三重県情報ネットワークと 1Gbps の専用線（帯域保障）で接続されている。
- クラウドサービスは、インターネットと 1Gbps(帯域保障)の回線で接続されている。
- Web 会議等、大容量の通信を行うアプリケーションのため、3Gbps（1Gbps 帯域保障）のブレイクアウト回線を準備している。
- 参加団体は、三重県情報ネットワークを通じてクラウドサービスを利用している。



3-4. 共通機能基盤

3-4-1. 概要

- 共通機能基盤は、情報システムがそれぞれ個別に整備していた機能の一部を、共通で利用できるようにした基本的な仕組みのこと。
- 「統合サーバ」、「リモート保守環境」、「職員アカウント集中管理システム」の３つの個別基盤から構成され、いずれもオンプレミスで運用している。

個別基盤名	概要
統合サーバ	・複数のサーバを 1 台の物理サーバ上で動作させる「仮想化技術」により、仮想サーバ（仮想マシン）を統合サーバ上で提供している。 ・主に中小規模の情報システムで利用されており、それぞれの情報システムでサーバを調達することによる重複投資を抑制するとともに、セキュリティ向上や業務負荷の軽減という効果を生み出している。
リモート保守環境	・遠隔地からインターネット経由で情報システムの運用保守ができる環境を提供している。 ・情報システムが接続されているネットワークの種類により、インターネット VPN 経由または IP-VPN 経由のいずれかにより三重県行政 WAN に接続して保守業務が可能。 ・それぞれのシステムにおける運用保守対応や緊急時対応等の投資を抑制するとともに、セキュリティの向上や業務負荷の軽減という効果を生み出している。
職員アカウント 集中管理システム	・三重県行政 WAN 上のコンピュータ、職員、組織情報、情報システム等を一元的に管理できる機能を提供している。 ・各システムにおける担当職員の業務量削減、利用者の負荷軽減、セキュリティ対策の向上の効果を実現している。

3-4-2. 機器等の構成

- 各個別の機器等の構成については以下のとおり。

個別基盤名	概要
統合サーバ	・物理サーバとして、統合用サーバ 9 台、DB 用統合用サーバ 2 台、メインストレージ 1 台、統合用サーバ上の仮想マシンとして、vCenter サーバ 1 台、SCVMM サーバ 1 台、監視サーバ 1 台、バックアップサーバ 1 台に加え、別拠点のバックアップ環境のバックアップストレージ 1 台から構成されている。

個別基盤名	概要
	・仮想化ソフトウェアとして統合用サーバについては「VMware 社製 VMware vSphere 6.7 Update 2」、DB 用統合用サーバについては「Microsoft Hyper-V 7.0」を用いている。 ・メイン環境とバックアップ環境の構成により、統合用サーバと DB 用統合用サーバにおいてライブマイグレーション機能のほか、高可用性機能を有する。 ・ストレージのレプリケーション機能により、メイン環境におけるメインストレージの一次バックアップ領域とバックアップ環境におけるバックアップストレージの二次バックアップ領域間においてレプリケーションを行っている。
リモート保守環境	・SSL-VPN 装置 2 台、IP-VPN 装置 2 台、VDI 接続制御 FW2 台から構成されている。 ・リモート接続する際の通信は暗号化を実施し、インターネット VPN 経由による接続については、事前登録された情報システム受託事業者の任意の端末のみ接続を許可、IP-VPN 経由による接続については、県から貸し出した専用のリモート接続端末のみ接続を許可している。 ・リモート接続時に端末の情報を収集し、特定のセキュリティを満たす端末のみ接続を許可している。
職員アカウント 集中管理システム	・統合サーバ上の 2 台の仮想マシンとして稼働している。 ・システムアカウントについてユーザからの申請を受け付け、審査、承認、通知に係る一連の機能を提供しているほか、各システムのアカウント名とパスワードの入力が省略できる自動ログオン機能を提供している。 ・各システム側から本システムで保有している職員情報（職員番号、職員名、所属情報等）を直接参照し利用することが可能。

3-5. インターネット接続環境

3-5-1. 概要

・ 従来、インターネット接続と内部事務を同一のネットワークで行っていたが、平成 27 年 12 月、総務省からインターネットに接続するネットワークと職員が通常使用しているネットワークを分離するよう要請があった。

・ この要請を受け、本県では、平成 29 年度から、インターネット接続のための仮想端

末基盤を整備し、インターネットへのアクセスを間接的に行うことで、インターネットと内部事務を行うネットワークを分離している。
- 仮想端末基盤は、VMWare Horizon を利用し、主に Microsoft Windows 2012 Server による SBC 方式を採用している。
- LGWAN 接続系から仮想端末基盤への同時接続可能ユーザ数は、1,500 ユーザである。

3-5-2. 機器等の構成

- プロキシ・インターネットゾーンに仮想端末基盤及びその管理に必要となる機能を構築している。
- 管理系の仮想サーバは、物理サーバ 3 台で構成され、ストレージは vSAN 構成としている。
- 端末系の仮想サーバは、物理サーバ 9 台で構成され、ストレージは vSAN 構成としている。
- 管理系の仮想サーバ内では、ロードバランサ、仮想端末管理機能、プロファイルサーバ等が動作している。
- 端末系の仮想サーバ内では、SBC 方式による仮想端末が 104 台動作している。
  また、特定システム向けに VDI 方式による仮想端末が 4 台動作している。
- 仮想端末からは、管理系仮想サーバ内のプロファイルサーバを移動プロファイルとして利用している。

3-6. メールシステム（庁内メール）

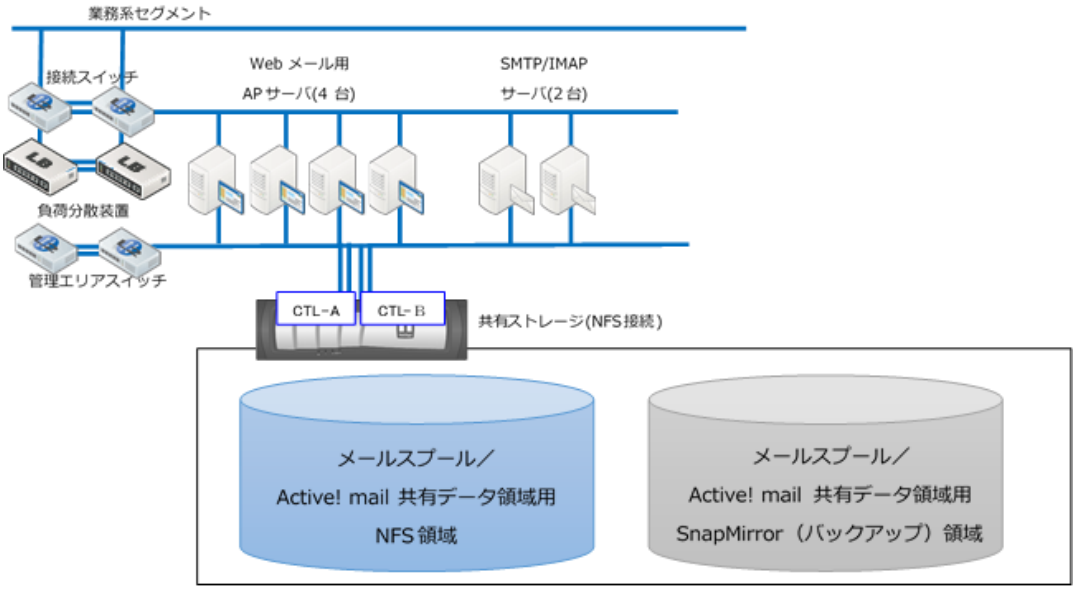
3-6-1. 概要

- Active! Mail（株式会社クオリティア）を利用したイントラネット内で運用している Web メール。
- 通信相手が職員のみに限定されているため、事務連絡や各種報告等を平文のままで送受信を行っている。
- アカウント登録数は、約 7,400 である。
- メールの過去 1 年間の状況として、受信件数は 1 ヶ月あたりピーク時で 200 万通、平均で約 180 万通、送信件数は 1 ヶ月あたりピーク時で約 62 万通、平均で約 53 万通である。

3-6-2. 機器等の構成

- Web メール用 AP サーバ 4 台、SMTP/IMAP サーバ 2 台、共有ストレージ 2 台（2 コントローラ）、負荷分散装置 2 台、接続用スイッチで構成している。
- 共有ストレージには、Web メールの管理データとメールデータを格納している。また、同一ストレージ上の異なる筐体上にバックップデータを格納している。
- Web メール機能はトランスウエア社製（現在のクオリティア社）の「Active! Mail」により構築している。

- Active! Mail は Web サーバ上に構成する必要があるため、Web サーバは「Apache HTTP Server」で構築している。
- 各サーバは仮想マシンではなく、物理サーバで構築している。
- Web メール用 AP サーバ、SMTP/IMAP サーバと共有ストレージの接続は、NFS で接続している。
- 共有アドレス帳・個人アドレス帳・シグネチャ等の各種設定は、Active! Mail 上にて管理している。



3-7. メールシステム（インターネットメール）

3-7-1. 全体構成

(1) 概要

- メールボックスを保有する内部メールサーバ、ウイルス対策を行うメール用ウイルスチェックサーバ、送信時に添付ファイルの暗号化や宛先の BCC 化を行う誤送信対策システム、インターネットからのメールの原本を保管する原本保管サーバ、インターネット及び LGWAN とメールの送受信を行う外部メールサーバ、LGWAN からのメールを振り分ける LGWAN 振分けサーバを整備している。
- 利用者は、利用端末にインストールされたメールクライアントソフトウェア(MozillaThunderbird)を利用してメールの送受信を行っている。
- 各サーバにてメール送受信の履歴を記録している。
- アカウント登録数は、約 7,200 である。
- メールの過去 1 年間の状況として、受信件数は 1 ヶ月あたりピーク時で 75 万通、平均で約 70 万通、送信件数は 1 ヶ月あたりピーク時で約 62 万通、平均で約 55 万通である。

(2) 機器等の構成

- 内部メールサーバはインターネットメール用仮想サーバ基盤上に構築されている。
- 誤送信対策システムサーバは共通機能基盤上に構築されている。
- メール用ウイルスチェックサーバはインターネットメール用仮想サーバ基盤上に構築されている。
- 外部メールサーバは共通機能基盤上に 2 台構築されている。
- 原本保管サーバ及び LGWAN 振分けサーバは、インターネットメール用仮想サーバ基盤上に構築されている。

3-7-2. システム設計・設定内容

(1) メール配送設定

- 内部メールサーバは利用端末から送信されたメールを受け付け、外部宛のメールであればメール用ウイルスチェックサーバに転送し、内部宛のメールであれば該当のメールボックスに格納する。また、LGWAN 振分けサーバまたは、原本保管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。
- メール用ウイルスチェックサーバは、内部メールサーバから転送された外部宛のメール及び外部メールサーバから転送された本県宛のメールに対し、ウイルスチェックを行った後、外部宛のメールは誤送信対策システムサーバ、本県宛のメールは LGWAN 振分けサーバに転送する。
- 誤送信対策システムサーバはメール用ウイルスチェックサーバから転送された外部宛のメールに対し、複数宛先の BCC 化や添付ファイルの暗号化等の措置を行った後、外部メールサーバに転送する。
- 外部メールサーバは、誤送信対策システムサーバから転送された外部宛のメールをインターネット/LGWAN へ転送する。また、インターネット/LGWAN から転送された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。
- LGWAN 振分けサーバは、LGWAN からのメールであれば、内部メールサーバへ転送し、インターネットからのメールであれば、原本保管サーバへ転送する。
- 原本保管サーバは、危険な添付ファイルの分離等の措置を行った後、内部メールサーバに転送する。
- 内部メールサーバ、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、原本保管サーバ、外部メールサーバ間の配送方法は、スタティック配送である。
- インターネット/LGWANから外部メールサーバへの配送方法はMX配送を行っている。
- 外部メールサーバにて、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。また、LGWAN へメールを送信する場合、送信元ドメインやあて先ドメインが「pref.mie.jp」の場合は、内部メールサーバで「pref.mie.lg.jp」に付け替えを行っている。
- 後方散乱メール(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、外部メールサーバにて破棄している。
- メールキューの保持期間は 5 日間である。
- メール転送を行ったログを 1 年間保存している。

(2) ウイルスチェック

メール用ウイルスチェックサーバにて以下のとおりメールのウイルスチェックを行っている。
- 外部宛のメールにてウイルスが検出された際は、メールの配送を停止し、管理者及び送信者宛にウイルスが検出された旨のメールを送信する。
- 本県宛のメールにてウイルスが検出された際は、ウイルスを駆除し、本文にウイルスの駆除を行った旨のメッセージを挿入したうえで LGWAN 振分けサーバに転送する。また、管理者にウイルスが検出された旨のメールを送信する。
- 暗号化等によりウイルスの検索ができなかった場合は、本文にウイルス検索を行っていない旨のメッセージを挿入したうえで転送先のサーバにメール転送を行う。
- ウイルスチェックは、Trend Micro 社の InterScan Messaging Security Virtual Appliance(IMSVA)を利用している。

(3) 誤送信対策

誤送信対策システムにて以下のとおりメールの誤送信対策を行っている。
- 宛先、CC、BCC に複数の外部のアドレスがある場合、宛先を送信者のアドレス、全ての送信先を BCC に変換し、本文に宛先の BCC 化を行った旨のメッセージを挿入したうえで外部メールサーバに転送する。また、送信者に対し、BCC 化を行った旨のメールを送信する。
- メールを一定時間保留し、保留時間内に送信者からの取り消し要求があればメールの削除を行う。また、送信者からの即時送信要求があれば、即時送信を行う。
- 取り消し要求、即時送信要求を行うための利用者認証機能付きの Web ページを提供している。
- 誤送信対策は、デジタルアーツ社の m-FILTER を利用している。

(4) 原本保管／添付ファイル分離

- インターネットから送信されたメールについて、危険な添付ファイルの分離を実施するとともに、原本をアーカイブする。
- 添付ファイルの分離を実施した場合、メール本文に分離が実施された旨のメッセージを追記して受信者に送信する。
- アーカイブされた原本メールに、業務システムからブラウザを通じてアクセスする。
- 原本保管／添付ファイル分離はデジタルアーツ社の m-FILTER を利用している。

3-8. グループウェアシステム

3-8-1. 概要

- CESS グループウェア（株式会社石川コンピュータ・センター）を利用した、各種業務及び職員に関する情報を共有するに運用しているグループウェアシステム。
- 本県では、平成 12 年度にグループウェアシステムを導入して以降、スケジュール管理や施設予約、電子職員録、文書共有等の機能を中心に活用しており、現行システムは平成 29 年度にオンプレミスにより構築したものであり、パッケージ製品を本県の業務体系に合わせてカスタマイズしている。

3-8-2. 機能と利用状況等

(1) 電子職員録

- 職員の氏名、職名、所属、連絡先等を所属ごとに一覧表示、検索する機能。
- 組織ツリーの表示機能を有しており、所属を選択することにより、所属内の職員を表示させることができる。
- 所属名、姓、名、内線番号等により、職員を検索することができる。

(2) スケジュール

- 各職員のスケジュールを月間、週間または 1 日の単位で表示する機能。
- 電子職員録と同様、組織ツリーの表示機能を有しており、所属を選択することにより、所属内職員のスケジュールを一覧表示（週間表示）することができる。
- また、任意の職員グループを作成し、スケジュールを一覧表示する機能を有する。

(3) 施設予約

- 貸出し可能な施設や備品を登録し予約を管理する機能。
- 日、時間単位で施設や備品を予約することができる。
- スケジュール登録と同時に施設を予約することもできる。
- 管理者により、各施設等の使用可能な曜日や時間帯、予約できる所属や職員の範囲を設定できる。

(4) 掲示板

- 庁内向けのお知らせ等を掲載期間や閲覧可能範囲を指定したうえで投稿する機能。
- 消耗品の所属間でのやり取りや周知情報の掲載に利用されている。

(5) ネットフォルダ

- 各種規程、事務連絡、申請書、マニュアル等の電子ファイルを検索しダウンロードする機能。
- ツリー構造による検索機能を有し、所属・業務別にファイルを表示できる。

3-9. 在宅勤務システム

3-9-1. 概要

(1) 在宅勤務システムは、コロナ禍における職員の接触機会の徹底的な低減を実現するため、令和 2 年 6 月に導入したシステムである。

(2) 本システムは、職員の自宅端末（Apple iOS 、Apple macOS、Google Android OS 、Microsoft Windows）から所属内の業務端末に接続するリモートデスクトップ方式を、外部サービスの提供（SaaS／DaaS 等）により実現している。

(3) 全職員を利用対象者とし、現在、最大 1,300 人程度が同時に利用できるライセンスを保有している。

(4) リモートデスクトップ方式や認証に係るソフトウェアについては、ほぼ全ての職員が端末にインストールできるよう 6,500 ライセンスを保有している。

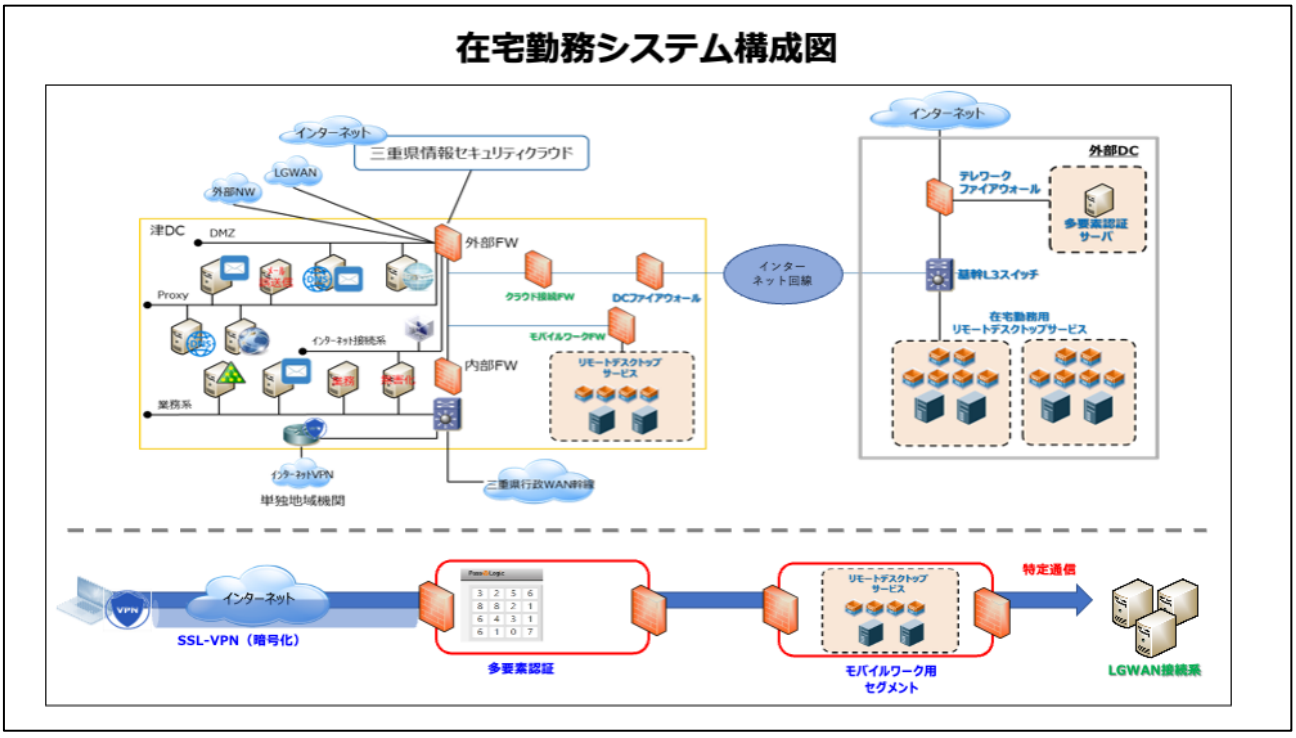
3-9-2. 機器等の構成

(1) SaaS／DaaS サービスと三重県行政 WAN は、クラウド FW を通じて専用線（1Gbps）で接続されている。

(2) SaaS／DaaS サービスは、1Gbps(ベストエフォート)の回線によりインターネットに接続されている。

(3) 職員の自宅端末は SaaS／DaaS サービスへ、インターネットを通じてアクセスし、多要素認証後に VPN 接続される。

(4) 職員は、SaaS/DaaS サービスから職員の業務端末へリモートデスクトップ接続し、業務を行う。



3-10. モバイルワークシステム

3-10-1. 概要

(1) モバイルワークシステムは、職員が出張・外出先等の庁外から業務をリモートで実施するためのシステムである。
(2) 別途整備したモバイルワーク用端末から、仮想端末基盤（SBC または VDI）に接続して利用する。
(3) 仮想端末基盤は、VMWare Horizon を利用し、主に Microsoft Windows 2016 Server による SBC 方式を採用している。
(4) 仮想端末基盤では、次のアプリケーションが利用できる。
- ブラウザ　Microsoft Edge
- オフィス　Microsoft Office
- PDF リーダ　Adobe Acrobat
- アーカイバ　7-Zip

(5) 最大 500 台のモバイルワーク用端末が仮想端末基盤にアクセスできる性能を有する。

3-10-2. 機器等の構成

(1) モバイルワークサーバゾーンに仮想端末基盤及びその管理に必要となる機能を構築している。
(2) 管理系の仮想サーバは、物理サーバ 2 台で構成されている。
(3) 端末系の仮想サーバは、物理サーバ 5 台で構成されている。
(4) ストレージは共有ストレージ（19.2TB）を使用している。
(5) 管理系の仮想サーバ内では、ロードバランサ、仮想端末管理機能等が動作している。
(6) 端末系の仮想サーバ内では、SBC 方式による仮想端末が 13 台動作している。
(7) 仮想端末は、共有ストレージのプロファイルを移動プロファイルとして利用している。
(8) モバイルワークシステムへのアクセスは、在宅勤務システムと回線を共用している。

3-11. 業務端末

3-11-1. 概要

(1) デジタル改革推進課で配付している業務端末（DK/KK 端末：5,512 台）、各課で購入・管理している業務端末（SK 端末：約 2,700 台）が導入されている。それぞれの端末の情報については、「6-5-1 端末の概要」を参照のこと。
(2) 三重県行政 WAN（LGWAN 系）に接続されており、全職員に一人一台パソコンまたは所属共用パソコンとして配付・導入されている。
(3) 庁内の認証基盤（オンプレミス版 AD）により、ログオン認証を行っている。
(4) 庁内システムへは、三重県行政 WAN を通じアクセスしている。
(5) インターネットへは、インターネット接続環境を通じてアクセスしている。

3-11-2. 機器等の構成

(1) Microsoft Office 2016 または 2013（Professional または Standard）がインストールされている。
(2) EPP として、トレンドマイクロ社ウイルスバスターコーポレートエディションがインストールされている。ただし、令和 4 年度中に、Microsoft Defender に更新する予定である。
(3) EDR として、Tanium がインストールされる予定となっている（令和 4 年度中予定）。
(4) 資産管理ソフトとして、クオリティソフト社の QNDαがインストールされている。ただし、令和 4 年度中に SKYSEA Client View へ更新される予定となっている。

3-12. モバイル端末

3-12-1. 概要

(1) A4 サイズ型モバイルパソコン（430 台）が導入されている。
(2) 内蔵 SIM によりインターネットに接続されており、モバイルワーク環境にアクセスする端末として、各所属に 1 台配付されている。
(3) モバイルワーク環境へは、画面転送方式によりアクセスを行うため、端末内にデータを持たないシンクライアントとなっている。

3-12-2. 機器等の構成

(1) EPP として、トレンドマイクロ社ウイルスバスターコーポレートエディションがインストールされている。
(2) Windows Firewall により、必要な通信以外はブロックされている。

4. プロジェクト管理

4-1. 業務計画書

提案受託事業者は、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、各業務を含む全体の体制及び役割と、作業工程及びスケジュール等の概要を定義すること。

4-2. 作業体制

「5-2 作業体制」を参照すること。

4-3. 進捗管理

以下に基づき進捗管理を行うこと。

(1) 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スケジュールとの差異を把握するために進捗管理を行うこと。

(2) 計画から遅れが生じた場合は、原因を調査し、本県に改善策を速やかに提示し、承認を得た上で、対策を実施すること。

4-4. 課題管理

本業務に関する各種業務を実施する上で発生する課題、問題事項等を適切に管理し、以下の要件に基づき解決を図ること。

(1) 受託事業者は、課題管理を行う際は、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。

(2) 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。

(3) 本業務を遂行する上で発生した課題、問題事項のうち、複数の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解決すること。

4-5. リスク管理

当初計画したスケジュールの実施にあたり工程の重複、遅延等防止のため、以下の要件に基づきリスク管理を行うこと。

(1) 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上、適切な管理を行うこと。

(2) 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あらかじめ検討し、発生した場合は速やかに対応できるよう準備すること。

(3) リスクが顕在化した際、検討済みの対策案を実施し、その結果を本県に報告すること。

4-6. 会議体

受託事業者は、本業務の遂行に当たっては、以下に示す会議を構成要素単位でオンサイトまたはオンライン等の最適な方式で開催すること。

なお、会議終了後 3 日以内に議事録を作成の上、本県に提出すること。

議事録には、開催日時・場所、出席者、配付資料、決定事項等を簡潔に記載すること。

フェーズ	会議体	会議内容	頻度
設計・構築移行期間	キックオフ会議	受託事業者が、業務計画書の内容を本県へ説明する会議として、契約後速やかに開催すること。	契約締結後 2 週間以内
	定例会議（週次）	本県への進捗報告を兼ねた週次会議を開催すること。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。	週次を想定
	設計・構築検討会議	設計・構築を実施する上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、開催頻度を本県と調整の上、決定する。	随時
運用期間	運用月次報告会議	本県への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。	月次を想定
	運用年次報告会議	本県への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。	年次を想定

5. 設計・構築等業務

5-1. 業務範囲

5-1-1. 受託事業者が実施する業務

(1) 本仕様書に基づき受託事業者が導入するハードウェア、ソフトウェア及びクラウドサービス等の設計・構築・テストを行う。
(2) 現行のシステムから必要なデータの移行を行う。
(3) 業務端末の移行を行う。
(4) 運用・監視・保守業務への引き継ぎを行う。

5-2. 作業体制

5-2-1. 作業体制

(1) 提案受託事業者は、設計・構築等業務全体を計画的かつ円滑に進めるため、十分な人員を確保するとともに、作業体制を構築する。さらに、設計・構築等業務を遂行できる知見を有する技術者を確保すること。
(2) 想定構成要素単位にプロジェクトを立ち上げ、それぞれが緊密に連携を図りながら作業を行う体制とする。
(3) 受託事業者は、本業務の履行に係る実施責任者を選定する。実施責任者は プロジェクトリーダ及び開発リーダを選任し、氏名等を書面で本県へ通知すること。
(4) 人員の中に業務の遂行に著しく不適当な者がいると認める場合には、本県は受託事業者に対してその理由を付して通知し、必要な措置を要求することができ、受託事業者はその趣旨に従い、誠実に対応すること。

5-2-2. 主要担当者に関する要件

(1) 提案プロジェクトリーダの資格要件

プロジェクトリーダとは、本業務の統括・運営管理に係る責任を持つ者である。なお、プロジェクトリーダに求める要件を以下に示す。

- 想定クラウド基盤(クラウド･ネットワーク･エンドポイントセキュリティを含む)及びビジネス・インテリジェンス（BI）ツール（以下、「BI ツール」という。）を用いた設計・開発におけるプロジェクト管理の経験を有すること。
- プロジェクト管理の実務経験を 5 年以上有すること。
- 想定アジャイル開発プロセス管理の実務経験を 3 年以上有すること。

(2) 提案開発リーダの資格要件

開発リーダとは、システムの設計・開発業務において、主体となって本県と調整する者である。なお、開発リーダに求める要件を以下に示す。

- 想定クラウド基盤(クラウド･ネットワーク･エンドポイントセキュリティを含む)

及び BI ツールを用いた設計・開発の経験を有すること。
- 設計・開発の実務経験を 5 年以上有すること。
- 想定高度情報処理技術者(試験区分は問わない)の資格を有するか、又はこれと同等の能力があること。
- 想定提案するクラウド基盤に関する資格(AWS Solutions Architect - Professional 相当)を有するか、又はこれと同等の能力があることが望ましい。

5-3. 設計・構築業務の管理

5-3-1. 基本事項

(1) 本節に記載の要件は、データ活用基盤の設計・構築には適用しない。
(2) データ活用基盤の設計・構築については、「8　構成要素の仕様（データ活用基盤）」を参照すること。

5-3-2. 管理要件

(1) 設計・構築業務の遂行にあたり、本仕様書及び業務計画書に基づき、進捗管理を行うこと。
(2) 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、承認を得た上で、対策を実施すること。
(3) 構築業務で発生する課題について、課題の認識、対策の責任者、対策の検討、解決状況を明確にするため、課題管理を行うこと。
(4) 発生している課題については、会議体等を通じて本県と随時協議し、対応状況の報告を行うこと。
(5) 各工程の達成を妨げるリスクを最小限にするためのリスク管理を行うこと。
(6) リスクは影響度合いを識別し、優先度を決定した上で対応を実施すること。
(7) 構築する DX 推進基盤の各システムが、本仕様書に記載の機能要件を満たすことを確認するため、品質管理を行うこと。

5-4. 設計

5-4-1. 基本事項

(1) 提案 DX 推進基盤の設計にあたっては、本仕様書のほか、「共通仕様書」に基づき、DX 推進に向けた、業務効率化及び生産性のさらなる向上に向けて、現状の課題解決や、3 つの構成要素による新たな取組の実現に主眼を置いた設計とすること。ただし、その実現方法については、受託事業者の創意工夫による提案を求める。
(2) 現行のネットワーク環境や関連システムの構築・運用事業者との協議等を本県の調整のもと実施したうえで、要件を踏まえた最適な全体設計（基本設計及び詳細設計）を行うこと。
(3) 本仕様書のほか、「共通仕様書」に基づき選定したクラウドサービスが適切に利用できるよう設計を行うこと。

(4) DX 推進基盤を構成する各構成要素の正常な稼働を確認するためのテスト設計を行うこと。
(5) 提案 現行システムから DX 推進基盤への移行を行うための移行設計を行うこと。
(6) 提案 DX 推進基盤に係る運用・保守設計を行うこと。
(7) 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。

5-4-2. 基本設計書・詳細設計書の作成

(1) 本仕様書に基づき導入する各構成要素に係るハードウェア及びソフトウェア等の基本設計書及び詳細設計書を作成し、本県の承認を得た上で作業を行うこと。
(2) 設計の妥当性をプロトタイプにより検証し、その結果を本県に提示し承認を得ること。
(3) 本業務に伴って導入するハードウェア、ソフトウェア、技術、構成の概要等、以下の情報を基本設計書に記述すること。
　（ア） 導入するハードウェア及びソフトウェア、クラウドサービスの選定結果
　（イ） ハードウェア一覧
　（ウ） ソフトウェア一覧
　（エ） 利用するサービスの一覧
　（オ） サービス及びコンポーネントごとの設計内容
　（カ） 機器設置計画書（ラック配置、機器実装、必要な電源工事の仕様）
　　※機器設置計画書に基づいて実装されたラック配置及び機器実装の最終結果を、ラック配置図及び機器実装図として提出すること
(4) 本業務に伴って導入するハードウェア及びソフトウェア、クラウドサービスにおける以下の設定内容等を、詳細設計書に記述すること。
　（ア） ネットワーク接続図
　（イ） パラメータ・設定値の一覧
　（ウ） その他、必要となる詳細設計一覧

5-4-3. 運用・保守設計書の作成

(1) 受託事業者は運用を開始するまでに、運用･監視･保守業務の実現方法について検討し、運用・保守設計を行うこと。なお、本県職員が実施する各種業務について、現行システムと同程度、もしくは、軽減されるよう十分配慮すること。
(2) 運用・保守設計に基づき、以下の項目を含む運用・保守設計書を作成すること。
　（ア） 運用計画書
　（イ） 運用年次計画書
　（ウ） 運用手順書
　（エ） 運用フロー
　（オ） 保守実施要領（切り分け手順・復旧方法）
　（カ） セキュリティインシデント対応要領（連絡・対応手順）

（キ） 各種管理台帳
（ク） 各種ひな形
（ケ） 取り扱い説明書
（コ） 運用テスト計画書
（サ） 運用テスト報告書

5-4-4. ユーザビリティ／アクセシビリティに関する事項

本業務で導入・整備する各種ツール類については、利便性を重視するため、ユーザビリティ・アクセシビリティの確保に向けた配慮を行うこと。

(1) 提案ユーザビリティ

ユーザビリティ要件については以下のとおりである。

No	分類	要件
1	画面の構成	直観的にわかりやすい画面構成であること
2	操作方法の わかりやすさ	直観的にわかりやすい操作手順であること
3	指示や状態の わかりやすさ	直観的にわかりやすい状態表示であること

(2) 提案アクセシビリティ

アクセシビリティ要件については以下のとおりである。

No	分類	要件
1	基準等への準拠	・JIS（日本産業規格） 「JIS X 8341-3 ： 2016『高齢者・障害者等配慮設計指針－情報通信における機器、ソフトウェア及びサービス－ 第 3 部：ウェブコンテンツ』」 ・総務省 公共分野におけるウェブアクセシビリティの確保の取り組みの充実に関する調査研究報告書「みんなの公共サイト運用ガイドライン（2016 年版）」 ・W3C 「ウェブ・コンテンツ・アクセシビリティ・ガイドライン（WCAG）2.0」 ・三重県ウェブアクセシビリティ方針 https://www.pref.mie.lg.jp/KOHO/HP/guide/
2	指示や状態の	例えば、色の違いを識別しにくいユーザを考慮し、メ

No	分類	要件
	わかりやすさ	ッセージを表示する等、色のみで判断するような設計は行わないこと
3	言語対応	本業務では日本語対応のみとする

5-5. 構築

5-5-1. 基本事項

(1) 受託事業者は、詳細設計書に基づき、ネットワークやハードウェア・ソフトウェア及びクラウドサービスの設定・構築作業を行うこと。
(2) 必要に応じて、ソフトウェアのインストールを行うこと。
(3) 機器の設置等のため、執務室に立ち入る場合は、原則として、平日の午前 8 時 30 分から午後 5 時 15 分とすること。その際、事前に作業スケジュールを示した上で本県の許可を得ること。
(4) 機器及び必要資材の搬入等を行う場合、詳細な施工方法、施工範囲、作業員名、スケジュール及び使用車両について、あらかじめ定めた書面をもって作業申請を行い、本県の承認を得ること。また、本県が行うべき作業がある場合には、これを明示すること。
(5) その他必要事項については、適宜本県と協議の上、決定すること。

5-5-2. 構築方式及び構築手法

(1) 提案構築方式としては、ウォーターフォール型とアジャイル型の長所を組み合わせることを想定している。ウォーターフォール型による工程の明確化及び、アジャイル型による本県の要求に合致したシステム構築を行うこと。
(2) 提案アジャイル型におけるプロトタイプとしては、標準パッケージシステムを活用した詳細仕様検討のプロトタイプ及び、処理方式などのシステム基盤面でのプロトタイプ検証などを想定している。そのため、要件定義段階から実際に稼働するシステム（プロトタイプ）をクラウド上で一部利用者へ開放し、一部利用者が操作しながら、アイデア、要望をヒアリングしていくこと。
(3) 提案プロトタイプ検証の内容及びスケジュールは受託事業者の提案によるものとするが、プロトタイプ検証を最低 2 回は行うこと。（本県の想定するマイルストーンは下表を参照すること）
(4) 想定プロトタイプ検証の途中段階においては、本仕様書で示す全要件を満たす必要はない。

No	想定マイルストーン	想定する検証等の概要	想定実施時期
1	一次機能検証	情報担当部門による機能性検証を実施し、抽出した要件を改修により反映させる。	令和 4 年 10 月を想定

No	想定マイルストーン	想定する検証等の概要	想定実施時期
2	二次機能検証	一般利用者による操作検証を実施し、抽出した要件を改修により反映する。	令和 4 年 11 月を想定
3	三次機能検証	一次及び二次検証を踏まえた三次機能性検証を実施する	令和 4 年 12 月を想定

5-6. テストに関する事項

5-6-1. 基本事項

(1) テスト設計に基づき、テストの内容、スケジュール等を詳細に記載したテスト計画書及び手順書を作成すること。また、アジャイル型で開発を進める部分については、スプリント単位で本県の承認を受けること。
(2) 機能の動作確認だけでなく、レスポンス時間などの性能に対しても検証を行うこと。
(3) 必要なシステムについては、バックアップデータからのリストア作業の検証を行うこと。
(4) 考えられる障害に対する対応策の検証を行うこと。
(5) 必要に応じて試行運用期間を設定するなど、本番までに十分なテストを行うこと。
(6) 各種テストにおいて必要なツール等の設計、作成または取得、導入等を行うこと。

5-6-2. テストの実施

(1) テストは受託事業者が行い、本県は必要に応じて任意のテストに立ち会うことができることとする。
(2) 受託事業者によるテストとは別に、本県は任意の機能について動作検証を行うことができることとする。その場合、受託事業者は操作方法等についてサポートを行うこと。
(3) テストの実施にあたり作成、使用した不要なテストデータは、受託事業者において削除すること。

5-6-3. テストの結果

(1) 全ての検証が問題なく終了したことを記録したテスト報告書を作成し、本県の承認を得ること。テスト報告書を本県が受理した後、本番運用に移行するものとする。
(2) テスト結果が期待されるものと異なる場合は、速やかに原因究明と改修を行った後、期待される結果となるまで繰り返し検証を行うこと。

5-7. 移行に関する事項

5-7-1. 基本事項

(1) 受託事業者は、現行システムにおける各システムの設定ファイル等、DX 推進基盤に引

き継ぐデータの種類を本県に提示した上で、最新のデータを収集し、引き継ぐこと。

(2) 移行が必要となるデータ（対象システムのファイル、設定ファイル、ユーザデータ等）の調査を行い、移行対象となるデータを確定すること。移行対象データの抽出に際し、対象データの提供方法、時期、フォーマットを指定した上で、本県に対して依頼、調整を行うこと。

(3) 現行システムで作業が必要になる場合は、事前に本県へ必要となる作業内容を提示し、了解を得ること。

(4) 安全性の確保と効率を考慮し、順次、移行を実施すること。

(5) 移行計画書に基づき実施した移行結果を報告書として取りまとめ、本県に提出すること。

(6) 本県の職員が自身でデータ移行を行う場合の問い合わせ対応については、「11-2-1　業務の内容（クラウド／業務端末／オンプレミスシステム共通）」に準ずるものとする。

(7) 全ての移行を令和 6 年 3 月 31 日までに完了すること。なお、DK 端末の設定変更作業は、令和 5 年 5 月から開始すること。

5-7-2. 移行計画書及び手順書の作成

(1) 移行設計に基づき、現行システムとの一時的な並行運用、業務システムとの連携、業務端末の変更点等も考慮した具体的な移行計画書及び手順書を作成し、本県の承認を得ること。

(2) 移行計画書及び手順書には、以下の項目を含めること。

（ア） 方針、概要
（イ） 前提条件
（ウ） 移行方法
（エ） スケジュール、フェーズの説明
（オ） 作業項目と作業担当者
（カ） 移行対象システム、機器、データ
（キ） 移行作業時の体制表及び役割分担
（ク） 移行作業後の試験項目、合否判定基準
（ケ） 移行を中断・切り戻す場合の切り戻し手順
（コ） 移行期間中の運用体制

(3) 移行計画の策定にあたり、現行システムの利用者に対して、可能な限り影響を与えない方法を検討すること。移行にあたり、本仕様書等に記載した機能以外の機器等が一時的に必要な場合には、受託事業者の費用負担において用意すること。

5-7-3. 業務端末の設定変更

(1) **提案** DX 推進基盤への移行に伴う業務端末の設定変更は、「9-2 クラウド・ネットワークセキュリティ」を参照して必要事項を定め、本業務内で受託事業者の責任において、作業に必要となる機材の準備も含め、全て行うこと。ただし、対象端末の把握、端末の

利用者への連絡、日程調整等の本県が実施すべき作業は除く。

(2)　提案遠隔操作で設定変更できない業務端末については、現地作業等を行うこと。想定なお、現地作業等は以下の項目を想定している。

（ア）マスタイメージの作成

端末のソフトウェア及び設定に係るマスタイメージを作成すること。

（イ）端末の回収

本県が指定する端末を職員から回収すること。

（ウ）再設定

（ア）で作成したマスタイメージを回収端末に展開すること。

（エ）端末の再配付

本県が指定する職員に端末を再配付すること。

・　新 DK 端末へ設定変更する業務端末の各庁舎別端末設置台数（R4.4 現在）は以下のとおり。

庁舎	所在地	台数
本庁舎	三重県津市広明町 13	約 1,400 台
桑名庁舎	三重県桑名市中央町 5-71	約 60 台
四日市庁舎	三重県四日市市新正 4-21-5	約 60 台
鈴鹿庁舎	三重県鈴鹿市西条 5 丁目 117	約 40 台
津庁舎	三重県津市桜橋 3-446-34	約 60 台
松阪庁舎	三重県松阪市高町 138	約 90 台
伊勢庁舎	三重県伊勢市勢田町 628 番地 2	約 60 台
伊賀庁舎	三重県伊賀市四十九町 2802	約 50 台
志摩庁舎	三重県志摩市阿児町鵜方 3098-9	約 30 台
尾鷲庁舎	三重県尾鷲市坂場西町 1 番 1 号	約 30 台
熊野庁舎	三重県熊野市井戸町 371	約 60 台

(3)　端末の再設定は、新 DK 端末として利用する「DK20」、「DK21」及び MW 端末の一部の合計 2,000 台程度を想定している。ただし、旧 DK 端末等に受託事業者が指定するエージェント等をインストールする必要が場合は、旧 DK 端末を含め、対象は全端末 8,000 台とする。

(4)　本契約期間中に旧 DK 端末を世代単位で機器更新し、新 DK 端末へ移行することを想定している。受託事業者は、新 DK 端末の調達・移行を行う事業者（別途、県が契約）に対し、設定等の支援を行うこと。

6. 構成要素の仕様（共通事項）

6-1. クラウドサービスに関する事項

6-1-1. 前提条件

(1) 選定するクラウドサービスについて、コミュニケーション基盤は、「政府情報システムのためのセキュリティ評価制度（ISMAP）」のクラウドサービスリストへの登録がなされていること。

(2) データ活用基盤及び情報セキュリティ基盤については、「政府情報システムのためのセキュリティ評価制度（ISMAP）」に登録されているか、情報セキュリティ管理・運用の基準となる以下のいずれか、または同等の認証を取得し、サービスの信頼性が確認できること。

・ISO/IEC 27017 によるクラウドサービス分野における ISMS 認証取得
・日本セキュリティ監査協会のクラウド情報セキュリティ監査による認定
・SOC2 報告書(Service Organization Control Report)の取得

なお、データ活用基盤で動作するサービスについては、国が示すスマートシティガイドラインに準拠していること。

(3) クラウドサービスにおいて一定のセキュリティレベルが確保されていることの保証として、クラウドサービスに対する情報セキュリティ監査報告書の内容及び取得・維持している各種認定・認証制度の基準、ガイドライン等について事前に確認し本県に提示すること。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。

(4) 選定するクラウドサービスは、国内に裁判管轄権があること。

(5) 本サービスを提供する施設等は、必要なセキュリティ及び災害対策等の措置がとられていること。

(6) 選定するクラウドサービスは、地理的に離れた 2 つ以上のリージョンでサービスが提供されており、大規模災害の場合でも別のリージョンへ切り替えが行われること。なお、本事項はコミュニケーション基盤のみの要件とする。

(7) 十分な稼働実績を有し、運用の自動化、サービスの高度化、情報セキュリティの強化、新機能の追加等に積極的かつ継続的な投資が行われているクラウドサービスを選定すること。

(8) クラウドサービスを利用する場合は、本仕様書に記載されているセキュリティ対策を遵守すること。

6-1-2. 基本要件

(1) クラウドサービスを使用した時に出力されるログを提供すること。又は、ログ検索機能を提供すること。

(2) クラウドサービスへのアクセスは機密漏えい防止のため、通信の暗号化を行うこと。

(3) クラウドサービスの契約終了時、業務データ等の消去を遅滞なく確実に実施すること。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。

(4) 業務データ等のバックアップは、データの完全性やデータリカバリのコストのバランスを踏まえ、同一クラウドサービスの内部で複数作成すること。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。

(5) 本業務において導入する全てのクラウドサービスは、情報セキュリティ基盤経由の通信のみに限定できること。ただし、その他の手法により、同等以上のセキュリティレベルの確保ができる場合、この限りではない。

(6) 提案本業務において導入する全てのクラウドサービスは、ユーザ属性及び端末属性により、アクセス範囲の制限が可能であること。想定具体的には、コミュニケーション基盤については、業務端末及び個人端末からアクセスできることとして、個人端末からアクセスする場合は、一定の制限（例：参照機能のみ・ダウンロード制限・ブラウザ上での編集作業に限定等）を行うことを想定している。

6-2. 情報セキュリティに関する事項

6-2-1. 方針

(1) クラウドサービスの利用や庁外へ持ち出し可能となる業務端末に関して、新たにゼロトラストセキュリティを採用する。ただし、旧 DK 端末からインターネットへアクセスを行う場合は、境界型（ペリメータ）セキュリティを採用する。

(2) 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」、「三重県個人情報保護条例」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。

(3) 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。

(4) 提案情報漏えいが疑われる、または発生した場合、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。

(5) 不要な通信は抑制すること。

6-2-2. 認証技術

(1) 利用者が DX 推進基盤を利用する際、アカウントの共有等による不正利用やなりすましを防止するため、多要素認証を行うこと。

(2) 運用担当者が DX 推進基盤のサービスにログインする際においても認証を行うこと。

(3) クラウドサービスを含む各業務システムへのアクセスはシングルサインオンを可能とすること。

(4) 不正にログインしようとする行為を検知又は防止する機能を有すること。

(5) 利用者に付与したアカウントを、その後別の利用者に付与しないこと。

(6) 認証情報を保存する場合に暗号化を行う機能を有すること。

(7) 認証に関しては、別途導入済の IDaaS(Soliton OneGate)と連携して行うことも可とする。ただし、データ活用基盤に関してはこの限りではない。

6-2-3. アクセス制御・権限管理

(1) アカウントはサービスにおける作業者の役割ごと（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。
(2) 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。
(3) 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。
(4) 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また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。
(5) 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。
(6) 提案 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、外部の認証基盤と連携する場合はこの限りではない。
(7) 想定 CSV ファイル等によるユーザの一括登録、削除が行えること。

6-2-4. ログの取得・管理

(1) DX 推進基盤で提供するサービスの証跡ログを収集すること。
(2) 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。
(3) 証跡の不当な消去や改ざんを防止するため、証跡に関するアクセス制御機能を備えること。
(4) 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。
(5) 提案 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。
(6) 想定 ログ保存システムを整備し、30 日より前のログを格納すること。

6-2-5. 暗号化・電子署名

(1) 外部に送信するデータについては暗号化を行うことで個人情報や機密情報が保護されるように対策を講ずること。
(2) 暗号及び電子署名のアルゴリズムについては、可能な限り、強度の高いアルゴリズムを想定した上で、設計・構築を実施すること。

6-2-6. ソフトウェアに関する脆弱性対策

(1) 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、入手する体制を整えること。

(2) 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上で本県へ報告すること。
(3) セキュリティホール対策の実施に際しては、事前に DX 推進基盤への影響検討、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。
(4) 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。
(5) 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。

6-2-7. 不正プログラム対策

(1) 本業務において導入するオンプレミスシステムの機器等について、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、当該電子計算機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。
(2) 本業務において導入するオンプレミスシステムの機器等について、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。

6-2-8. セキュリティインシデントへの対応

(1) 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。
(2) 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。
(3) 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。
(4) 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提供時間内において、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。
(5) 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、本県と協議の上、決定すること。
(6) 業務端末への侵入検知と対応は、別途契約済みの EDR（Tanium）を利用すること。

6-3. サービスレベルの管理に関する事項

DX 推進基盤について、24 時間 365 日稼動できる体制を確保するものとする。SLA は DX 推進基盤の運用・監視・保守業務開始時点から適応する。なお、運用・監視・保守業務開始の時期は、本県と受託事業者との協議において判断する。

なお、サービスレベル基準値を下回った場合、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。

6-3-1. 指標の設定

運用・監視・保守業務の品質の維持・向上を図るため、受託事業者は「別紙 1　サービスレベル設定基準（運用・監視・保守）」に基づく SLA を本県と締結すること。

6-3-2. SLA のモニタリング

受託事業者は SLA の履行状況について報告を月 1 回行うこと。

6-3-3. 改善

(1) 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下で行っていくこと。
(2) 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、結果対応について報告すること。
(3) 改善に関する費用は受託事業者が負担すること。

6-3-4. 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。
(1) 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
(2) 本県又は他の事業者の過失及び故意による障害の場合
(3) 受託事業者の瑕疵によらず障害復旧が行えない場合
(4) 受託事業者の瑕疵によらず障害監視が行えない場合
(5) 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
(6) 本県及び受託事業者双方の協議の上、計測の除外とした場合

6-3-5. 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 または SLO に準ずるものとする。
提案なお、各クラウドサービスの SLA または SLO を事前に提示し、本県の承認を得ること。

6-4. ソフトウェアに関する事項

(1) 構成要素単位で記載している要件を満たすソフトウェア構成とすること。
(2) 直観的に操作しやすい UI（ユーザインターフェース）を有すること。
(3) 快適に操作できるレスポンス（画面遷移 3 秒以内）を確保すること。
(4) 令和 10 年 3 月 31 日までに製品サポートの終了が予定されていない製品の選定を行うこと。また、上記期間までに製品サポートが終了することとなった場合は、受託事業者の責任において、ハードウェアの交換やソフトウェアのバージョンアップ等を実施し、製品サポートを継続すること。
(5) 調達するソフトウェアについては、国、地方自治体又は民間企業における導入・稼働実

績等を有し、本県の要件（業務端末数等）に対して動作保証できるものを提供すること。

(6) ソフトウェアライセンス違反を犯さないように、受託事業者の責任において、調達すること。

(7) 受託事業者が導入するソフトウェアが、本仕様書どおりの機能を提供できない場合には、本県と協議の上、その代替ソフトウェアを提供すること。

6-5. 端末等に関する前提条件

6-5-1. 端末の概要

(1) デジタル改革推進課において配付している業務端末（DK 端末／5,326 台、KK 端末／186 台）

- 「DK」または「KK」から始まる管理番号を付与し、三重県行政 WAN に接続している。
- 概ね 7 年程度で機器更新を行っている。
- OS は、Microsoft Windows 10 Pro（OEM 版）を利用している。
- Office ソフトは、以下のいずれかを利用している。
  Microsoft Office 2013 Professional Plus（永続版）
  Microsoft Office 2016 Professional Plus（永続版）
  Microsoft Office 2016 Standard（永続版）
- 「DK20」、「DK21」は画面サイズが 13.3 インチのモバイルパソコンとなっている。うち、「DK21」は SIM による通信機能を有している。
- DX 推進基盤において、「DK20」、「DK21」を新 DK 端末として運用する。また、「DK17」、「DK18」、「DK19」、「KK17」、「KK18」、「KK19」については、旧 DK 端末として運用する。
- 各端末の台数及び構成は「別紙 2　デジタル改革推進課において配付している業務端末」のとおり。

(2) 各課において購入・管理している業務端末（SK 端末／2,700 台程度）

- 「SK」から始まる管理番号を付与し、三重県行政 WAN に接続している。
- OS は、Microsoft Windows 10 Pro（OEM 版）または、Microsoft Windows 8.1 Pro（OEM 版）を利用している。
- Office ソフトは、以下のいずれかを利用している。
  Microsoft Office 2013 Professional Plus（永続版）
  Microsoft Office 2016 Professional Plus（永続版）
  Microsoft Office 2016 Standard（永続版）
- DX 推進基盤において、SK 端末は、旧 DK 端末と同様の取り扱いとする。

(3) デジタル改革推進課において調達・管理しているモバイル端末（MW 端末／430 台）

- 「MW」から始まる管理番号を付与し、SIM によりインターネットに接続している。
- 画面サイズが 13.3 インチ、12.3 インチ、10 インチいずれかのモバイルパソコンとなっている。また、全ての MW パソコンが SIM による通信機能を有している。
- OS は、Microsoft Windows 10 Pro（OEM 版）を利用している。
- シンクライアントとして利用するため、Office ソフトは導入していない。
- DX 推進基盤において、MW 端末の一部を新 DK 端末と同様の取り扱いとして運用する。

(4) 各職員の個人端末（BYOD 端末）

- 各所属員が所有する PC やタブレット、スマートフォンとし、それぞれインターネットに接続している。
- 提案 DX 推進基盤において、コミュニケーション基盤の一部機能を利用する端末として活用する。
- 想定 DX 推進基盤において、情報セキュリティ基盤を通じて、セキュリティ確保を行い、コミュニケーション基盤の一部機能を利用する端末として活用する。
- BYOD 端末において、対象とする OS は、以下のとおりとする。
  Apple iOS 最新版
  Apple macOS 最新版
  Google Android OS 最新版
  Microsoft Windows 10 Pro/Home
  Microsoft Windows 11 Pro/Home

6-5-2. ライセンスの取り扱い

本業務における、端末に係るライセンスの取り扱いは以下のとおりとする。

(1) OS

- 提案 DK 端末、KK 端末、SK 端末、MW 端末ともに、今後も購入する PC に付属の Microsoft Windows を利用する予定であるが、本契約において Microsoft Windows ライセンス、または Microsoft Windows Enterprise へのアップグレードライセンスの導入を妨げるものではない。
- ただし、Microsoft Windows ライセンス、または Microsoft Windows Enterprise へのアップグレードライセンスを導入する場合は、全ての職員が常に最新版を利用できること。

(2) オフィスソフト

- 提案 DK 端末、KK 端末、SK 端末ともに、今後も永続版の Microsoft Office を購入し利用する予定であるが、本契約において Microsoft Office のライセンス導入を妨げるものではない。
- ただし、Microsoft Office のライセンスを導入する場合は、全ての職員が常に Microsoft Ofiice 365 ProPlus 相当の最新版を利用できること。

(3) その他

- 庁内システムにおいて、Microsoft Windows Server を利用していることから、Microsoft Windows Server 2019 UserCAL 3,092 ライセンス、Microsoft Windows Server 2019 DeviceCAL 167 ライセンス、Microsoft Windows Server 2022 UserCAL 4,591 ライセンス、Microsoft Windows Server 2019 DeviceCAL 166 ライセンスを購入している。
- 提案 今後も、別途、Microsoft Windows Server CAL を必要数購入する予定であるが、本契約においての CAL の導入を妨げるものではない。
- ただし、CAL を導入する場合は、全ての職員が利用できること。

6-5-3. 閲覧ブラウザ

(1) DK/KK/MW 端末
- Google Chrome 最新版
- Microsoft Edge 最新版

(2) SK 端末
- FireFox 最新版
- Google Chrome 最新版
- Microsoft Edge 最新版

(3) BYOD 端末
- Apple Safari 最新版
- FireFox 最新版
- Google Chrome 最新版
- Microsoft Edge 最新版

6-6. 機器設置に関する前提条件

(1) 本県が指定する IDC 内のラックを使用すること。ラックの規格については H2,000mm×W600mm×D900mm(35U)で、うち 15U 程度が利用可能である。
(2) 利用できる電源容量は、1 ラックあたり 100V，20A までとする。
(3) 上記を越えるハウジングスペースや電源容量が必要な場合は、追加が可能だが、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。
(4) ラック間の配線は、IDC 事業者が有償で行う。その作業費用を負担すること。
(5) ラック間の配線は、申請から実施まで 2 週間程度を要するため、余裕をもって設置計画を立てること。

7. 構成要素の仕様（コミュニケーション基盤）

7-1. 目的

行政 DX の推進に向けて、コロナ禍を契機として運用を開始したテレワークの一層の定着化を図るほか、職員が場所や時間、端末の制約を受けずに円滑なコミュニケーションを可能にする環境を提供することが、フレキシブルで多様な働き方の実現に不可欠となる。

現在の庁内メールやインターネットメール、グループウェアの、コミュニケーション系システムはオンプレミス方式であり、職員からの改善要望も多く、いずれも令和 4 年度または令和 5 年度中に保守期限を迎えることから､今回の DX 推進基盤の整備にあわせて抜本的な見直しを行う。

見直しに際しては、クラウドサービスへの移行・刷新を前提とし、加えてチャットやファイル共有等のツールを導入することで、統合的なコミュニケーション基盤として、業務効率化と生産性のさらなる向上につながる環境が最適化できると考えている。

今回の整備・運用を経て、今後職員は、業務効率化と生産性向上により捻出できた時間を、県民に寄り添う良質なサービスを創出するための企画立案･実施に充てることが可能となり、DX による組織改革の進展が期待できる。

7-1-1. メールシステム／メールリレーシステム

現行の職員向けメールシステムは、庁外向け（インターネットメール及び LGWAN メール）と庁内向け（庁内メール）がそれぞれ別システムとして運用されているが、両メールシステムを統合してクラウドサービスに移行することにより、運用に係る業務負荷の縮減や職員の利便性向上をめざす。

移行にあたっては、現環境と同様、インターネットメール、LGWAN メールを一つの環境で送受信できるよう利便性を高めるとともに、職員が庁外向けと庁内向けのメール及びアドレスが容易に区別できるような仕組みとなっていることが望ましい。

また、前述のとおり「三層の対策」の強靱化モデルをαモデルからβ’モデルに変更するが、インターネットや LGWAN ネットワーク経由で送受信を行うメールのセキュリティを確保し、適切に運用管理する仕組みを整備する。

さらに、インターネットメール、LGWAN メールとも送受信時において、ウイルスチェック及び無害化処理、誤送信対策等を必須とするが、それらを実現するために既存システムを利用することも可としており、そうした場合のメールリレーの仕組みについても整備する。

7-1-2. Web コミュニケーション／ファイルストレージ

現在のグループウェアで実施している、予定管理や施設予約等の機能の刷新に留まらず、チャットや、職員間または外部とのファイル（機密情報を除く。）交換・共有を可能とするファイルストレージなど、コミュニケーションの活性化につながる新たな仕組みを導入することで、迅速な情報共有や意思決定を可能とし、職員のみならず県全体における生産性向上に貢献するとともに、組織の活性化につなげていく。

7-1-3. 業務効率化ツール（ノーコード／ローコードツール）

職員のみでアプリケーションの内製化が可能なノーコードまたはローコードツールを導入することにより、業務の担当職員が自らデジタル化による課題解決を図るとともに、類似の課題について横展開を進め、本県の業務効率化と行政サービス向上につなげていく。

また、アプリケーションを内製化することで、開発速度の向上とともに柔軟なシステム開発を実現するほか、システム全体の把握を可能とすることでノウハウの蓄積や人材育成につなげていく。

当面は庁内業務の効率化に重点を置いたアプリケーションの内製化に取り組むことを想定しているが、県民及び事業者等に対しても、一定規模の範囲でデジタル手続等の提供（公開）が可能となる環境を導入できることをめざす。

なお、プログラミングスキルが必要なツールを導入する場合は、職員への研修も含めて提案することが必要である。

7-2. メールシステム

7-2-1. 機能要件

(1)　基本機能

- クラウドサービス内でメールシステム機能を提供すること。
- 提案 インターネットと LGWAN の両方のメールを送受信できる仕組みであること。
- 想定 インターネットと LGWAN の両方のメール送受信に係る経路は、「7-2-2 概略図（想定）」のとおりとする。
- 提案 マルチドメイン（pref.mie.lg.jp 及び mieken.jp）での運用が可能であること。
- 想定 ドメインごとに、メール送受信範囲の設定が可能であること。具体的には、mieken.jp は職員間の送受信に限定し、pref.mie.lg.jp は外部との送受信も可能とすること。
- 想定 一つのメールボックスでマルチドメインに対応できること。
- 提案 組織に対して、メールアドレスを割り当てる機能を有すること。
- POP 及び IMAP によりメールの受信が可能であること。
- Web メール、メールクライアントのどちらかで利用できること。
- メールアカウントのパスワードリセットが行えること。
- パスワードの世代管理や利用文字などのパスワードポリシーを詳細に設定管理が可能であること。ただし、IDaaS 経由のシングルサインオンを実施する場合はこの限りではない。
- 後述する予定表等に予定が追加された場合、該当者にメールが送信されるなど、グループウェア機能と連携が可能であること。
- 現行の外部メールサーバは、令和 7 年 12 月末まで利用可能である。
- 現行の外部メールサーバの保守終了後は、DX 推進基盤の運用終了まで、本県により保守延長を行う。

(2) メール送受信

- メールの本文は、テキスト形式とリッチテキスト形式での作成が切換選択できること。
- 作成中のメールが自動で一時保存できること。
- 添付ファイルの登録が、ドラッグ＆ドロップ操作でできること。
- メール作成時に設定した宛先を後からドラッグ＆ドロップ操作で宛先欄（To･Cc･Bcc）のいずれにも移動できること。
- アドレス帳より送信先を指定できること。
- 提案アドレス帳は、組織単位でのツリー構造で表示・選択が可能であること。
- システム内でのメール送信については、受信者がメールを開封したか否かの確認機能があること。
- メール本文に署名を自動登録できること。
- 返信、全員へ返信、転送等が行えること。また、返信への宛先は任意に削除して送信できること。
- メールの遅延送信の設定をユーザで行える機能を有すること。
- 削除したメールは一旦ごみ箱に格納されること。
- 削除したメールはごみ箱へ格納され、一定期間は任意のタイミングで削除できること。
- ごみ箱から削除したメールを一定期間ユーザ操作で復元できること。
- 重要なメールにフラグをつけて、他のメールと差別化できること。
- 階層化可能なフォルダやラベルによりメールを管理できること。
- メールをドラッグ＆ドロップ操作でフォルダに移動またはラベル付けできること。
- 添付ファイルの本文も含め、キーワードによる検索が可能なこと。
- 受信メールの条件振り分けが可能なこと。
- 受信メールを自動転送する機能を有すること。
- メールのスレッド表示ができること。
- 組織メールアドレスに一斉送信する機能を有すること。

(3) 管理者向け機能

- 管理者から権限を与えられたユーザが、組織メールアドレスの利用者を追加・削除を行える機能を有すること。
- 組織メールアドレスの閲覧権限、送信権限を別の利用者アカウントに割り当てる機能を有すること。
- CSV 等のファイルを利用して、ユーザの一括登録、削除が行えること。
- メールアカウントごとに自動転送設定を制限できる機能を有すること。
- メールアカウントのパスワードリセットが行えること。
- パスワードの世代管理や利用文字などのパスワードポリシーを詳細に設定管理が可能であること。

(4) メール無害化

- 無害化処理対象のファイルは送信メールサイズの最大値まで処理できること。
- メール無害化は、現行の原本保管／添付ファイル分離システムを利用することができる。なお、現行の原本保管／添付ファイル分離システムは、令和 6 年 3 月末まで利用可能である。
- 現行の原本保管／添付ファイル分離システムの保守終了後は、DX 推進基盤の運用終了まで、本県により保守延長を行う。
- 提案 LGWAN へ送信するメールについて、添付ファイルの無害化（悪性コードの除去）を行うこと。
- 想定マクロ付ファイルを送信する場合、職員側での簡単な操作により送信できる仕組みを持つこと。

(5) メールセキュリティ

- 提案迷惑メールを自動判定し、フォルダに分類またはラベリングできる機能を有すること。
- 提案メール送受信時にマルウェア（ウイルス及びスパイウェア）対策を行うこと。
- マルウェア（ウイルス及びスパイウェア）対策は、現行のウイルスチェック用サーバを利用することができる。なお、現行のウイルスチェック用サーバは、令和 6 年 3 月末まで利用可能である。
- 現行のウイルスチェック用サーバの保守終了後は、DX 推進基盤の運用終了まで、本県により保守延長を行う。
- 管理者の操作により送受信可能な添付ファイルの拡張子を設定できること。
- 送信元として指定できるドメインの制限ができること。
- 第三者中継（オープンリレー）を防ぐこと。
- バックスキャッター（後方錯乱）の対策機能を有すること。
- メールクライアントとメールサーバ間の通信は TLS で暗号化すること。
- メール送受信が可能な機器を IP アドレス等で制限できること。

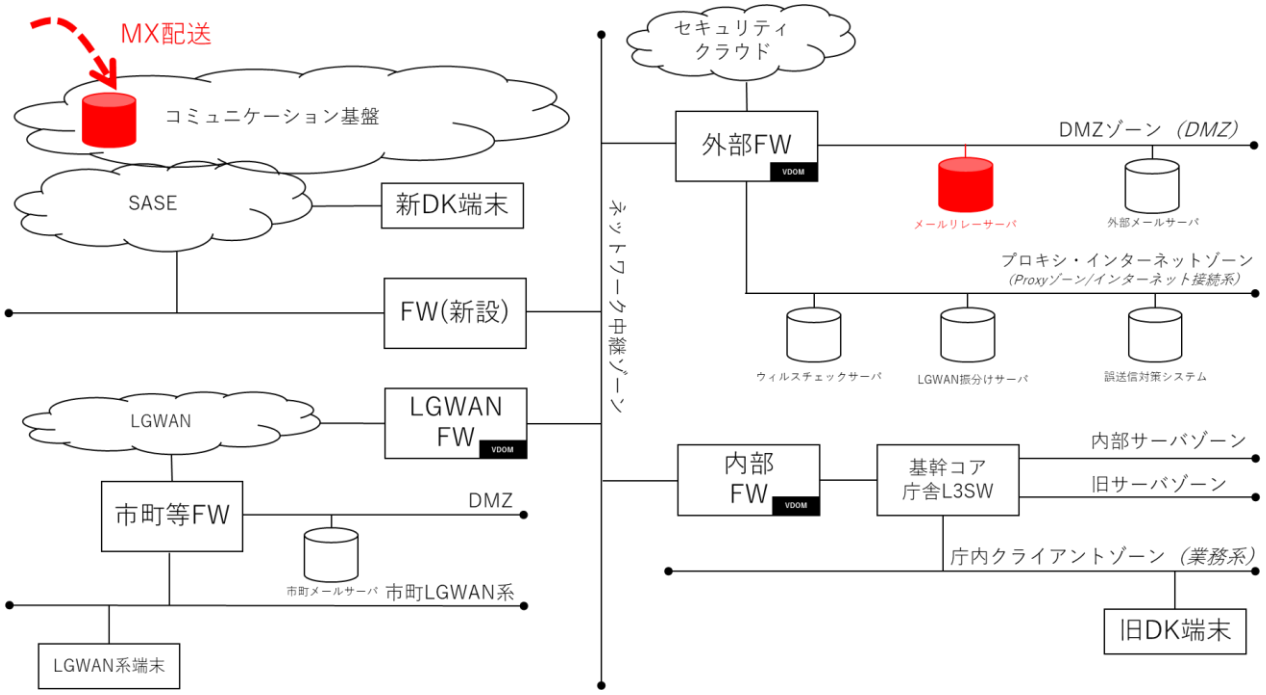
(6) メール誤送信対策

- 現行のメール誤送信対策システムを利用することにより、メール送信ディレイ及び強制 Bcc 化等の対策を行うこと。
- 現行のメール誤送信対策システムは、令和 6 年 3 月末まで利用可能である。
- 現行メール誤送信対策システムの保守終了後は、DX 推進基盤の運用終了まで、本県により保守延長を行う。

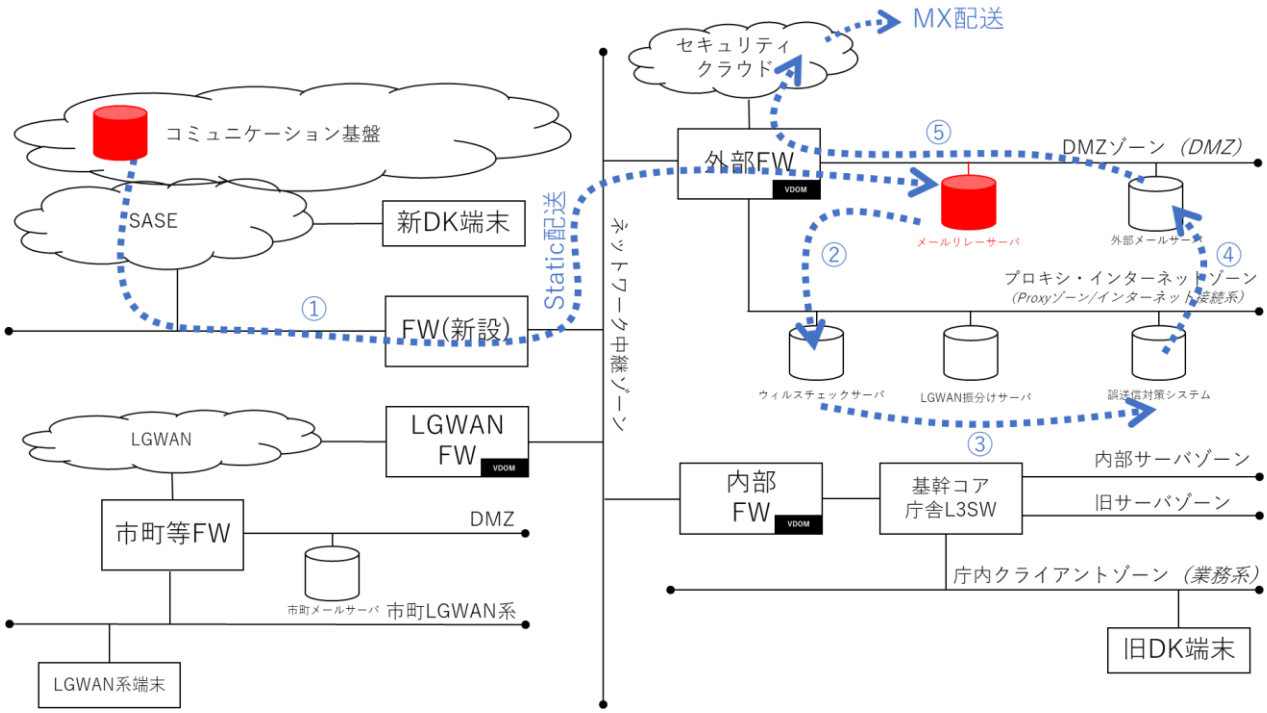
7-2-2. 概略図（想定）

想定各メールの配送ルート（案）を下記に示す。ただし、各メールの配送ルートについては、受託事業者が提案するものとし、案のとおり実現する必要はない。

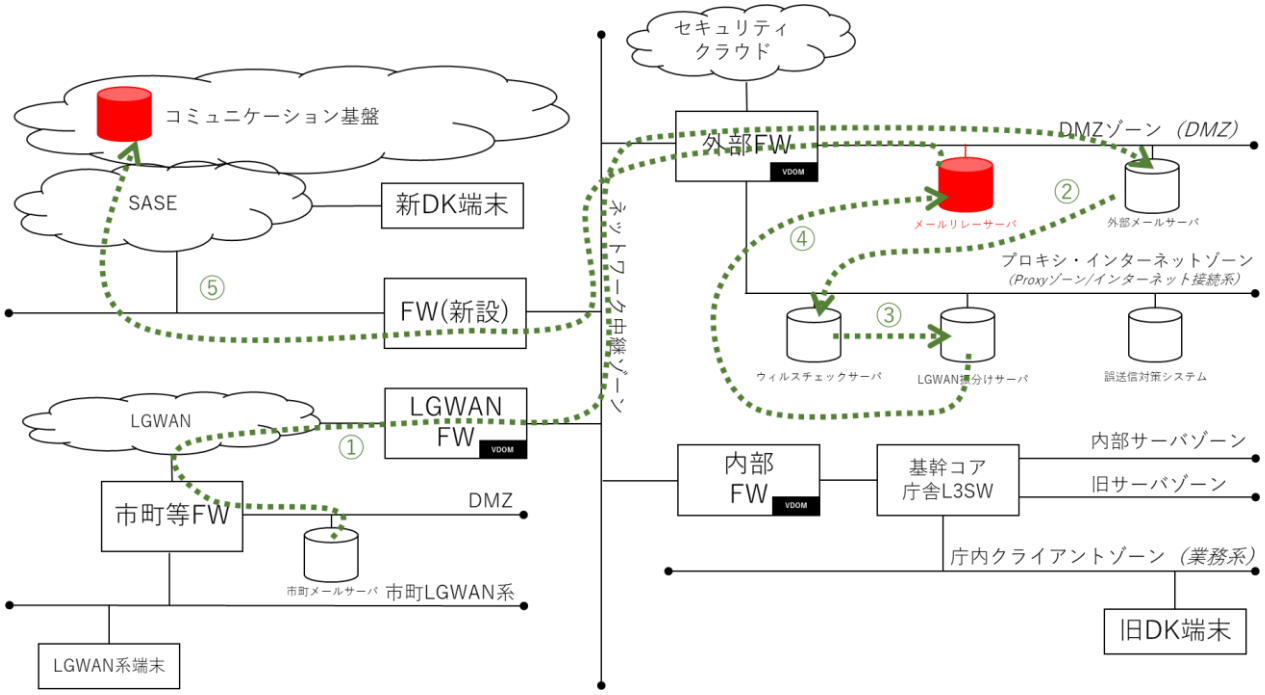
（1） インターネットメール（受信）



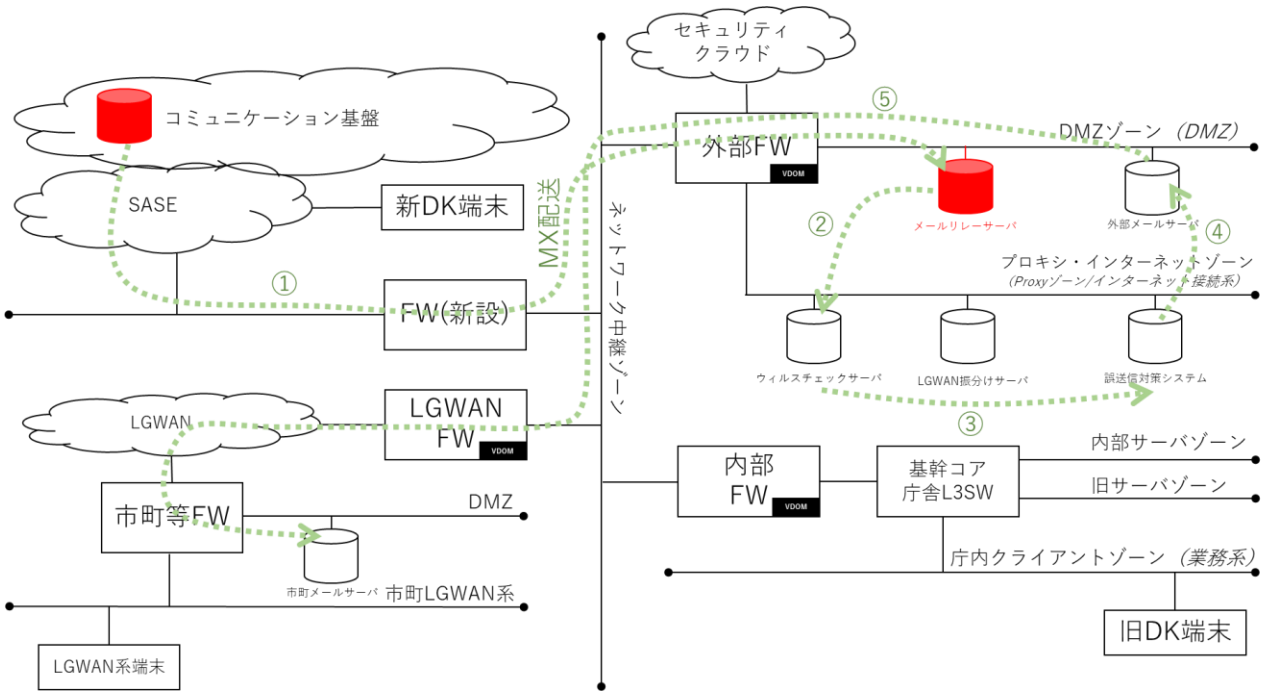
（2） インターネットメール（送信）



（3） LGWAN メール（受信）



（4） LGWAN メール（送信）



7-2-3. 非機能要件

（1） システム稼働環境

・ 本機能は、クラウドサービスの利用を前提とする。
・ クラウドサービスの詳細は「6-1 クラウドサービスに関する事項」を参照すること。
・ ユーザ数 7,500（アカウント）、業務端末 8,000 台程度が問題なく利用できる環境を

整備すること。

- 1 分間に 1,500 通のメール送受信に耐えられる環境を整備すること。
- 90 万通／月のメールを処理できるシステムとすること。
- アクセス集中時にも安定的に稼働ができ、快適に操作できるレスポンスを確保すること。
- 同程度のアカウント数での導入実績があり、現在も利用中又は利用可能なシステムであること。
- 1 メールアカウント当たりメールボックスとして 50GB 以上が割り当てられていること。また 100GB 以上拡張可能なこと。

(2) 移行に関する事項

- 現行システムから移行時において、メールの送受信が停止することがないように行うこと。ただし、夜間帯・閉庁日かつ職員に事前アナウンスを行う前提で、メールの送信を停止することは可とする。
- メールの受信については、外部メールサーバにスプールする等、停止することがないよう移行作業を行うこと。
- 個人アドレス帳のデータ移行については、職員がデータ移行を簡易に行える仕組みを提供すること。

(3) 監視に関する事項

- 提案メールシステムの稼働状況を監視し問題発生時に運用管理者に通知する仕組みを構築すること。ただしクラウドサービス特有の事情があれば、その旨を明記の上、提案すること。
- 提案メールシステムのリソースを監視し、事前に取り決めたしきい値を超過した時に運用管理者に通知する仕組みを構築すること。ただしクラウドサービス特有の事情があれば、その旨を明記の上、提案すること。
- 提案メールシステムの各種ログを監視し、事前に取り決めたログが記録された時に運用管理者に通知する仕組みを構築する。ただしクラウドサービス特有の事情があれば、その旨を明記の上、提案すること。

(4) 情報セキュリティに関する事項

- 「6-2 情報セキュリティに関する事項」を前提とした情報セキュリティ対策を実施すること。

(5) ソフトウェアに関する事項

- 「6-4 ソフトウェアに関する事項」を前提としたソフトウェア構成とすること。

(6) 機器設置に関する事項

・ 機器を導入する場合は、「6-6　機器設置に関する前提条件」を参照し設置すること。

7-3. メールリレーシステム

7-3-1. 機能要件

(1) 提案メールシステムから転送されたインターネットメールについて、セキュリティクラウドを通じてインターネットへ配送する機能を有すること。

(2) 提案メールシステムから転送された LGWAN メールについて、LGWAN ネットワークへ配送する機能を有すること。なお、配送先のメールサーバの指定には LGWAN ネットワークの名前解決が行える内部 DNS サーバを参照しての MX 配送の仕組みを用いること。

(3) 提案 LGWAN ネットワークから受信した自ドメイン宛て(pref.mie.lg.jp)のメールを、メールシステムに配送する機能を提供すること。

(4) メールリレー機能におけるメールログやシステムログを個々のログファイルに出力すること。

(5) 接続元 IP アドレスによる接続又は配送制限が行えること。

(6) 想定三重県行政 WAN 内にメールリレー用のサーバを設置すること。

7-3-2. 非機能要件

(1) システム稼働環境

・ メールリレー機能を実現するサーバは 1 台で障害が発生した場合にも、継続して処理が可能になるよう、2 台以上の構成とすること。

・ 障害時の復旧を目的とし、システムイメージバックアップをシステム変更時及び定期的に取得し保管できるようにすること。

・ 障害発生時にサービス停止時間が生じないよう、機器の部分的な障害時にもサービスが停止することなく、機器の交換が行える構成とすること。

・ メールリレーサーバは既存の共通機能基盤上に構築することも可とする。共通機能基盤を利用する場合は、「別紙 3　統合サーバの利用について」を参照すること。

・ なお、既存のインターネットメールシステムの設定変更が必要になる場合は、別途既存事業者に対して、設定変更に関する依頼等などを行うこと。

(2) 監視に関する事項

・ 提案メールリレーシステムの稼働状況を監視し問題発生時に運用管理者に通知する仕組みを構築すること。ただしクラウドサービス特有の事情があれば、その旨を明記の上、提案すること。

・ 提案メールリレーシステムのリソースを監視し、事前に取り決めたしきい値を超過した時に運用管理者に通知する仕組みを構築すること。ただしクラウドサービス特有の事情があれば、その旨を明記の上、提案すること。

・ 提案メールリレーシステムの各種ログを監視し、事前に取り決めたログが記録された時に運用管理者に通知する仕組みを構築する。ただしクラウドサービス特有の事情があれば、その旨を明記の上、提案すること。

(3) 情報セキュリティに関する事項

・ 「6-2 情報セキュリティに関する事項」を前提とした情報セキュリティ対策を実施すること。

(4) ソフトウェアに関する事項

・ 「6-4 ソフトウェアに関する事項」を前提としたソフトウェア構成とすること。

(5) 機器設置に関する事項

・ 機器を導入する場合は、「6-6　機器設置に関する前提条件」を参照し設置すること。

7-4. Web コミュニケーション

7-4-1. 機能要件（予定表／施設予約／電子職員録／掲示板／チャット／Web 会議）

(1) 予定表

・ 提案予定表の閲覧、更新（登録・編集・削除）ができること。
・ 職員の予定を月間、週間、1 日の単位で表示できること。
・ 提案組織ツリー構造から所属や任意グループを選択し、メンバーの予定を並べて表示できること。
・ 予定ごとに、公開・非公開や、閲覧可能な範囲を指定でき、カテゴリや重要度等に応じて表示色が指定できること。
・ 会議予定の登録または編集時に会議への出席者の空き時間検索が可能であること。
・ 会議への出欠のステータスが容易に確認可能であること。
・ 繰り返しの予定を一括で作成できること。
・ 予定表は一覧表示が可能で、一覧表示の画面で、予定の開始・終了時刻、件名、場所が表示されること。
・ 登録した予定時間（又は分／日）前にアラームを通知するよう設定できること。
・ 予定は重複して登録できること。また、予定の重複が分かるように表示されること。
・ メールシステムやチャットと連動して、会議予定の登録または編集時に、関係者へ通知できること。
・ 職員が休暇や時間外勤務、出張、各種手当等の手続を行う「総務事務システム」を利用して申請（新規・変更・取消）した休暇（振替・代休等）、早出・遅出・在宅勤務、出張について、「総務事務システム」から出力される CSV ファイルを取り込み、職員の予定表へ反映される機能を有すること。

(2) 施設予約

- 提案施設の予約処理が実施できること。
- 施設の予約状況を日単位、週単位、月単位で表示できること。
- 予約者、会議名等の表示が可能であること。
- 会議室、備品等の一時利用停止が設定可能であること。
- 重複予約の制限が可能であること。
- 会議室を予約できるユーザ、グループを設定可能であること。
- 管理者が設備の登録、更新、削除の管理を行えること。設備ごとにアクセス権の設定が可能であること。
- 指定した会議室の空き時間を検索できること。また、指定した時間帯に利用可能な会議室を検索できること。
- メールシステムやチャットと連動して、会議室を予約した際に、関係者へ通知メールを送信できること。
- 施設単位で、予約可能期間の制限が可能であること。

(3) 電子職員録

- 提案組織ツリー構造を表示し、組織を選択することで、職員の氏名、職名、所属、メールアドレス、電話番号等を、所属ごとに一覧表示、検索できること。
- また、氏名、職名等のキーワードにより、職員の検索が可能であること。
- 公開範囲の設定ができること。
- データのインポート・エクスポート機能を有していること。
- 人事異動及び組織改編に伴う変更が容易であること。
- 職員がプロフィール等を登録でき、他の職員が検索・参照できる機能を有すること。

(4) 掲示板

- 提案庁内向けのお知らせ等は閲覧可能範囲を指定したうえで記事として投稿可能であること。
- 記事には、ファイルや画像の添付が可能であること。
- 記事は、カテゴリ毎に分類し表示ができること。
- 記事のアドレスをメールシステムやチャットと連携し、周知可能であること。
- 希望する記事が投稿された場合、メールシステムと連携し、通知が受信できること。

(5) チャット

- 提案1 対 1 の利用者間や、任意に作成したグループ内でテキストチャットを行えること。
- 既読機能または、リアクションを返信する機能を有すること。
- 1 対 1 の利用者間や、任意に作成したグループ内でファイル共有を行えること。
- ファイル共有の禁止の設定が可能であること。

- 送受信した過去のメッセージを確認できること。
- 提案使用者のプレゼンス（在席状況）を表示できること。
- 相手がオフラインであってもチャットメッセージを送信できること。
- キーワード検索が可能なこと。
- チャットの履歴をアーカイブや会話履歴として保存可能なこと。
- インターネット経由で外部ユーザとのチャットを行う機能を有すること。なお、内部ユーザ及び外部ユーザの判別ができること。

(6) Web 会議

- 提案映像及び音声を用いた Web 会議が開催できること。
- 映像や音声のソースには、端末に接続された Web カメラや内部マイクだけでなく、外部入力も利用できること。また、ノート PC やタブレット内蔵の Web カメラやマイクも利用できること。
- アプリケーション画面やファイルの共有ができること。
- 招待された外部関係者が、システムの利用登録手続きをすることなく、会議に参加できること。
- 日時を指定した Web 会議予約が可能であること。
- メールにより参加者を招待できること。
- 会議の予約や開催は、メールシステムや予定表等と連携できること。
- 会議の録音及び録画が可能であること。録音及び録画データは、クラウド及びローカル PC に保存できること。
- ホワイトボード機能を有すること。
- 会議に参加している利用者が、任意に選択した他の利用者と 1 対 1 又は複数で会議開催中にリアルタイムでテキストチャットが行えること。
- 会議室に別の小会議室を作成し、参加者を任意に割り振り可能であること。
  また、時間を定め、会議室に呼び戻す機能を有すること。
- 1 会議室あたり、250 人以上が参加可能であること。
- 会議は、24 時間以上継続可能であること。
- 提案イベント方式の会議が開催可能であること。
- 想定ウェビナー機能を利用し、パネリストと視聴者を区別したイベントが開催できること。
- 想定 Q&A 機能により、視聴者からパネリストへ質問が行えること。

7-4-2. 機能要件（管理機能／連携機能）

(1) 管理機能

- 長期利用しないアカウントを利用停止状態にする機能を有すること。
- 利用者アカウントは、ディレクトリサービスや IDaaS との連携が可能であること。

(2) 連携機能

・ 予定表・Web 会議などの機能と連携できる機能を有すること。

7-4-3. 非機能要件

(1) システム稼働環境

・ 本機能は、クラウドサービスの利用を前提とする。
・ クラウドサービスの詳細は「6-1 クラウドサービスに関する事項」を参照すること。
・ 7,500 人以上の職員が利用できること。

(2) 情報セキュリティに関する事項

・ 「6-2 情報セキュリティに関する事項」を前提とした情報セキュリティ対策を実施すること。

(3) ソフトウェアに関する事項

・ 「6-4 ソフトウェアに関する事項」を前提としたソフトウェア構成とすること。

(4) 機器設置に関する事項

・ 機器を導入する場合は、「6-6　機器設置に関する前提条件」を参照し設置すること。

7-5. ストレージサービス

7-5-1. 機能要件

(1) 共通事項

・ 提案職員向けのファイルサーバ機能を提供すること。
・ 提案職員間または必要に応じて外部とのファイル交換・共有が可能であること。
・ Web ブラウザベースでファイルの保存が可能であること。
・ フォルダ・ファイルが業務端末のエクスプローラ上で表示できること。
・ ファイルのダウンロードを行わずにプレビューができること。
・ ドラッグ＆ドロップによるファイルのアップロードができること。
・ フォルダや複数ファイルを指定した一括アップロードができること。
・ ファイルを誤削除した場合等に備え、一定期間内であれば職員自身の操作によるファイル復元手段を有すること。
・ 以前（50 世代前）のファイルバージョンへ復元できること。
・ 業務端末及び個人端末を用いて、インターネット経由でアクセスできること。ただし、個人端末からアクセスする場合は、参照及び端末へのダウンロードを前提としない、ブラウザ上での編集作業等に制限を行うことも想定しているため、その設定については本県と協議のうえ決定すること。

- 名前・最終更新日等に基づきフォルダ・ファイルの並べ替えができること。
- フォルダ等へのリンク（URL）指定による共有が可能であること。
- フォルダ共有は同一フォルダ内においても職員単位で適切な権限を付与できること。
- ファイルのリアルタイムの共同編集ができること。
- Microsoft Office のファイルを Web ブラウザ上のエディタで開くとともに、編集ができること。なお、ファイルが編集可能な Web ブラウザは、クラウドサービス指定のブラウザで問題はない。
- アクセス権を持つフォルダ・ファイルに対して、フォルダ名・ファイル名・本文を対象に、キーワードを指定した全文検索ができること。また、AND 条件や OR 条件などの検索オプションの指定ができること。

(2) 管理事項

- 職員に対して個別のファイル格納領域を割り当て、利用できる機能を有すること。
- IDaaS 等との連携によるシングルサインオン認証機能を有すること。
- IDaaS 等との連携によるアクセス制御ができること。
- フォルダ、ファイル単位にアクセス不可、閲覧のみ、編集可能などのアクセス権が設定できること。
- フォルダ／ファイルへのアクセス権限は、グループ単位又は職員単位で指定できること。なお、アクセス権限は、「ファイルのアップロード」「ファイルのダウンロード」「プレビュー」「編集」「削除」など詳細な設定ができること。
- フォルダのアクセス制御を行い、職員によるフォルダ構成の変更や削除・移動ができない設定とすること。ただし、職員にて作成したサブフォルダを除く。
- 作成・編集を行ったユーザ情報が記録されること。
- 提案部局や所属に対してファイルの保存領域を確保し、アクセス制御を行うことにより、部局や所属単位でのファイル共有を可能とすること。
- インターネット経由で外部とのファイル交換･共有を行う機能を有すること。なお、外部共有を防止する機能を有すること。
- 個人端末から利用する場合、データのダウンロードやアップロードの制御が可能であること。
- 職員の登録／削除、パスワードのパラメータ設定、特定のフォルダへのアクセス権限の設定等が行えること。
- 利用者毎に利用可能な保存容量、フォルダ招待の制限などの設定ができること。
- 職員が削除された場合に管理者がフォルダ・ファイル等の所有権を別職員に割り当てることができること。
- 管理者によるフォルダやファイルに適用できるメタデータのテンプレートの作成及び利用者によるメタデータの作成ができ、このメタデータ情報に基づいた検索ができること。
- すべての職員のログを追跡し、レポートを作成できること。

- 職員別のアクセス数等の利用状況レポートを管理者が簡易な操作で作成し、CSV 形式等で出力できること。
- ユーザ操作の監査ログ（操作ログ）は自動で記録され、アカウント内すべての活動の監査証跡が残せること。クラウドサービスの監査ログ機能を利用する場合、証跡ログ内容を提案時に提示すること。
- 管理者がユーザのフォルダ・ファイルに対する監査ログ（操作ログ）を閲覧及びダウンロードできること。
- 監査ログ（操作ログ）のログファイルは CSV 形式で、日時、職員アカウント情報を含めること。

7-5-2. 非機能要件

(1) システム稼働環境

- 本機能は、クラウドサービスの利用を前提とする。
- クラウドサービスの詳細は「6-1 クラウドサービスに関する事項」を参照すること。
- 7,500 人以上の職員が利用できること。
- 部局・所属、または職員ごとに 1TB 以上のファイル格納領域を割り当てることが可能であること。
- 単一ファイルのアップロード容量上限が 10GB 以上であること。

(2) 情報セキュリティに関する事項

- 「6-2 情報セキュリティに関する事項」を前提とした情報セキュリティ対策を実施すること。

(3) ソフトウェアに関する事項

- 「6-4 ソフトウェアに関する事項」を前提としたソフトウェア構成とすること。

(4) 機器設置に関する事項

- 機器を導入する場合は、「6-6　機器設置に関する前提条件」を参照し設置すること。

7-6. 業務効率化ツール（ノーコード／ローコードツール）

7-6-1. 機能要件

(1) 基本事項

- 提案職員が、プログラミングのスキルをほぼ必要とせず、庁内の業務アプリケーションを容易に開発できる業務効率化ツール（ノーコード／ローコードツール）を導入すること。
- 一度開発したシステムは、OS やミドルウェア、ブラウザ等のバージョンアップに影響されないよう永続的に利用できること。

・ 提案開発したアプリケーションについては、職員間での業務利用のほか、県民・事業者等を利用対象とした公開機能を有すること。

(2) データベース機能

・ 導入するツールについては、固定のデータベースの保有は必須とせず、例えばエクセル等のデータソースを柔軟に選択できることも可とする。
・ データベースが固定されているツールについては、開発するシステムごとに、データベースの作成や設定、管理作業等を実施することが可能であること。
・ コンピュータ等の専門知識や技術がない利用者に対しても、簡易な操作でデータベースの作成・設定が可能であること。
・ システムに保管されたデータは再利用が可能であり、サインインを前提としたアプリケーションで機能の中で、CSV 等の汎用的なデータ形式で入出力できること。
・ 1 レコード（登録データ）に関連付けて、ファイルなどを登録・添付することが可能であること。もしくは該当データにクラウドストレージのリンク情報を記載することで、ファイルを紐づけて管理することができること。
・ データの項目ごとに「必須項目」や「規定値」等の設定が可能であること。

(3) システム画面作成・管理機能

・ 本ツール上から、マウス等による簡単な操作で画面作成や画面レイアウトの設定・変更、項目配置等が可能であること。
・ 利用する業務システムごとに、状況に応じて異なる画面を設定可能であること。
・ 蓄積されている情報を簡単に検索できる機能を有すること。

(4) モバイル化支援機能

・ 本ツール上から、必要に応じて業務システムをモバイル化するための設定が可能であること。
・ 利用する業務システムごとに、状況に応じてモバイル化の設定が可能であること。
・ Apple iOS 及び Google Android OS 端末に専用のモバイルアプリケーションが提供されていること。

(5) データ集計・分析機能

・ 提案蓄積されたデータを複数のグラフとして表示または可視化する機能を有すること。
・ 可視化する際には、データのグループ化、絞り込み、集計が可能であること。

7-6-2. 非機能要件

(1)　システム稼働環境

・ 本機能は、クラウドサービスの利用を前提とする。
・ クラウドサービスの詳細は「6-1 クラウドサービスに関する事項」を参照すること。
・ 提案利用者の区分や要件は以下のとおりとする。

利用者	内容	要件
職員等	開発、登録、更新、メンテナンス等のシステム管理権限	500 以上
県民	閲覧・起票権限（外部公開）	10,000 以上

(2)　情報セキュリティに関する事項

・ 「6-2 情報セキュリティに関する事項」を前提とした情報セキュリティ対策を実施すること。

(3)　ソフトウェアに関する事項

・ 「6-4 ソフトウェアに関する事項」を前提としたソフトウェア構成とすること。

(4)　機器設置に関する事項

・ 機器を導入する場合は、「6-6　機器設置に関する前提条件」を参照し設置すること。

8. 構成要素の仕様（データ活用基盤）

8-1. 目的・構成

8-1-1. 目的

産業界において、サービス提供を通じて収集したデジタルデータの活用を競争力の源泉とする動きが活性化する中、行政においても、さまざまな課題の解決に向けて先進的なデータ活用事例が登場するなど、今後、データが重要な財となっていくことに異論の余地はない。

現在、政府において、データに関する各種戦略が定められるとともに、ベース・レジストリの整備に向けた検討が進められている中、本県においても、多様なデータから住民等のニーズや本県が抱える課題を的確かつ迅速に把握し、データを活用した合理的な判断と政策立案（EBPM）を推進できる仕組みを整備することが極めて重要となる。

本業務においてこうした仕組みを確立していくため、様々な課題解決に必要となるデータの範囲や収集・分析方法等を明確にするデータ活用方針を策定するとともに、データの収集・蓄積・加工・分析や、ダッシュボード・データカタログ等の技術導入を通じた可視化が可能となるデータ活用基盤の整備に取り組む。

さらに、データ活用方針の策定やデータ活用基盤の構築・運用に取り組む中で、県保有データの活用に留まらず、市町や企業等が保有する外部データと連携した、分野間・地域間のデータ流通による、地域課題の解決や新たなサービスの創出など、地域の活性化につながる取組の展開をめざす。

8-1-2. 構成

名称	機能	主なユーザ
データ活用基盤	・ データの「収集・蓄積・加工・分析」を一貫して実施できる基盤。 ・ ETL 方式（各システムからデータの抽出・変換・書き出し）や DWH（ETL の抽出データ保管）、BI ツール等で構成される。	県職員 市町職員
ダッシュボード	・ オープンデータのほか、本業務において設定する課題テーマ単位に、関連するデータを一目で理解できるよう可視化し、利用者に提供する。 ・ （例）地図情報を含むデータを地図上で可視化する機能。	住民・企業等
データカタログ	・ オープンデータなど、利用者がデータ資産を適切に活用できるように統制･管理するとともに、データの発生元やデータの定義、導出方法など品質やメタ情報を整備する。	住民・企業等

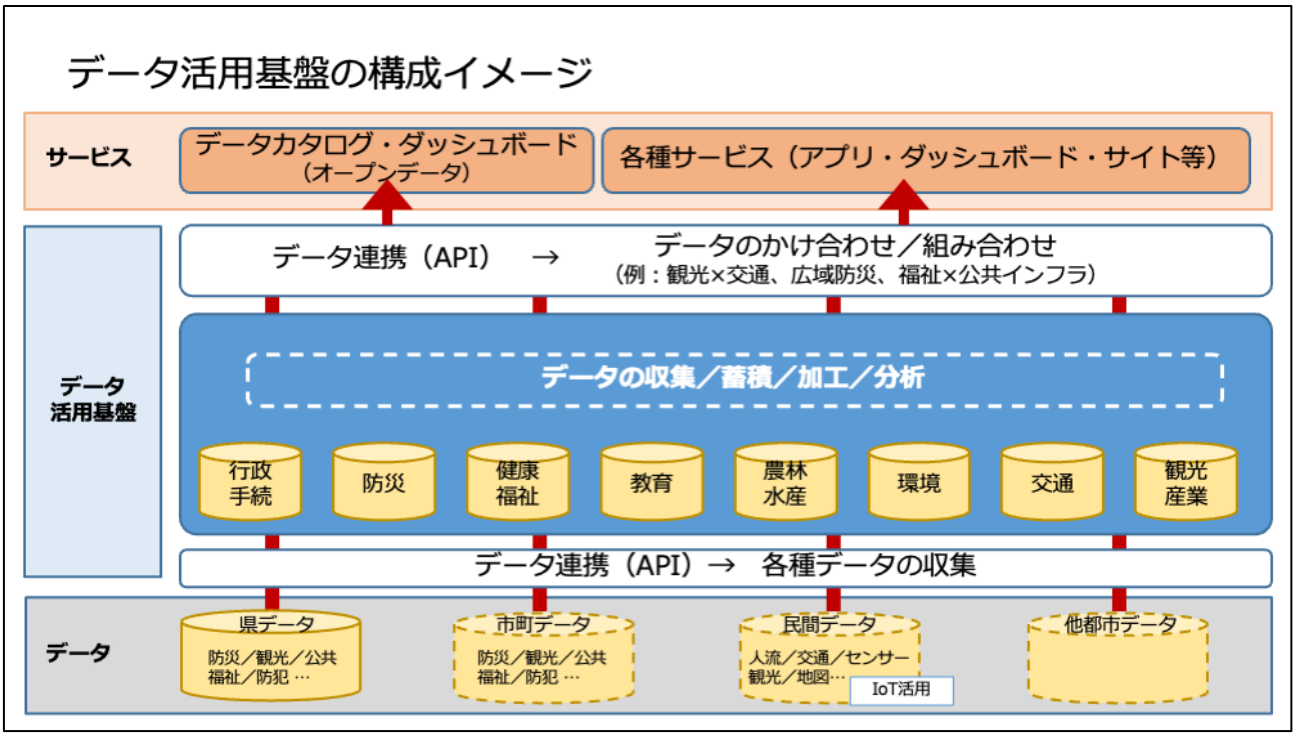
8-1-3. システムの構成に関する全体の方針

システムの構成に関する全体の方針については、以下のとおりである。

No	分類	方針
1	システムアーキテクチャ	本情報システムのシステムアーキテクチャは、前提事項である外部サービス利用型とする
2	アプリケーションプログラムの設計方針	本情報システムを構成する各コンポーネント（特定単位の機能）間は疎結合、再利用性を考慮した設計とすること
3	ソフトウェア製品の活用方針	広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する
4	データ活用基盤の方針	提案するクラウド環境が提供するサービス、機能を可能な限り活用し、可用性に優れたシステム構成とする

8-2. 概略図

データ活用基盤の概略図を以下に示す。



これは、あくまでも現時点において県が想定する概略図である。

本仕様書に記載する要件を全て満たすことは前提条件となるが、ベース・レジストリなどデータ活用に対して国が示す方針への対応や、将来的な他団体との連携を見据え、最適な構成・機能を提案・設計・構築するとともに、効果的・効率的な運用を行うこと。

8-3. 作業方針及びスケジュール

本項目で示す要件については、全て提案とする。

8-3-1. 作業方針

(1) データの「収集・蓄積・加工・分析」を一貫して行うクラウド基盤と BI ツール、さらに、データ活用方針に基づき、課題テーマ単位で必要となるデータの収集等を行い、API・データカタログ・ダッシュボード等の開発を行う。

(2) データ活用基盤の構築・運用にあたっては、本県保有データの調査やヒアリング等を通じて現状と課題を把握し、オープンデータの充実や課題への対応等をデータ活用方針として策定し、本方針に基づきデータ活用を推進していく。

(3) データ活用の検討・実践については、課題テーマごとに柔軟な対応が求められることから、アジャイル型の開発方針をベースとして作業を行うことを想定している。

(4) データ活用基盤は、内閣府「戦略的イノベーション創造プログラム（SIP）第２期／ビッグデータ・AI を活用したサイバー空間基盤技術におけるアーキテクチャ構築及び実証研究事業」による「スマートシティリファレンスアーキテクチャ・ホワイトペーパー」（以下、「ホワイトペーパー」という。）に準拠した構成とする。

(5) 作業の概要は「8-4 作業の概要」のとおりとし、受託事業者は、アジャイル開発を含め、より効果的な手法を提案し、柔軟かつ効果的なデータ活用基盤の運用を実現する。

(6) データ活用基盤の整備にあたっては、「4. プロジェクト管理」「5. 設計・構築等要件」を参照する。

8-3-2. スケジュール

データ活用基盤に係る作業スケジュールを以下に示す。

スケジュール（データ活用基盤）

8-4. 作業の概要

本項目で示す要件については、全て**提案**とする。

8-4-1. データの調査及びデータ活用方針の策定・運用

(1) 本県保有データの調査（令和 4 年度）

- オープンデータの提供を含めて、データ活用基盤で収集するデータを把握するため、本県と連携して、本県所有データの悉皆調査を実施する。
- なお、本調査は、受託事業者が決定するまでに本県により先行実施する想定であり、受託事業者は一次収集された結果をもとにオープンデータの整備と課題テーマの設定に向けた助言・支援等を行うこと。

(2) 課題テーマの設定（令和 4 年度）

- 本県保有データの悉皆調査と合わせて、担当部局（所属）へのヒアリングを行い、事業等のニーズや課題について把握する。
- ヒアリングにより把握した事業等のニーズや課題に対して、データを有効活用することで解決につながる可能性が高いと判断できる事業等については、優先度やデータの収集・入手、分析・可視化の手法等の検討を行い、各年度において対応する課題テーマとして設定する。
- 課題テーマについては、令和 5 年度から令和 9 年度において、毎年度 3 テーマ程度を新規設定する（最終目標 15 テーマ程度）。

(3) データ活用方針の策定（令和 4 年度）

- 受託事業者は、本県保有データの調査や課題テーマの設定を行うとともに、オープンデータの充実や課題テーマの解決に取り組むためのデータ活用方針を策定する。
- データ活用方針は、本業務の期間（令和 4 年度～令和 9 年度）を対象とした中期的計画とする。

(4) データ活用方針の実行・修正等（令和 5 年度～令和 9 年度）

- データ活用方針の実行にあたっては、データ活用基盤の構築・運用、さらにはオープンデータや課題テーマへの対応等について適切な進捗管理を行う。
- 社会情勢の変化等、様々な要因により、当初計画で設定した課題テーマの見直しが必要となった際には、都度ヒアリングを行い、連携するデータの収集・入手、分析・可視化の手法等について柔軟に見直しを行う。

8-4-2. データ活用基盤の構築及び運用

(1) データ活用基盤の構築（令和 4 年度）

- データ活用方針に基づき、必要なデータの収集・蓄積・加工・分析を行い、その結果を可視化できるデータ活用基盤一式を設計・構築する。
- 本県の保有データに留まらず、将来的な市町・企業等の保有データとの連携を見据えた、分野・地域間連携を可能とするデータ活用基盤を構築する。
- データ活用基盤の各種機能の要件については、「8-5 データ活用基盤の要件」を参照する。

(2) データ活用基盤の運用（令和 5 年度～令和 9 年度）

- データ活用基盤の構築作業及び機能・性能の検証を完了した後、令和 5 年度からデータ活用基盤の運用を開始する。
- 令和 4 年度に実施する、県保有データの調査及び課題テーマの設定に基づき、オープンデータのデータカタログや、課題テーマに応じたダッシュボード等によるデータの可視化等を行っていくための運用を行う。
- データ活用基盤については、令和 5 年度から令和 7 年度の 3 年間を実証運用期間とし、課題テーマにおける様々なレベルでの試行運用を行い、令和 8 年度から本格運用を行う想定とする。
- ただし、検証により実効性が確認できたものものについては、実証運用期間内であっても、先行して本格運用を行うことで差し支えない。

8-4-3. オープンデータのデータカタログ・ダッシュボードの構築及び運用

(1) 構築（令和 4～5 年度）

- 令和 4 年度に実施した県保有データの調査結果に基づき、オープンデータのデータカタログを構築する。なお、オープンデータの構築にあたっての要件は「8-5 データ活用基盤の要件」を参照する。
- オープンデータの公開については、公式サイト内に公開している現行から、分野横断的な検索機能等を有するデータカタログに移行する。
  現行（三重県オープンデータライブラリ）：
  https://www.pref.mie.lg.jp/it/hp/87579000001.htm
- 県保有データの調査結果等に基づき、民間での有効活用が見込まれるオープンデータの収集・公開方法について、本県への助言・支援を行う。
- オープンデータのデータカタログのうち、必要なデータについてはダッシュボードを通じて情報を提供するなど、積極的な可視化に取り組む。
- データカタログ・ダッシュボードの構築にあたっては、オープンソース等を使用することも差し支えない。
- データカタログの公開にあたり、情報セキュリティや個人情報保護等の取り扱いに関するガイドラインの作成及び支援を行うこと。

(2) 運用（構築後～令和 9 年度）

- データカタログ等の構築後、令和 9 年度まで運用を行うこと。
- 本県が指定するデータ及びカタログ情報（以下、「メタデータ」という。）等を、データカタログに搭載するための技術的な支援を行う。
- 本県職員がデータカタログの管理にあたり使用する操作マニュアルを作成・管理すること。

8-4-4. 課題テーマに基づく API・ダッシュボード等の開発及び運用

(1) API・ダッシュボード等の開発（令和 5 年度～令和 9 年度）

- 課題テーマに合わせて、データを活用するための仕組みとして API・ダッシュボード等を開発・公開すること。なお、API・ダッシュボード等の開発にあたっての要件は「8-5 データ活用基盤の要件」を参照する。

(2) 技術的な支援の実施（令和 5 年度～令和 9 年度）

- 課題テーマに関するデータの提供者に対して、データの整形等に関する技術的な支援・助言を行う。
- 課題テーマに関するデータの提供者に対して、データ活用基盤の各機能の説明を行うとともに、操作に関する研修を行う。
- データ活用基盤の事例の紹介など、データ活用に関する情報提供を行う。

8-5. データ活用基盤の要件

本項目で示す要件については、全て**提案**とする。

8-5-1. 機能要件

(1) ホワイトペーパーへの準拠

ホワイトペーパーに記載されている、都市 OS（本業務におけるデータ活用基盤に相当）に関する次の要件(相互運用、データ流通、拡張容易)を満たす構成とする。

要件	概要
相互運用 （つながる）	都市 OS が提供する API やデータが、同一形式あるいは機械的な変換により、各種スマートシティサービスや他都市 OS との連携を実現する仕組み。
データ流通 （ながれる）	地域内外の異種データの流通を実現するための機能（ブローカー）として、「①多種多様なデータの取り扱い」「②都市 OS 内外のデータを仲介」する仕組み。

要件	概要
拡張容易 （つづけられる）	地域が解決する課題や、めざすべき将来像に応じて、機能追加や更新を継続的に行える必要があり、ビルディングブロック方式のような機能の組み換えを柔軟に行える仕組み。

国内外のスマートシティの考え方や都市 OS の特徴をふまえ、ホワイトペーパーに提示されている、次の各要素を満たす構成とすること。

構成要素	概要
サービス連携	サービス(アプリ等)や他都市 OS との連携を実現する機能群 データ利用を容易にする等の API 群と API の公開可否制御などの API 管理、分野を問わない共通的なサービス（住民ポータル等）により連携を実現
認証	利用者のユーザ利用権限やサービス利用範疇等を管理する機能群 ユーザの ID、属性、パスワード等を一元管理し、また、各利用者のデータ利用範囲やサービス利用範囲等を一元管理することによって安全で使い勝手の良いサービス利用を実現
サービス マネジメント	サービス(アプリ等)の管理機能を提供する機能群 サービス(アプリ等)の登録､公開等の管理やサービス利用履歴の管理を実施
データ マネジメント	データの保存、蓄積及び、効率的にデータ利用するための機能群 多種多様なデータを管理し、サービス(アプリ等)から画一的、効率的なデータ利用を実現
アセット マネジメント	IoT や行政システム等からのデータ取得を管理する機能群 データの取得元の情報（認証情報等）や状態（接続状況等）を管理し、データ収集を実現
外部データ 連携	IoT や行政システム等とのデータ連携を実現する機能群 データの取得元、連携先とのシステム的な差異（データモデルやプロトコル等）を変換等で吸収し、データ連携を実現
セキュリティ	都市 OS の外部/内部の脅威から防御するための機能群 認証、暗号化、不正アクセス防止、不正アクセス検知・遮断技術等により安全に都市 OS が稼働できることを実現
運用	都市 OS の正常稼働や拡張のための機能を提供する機能群 都市 OS の正常稼働の監視や拡張を踏まえた構成管理により、都市 OS の維持、発展を実現

(2)　データ活用基盤の搭載機能

データ活用基盤に搭載する機能については、以下のとおりとする。

なお、以下の機能を満たした上で、バイナリデータストレージ(画像・動画などのバイナリーデータ、口コミ情報などの非構造化データを蓄積して管理するストレージ)などのより高度な分析を可能とする環境の整備について提案を行うこと。

構成要素	機能	概要
サービス連携	ダッシュボード(地図等)	・蓄積データの可視化 ・地理情報を含むデータを地図上で可視化
	API 公開（管理）	・データを API として提供する機能 ・公開した API の管理
認証	認証・認可 ユーザ管理	・API へのアクセス権限を制御する機能、API キー、認証・認可 ・管理画面へのアクセス権限制御などのユーザ管理機能
サービスマネジメント	サービス管理	・API を利用するサービスの管理機能 ・API の利用状況を蓄積・参照できる機能
データマネジメント	データ管理	・データの参照・更新履歴を蓄積・参照できる機能
	データ公開	・データを一覧化し、利用方法を公開するデータカタログサイト
	データ仲介	・外部システム等からデータを取得し、API 等を通じてサービスや他データ活用基盤へ提供する機能
	データ分析	・データの収集・分析・可視化を行い、業務や経営の意思決定に活用する仕組み（BI ツール）
	データストレージ	・データを蓄積し、分析ツール等へのインターフェースを提供する機能
アセットマネジメント	―	・センサーやスマートメーター等 IoT などのデータを収集する機能
外部データ連携	―	・標準的な API をはじめ、様々なインターフェースに対応可能な、外部システム等との接続機能
セキュリティ	―	・システムの脆弱性対応、ロギング、アクセス制

構成要素	機能	概要
		御など
運用	―	・バックアップ、障害対応、パフォーマンス管理、監視など

(3) オープンデータのデータカタログ・ダッシュボードの機能要件

オープンデータのデータカタログ・ダッシュボードに搭載する機能については、以下のとおりとする。

構成要素	機能	概要
全般	カタログ要件	・蓄積した様々なデータを可視化・管理するための機能 ・ユーザビリティ／アクセシビリティの確保（デザインは本県と協議を行い決定する） ・地理情報を含んだデータを地図上で可視化する機能 ・検索機能の充実
	構成	・以下コンテンツを想定（詳細は本県と協議を行い決定する） 最新情報／オープンデータの説明／データカタログ／検索／活用事例紹介／要望の受付／閲覧ランキング／FAQ／利用規約・利用方法　など
	ログ取得	・アプリケーションログの記録
	ドメイン	・本県のオープンデータカタログであることが判別できるドメインの設定（詳細は本県と協議を行い決定すること） ・ドメインは使用しなくなった際、速やかに停止できること
利用者画面	新着情報	・新規データセット公開や更新作業と連動して内容を自動通知する機能
	検索機能	・キーワードのほか、タグ、組織など複数の検索機能を有する
ダッシュ	グラフ	・数値等を基としたデータのグラフ表示機能

構成要素	機能	概要
ボード機能	地図	・ 座標値等を基としたデータの地図表示機能
	印刷	・ 表示状況の印刷機能（プレビュー機能あり）
管理用	管理機能	・ 利用者登録（変更・削除）機能 ・ ログイン認証（ID・パスワード等）機能 ・ アクセスログの確認・取得・保存機能 ・ 利用者単位の管理権限設定機能 ・ 新規ページ作成（編集・削除）機能
	カタログ機能	・ データセットの登録（編集・削除）機能 ・ データセットの公開（非公開）機能 ・ 一括登録（編集・削除）機能 ・ データセットの組織・グループ・タグ設定 ・ メタデータの登録（編集・削除）機能 ・ 複数データ形式の登録（削除）機能 CSV／XLS／XLSX／PDF／XML／HTML／JPG／RDF 等 ・ Shape／GeoJSON 等のデータ登録（削除） ・ データサイズの上限設定機能 ・ データのダウンロード数の集計機能 ・ データの閲覧数の集計機能 ・ データの CSV 等での一括出力機能 ・ 登録データのセット／ファイル数の集計機能

8-5-2. 非機能要件

(1) API 等開発

- 課題テーマに合わせて、データを連携するための仕組みとして API を開発・公開するとともに、連携結果についてはダッシュボードで公開する。
- 連携結果のうち、必要なデータについてはデータカタログでも公開する。
- 本県保有データに留まらず、市町及び企業等の保有データとの連携が必要である場合、データ提供者と協力し、データ連携のための効果的な仕組みを実装する。
- テーマ設定に関するデータの提供者に対し、データの標準化等に関する技術的な指導等を行う。
- データ活用基盤の各機能の説明を行うとともに、操作に関する講習を行う。
- データ活用基盤の事例の紹介など、データ利活用に関する情報提供を行う。

(2) 開発イメージ（想定）

課題テーマは、本業務の調達後に実施するニーズ調査等の結果に基づき設定することと

なるため、現段階では開発イメージを提示することができない。

ただし、今後、本県が取り組むデータ活用のイメージは、先進事例とされる香川県高松市の「スマートシティたかまつ」プロジェクト（平成 29 年度から実施）の取組と近い内容を想定しているため、当該プロジェクトの内容を参照すること。

「スマートシティたかまつ」
https://www.city.takamatsu.kagawa.jp/kurashi/shinotorikumi/machidukuri/smartcity/index.html

分野	項目	概要
防災	IoT を活用したリアルタイムの情報収集	水位や避難所安全情報などをセンサーで取得し、早期に安全対策を実施。 （河川・護岸の水位） ・ 水位センサー・潮位センサー（13 拠点） （避難所の情報） ・ スマートメーター（30 拠点） ・ スマートフォンアプリ （データの可視化） ・ ダッシュボード
観光	GPS を活用したログデータの情報収集	レンタサイクル（50 台）の利用動態から特に外国人観光客の動態を分析し、観光・MICE の進行に向けた施策を展開する。 （GPS ロガーによるデータ蓄積） ・ 起終点（座標データ） ・ 利用経路・行動範囲（座標データ） ・ 移動時間・滞在時間（ログの取得時刻） （利用者データ） ・ 利用者（年代、国籍、利用目的等）

(3) 実証期間（令和 5 年度～令和 7 年度）

- データ活用基盤は、令和 8 年度からの本格運用を見据えて、令和 5 年度から令和 7 年度までの 3 年間を実証期間とする。
- データ活用基盤及び開発物の動作障害等を定期的に確認し、発生時は対応すること。
- 構成機器のリソース状況を定期的に確認し、性能改善につながるような調整や設定変更の対応を実施すること。
- データ活用基盤を構成する API 等のプログラムソースや設定ファイルのバックアップを取得し、世代管理を行うこと。
- ハードウェア、ソフトウェアの修正プログラムやバージョンアッププログラムは、評価したうえで随時適用すること。

・ データ活用基盤に関係する構成等の変更が発生した場合は、関係資料の修正を実施し、提出分は既存資料の差し替えを行うこと。
・ 実証結果の評価を行うこと。

(4) データ活用基盤のサービス利用要件（想定）

サービス	内容	目標
サービス提供時間	・ 利用者がサービスを利用できる時間（メンテナンス等の計画停止やネットワーク障害等の他の要因による停止時間を除く）	24 時間 365 日
利用者数	・ ID 管理機能に登録可能なアカウント数	500 以上
データ量	・ 蓄積可能なデータ量	10TB 以上

(5) システム稼働環境

・ 本機能は、クラウドサービスの利用を前提とする。
・ クラウドサービスの詳細は「6-1 クラウドサービスに関する事項」を参照すること。

(6) 情報セキュリティに関する事項

・ 「6-2 情報セキュリティに関する事項」を前提とした情報セキュリティ対策を実施すること。

(7) ソフトウェアに関する事項

・ 「6-4 ソフトウェアに関する事項」を前提としたソフトウェア構成とすること。

(8) 機器設置に関する事項

・ 機器を導入する場合は、「6-6　機器設置に関する前提条件」を参照し設置すること。

9. 構成要素の仕様（情報セキュリティ基盤）

9-1. 目的

DX 推進基盤では、場所や時間、端末等の制約を受けない業務環境の実現に向けて、クラウドサービスを活用するとともに、新たなテレワーク環境を整備する。

クラウドサービスの活用及び業務端末の持ち出しにより、現在のデータセンターを中心とした境界内（三重県行政 WAN）は安全とする考え方（境界型防御）から端末単体やユーザが信用できない前提として、暗号化や情報資産保護等のセキュリティ対策を徹底する「ゼロトラストセキュリティ」へ転換させていく必要がある。

さらに、庁外への業務端末の持ち出しは、インターネット接続によるマルウェア感染や業務端末の紛失よるデータ漏えい、ID 及びパスワードの漏えいによる不正ログオン等、様々な脅威にさらされる可能性があり、これらを防ぐ強固な業務端末のセキュリティ対策が必要となる。

一方、現在のテレワーク環境においては、三重県行政 WAN 上に VPN の接続口を設置し、業務端末から接続する VPN で安全な通信を実現している。

しかし、VPN の接続口を持つ構成は、多数接続による帯域逼迫や、装置の欠陥を突いた不正アクセスによる情報流出が強く懸念され、VPN の接続口を持たない構成に加え、通信量に応じ柔軟に帯域を拡張できる仕組みが必要となる。

これらの課題を解決するため、情報セキュリティ基盤では、クラウドサービス上に実装された以下の機能を利用するとともに、多要素認証、データ暗号化をはじめとする端末セキュリティの強化を図ることで、安全なクラウドサービスの活用や、テレワーク環境を実現する。

(1) ゼロトラストセキュリティの考え方に基づく端末及びユーザ認証
(2) 通信経路の暗号化
(3) インターネットへの安全なアクセス
(4) シャドーIT の利用に係る脅威の可視化と評価
(5) 三重県行政 WAN 上の VPN 接続口を排したテレワーク環境の実現
(6) 通信監視による脅威の検出と緊急対応

9-2. クラウド・ネットワークセキュリティ

9-2-1. 機能要件

(1) 基本要件

- 提案 情報セキュリティ基盤をクラウドサービスとして提供し、業務端末から接続できること。ただし、要件を満たす限り、複数製品（サービス）の組み合わせによる実装も可とする。
- 想定 情報セキュリティ基盤を SASE（Secure Access Service Edge）として提供する。
- 提案 情報セキュリティ基盤の仕様に基づき、FW(新設)の機器選定をしたうえで、機器の導入及び必要な設定を行うこと。
- 提案 FW（新設）から情報セキュリティ基盤へ安全な接続が可能であること。

- 想定新 DK 端末の安全を確保したうえで三重県行政 WAN に接続するために必要となるテレワーク系（庁内）を新設し、FW（新設）に接続する。
- 想定業務端末から SASE へエージェントを通じた接続が可能であること。
- 想定エージェントは、Apple iOS 、Apple macOS、Google Android OS 、Microsoft Windows の最新版に対応していること。
- 想定エージェントの機能を無効化できないようにする機能を有すること。
- 提案新 DK 端末から情報セキュリティ基盤へ接続する際は、端末及びユーザのアイデンティティに係る認証が可能であること。具体的には、ユーザ ID 及びパスワードに加え、以下に示すいずれかの項目で認証が可能であること。

（ア）HIP（Host Information Profile）
（イ）証明書
（ウ）コンテキストアウェア

- 提案ユーザ ID 及びパスワード認証には、IDaaS または庁内のオンプレミス認証基盤を利用すること。ただし、必ず端末認証を併用できること。
- 想定ユーザ認証に係る通信を情報セキュリティ基盤経由とする場合は、該当の通信のみが行える情報セキュリティ基盤への VPN を事前に構成する。ただし、その場合も端末認証を行う。
- 想定テレワーク系（庁外）へ接続している時は、新 DK 端末へのログオン前に、証明書認証による SASE との VPN を構成し、そのトンネルによりオンプレミス認証基盤での認証を行う。認証成功時には全ての通信を許可する。
- 想定テレワーク系（庁内）へ接続している時は、新 DK 端末へのログオン前に、FW（新設）で証明書認証を行い、その後、オンプレミス認証基盤での認証を行う。認証成功時には全ての通信を許可する。
- 想定新 DK 端末にログオン後、SASE へのシングルサインオン接続を行う。
- マルウェア対策が可能であること。
- FWaaS により、新 DK 端末からインターネットへのアクセスを制御できること。
- 情報セキュリティ基盤を経由したインターネットアクセスについて、送信元 IP アドレスを特定レンジに固定できること。
- 提案通信回線や情報セキュリティ基盤に障害が発生しても、業務端末による業務の継続が可能であること。
- 想定障害発生の有無にかかわらず、テレワーク系（庁内）からインターネット系へ通信を迂回させることで新 DK 端末から業務システムへのアクセスが可能であること。
- 想定テレワーク系（庁内）に接続された新 DK 端末から、情報セキュリティ基盤を経由せずコミュニケーション基盤へアクセスできる暫定的な設定を行うこと。
- 想定テレワーク系（庁外）に接続された新 DK 端末から、情報セキュリティ基盤を経由せずコミュニケーション基盤へアクセスできる暫定的な設定を行うこと。
- 想定旧 DK 端末から、情報セキュリティ基盤を経由せずコミュニケーション基盤へアクセスできる暫定的な設定を行うこと。

(2) セキュアウェブゲートウェイ（SWG）

- 提案新 DK 端末からの Web アクセスに対して、ウイルス、マルウェア等の脅威検出ができること。
- カテゴリ分類によるコンテンツフィルタ機能を有すること。
- 独自のポリシーにより、Web アクセスの許可/不許可の設定が可能であること。
- 想定インターネット上の悪意のあるサイト又は過去に悪用されたドメインなどのリスクを判定し、実際に接続すること無しにブロックできること。

(3) クラウドアクセスセキュリティブローカー（CASB）

- 提案（可視化）クラウドサービス毎に、利用状況の可視化が可能であること。
- （脅威防御）ポリシーに基づき、許可されていないクラウドサービスへのアクセスを遮断できること。
- （脅威防御）クラウドサービスの利用に関し、特定のテナント ID だけアクセスできるよう制御が可能であること。

(4) ゼロトラストネットワークアクセス（ZTNA）

- 提案新 DK 端末から、情報セキュリティ基盤を経由して、三重県行政 WAN 内部の業務システムへ安全にアクセスできる機能を提供すること。
- 新 DK 端末から、許可された範囲の業務システムへのアクセスを制御する方式とすること。
- 業務システムへのアクセスは、リバース Proxy や専用コネクタ等を必要としない方式(新 DK 端末から業務システムへ IP によりアクセスする方式)も可能とすること。
- 提案新 DK 端末から、業務システムへのアクセスはシングルサインオンが可能であること。なお、業務システムへのシングルサインオンに係る方式は、Windows 統合認証、Kerberos 認証、NTLM 認証の全てに対応できること。
- 提案情報セキュリティ基盤に障害が発生しても、新 DK 端末による業務の継続が可能であること。
- 想定テレワーク系（庁内）からインターネット系へ通信を迂回させることで新 DK 端末による業務の継続が可能であること。

(5) セキュリティオペレーションセンター（SOC）

- 日本国内に SOC（Security Operation Center）を設置し、運用すること。
- SOC は 24 時間 365 日の有人運用とすること。
- SOC では、情報セキュリティ基盤から出力されるログ（FWaaS/SWG/ZTNA）について、分析を行うこと。
- ログ分析を通じて、情報セキュリティ基盤におけるセキュリティインシデント等を検知できること。

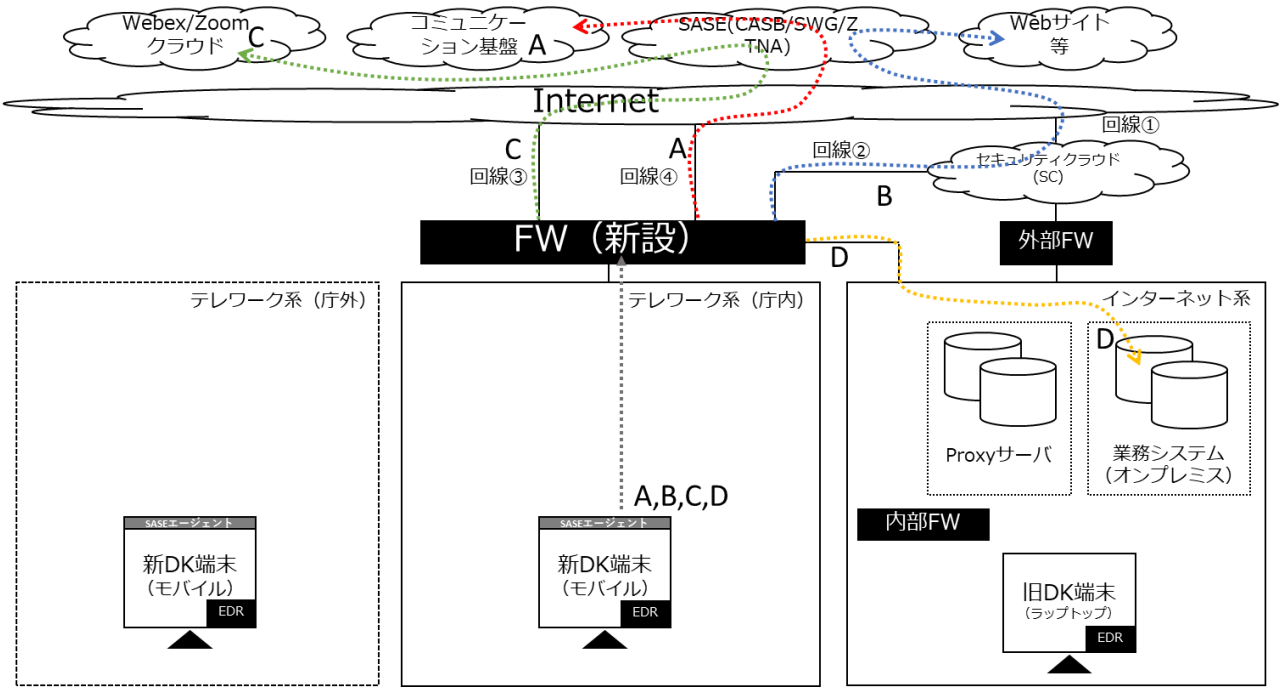
- 提案一定の危険度以上のインシデントについては、県担当者及び別途契約済みの SOC に電話等による緊急連絡を行うこと。
- 提案別途契約済みの SOC と連携し、県担当者の指示に基づく緊急対応を行うこと。

9-2-2. ネットワーク構成（例）

本項で示す項目については、全て想定とする。

通信ルート設計については、要件を満たす通信ルートを受託事業者が提案するものとし、アクセスルート（例）のとおり実現する必要はない。

（1） 新 DK 端末（庁内）からのアクセスルート（例）

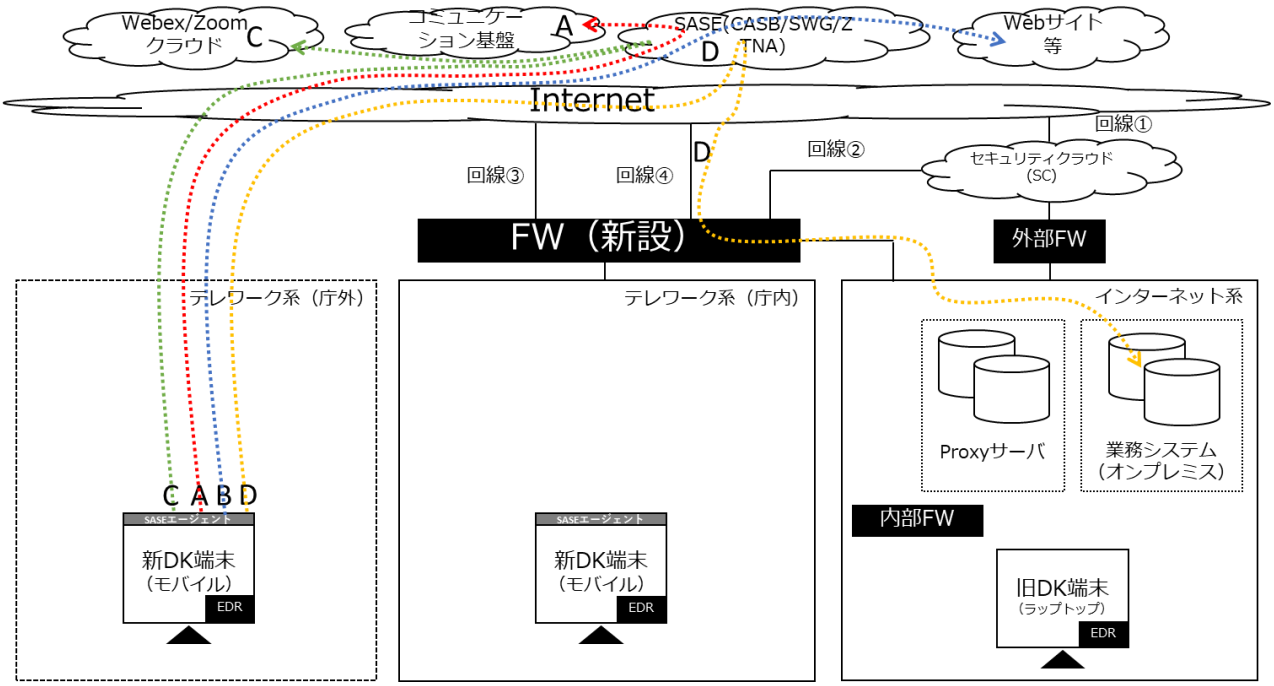


- ルート A は、コミュニケーション基盤へのアクセスルートを示す。
- ルート B は、インターネット上の Web サイトへのアクセスルートを示す。
- ルート C は、既存の Web 会議システム（Webex/Zoom）へのアクセスルートを示す。
- ルート D は、インターネット系の業務システムへのアクセスルートを示す。
- 回線①及び回線②は、調達済みのセキュリティクラウドのブレイクアウト回線（3Gbps/1Gbps 帯域保障）を指す。
- 回線③は、調達済みの Web 会議用インターネット回線（1Gbps ベストエフォート）を指す。
- 回線④は、調達済みのインターネット回線（1Gbps/200Mbps 帯域保障）を指す。
- 新 DK 端末が SASE と通信を行う際は、端末及びユーザのアイデンティティに係る認証を SASE または FW（新設）で行う。万一、SASE に障害が発生した場合は、FW（新設）で認証を行う。
- 新 DK 端末からの通信は、ルート A～C ともに SASE 経由とするが、SASE との VPN セッションは、FW（新設）から確立することで、新 DK 端末からの VPN セッション数を

低減させる。

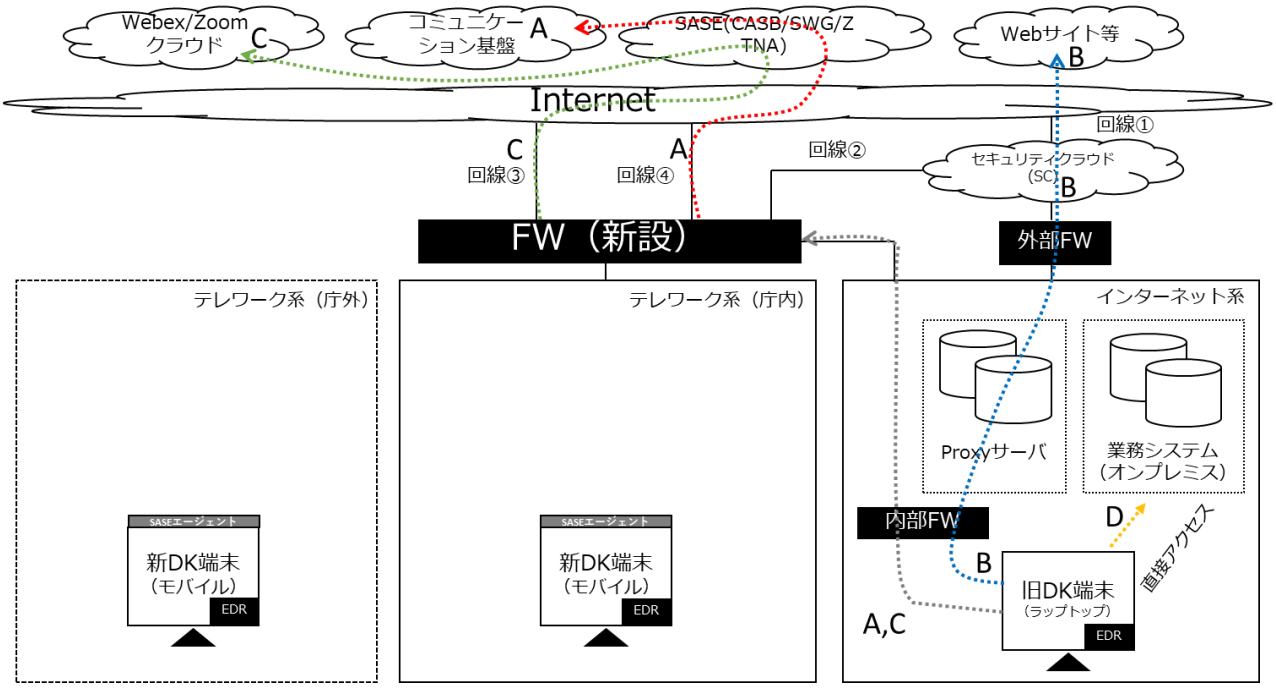
・ 新 DK 端末がテレワーク系（庁内）に接続されていることを検知し、ルート D の通信のみを FW（新設）でインターネット系へブレイクアウトさせる。

（2） 新 DK 端末（庁外）からのアクセスルート（例）



・ ルート A は、コミュニケーション基盤へのアクセスルートを示す。
・ ルート B は、インターネット上の Web サイトへのアクセスルートを示す。
・ ルート C は、既存の Web 会議システム（Webex/Zoom）へのアクセスルートを示す。
・ ルート D は、インターネット系の業務システムへのアクセスルートを示す。
・ 回線①及び回線②は、調達済みのセキュリティクラウドのブレイクアウト回線（3Gbps/1Gbps 帯域保障）を指す。
・ 回線③は、調達済みの Web 会議用インターネット回線（1Gbps ベストエフォート）を指す。
・ 回線④は、調達済みのインターネット回線（1Gbps/200Mbps 帯域保障）を指す。
・ テレワーク系（庁外）に接続された新 DK 端末からの通信は、ルート A～D ともに SASE 経由とし、SASE との VPN セッションは、新 DK 端末にインストールされたエージェントから確立する。なお、テレワーク系（庁外）に接続されているか、テレワーク系（庁内）に接続されているかは、エージェントにより自動判別される。
・ 新 DK 端末と SASE 間の通信を行う際は、端末及びユーザのアイデンティティに係る認証を SASE で行う。

（3） 旧 DK 端末からのアクセスルート（例）



- ルート A は、コミュニケーション基盤へのアクセスルートを示す。
- ルート B は、インターネット上の Web サイトへのアクセスルートを示す。
- ルート C は、既存の Web 会議システム（Webex/Zoom）へのアクセスルートを示す。
- ルート D は、インターネット系の業務システムへのアクセスルートを示す。
- 回線①及び回線②は、調達済みのセキュリティクラウドのブレイクアウト回線（3Gbps/1Gbps 帯域保障）を指す。
- 回線③は、調達済みの Web 会議用インターネット回線（1Gbps ベストエフォート）を指す。
- 回線④は、調達済みのインターネット回線（1Gbps/200Mbps 帯域保障）を指す。
- インターネット系に接続された旧 DK 端末からの通信は、ルート A 及び C は SASE 経由とし、ルート B はセキュリティクラウド経由、ルート D は直接アクセスとする。
- ただし、SASE がダウンした場合、ルート A 及びルート C はセキュリティクラウド経由とする。
- 旧 DK 端末から SASE へのアクセスは、FW（新設）から確立した VPN セッションを利用する。
- ルート A 及び C は、既設の内部 FW（Fortigate 600E）等によるアプリケーション／サービス識別ルーティングにより、通信の振り分けを行う。

9-2-3. 非機能要件

（1） 端末及び拠点数

- 情報セキュリティ基盤への接続端末数は 8,000 台（新 DK 端末及び旧 DK 端末等）とする。

・ 情報セキュリティ基盤への接続拠点は、1 拠点とするが、複数回線による接続が可能であること。

(2) 利用者数

・ 情報セキュリティ基盤の利用者は、7,500 人以上とする。

(3) 情報セキュリティに関する事項

・ 「6-2 情報セキュリティに関する事項」を前提とした情報セキュリティ対策を実施すること。

(4) ソフトウェアに関する事項

・ 「6-4 ソフトウェアに関する事項」を前提としたソフトウェア構成とすること。

(5) 拡張性

・ 提案 接続回線数や拠点数の増加、帯域増強に備え、柔軟な拡張性を有する構成とすること。
・ 想定 SD-WAN 技術を用いた複数回線の動的な切り替えや、拠点の接続等が可能であること。

(6) FW（新設）に関する非機能要件

・ 「(1) 端末及び拠点数」及び「(2) 利用者数」に示す要件に対応できる機種を導入すること。
・ 2 台以上の冗長構成とすること。

(7) 機器設置に関する事項

・ 機器を導入する場合は、「6-6　機器設置に関する前提条件」を参照し設置すること。

9-3. エンドポイントセキュリティ

9-3-1. 機能要件

(1) 端末ネットワーク

・ SplitTunnel で指定した通信を除き、新 DK 端末からの通信は、情報セキュリティ基盤または FW（新設）を通じた通信に限定できること。
・ 新 DK 端末から外部への通信について、一部の通信を SplitTunnel として許可できること。
・ 外部から新 DK 端末への通信を全て遮断すること。

(2) ログオン認証

- 提案新 DK 端末へのログオンは、ID 及びパスワードまたは PIN コードに加え、生体認証を行うなど、多要素認証とすること。
- 提案ログオン認証は、IDaaS または庁内のオンプレミス認証基盤を利用すること。
- 想定新 DK 端末へのログオンは、ブート時に Bitlocker の PIN コードを求めることに加え、ログオン画面で指紋認証を行う多要素認証とする。

(3) データセキュリティ

- 提案新 DK 端末に内蔵している全てのストレージについて、全体の暗号化を行うこと。なお、全ての新 DK 端末には TPM チップが内蔵されているものとする。
- 提案端末の暗号化に係る回復キーを管理者側で一元管理する方法を提供すること。
- 新 DK 端末に内蔵している全てのストレージについて、利用者による暗号化の解除ができないようにすること。
- ローカルドライブ上へのデータ保存も可能とすること。

(4) 端末管理

- 新 DK 端末の設定ポリシー（ストレージ暗号化の強制、パスワード強度の設定等）について、一元管理、適用が可能であること。
- 新 DK 端末について、セキュリティパッチの適用状況の把握、強制適用が可能であること。
- 提案新 DK 端末について、EPP の更新状況の把握が可能であること。
- 想定新 DK 端末について、EPP の強制更新が可能であること。
- 提案新 DK 端末について、管理者が設定したポリシー(パッチ適用状況、EPP 更新状況等)に違反した端末を情報セキュリティ基盤と連携し、接続を不可にできること。
- 想定ドライブ暗号化がなされていない端末の SASE 接続を不可にできること。
- 想定管理者が設定したポリシーにより SASE への接続を不可とする場合も、端末アップデート等の管理通信は可能とすること。
- 提案新 DK 端末について、脆弱性を抱える端末の特定と対処が可能であること。
- 新 DK 端末について、利用者からの紛失申告に基づき、データのリモートワイプができること。
- 新 DK 端末について、許可していないアプリがインストールされているかどうかをモニタリングする機能を有すること。
- 新 DK 端末について、USB メモリー等の利用を規制できること。
- Microsoft Windows 以外の OS（Apple iOS 、Apple macOS、Google Android OS）の管理に対応していること。
- 提案新 DK 端末について、簡便かつ効率的な管理ができる機能を有すること。
- 想定既存の統合管理システムと連携し、一つの管理画面で全ての端末(新 DK 端末、旧 DK 端末、BYOD 端末）の管理が行えること。

・ 想定端末に対してゼロタッチデプロイが可能であること。

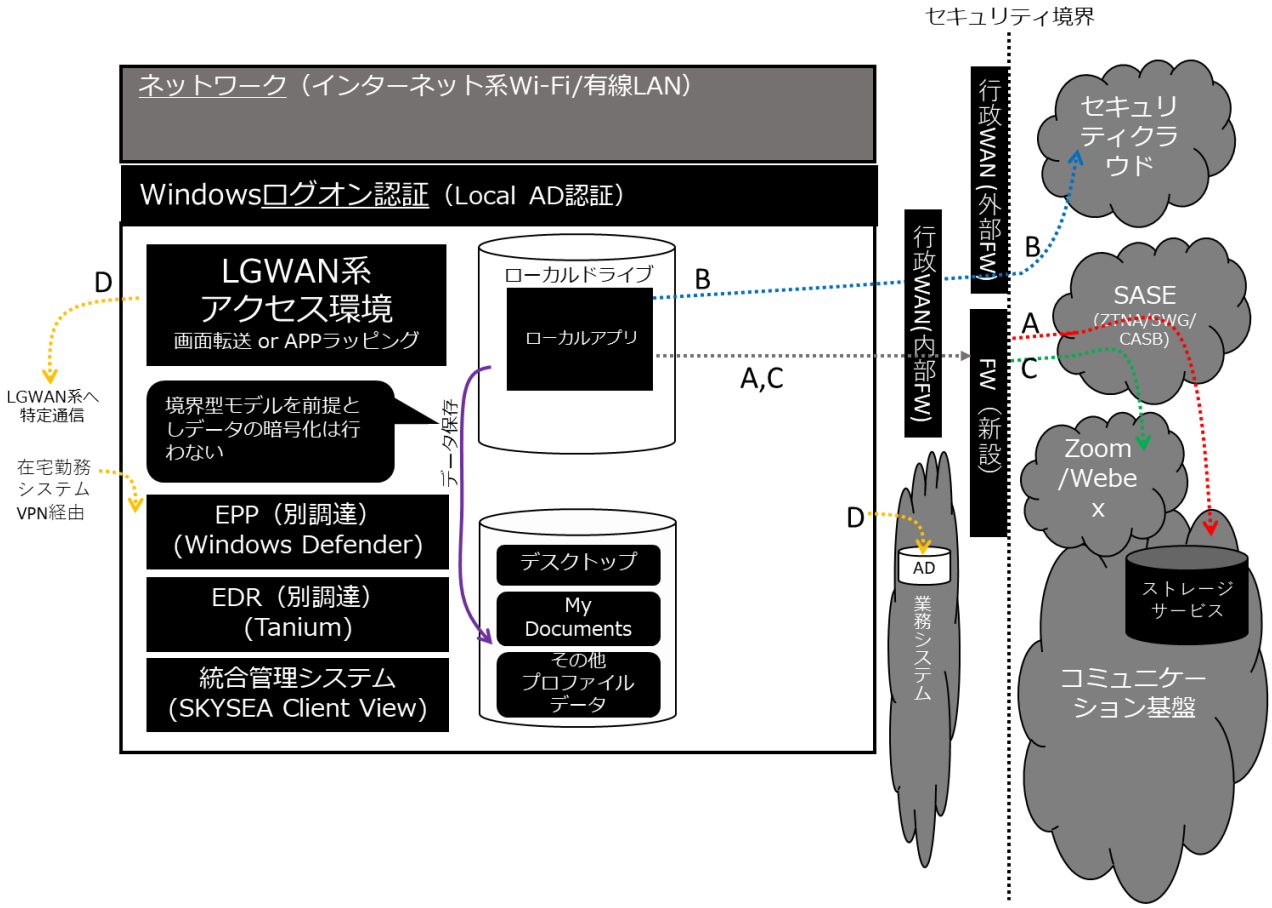
9-3-2. 端末構成

提案新 DK 端末及び旧 DK 端末「9-2 クラウド・ネットワークセキュリティ」、「9-3 エンドポイントセキュリティ」の要件をふまえた構成とすること。

なお、想定以下に本県が想定する新 DK 端末及び旧 DK 端末の構成例を示す。

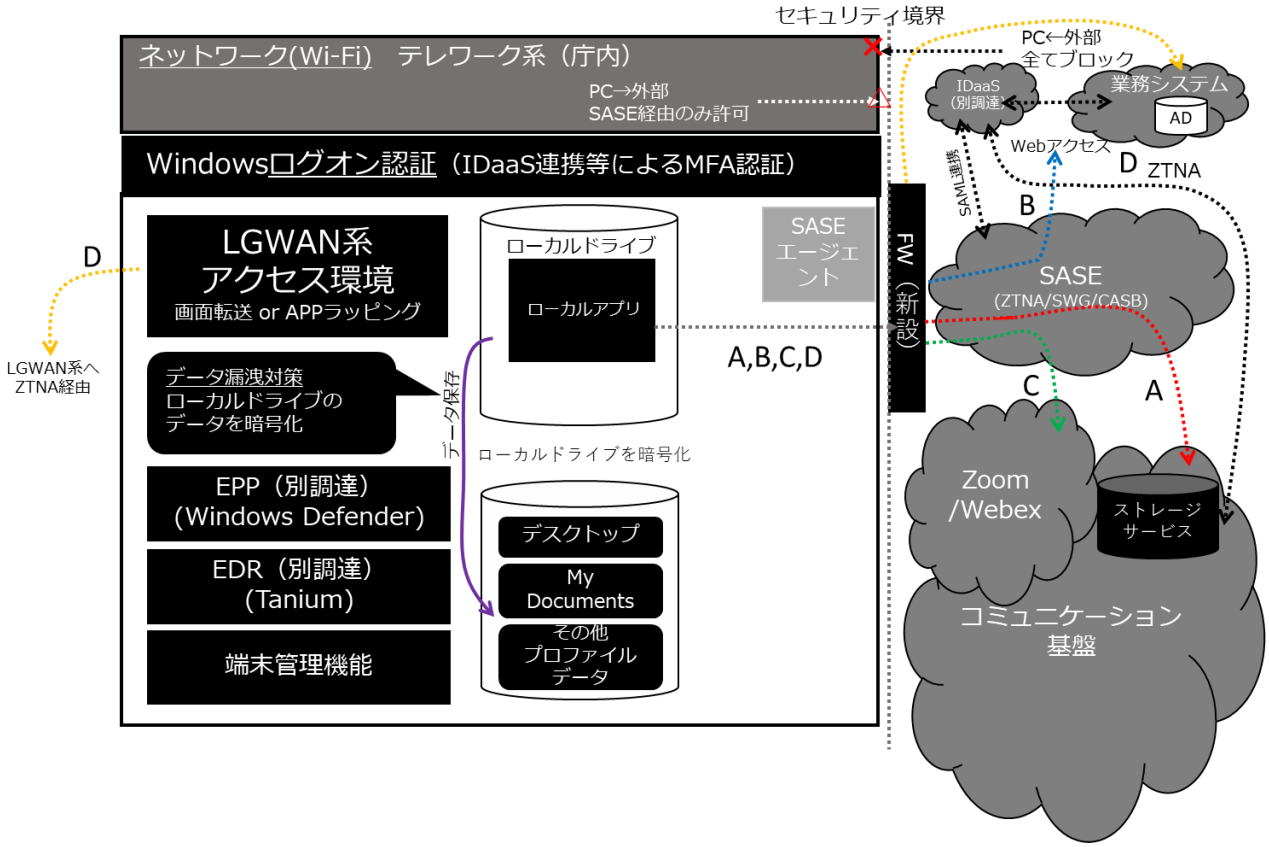
（1） 構成例（旧 DK 端末）

・ インターネット系に接続し、三重県行政 WAN の外部ファイアウォールまたは、テレワーク系（庁内）に新設したファイアウォールによる境界型防御モデルを採用する。
・ 庁外への持ち出しは不許可とし、ストレージの暗号化は行わない。
・ 庁内業務システムへの接続は、三重県行政 WAN 経由（ダイレクトアクセス）とする。
・ コミュニケーション基盤への接続は、全て SASE 経由とする。
・ コミュニケーション基盤以外の Web アクセスは、セキュリティクラウド経由とする。
・ EPP 及び EDR をインストールする。
・ LGWAN 系へのアクセスは、別途調達する LGWAN 系に接続された仮想端末基盤を利用する画面転送方式か、セキュアコンテナ方式によるものとする。
・ 以下に旧 DK 端末の構成例を示す。



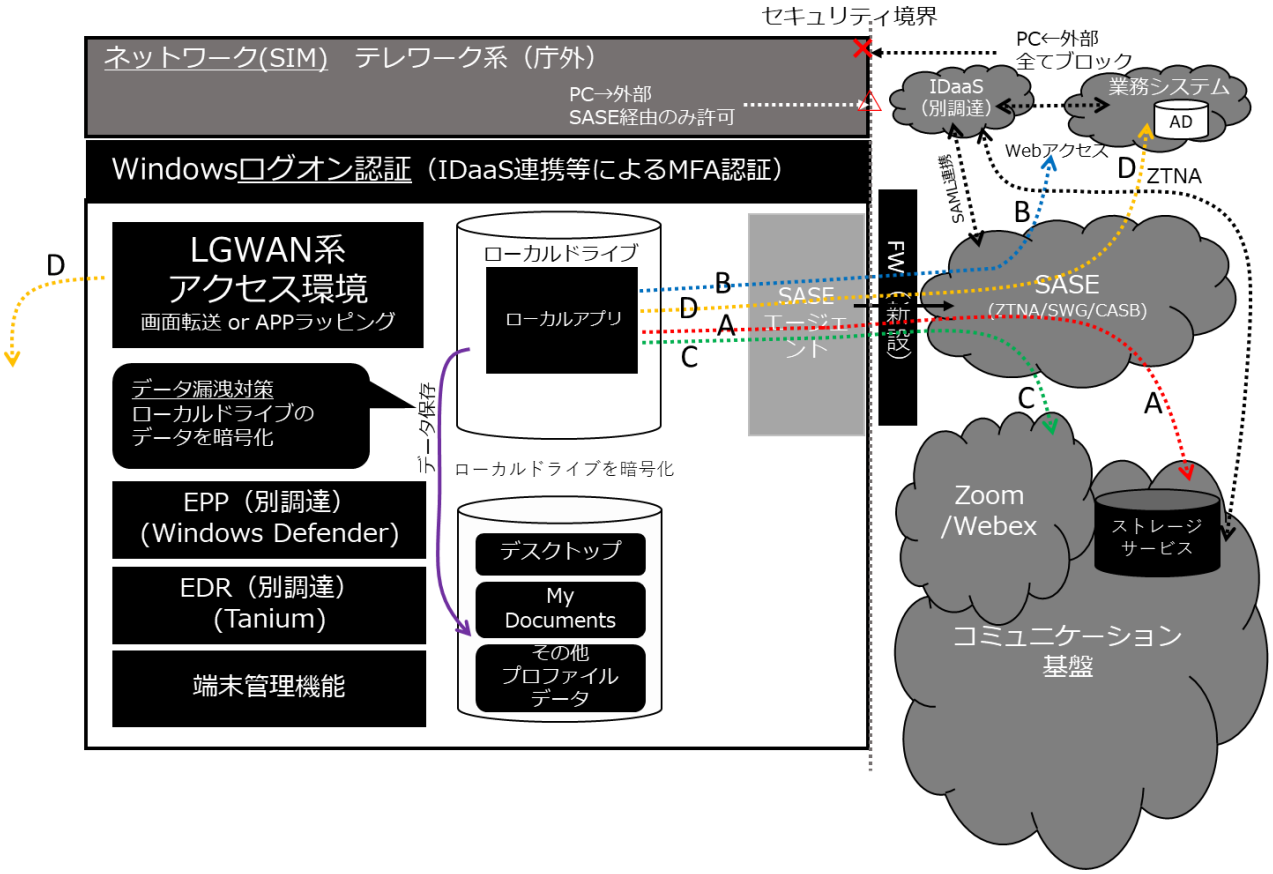
（2） 構成例（テレワーク系（庁内）に接続された新 DK 端末）

・ テレワーク系（庁内）の Wi-Fi に接続する。
・ 庁外への持ち出しを可能とし、ストレージの暗号化を行う。
・ 業務システムへの接続は、FW（新設）によるインターネット系へのブレイクアウト通信経由とする。
・ コミュニケーション基盤への接続は、全て SASE 経由とする。
・ コミュニケーション基盤以外の Web アクセスについて、SASE 経由とする。
・ EPP 及び EDR をインストールする。
・ LGWAN 系へのアクセスは、FW（新設）によるインターネット系へのブレイクアウト通信経由とし、別途調達する LGWAN 系に接続された仮想端末基盤を利用する画面転送方式か、セキュアコンテナ方式によるものとする。
・ 以下にテレワーク系（庁内）に接続された新 DK 端末の構成例を示す。



（3） 構成例（テレワーク系（庁外）に接続された新 DK 端末）

・ テレワーク系（庁外）に SIM 等で接続する。
・ 庁外への持ち出しを可能とし、ストレージの暗号化を行う。
・ 全ての通信を SASE 経由とする。
・ EPP 及び EDR をインストールする。
・ LGWAN 系へのアクセスは、SASE 経由とし、別途調達する LGWAN 系に接続された仮想端末基盤を利用する画面転送方式か、セキュアコンテナ方式によるものとする。
・ 以下にテレワーク系（庁外）に接続された新 DK 端末の構成例を示す。



9-3-3. 非機能要件

(1)　情報セキュリティに関する事項

・　「6-2 情報セキュリティに関する事項」を前提とした情報セキュリティ対策を実施すること。

(2)　ソフトウェアに関する事項

・　「6-4 ソフトウェアに関する事項」を前提としたソフトウェア構成とすること。

(3)　対象端末数

・　対象端末数は、8,000 台以上とする。

(4)　機器設置に関する事項

・　機器を導入する場合は、「6-6　機器設置に関する前提条件」を参照し設置すること。

10. 研修等支援業務

本業務で整備する各種ツール等については、職員が操作方法等を理解し、円滑に利用できるよう、研修やマニュアル等コンテンツの作成などの支援業務を行うこと。

その考え方は以下のとおりとするが、最適な実施方法等について提案を行うこと。

なお、データ活用基盤の運用に向けて必要となる研修については、「8 構成要素の仕様（データ活用基盤）」に記載する内容を参照すること。

10-1. 対象者別研修等

10-1-1. 対象者

- 一般職員（各種ツール等の利用者）
- 管理者（各種ツール等の管理者、ヘルプデスク担当事業者等）

10-1-2. 一般職員向け

(1) 提案運用期間中は、毎年度、一般職員向け研修を実施すること。

(2) 想定研修等の内容は、ユースケースなどの具体的な事例を用いて、ツールへの理解度向上及び利用促進につながる内容とすること。

(3) 想定研修を行う場合はオンライン開催を前提とし、ライブ方式や動画配信等のオンデマンド方式、またはこれら方式の組み合わせなど、より効果的な実施方法を提案すること。

(4) 職員が、本業務で整備する各種ツール等の利用を促進するため、研修やマニュアル等コンテンツの作成を行うこと。

(5) 現段階の想定として、令和 4 年度においては令和 4 年 12 月から令和 5 年 3 月にかけて職員が研修の受講（視聴）またはマニュアル等を確認できるよう環境を準備すること。なお、この時期については、DX 推進基盤の整備状況を踏まえ本県と協議を行うこと。

(6) ライブ方式で実施した研修内容は録画し、後日閲覧することについて、承諾すること。録画することを許容しない場合は、研修内容の動画をオンデマンドで見ることに対する手段を別途提供すること。

10-1-3. 管理者向け

(1) 対象職員及びヘルプデスク担当事業者等の約 20 人に対する研修をオンライン前提で実施することとし、時間は 1 回 3 時間程度を 2 回実施すること。

(2) DX 推進基盤で使用する各システムの基本操作に加えて、設定や管理機能及び操作方法についての研修を行うこと。

(3) 研修はオンサイトでの実施も可能とするが、どの方式で実施するかは本県と調整の上で決定すること。

10-2. 研修方法

10-2-1. オンライン研修

(1) 提案オンライン研修については、e-learning やライブ配信等、より効果的な方式について提案を行い実施すること。
(2) 提案実施方式を踏まえ、最適なコンテンツを準備すること。
(3) オンライン研修で使用する発信側の環境については、受託事業者で用意すること。

10-2-2. オンサイト研修

(1) オンサイト研修の開催日時や場所については、本県の会議室等の空き状況を踏まえて、計画を作成すること。
(2) 上記計画の決定後、研修対象者、職員数、研修内容等について、詳細スケジュールを調整すること。
(3) オンサイト研修で職員が使用する機材は本県側で用意する。

10-2-3. 利用者マニュアル

(1) DX 推進基盤を利用する上で必要となる操作方法等について、「利用者マニュアル」を作成すること。利用者マニュアルには、各種ツールの機能や利用方法について、初心者でも理解しやすい内容を記載すること。
(2) 各種機能のうち、職員にとって影響が大きいと考えられる箇所については重点的に研修する等、職員の利便性確保に十分配慮すること。

10-2-4. 管理者マニュアル

(1) DX 推進基盤を運用する上で必要となる操作方法等について、「管理者マニュアル」を作成すること。
(2) 各種機能のうち、運用上で必要となる操作方法等について、マニュアルの内容に含めること。

11. 運用・監視・保守業務

11-1. 共通事項

11-1-1. 管理・連絡体制

(1) 提案 DX 推進基盤の運用・監視・保守を行い、別途委託済みのヘルプデスク及び運用管理 SE、その他システムの受託事業者と連携し、迅速な対応が可能な体制を整えること。

(2) 想定運用・監視・保守業務は、本庁舎に常駐または遠隔で本仕様書に記載する業務が滞りなく遂行できる体制を整えること。

(3) 運用・監視・保守業務に従事する者のうち、1 名をリーダとして、全ての業務について把握するような体制を整えること。

(4) リーダとして運用・監視・保守業務に従事する者は、以下のいずれかの要件を満たすこと。

- 「情報処理技術者（IT サービスマネージャ）」を有し、中央省庁、都道府県または、地方自治法第 252 条の 19 第 1 項の規定により政令で指定する人口 50 万人以上の市、又は民間企業において、端末機器が 1,000 台以上である情報システムの運用統括業務（運用責任者）の経験を 5 年以上有すること。
- 運用業務の経験を 15 年以上有し、中央省庁、都道府県または、地方自治法第 252 条の 19 第 1 項の規定により政令で指定する人口 50 万人以上の市、又は民間企業において、端末機器が 1,000 台以上である情報システムの運用統括業務（運用責任者）の経験を 5 年以上有すること。

(5) 担当者として運用・監視・保守業務に従事する者は、以下の要件を満たすこと。
情報システム又は情報通信ネットワークの設計、開発、構築、運用、保守等の実務経験を 1 年以上有すること。

(6) 必要に応じ、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。

(7) 契約後速やかに運用業務に従事する者の名簿を提出すること。要員に変更・追加が発生した場合も同様とする。

(8) 常駐により、運用・監視・保守業務に従事する者は、予め身分を証明する書類を県へ提出すること。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。

(9) 病気等で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。

(10) 本県からの障害連絡を 24 時間受けられるように、携帯電話を受信できるようにしておくこと。

(11) 緊急時の連絡体制を確保すること。

11-1-2. 業務時間

(1) 提案運用業務の業務時間は、平日の 8 時 00 分から 17 時 15 分までを含むものとし、複数名が業務に従事すること。

(2) 休日・時間外についても必要に応じ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
・ 選挙開票作業待機・・・休日待機を国政、県政選挙の度
・ 年度末移行作業・・・年度末、年度始の休日・時間外作業を数日程度

(3) 保守業務における障害対応等は、24 時間 365 日行うこと。

(4) 提案監視業務は、24 時間 365 日行うこと。ただし、受託事業者において導入した監視システムによる無人監視も可とする。

11-2. 運用・監視業務

11-2-1. 業務の内容（クラウド／業務端末／オンプレミスシステム共通）

(1) アカウント管理

・ 本業務にて独自でユーザ管理を行う場合は、異動等に合わせてユーザ情報の更新を行うこと。なお、年度途中の異動等に関する作業も含む。
・ 年度末において、人事異動に伴う大量の各種設定変更が発生するが、計画的に作業が進められるよう、十分な事前準備を行ったうえで、対応を行うこと。

(2) 日常の設定変更

・ 定常業務に伴い設定の変更が発生する場合には、事前に承認された作業計画書に基づき作業を実施すること。変更作業後は、結果を確認し本県に報告すること。
・ 設定変更に伴い、問題が生じた場合は作業を中止し、切り戻しを実施すること。
・ 設定変更作業の前後で、設定等のバックアップを行うこと。
・ 新 DK 端末について、アップデート作業（セキュリティパッチの適用等）を行うこと。
・ 構成情報を更新すること。

(3) 日常運用業務に対する支援

・ 本県職員からの DX 推進基盤の操作方法等に係る問い合わせは、別途調達済みのヘルプデスクが一次受付を行う。本業務においては、一次受付においてヘルプデスクでの対応が困難であると判断した案件について対応を行うこと。
・ 本県の本県職員でなくても実施可能な業務については、受託事業者が極力対応を行うこと。

(4) 本県からの技術的な問い合わせ対応

・ 本県からの DX 推進基盤に関する各種問い合わせに対応すること。なお、問い合わせは利用者ではなく、本県の特定のシステム担当職員が行うこととする。
・ 問い合わせを受けた案件は、本県から指定がある場合を除き、原則翌開庁日の 17 時までに回答を行うこと。

(5) 稼働及び性能監視

・ DX 推進基盤の稼働状況について、24 時間 365 日監視を行うこと。
・ DX 推進基盤におけるリソース使用率の測定を行うこと。
・ 稼働状況及びリソース使用率の異常を検知すること。

- 異常を検知した場合、運用計画書に従い、緊急度合いの判断及び保守対応要否の一次切り分けを実施すること。
- 異常発生時は、緊急度合いに応じて、運用計画書に従い、本県担当者へ電話等で通報すること。
- 稼働監視を行うにあたり、業務端末等にエージェントソフトウェアの導入やログインアカウントが必要な場合は、本県の承認を得ること。

(6) ログ管理

- 本県の指示に従い、DX 推進基盤のログ情報を汎用的な形式（XML、CSV などのテキストファイルを想定）で抽出、保存すること。なお、抽出する形式や内容については、システム運用期間中に協議のうえ決定する。

(7) ドキュメント管理

- 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要項を作成すること。
- 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。
- 本業務の作業内容に関する運用月次報告会議及び運用年次報告会議を実施すること。
- 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、履歴管理を行った上で更新の都度提出すること。
- システムの構成・仕様・設定等をドキュメント化し管理すること。
- 運用作業の実施手順、ルールを標準化し、マニュアルとして整備すること。
- 運用作業により、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上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上で、承認を受けること。
- 作成したドキュメントは随時更新の上で、本県担当者と共有できるように本業務で構築するファイルストレージ上に保存すること。なお、ファイルストレージのアクセス権やフォルダの階層設計など含めて、適切に実施すること。

11-2-2. 業務内容（オンプレミスシステムの運用に係る特記事項）

(1) データバックアップ・リストア

- 各機器について、定期的にバックアップを行うこと。
- 障害発生時等、必要に応じてバックアップからのリストアを行うこと。

(2) セキュリティパッチによる影響等の情報提供

- 本システムで使用するソフトウェア製品に関するバグフィックス、セキュリティ対応等のパッチがリリースされた場合、速やかにその内容の調査を行い、適用の可否を本県に報告すること。また、適用できない場合は、適用するためのシステム改修の内容を本県に報告すること。なお、パッチリリースから情報の提供までの期間は

1 週間以内とする。

(3) セキュリティパッチの適応作業

- 本システムへの影響がないと判断されたパッチのインストールを行うこと。
- パッチ適用による障害が発生した場合は、受託事業者にて障害対応を行うこと。

(4) OS 等のソフトウェアバージョンアップ、リビジョンアップの情報提供

- 本システムで使用するすべてのソフトウェア製品のバージョンアップ製品がリリースされた場合、その内容の調査、本システムに対する影響の調査、適用の検討、本システムの改修が必要な場合はその内容に係る情報の提供を行うこと。
- 契約期間中に本システムで利用しているソフトウェアのバージョンのサポートが終了する場合、速やかにバージョンアップ版ソフトウェアの取得を行い、継続してサポートが受けられるように対応を行うこと。その際に発生する全ての作業については本業務の契約範囲とする。
- サポートが終了となるソフトウェアのバージョンアップに伴い、他のソフトウェアのバージョンアップが必要となる場合は、そのソフトウェアのバージョンアップ版の取得及びバージョンアップ作業も本業務の契約範囲とする。
- なお、ソフトウェア製品に対してパッチが適用されない、または、セキュリティホールの有無をそのソフトウェア開発業者が確認しなくなった時点でサポートの終了と判断する。

11-3. 保守業務

11-3-1. 障害対応

(1) 障害切り分け

- 提案 DX 推進基盤の障害発生時に、障害箇所の切り分け対応を行うこと。
- 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。

(2) 関係者への連絡

- DX 推進基盤に障害が発生した場合、本県業務への影響を評価し、速やかに本県へ連絡すること。
- 障害原因が、三重県情報ネットワーク等、本契約の範囲外にある場合、その旨を速やかに本県へ連絡すること。

(3) 障害時の対応

- 障害切り分けの結果、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、または、切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、不良部位の切分け及び修理・修正・交換を行うこと。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。
- 機器等に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 2 時間以内とすること。

- ただし、大規模災害発生時はこの限りではないが、可能な限り速やかに対応すること。
- 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。
- 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。
- 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。
- 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。
- HDD・SSD 等の記憶装置不具合品又は HDD・SSD 等の記憶装置を搭載する故障機は交換後にメーカ返却せず本県の指定場所へ保管し、DX 推進基盤撤去時に「12-1 撤去及びデータ消去業務の管理」に記載とおりの措置を講じること。
  なお、上記の対応が困難な機器は、機密性の高い情報を保持しない、かつメーカ／保守委託先と機密保持契約が締結されている前提で不具合品及び故障機引き上げ時に都度本県の承諾を得ること。
- クラウドサービスが障害原因であると判明した場合は、障害に係る情報の収集及び復旧に努めるとともに、復旧目途を本県に連絡すること。なお、復旧時間等の詳細については、各クラウドサービスの SLA に準ずる。

11-3-2.障害後是正処置・予防措置

(1) 受託事業者が納入した機器やサービス等に起因する障害だけでなく、DX 推進基盤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、サービスの改善等の是正措置・予防措置を講じること。

(2) 直ちに障害原因が判明しない場合は、本県の了承を得た上で、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。

(3) 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し、障害報告書として随時提出すること。また、常に活用できるように保存すること。

12. 契約終了時の措置

12-1. 撤去及びデータ消去業務の管理

(1) データ消去作業計画書

- 受託事業者は、作業開始前に撤去及びデータ消去作業に関する「データ消去作業計画書」を作成し、本県に提出して承認を得ること。
- 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定義すること。

(2) 作業体制

- 本県との窓口となり進捗管理及び課題管理、問題解決を行える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。
- 受託事業者は、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。

12-1-1. 機器の撤去

(1) 撤去の範囲

撤去範囲については、原則、本業務において受託事業者が提供する機器類一式とする。県庁舎、データセンター等の全ての拠点を対象とする。残置については、本県と受託事業者が協議の上、決定すること。

(2) 撤去の時期

次期 DX 推進基盤への移行に合わせて、DX 推進基盤に関する機器の撤去を開始し、令和 10 年 3 月 31 日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は取り外すこと。
- 天井や壁に取付けた機器は取り外すこと。
- 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は、補修すること。
- 受託事業者が用意した LAN ケーブル等の配線は、撤去すること。

12-1-2. 機器のデータ消去・破壊

本項目は、本業務で導入したオンプレミスシステムについての要件を記載している。

(1)　データ消去・破壊の範囲

本業務において受託事業者が提供する機器類一式とする。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

受託事業者は、令和 10 年 3 月 31 日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

- 受託事業者は、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・破壊の作業場所

- 県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、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。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。

12-2. 次期事業者への引継

12-2-1. 概要

次期 DX 推進基盤への更新の際には、本県からの依頼に基づき質疑応答、業務の引継及び移行に伴う作業を行うこと。

12-2-2. 対応内容

発生する引継作業等を以下に示す。記載された作業の引継元は、受託事業者を前提とする。

対応時期	引継先	対応内容
次期 DX 推進基盤の仕様策定時（令和 8 年度）	本県	1.　DX 推進基盤の各システムに関する情報・データの提供
次期 DX 推進基盤の調達時（令和 9 年度）	次期 DX 推進基盤に関与する調達支援事業者	1.　設計・開発及び運用保守に係る資料・情報 2.　引継資料一覧 3.　残存課題、リスク引継事項 4.　DX 推進基盤特性に伴う個別の引継
次期 DX 推進基盤の設計・構築時（令和 9 年度）	次期 DX 推進基盤に関与する設計・構築事業者	

対応時期	引継先	対応内容
		事項 5. 改善提案引継事項 6. 本県で新たに作成された規定等
次期 DX 推進基盤の移行時（令和 9 年度）	次期 DX 推進基盤に関与する設計・構築事業者	1. DX 推進基盤に格納された各種データ類 2. 移行に必要な DX 推進基盤における各システムの設定作業を行う

12-2-3.引継方法

(1) 令和 9 年度に決定が予定される次期 DX 推進基盤に係る契約事業者等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。

(2) 上述の引継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受託事業者は引継内容を常に整理しておくこと。
なお、次期 DX 推進基盤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、DX 推進基盤からデータを抽出し、本県に提供すること。

13. 別紙

別紙 1　サービスレベル設定基準（運用・監視・保守）
別紙 2　デジタル改革推進課において配付している業務端末
別紙 3　統合サーバの利用について