第 2 期三重県 DX 推進基盤
整備及び運用保守業務
（コミュニケーション及びセキュリティ基盤）
調達仕様書（案）

令和 8 年 9 月

目次

1. はじめに

1-1. 業務名

第 2 期三重県 DX 推進基盤整備及び運用保守業務(コミュニケーション及びセキュリティ基盤)

1-2. 本仕様書の位置付け

本仕様書は第 2 期三重県 DX 推進基盤整備及び運用保守業務(コミュニケーション及びセキュリティ基盤)(以下、「本業務」という。)に関する調達内容を記載している。

DX 推進基盤の整備に関する全体概要については、「第 2 期三重県 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」、「加点」、「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**、**加点**、**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。
加点	本県が実現を期待する付加的な要件であり、提案および実現は必須としない。 提案があった場合は、評価基準に基づき加点する。
想定	本県が想定する実現方法の一例を記載したものである。

1-4. 用語の定義

本仕様書で使用する略語・用語について、以下に記載のとおり定義する。

略語	正式名称	説明
現行システム	三重県 DX 推進基盤	令和 4 年度に調達し、令和 9 年度末まで運用するシステム全体を指す。
DX 推進基盤	第 2 期三重県 DX 推進基盤	本業務において調達するシステム全体を指す。

略語	正式名称	説明
BYOD	個人所有端末の業務利用 (Bring Your Own Device)	職員個人が所有するスマートフォンやタブレット等の端末を業務に利用すること。
CASB	クラウドアクセスセキュリティブローカー (Cloud Access Security Broker)	クラウドサービス（SaaS）の利用状況を可視化し、未許可サービス（シャドーIT）の検出やアクセス制御を行う仕組み。
EDR	エンドポイント検知・対応 (Endpoint Detection and Response)	端末の挙動を常時監視し、不審な挙動の検知から封じ込め等の対応までを行う仕組み。
EPP	エンドポイント保護プラットフォーム (Endpoint Protection Platform)	マルウェアやランサムウェア等の脅威をリアルタイムに防御する、端末向けの保護機能。
ESP	メールセキュリティプラットフォーム (Email Security Platform)	メールやビジネスチャット経由の脅威（フィッシング、不正 URL 等）を検知・防御する仕組み。
FWaaS	サービス型ファイアウォール (Firewall as a Service)	ファイアウォール機能をクラウドサービスとして提供するもの。
IDaaS	ID・認証管理サービス (Identity as a Service)	シングルサインオン（SSO）や多要素認証等の ID・認証機能をクラウドサービスとして提供するもの。
IDS	侵入検知システム (Intrusion Detection System)	ネットワーク上の不正な通信を検知し、管理者に通知する仕組み。通信の遮断までは行わない。
IPS	侵入防御システム (Intrusion Prevention System)	ネットワーク上の不正な通信を検知したうえで、自動的に遮断・防御まで行う仕組み。
ISMAP	政府情報システムのためのセキュリティ評価制度 (Information system Security Management and Assessment Program)	政府情報システムにおけるクラウドサービスのセキュリティ水準を評価する制度。

略語	正式名称	説明
ISPM	ID セキュリティ状態管理 (Identity Security Posture Management)	ID・権限に関するリスクを継続的に分析し、過剰な権限や不審なアカウントを可視化する仕組み。
ITDR	ID 脅威検知・対応 (Identity Threat Detection and Response)	ID・認証情報に対する脅威や異常な挙動を検知し、対応する仕組み。
LGWAN	総合行政ネットワーク	地方公共団体等を相互に接続する行政専用のネットワーク。
MFA	多要素認証 (Multi-Factor Authentication)	パスワードに加え、ワンタイムコードや生体認証等、複数の要素を組み合わせて本人確認を行う認証方式。
PAM	特権アクセス管理 (Privileged Access Management)	特権アカウントの利用を厳格に管理し、必要に応じて一時的な権限付与や操作記録を行う仕組み。
SASE	セキュアアクセスサービスエッジ (Secure Access Service Edge)	ネットワーク接続機能とセキュリティ機能（ZTNA、SWG、FWaaS 等）をクラウドサービスとして統合的に提供する枠組み。
SDPP	セキュリティデータパイプラインプラットフォーム (Security Data Pipeline Platform)	複数のログ・テレメトリを収集・加工し、SIEM 等の分析基盤へ配信する基盤。本仕様書上の要求事項ではなく、あくまで参考情報として記載するもの。
SIEM	セキュリティ情報イベント管理 (Security Information and Event Management)	各種ログ・イベント情報を一元的に収集・相関分析し、脅威の検知や可視化を行う仕組み。
SLA	サービスレベルアグリーメント (Service Level Agreement)	提供するサービスの品質水準に関して受託事業者と本県との間で合意する事項。
SLO	サービスレベルオブジェクティブ (Service Level Objective)	SLA の達成状況を測るための具体的な目標値。
SOC	セキュリティオペレーションセンター (Security Operations Center)	セキュリティに関する監視・分析・対応を専門的に行う組織・機能。

略語	正式名称	説明
SSO	シングルサインオン (Single Sign-On)	一度の認証で複数のシステム・サービスを利用できるようにする仕組み。
SSPM	SaaS セキュリティ設定管理 (SaaS Security Posture Management)	SaaS 環境における設定不備や過剰な共有設定等を継続的に評価・是正する仕組み。
SWG	セキュアウェブゲートウェイ (Secure Web Gateway)	Web 通信を監視し、マルウェアや不正サイトへのアクセス等の脅威を検知・防御する仕組み。
TVM	脅威・脆弱性管理 (Threat and Vulnerability Management)	資産や脆弱性を継続的に可視化し、脅威情報に基づき対応の優先順位付けを行う仕組み。
UEM	統合エンドポイント管理 (Unified Endpoint Management)	PC やモバイル端末等を一元的に管理し、セキュリティポリシーの適用や準拠状況の確認を行う仕組み。
VPN	仮想プライベートネットワーク (Virtual Private Network)	公衆回線上に暗号化された仮想的な専用通信路を構築し、安全な通信を実現する技術。
XDR	統合的検知・対応 (Extended Detection and Response)	EPP、EDR、ITDR、ESP 等、複数領域のセキュリティ情報を統合的に相関分析し、検知から対応までを一体的に行う仕組み。
ZTNA	ゼロトラストネットワークアクセス (Zero Trust Network Access)	ユーザ・端末の状態を都度検証したうえで、必要な業務システムへのアクセスのみを許可する仕組み。

2. 本業務の概要

2-1. 目的

DX 推進基盤は、行政 DX のさらなる推進を支える基盤として、現行システムで実現したクラウド活用によるコミュニケーション環境及びゼロトラストセキュリティを継承・発展させるとともに、業務効率化、利便性向上及び運用コストの最適化を図ることを目的とする。

コミュニケーション基盤においては、職員間の円滑な情報共有や多様な働き方を支える機能を維持しながら、サービスやライセンス構成の最適化による費用対効果の向上を図る。また、業務効率化ツールの活用促進や利用環境の改善を通じて、職員自らが業務改善を実現できるデジタル活用基盤を整備し、組織全体の生産性向上をめざす。

セキュリティ基盤においては、ゼロトラストセキュリティの考え方をさらに発展させ、ID を中心とした認証・認可の強化、多要素認証や端末管理機能の高度化、脅威の早期検知及び迅速な対応を実現することで、高度化・巧妙化するサイバー攻撃に対する防御力を向上させる。特に、認証基盤及び ID 管理の強化を通じて、ランサムウェアをはじめとする高度な脅威への対応力を高め、安全な業務環境を確保する。

また、コミュニケーション基盤、セキュリティ基盤及び認証管理基盤を統合的に整備・運用することで、管理負荷の軽減、運用効率の向上及びガバナンス強化を実現し、安全性と利便性を両立した持続可能な DX 推進基盤を構築する。これにより、職員の業務品質及び行政サービスのさらなる向上を実現し、県民サービスの向上につなげることを目的とする。

2-2. 本業務の内容

本業務では以下の環境整備、現行システムからの移行、運用・保守を行う。

(1) コミュニケーション基盤

ビジネスチャット、グループウェア、庁内メール、インターネットメール、ファイルストレージ、Web 会議、業務効率化ツールをクラウドサービスとして提供する。

個人所有端末（スマートフォン、タブレット含む）からも、コミュニケーション基盤のサービスに限り、使用可能とする。

(2) セキュリティ基盤

ゼロトラストの考え方に基づくセキュリティ強化（エンドポイント、ID、クラウド等）に加え、業務端末の持ち出しを可能とするための環境（SASE 等）を整備する。

また、従来の統合認証基盤（Active Directory、資産管理ソフト、ウイルス対策システム、導入ソフトウェアのアップデート環境等）を本基盤に統合し、認証基盤や、庁内ネットワークのセキュリティ強化を図る。

プロジェクト管理や設計・構築、研修、運用保守等における主な業務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
設計・構築等業務	DX 推進基盤の設計、構築、テスト、移行等 各構成要素の仕様
研修業務	DX 推進基盤の研修
運用保守業務	DX 推進基盤の運用・監視・保守

2-3. 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。

2-4. 契約期間

契約期間は、令和 8 年度の契約締結日から令和 15 年 3 月 31 日までとする。

2-5. 支払

2-5-1. 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。

・令和 8 年度　　%
・令和 9 年度　　%
・令和 10 年度　　%
・令和 11 年度　　%
・令和 12 年度　　%
・令和 13 年度　　%
・令和 14 年度　　%

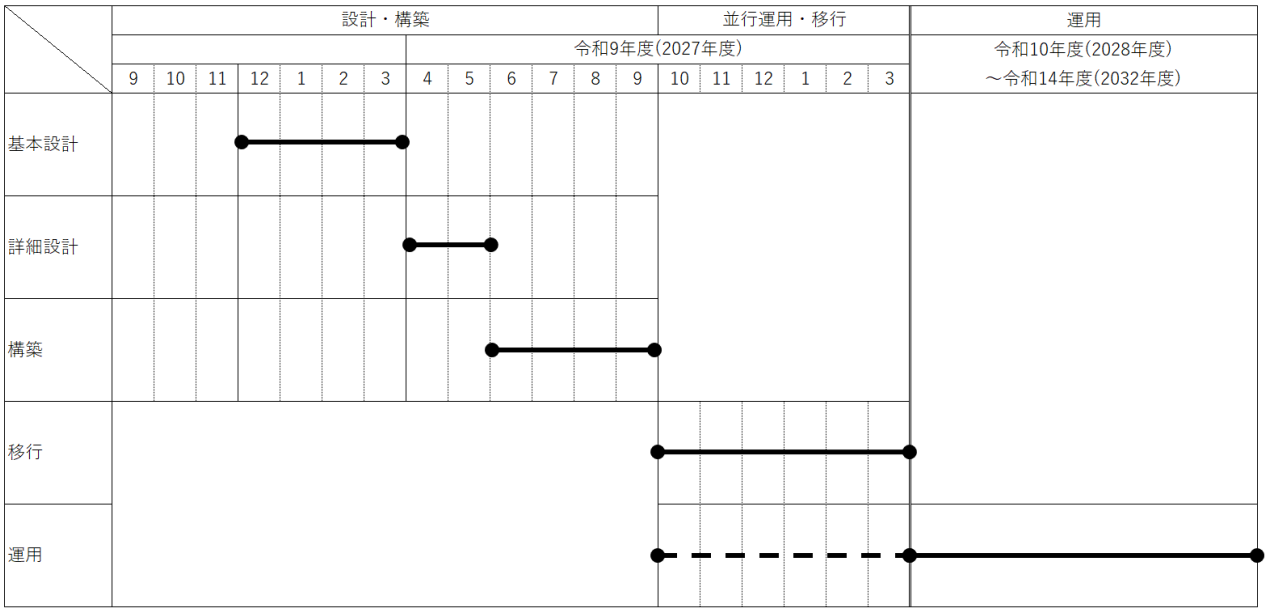
2-5-2. 内訳資料の提出

上記支払条件を踏まえて、契約締結後、速やかに、契約額の内訳資料（税抜き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。

2-6. 全体スケジュール

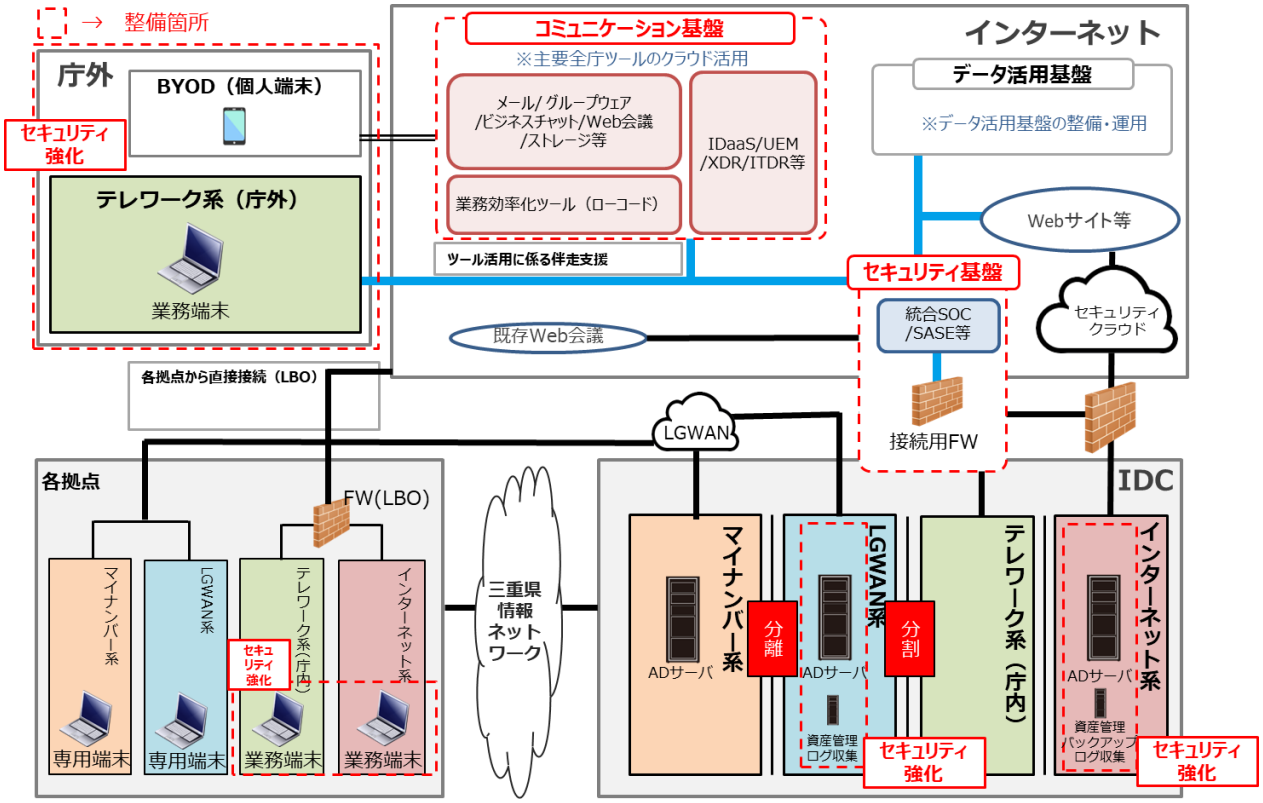
本業務の全体スケジュールを以下に示す。



設計・構築：契約締結後～令和 9 年 9 月末
並行運用・移行：令和 9 年 10 月～令和 10 年 3 月末
運用：令和 10 年 4 月～令和 15 年 3 月末

2-7. 概略図と責任分界

2-7-1. 概略図



2-7-2. 責任分界

概略図で示したとおり、本業務の主な範囲はコミュニケーション基盤及びセキュリティ基盤の整備であり、接続する業務端末やサーバ、ネットワークのセキュリティ強化（破線囲み部分）を含め整備対象となり、主な責任分界となる。

2-8. 利用者数及び端末台数

DX 推進基盤の利用者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	詳細
利用者数	7,700 人以上	一人一台PC利用（正規職員）：5,850名 共用PC利用（会計年度任用職員）：1,850名
端末台数	10,000 台以上	一人一台 PC のうち、庁外持ち出し PC：約 4,000 台 （令和 8 年度末見込み） BYOD 端末　約 1,000 台

2-9. 成果物

2-9-1. 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。

2-9-2. 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。

2-9-3. 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。

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 9 年 3 月末
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 9 年 5 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 9 年 6 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 9 年 7 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 9 年 9 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 9 年 8 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 9 年 9 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	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 9 年 12 月末
10	運用保守月次報告書	本業務において対象期間中に実施した運用実績、保守実績、障害事象、対応状況等の運用状況、作業報告等の月次結果を報告するもの	毎月末
11	運用保守年次報告書	本業務において対象期間中の運用状況等の年次結果を報告するもの	毎年度末

No.	成果物	内容	提出期限（予定）
12	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
13	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 9 年 8 月末
14	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されたもの 「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）」内の「ドキュメント管理」を参照すること	令和 9 年 9 月末
15	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 「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）」内の「ドキュメント管理」を参照すること	令和 9 年 12 月末

2-9-4. 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。

2-9-5. 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
総務部 デジタル推進局 デジタル改革推進課　情報基盤班

3. 現行システムの概要

DX 推進基盤における、コミュニケーション・セキュリティ基盤の主要な機能群である、コミュニケーション基盤、セキュリティ基盤、統合認証管理基盤システムの現行システムにおける概要と構成、課題について以下に記載する。

3-1. コミュニケーション基盤

(1) 概要

コミュニーション基盤では、庁内メールやインターネットメール、グループウェアの各システムについて、オンプレミス方式からクラウドサービスへ移行・刷新した。

また、各種業務のニーズや課題に対して、業務の内容を理解している職員が、自ら課題解決のためのアプリケーション等を容易に内製し、展開することができる業務効率化ツール（ノーコード／ローコード）を導入している。

(2) 構成

統合ツール	Microsoft Office 365 E3 Microsoft Enterprise Mobility + Security E3
ビジネスチャット	Slack Enterprise Grid

(3) 課題

クラウドサービスについて、機能が充実しているものの利用料が非常に高価であり、費用対効果を高めていくことが課題となっている。

また、特に業務効率化ツールについては、現時点で機能を有効に利用できているとは言えず、より利用しやすい製品とすることや、職員に対する利用方法の教育等の環境整備が課題となっている。

3-2. セキュリティ基盤

(1) 概要

インターネットアクセスによるコミュニケーションの強化を前提とした業務環境の整備に向けて、庁内ネットワークを「三層の対策」における β'モデルとして運用している。

また、庁外持出しパソコンによるテレワーク環境の強化を見据え、従来型の「境界型防御」から「ゼロトラストセキュリティ」への転換を行った。

(2) 構成

IDaaS	Microsoft Entra ID P1 （Microsoft Enterprise Mobility + Security E3 に含まれる）
UEM	Microsoft Intune

	（Microsoft Enterprise Mobility + Security E3 に含まれる）
SASE	PaloAlto 社 Prisma Access
接続用 FW	PaloAlto 社 PA-3420（2 台冗長構成）

(3) 課題

クラウドサービス向けのトラフィックを全てデータセンターに集約してアクセスさせる方式をとっているが、増大するトラフィックによる回線輻輳等が発生する恐れがあるため、インターネットアクセス経路の最適化が課題となっている。

また、SASE に接続している庁外持出しパソコンにおいては、接続エージェントを導入し、デバイスの健全性等に基づく継続的なアクセス評価や生体認証による端末ログオン等を実施しているが、アクセスできなくなった端末への対応が生じる等、セキュリティと利便性のバランスが課題となっている。

3-3. 統合認証管理基盤システム

(1) 概要

庁内端末のログオン認証や、オンプレミスシステムのシングルサインオンを行うため、庁内認証基盤を導入している。

また、各業務端末の資産管理やリモートサポートを実施するため、資産管理ソフトを導入している。

(2) 構成

庁内認証基盤	Active Directory（Windows Server 2019）
資産管理ソフト	Skysea Client View
EPP	Microsoft Defender, TrendMicro ApexOne
EDR	Tanium

(3) 課題

ランサムウェア感染等、高度化するセキュリティリスクに対して、十分に対応できているとは言えない状況となっている。

特に Active Directory における ID セキュリティを高める必要がある。

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。

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）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）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. 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、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) 想定 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。
(4) 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
(5) ハードウェア一覧
(6) ソフトウェア一覧
(7) 利用するサービスの一覧
(8) サービス及びコンポーネントごとの設計内容
(9) 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
(10) 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。
(11) ネットワーク接続図
(12) パラメータ・設定値の一覧
(13) 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。
(3) 運用計画書
(4) 運用年次計画書
(5) 運用手順書
(6) 運用フロー
(7) 保守実施要領（切り分け手順・復旧方法）
(8) セキュリティインシデント対応要領（連絡・対応手順）
(9) 各種管理台帳
(10) 各種ひな形
(11) 取り扱い説明書
(12) 運用テスト計画書
(13) 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（2024 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 わかりやすさ	例えば、色の違いを識別しにくいユーザを考慮し、メ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、適宜本県と協議のうえ、決定すること。

5-5-2. 構築方式及び構築手法

(6) 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。
(7) 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。
(8) 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）
(9) 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 9 年 6 月を想定
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 9 年 9 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 9 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) 提案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 10 年 3 月 31 日までに完了すること。

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。
(3) 方針、概要
(4) 前提条件
(5) 移行方法
(6) スケジュール、フェーズの説明
(7) 作業項目と作業担当者
(8) 移行対象システム、機器、データ
(9) 移行作業時の体制表及び役割分担
(10) 移行作業後の試験項目、合否判定基準
(11) 移行を中断・切り戻す場合の切り戻し手順
(12) 移行期間中の運用体制
(13) 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が必要な場合は、「8-1 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) 提案移行が必要な場合において、遠隔操作で設定変更が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。

（オ）各庁舎別端末設置台数

業務端末（NK 端末）の各庁舎別端末設置台数（令和 8 年 8 月時点）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 1,474 台
桑名庁舎	三重県桑名市中央町 5-71	約 142 台
四日市庁舎	三重県四日市市新正 4-21-5	約 174 台
鈴鹿庁舎	三重県鈴鹿市西条 5 丁目 117	約 117 台
津庁舎	三重県津市桜橋 3-446-34	約 180 台
松阪庁舎	三重県松阪市高町 138	約 185 台
伊勢庁舎	三重県伊勢市勢田町 628 番地 2	約 215 台
伊賀庁舎	三重県伊賀市四十九町 2802	約 145 台
志摩庁舎	三重県志摩市阿児町鵜方 3098-9	約 42 台
尾鷲庁舎	三重県尾鷲市坂場西町 1 番 1 号	約 99 台
熊野庁舎	三重県熊野市井戸町 371	約 98 台

(3)　業務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ある場合は、対象は「利用者数及び端末台数」に示す全ての業務端末とする。ただし、BYOD 端末は除く。

(4)　本契約期間中に業務端末を世代単位で機器更新することを想定している。受託事業者は、業務端末の調達・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) 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。
(3) 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。
(4) 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。
(5) 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。
(6) 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。
(7) 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。

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、ゼロトラストセキュリティを採用する。ただし、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) 提案ゼロトラストセキュリティ及び境界型セキュリティは、本業務や本県の他システムの状況に応じた実装とすること。
(3) 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。
(4) 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。
(5) 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。
(6) 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、多要素認証が可能であること。
(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) 提案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) 提案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。

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。

(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。

(8) 提案特権アクセス管理において Tier モデルを適用し、管理アカウント、管理端末、管理対象資産を Tier 0、Tier 1、Tier 2 に分類して設計すること。

(9) 想定 Tier 0 には、認証基盤、ID 管理基盤、ディレクトリサービス、証明書基盤、同期基盤、およびこれらを管理または制御可能なアカウント、端末、システムを含めること。

(10) 想定上位 Tier の認証情報が下位 Tier の端末またはシステム上で使用、保存、入力されないよう、アカウント分離、端末分離、アクセス経路制御、ログ監視を実装すること。

(11) 想定管理アカウントは Tier ごとに分離し、通常業務用アカウントとの共用を禁止すること。また、サービスアカウントについても Tier をまたいだ共用を禁止すること。

(12) 想定 Tier 0 管理操作は、専用の管理端末または同等のセキュリティを備えた管理環境からのみ実施可能とし、一般利用端末、メール利用端末、Web 閲覧端末からの管理操作を禁止すること。

(13) 想定 Tier 分類設計書、管理アカウント設計書、管理端末設計書、アクセス経路設計書、移行計画書、運用手順書、試験結果報告書を成果物として提出すること。

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。

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) 提案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。

6-3. 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用する。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 を遵守できない場合は、原因を特定して報告するとともに、改善策及び対応結果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 15 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／2,331 台、NK 端末／2,872 台）

「DK」または「NK」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 5～6 年程度で機器更新を行っている。

OS は、Microsoft Windows 11 Pro 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 365 E3

Microsoft 365 Apps for Enterprise

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 及び KK 端末／約 2,700 台程度）

「SK」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。

OS は、Microsoft Windows 11 Pro 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 365 E3

Microsoft 365 Apps for Enterprise

Microsoft Office 2024 Professional Plus（永続版）

Microsoft Office 2024 Standard（永続版）

DX 推進基盤において、SK 及び KK 端末は、DK 端末と同様の取り扱いとする。

(3) 各職員の個人端末（BYOD 端末）

各所属員が所有するタブレット、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。

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/iPadOS（現行システムにおける登録台数：約 800 台）

Google Android OS（現行システムにおける登録台数：約 250 台）

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

DK 端末、NK 端末、KK 端末、SK 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。本契約において Microsoft Windows Enterprise へのアップグレードライセンスを導入すること。

(2) オフィスソフト

DK 端末、NK 端末、KK 端末、SK 端末ともに、本契約において Microsoft Office のライセンスを導入すること。

ただし、インターネットに接続できない業務端末において、過去のバージョン固定製品が必要な場合の使用権が付帯されたライセンス契約とすること。

(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、本契約において、Windows Server の全職員が利用可能な User CAL を導入すること。

6-5-3. 閲覧ブラウザ

(1) NK/DK/KK 端末

Google Chrome 最新版

Microsoft Edge 最新版

(2) SK 端末

Google Chrome 最新版

Microsoft Edge 最新版

(3) BYOD 端末

Apple Safari 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。

6-7. オンプレミス機器に関する事項

6-7-1. 機器の調達・廃棄

必要なハードウェア・ソフトウェア一式の取得・設定を行うこと。

業務終了後に機器撤去およびデータ完全消去を行うこと。

データ消去および機器廃棄の証明書を提出すること。

6-7-2. ハードウェア

性能要件を満たすようサーバサイジングを行うこと。
性能不足時はハードウェア増強を行うこと。
サブシステム間でのサーバ兼用を原則行わないこと。
物理サーバは冗長構成とし安定的な運用を行うこと。
バックアップ・リストアシステムに必要なストレージを適切に選定すること。

6-7-3. ソフトウェア

最新バージョンの使用権を確保すること。
最新のセキュリティパッチを適用した状態で納入すること。
要件を満たすソフトウェアを選定すること。

7. 構成要素の仕様（コミュニケーション基盤）

7-1. メールシステム

7-1-1. 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、「7-1-2 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。
提案ドメインごとに、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。
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。
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。

(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。

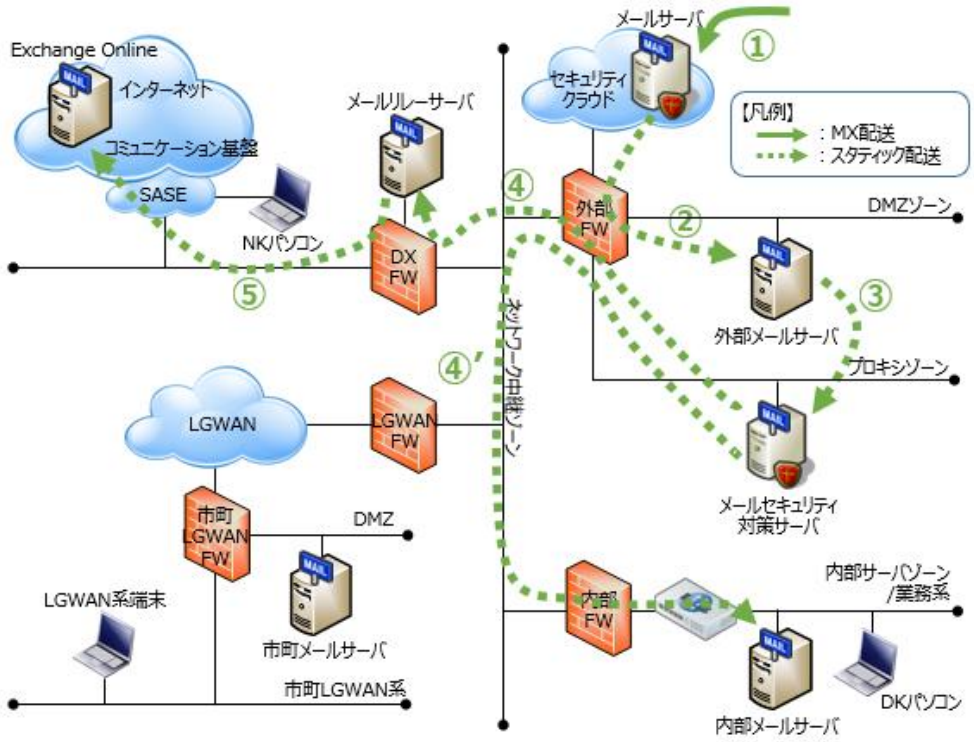
(3) 管理者向け機能

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。

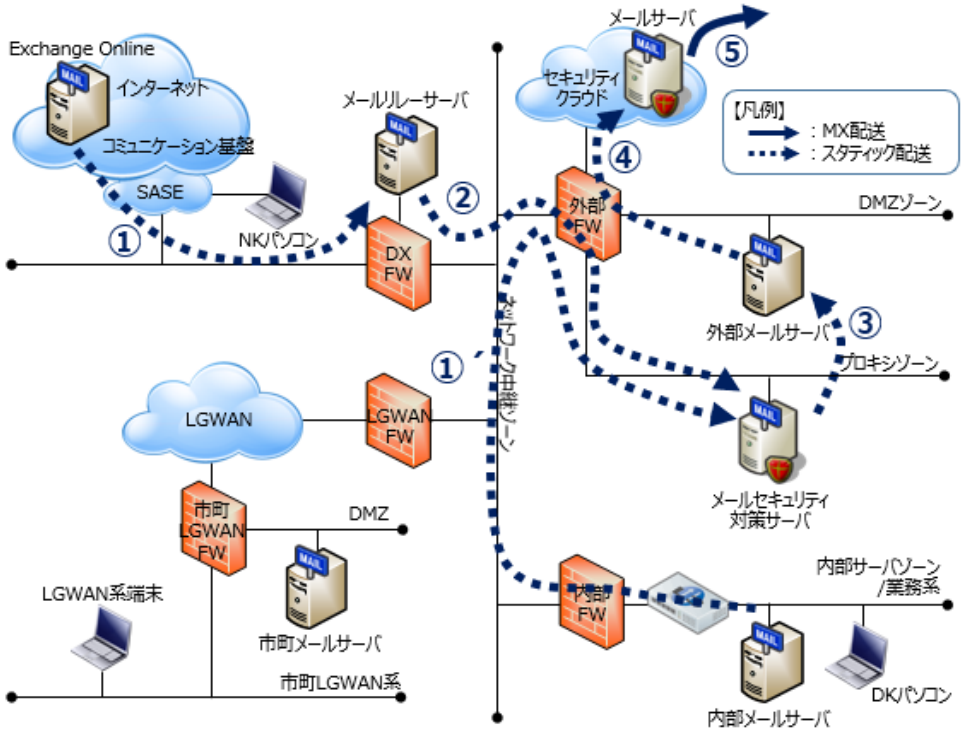
7-1-2. 概略図（想定）

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。

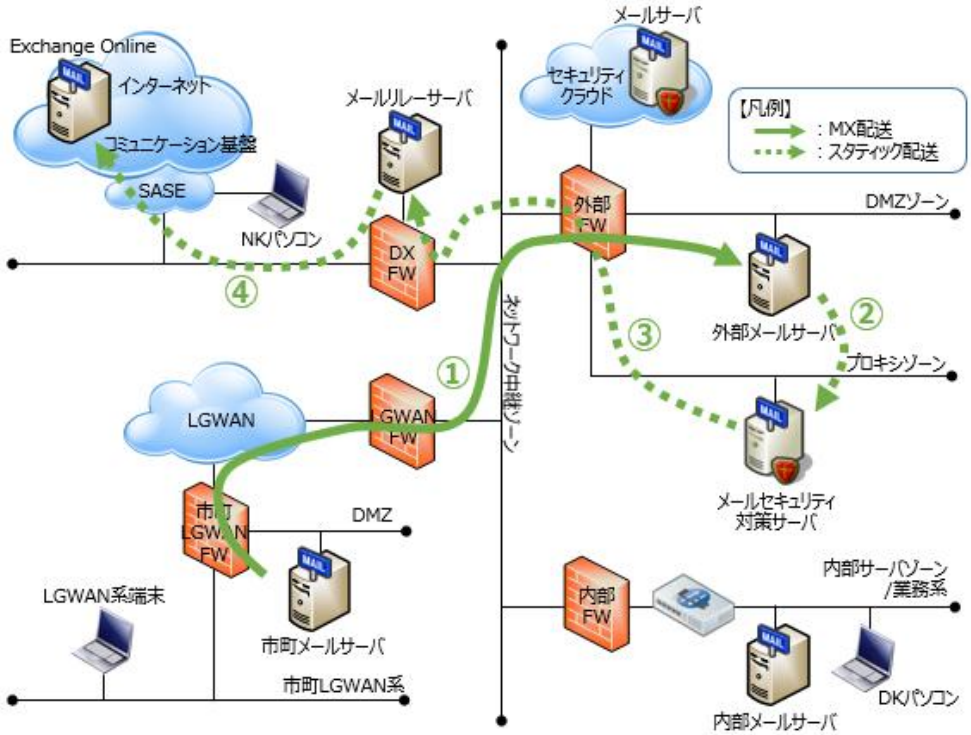
(1) インターネットメール（受信）



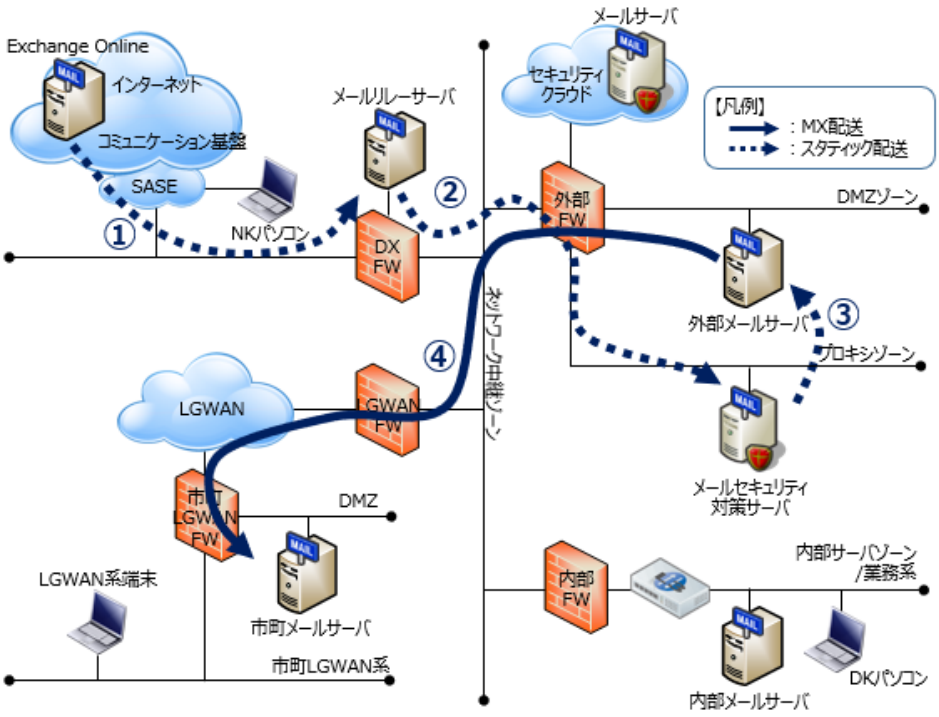
（2） インターネットメール（送信）



（3） LGWAN メール（受信）



(4)　LGWAN メール（送信）



7-1-3. 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。
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（メールボックス）の保存容量について、正規職員は 100GB 以上、会計年度任用職員は 2GB 以上、共有メールボックスは 50GB 以上割り当てられていること。
また、正規職員の保存容量については追加でアーカイブ領域を提供し 100GB 以上の保存を可能とすること。

(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。

7-2. メールリレーシステム

7-2-1. 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) 提案接続元 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。

7-2-2. 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。

7-3. Web コミュニケーション

7-3-1. 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。
管理者が CSV 等によるデータのインポートで複数の施設が一括で予約できること。
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。
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、1,000 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。
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。
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。

7-3-2.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。

7-3-3.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。

(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。

7-4. ストレージサービス

7-4-1. 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機能を有すること。
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。
提案監査ログ（操作ログ）の保存期間は 1 年以上とすること。
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。

7-4-2. 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。
- 正規職員ごとに 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。また、会計年度任用職員ごとに 2GB 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。

・ 正規職員においては、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。

7-5. 業務効率化ツール（ノーコード／ローコードツール）

7-5-1. 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。

(1) 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の機能において、CSV 等の汎用的なデータ形式でデータを入出力できること。
・ 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。

(2) 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。

(3) 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。

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。

(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.オフィスソフト

全ての職員が常に Microsoft 365 Apps for enterprise 相当の最新版を利用できること。

7-7.業務用 AI チャットツール

生成 AI を利用した業務用の AI チャットツールを提供すること。
入力したプロンプトやファイルをプロバイダーの学習に利用しないよう制御すること。

7-8.Windows ライセンス

全ての職員に対して Windows Enterprise（E3 相当）のアップグレード権および機能（セ

キュリティ・管理機能を含む）がサブスクリプションとして割り当てられていること。

8. 構成要素の仕様（情報セキュリティ基盤）

8-1. クラウド・ネットワークセキュリティ

8-1-1. 機能要件

(1)　基本要件

提案ゼロトラストの考え方に基づき、利用者や端末、ネットワーク通信等の状況からリスクや安全性を継続的に確認すること。
提案確認したリスクや安全性に応じて、利用者に必要最小限のアクセスだけを許可するとともに、様々な脅威を検知し、防御・対応できる仕組みをクラウドサービスとして提供すること。

(2)　ID/認証/権限管理

〔IDaaS〕
Active Directory と ID の連携を行うこと。
提案シングルサインオン（SSO）により、クラウド／オンプレミスアプリケーションの統合認証ができること。
多要素認証（MFA）による強固な認証ができること。
条件により、ユーザ・端末・場所に応じたアクセス制御ができること。
UEM と連携することで、デバイス準拠状態に基づき、安全な端末のみアクセスを許可できること。
加点サインインリスク・ユーザリスク（漏えい資格情報、異常行動等）を検知し、自動的にアクセス制御へ反映できること。
加点 ID のリスクスコアに基づくアクセス制御が可能であること。
加点 XDR 機能と連携できること。

〔ITDR〕
加点オンプレミスおよびクラウドの ID を横断して認証・挙動・権限のリスクを継続的に可視化できること。
加点アカウント侵害や異常活動を検知して自動的にアクセス制御や封じ込めを実行できること。

〔ISPM〕
加点 ID・権限・認証状態を継続的に分析し、過剰権限やリスクの高いアカウントを可視化することで、ゼロトラストの考え方に基づく適切なアクセス制御が可能であること。

〔PAM〕
加点特権アカウントの利用を厳格に管理し、必要に応じて一時的な権限付与と操作の可視化・記録（権限付与、有効化、承認履歴）を行うことで、不正利用や内部リスクを

防止できること。

(3) 端末・脆弱性・マルウェア対策

〔脆弱性管理（TVM)〕

加点端末の資産と脆弱性を常時可視化するとともに、実際の脅威に基づいて優先順位付けを行い、UEM 等と連携して修正・アクセス制御を一体的に実行できること。

〔UEM〕

提案業務端末やモバイル端末を一元的に管理し、セキュリティポリシー適用やデバイス準拠状態に基づくクラウドサービスへのアクセス制御が可能であること。
管理対象アプリに対し、業務データの暗号化・転送制限、認証制御、利用条件の設定および選択的消去を実施できること。

〔パッチ管理機能〕

提案 Microsoft Windows や Microsoft Office 等、Microsoft 社製アプリケーションのパッチ等を自動的かつ段階的に配布し、適用状況を可視化したうえで脆弱性を継続的に解消できること。

〔EDR/EPP〕

マルウェアやランサムウェアなどの脅威をリアルタイムで防御・検知し、振る舞いベースおよびクラウド連携によりエンドポイントを包括的に保護できること。
加点エンドポイントの挙動を常時監視し、脅威の検知・可視化から自動的な封じ込め・対応まで一体的に実行できること。

(4) メール・統合脅威検知

〔ESP〕

提案メールの脅威（フィッシング、マルウェア、不正 URL 等）を高度に検知し、攻撃から防御できること。
リンクや添付ファイルの無害化（悪性ファイルの検査、ブロック及び隔離）とユーザ保護を継続的に実現できること。
想定ビジネスチャット経由の脅威についてもメールと同等の検知・防御が可能であること。

〔XDR〕

加点 EPP、EDR、ITDR、ESP 等、複数領域のシグナルを相関分析し、脅威の検知から可視化、対応までを一体的かつ自動的に実行できること。

(5) SaaS・クラウド利用管理

〔SSPM〕

加点 Microsoft 365 などの SaaS 環境における設定や共有状態を継続的に評価し、設定不備や過剰権限を自動的に検出・是正できること。

〔CASB〕

提案 クラウドサービス（SaaS）の利用状況を可視化し、未許可サービス（シャドーIT）の検出ができること。

提案 クラウドサービスへのアクセスについて、許可／制限／遮断のポリシー制御が可能であること。

加点 クラウドサービスの利用状況および操作ログを取得し、監査および追跡が可能であること。

(6) Web サイト及び業務システムへのセキュアなアクセス

〔SASE（基本機能）〕

提案 ネットワーク接続とセキュリティ機能（ZTNA、SWG 等）を情報セキュリティ基盤（SASE）として統合的に提供し、ID、デバイス、アプリケーションのコンテキストに基づき、安全かつ最適なアクセス制御とトラフィック保護を実現すること。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。

情報セキュリティ基盤は、クラウドサービスとして提供すること。

NK 端末からエージェントを通じ、情報セキュリティ基盤へ接続が可能できること。

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。

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 NK 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、IDaaS との連携による SAML 認証に加え、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

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、NK 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端末のログオン認証を行う。また、端末へのログオン後、SASE エージェントの SAML 認証を行い、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、NK 端末へのログオン前に、接続用 FW で証明書認証を行い、その後、オンプレミス認証基盤で端末のログオン認証を行う。ま

た、端末へのログオン後、SASE エージェントの SAML 認証を行い、成功時には全ての通信を許可する。
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。

〔SASE（接続用 FW)〕
提案 SASE の仕様に基づき、接続用 FW 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。ただし、三重県が保有する現行システムの接続用 FW（PA-3420×2 台）について、受託者による保守延長が可能であれば、継続利用も可とする。
接続用 FW は冗長化すること。
提案接続用 FW 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。
NK 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）を接続用 FW に接続すること。

〔SASE（ZTNA)〕
テレワーク系（庁外）の端末から、SASE を経由し、三重県行政 WAN 内の業務システムへ安全にアクセスできること。
業務システムへのアクセスは、三層分離のネットワーク境界を維持しつつ、ユーザ認証、デバイスの準拠状態、アクセス元コンテキストに応じてアクセス可否を制御できること。
業務システムへのアクセスは、既存のネットワーク分離構成と整合を保つため、IP ベースでのアクセスを併用可能としつつ、アプリケーション単位のアクセス制御を段階的に適用できること。
テレワーク系（庁内/庁外）の端末から業務システムへのアクセスにおいて、シングルサインオン（SSO）が可能であり、Active Directory 等の認証基盤（Kerberos 等）と連携できること。
提案 SASE に障害が発生した場合においても、既存ネットワーク経路または代替アクセス経路により業務継続が可能であること。
加点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 NK 端末から業務システムへのアクセスが可能であること。
加点テレワーク系（庁内）からインターネット接続系の NAS 等へ、別途導入予定の FW(LBO)を通じて拠点内接続ができること。
加点テレワーク系（庁内）からインターネット系へ通信を迂回させた場合も、SASE 経由と同等のセキュリティが担保できること。

〔SASE（SWG)〕
テレワーク系（庁内/庁外）の端末からの Web 通信に対して、マルウェア、ウイルス、不正スクリプト等の脅威をリアルタイムに検知・防御できること。
URL カテゴリ分類に基づくコンテンツフィルタリング機能を有し、業務要件に応じたアクセス制御（許可／制御／遮断）が可能であること。

管理者が定義したポリシーに基づき、ユーザ、端末、アクセス先等の条件に応じた柔軟な Web アクセス制御が可能であること。
インターネット上の既知の悪性サイト、フィッシングサイト、不審なドメイン等について、レピュテーション情報や脅威インテリジェンスに基づき、実際に接続する前に遮断できること。
マルウェア対策が可能であること。
提案テレワーク系（庁内）に接続された NK 端末からの Web 通信について、接続先サービスを識別のうえ、別途導入予定の FW（LBO）及び SASE を通じて LBO 接続できること。

〔SASE（FWaaS)〕
加点ネットワーク通信に対して、送信元／宛先 IP アドレス、ポート、プロトコルに基づく通信の許可／遮断制御が可能であること。
加点アプリケーション識別（App-ID 等）により、ポート番号に依存しないアプリケーションレベルでの通信制御が可能であること。
ユーザ ID およびグループ情報に基づき、ユーザ単位でのアクセス制御が可能であること。
加点既知および未知の脅威に対して、侵入検知・防御（IDS/IPS）機能により、IDS による検知及び IPS による遮断をリアルタイムに行えること。
通信内容を解析し、マルウェア、不正通信、C&C 通信等の脅威を検知・遮断できること。
SSL/TLS で暗号化された通信に対して、復号および検査（SSL インスペクション）が可能であること。
ポリシーに基づき、送信トラフィックおよび受信トラフィックのログを取得し、可視化・監査が可能であること。
加点地理情報（ジオロケーション）に基づくアクセス制御（国別制御）が可能であること。
加点仮想パッチやシグネチャにより、脆弱性攻撃からの防御が可能であること。
加点帯域制御や QoS 制御により、業務通信の優先制御およびトラフィック最適化が可能であること。
冗長化および分散配置により、高可用性（HA）および障害時の通信継続性を確保できること。
クラウド基盤上で提供され、端末を問わず一貫したセキュリティポリシーを適用できること。

(7) 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 Operations 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（ITDR/EPP/EDR/ESP/XDR/SWG/FWaaS 等）から出力されるログおよびイベントの相関分析を行うこと。
ログ及びイベント分析を通じて、セキュリティインシデント等を検知できること。

提案一定の危険度以上のインシデントについては、県担当者へ電話等による緊急連絡を行うこと。

提案県担当者の指示に基づく緊急対応を行うこと。

加点 SASE、EDR、セキュリティクラウド等の SOC 窓口を一元化すること。

8-1-2. テレワーク PC(NK 端末)設計・構築

庁外にあるテレワーク PC の構成管理、リモートワイプ等の MDM 機能を提供すること。

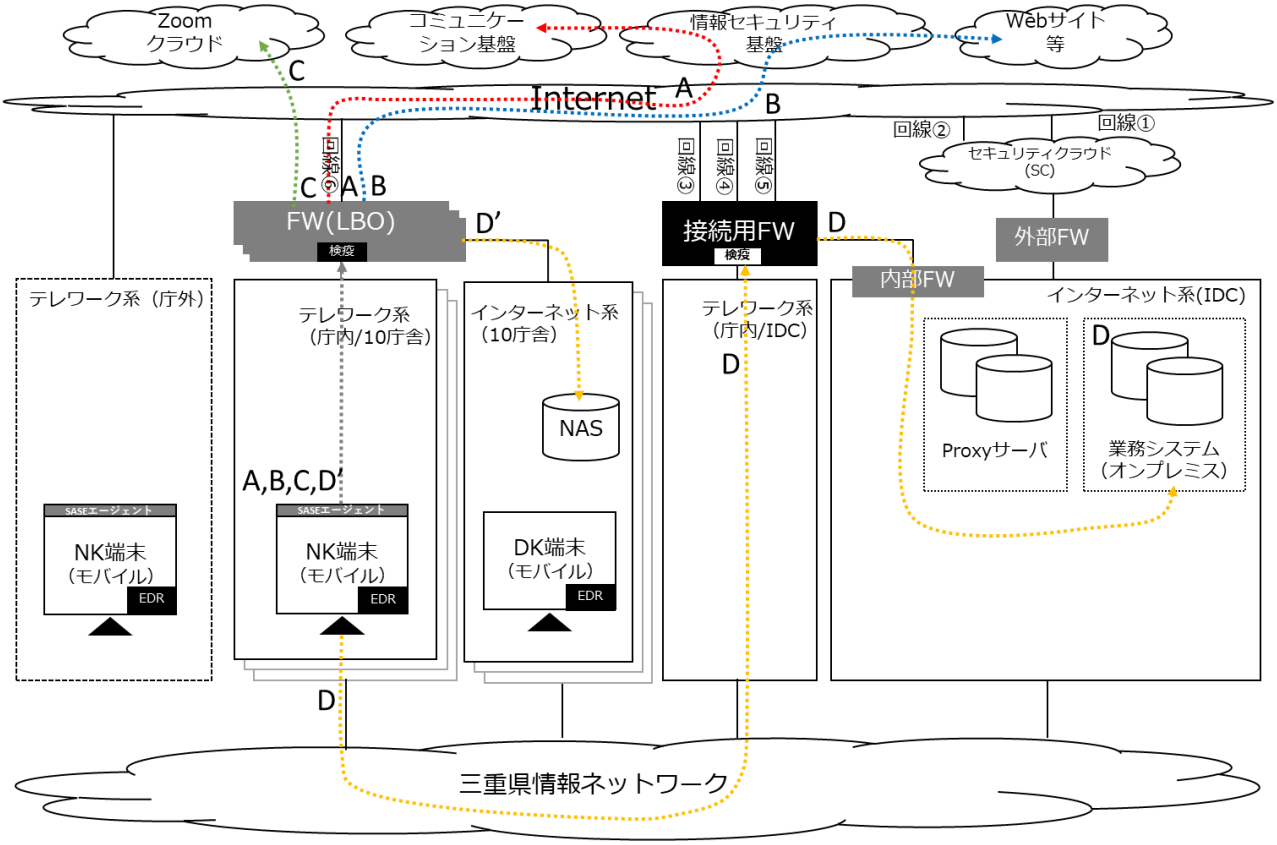
業務端末（別契約）をテレワークに使用できるように設計し、必要な設定変更やエージェントの導入を行うこと。

8-1-3. 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。

（8） NK 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（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。

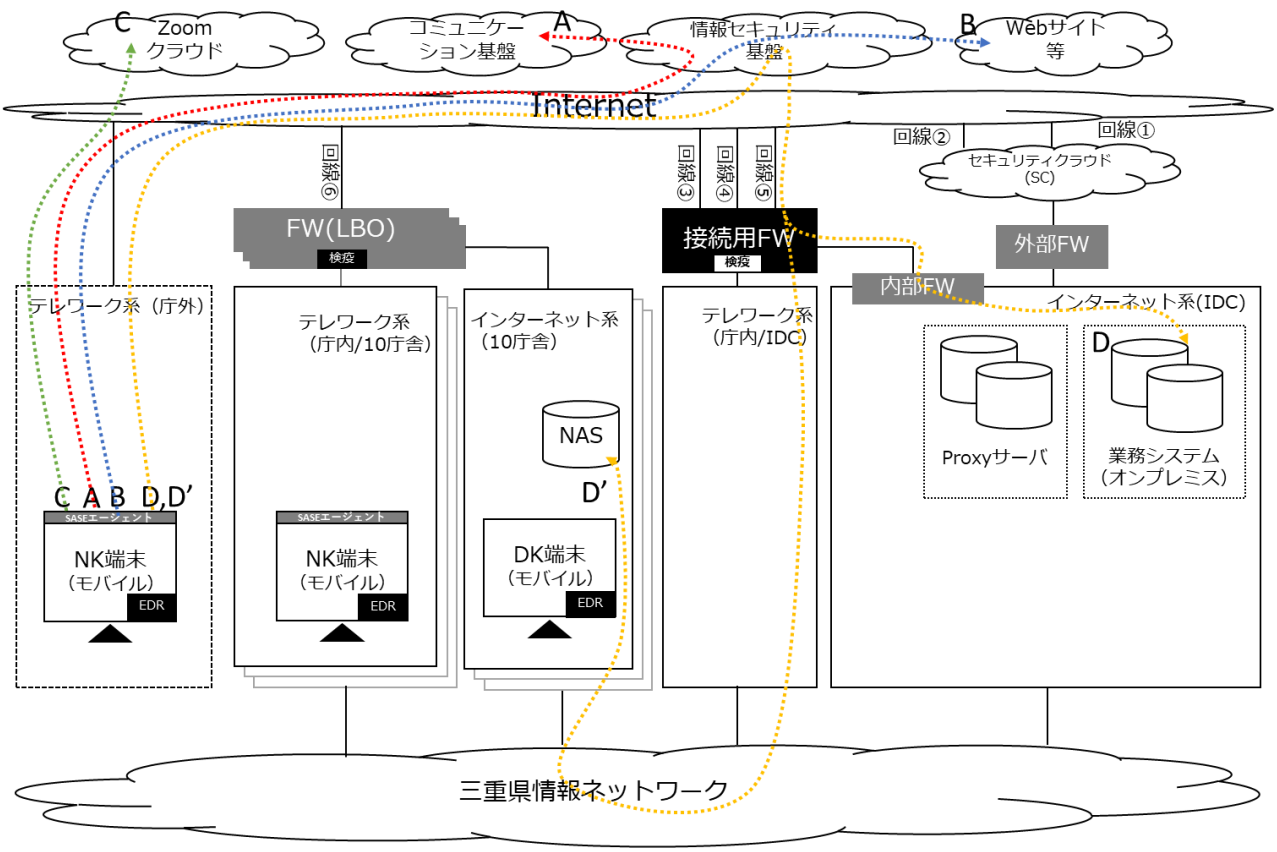
ルート D'は、インターネット系の NAS 等へのアクセスルートを示す。

回線①はセキュリティクラウドの接続回線、回線②は、セキュリティクラウドのブレイクアウト回線（3Gbps/1Gbps 帯域保証）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 帯域保証）を指す。
回線⑤は、別途調達予定のインターネット回線（6Gbps ベストエフォート）を指す。
回線⑥は、別途調達予定のインターネット回線（本庁 2Gbps ベストエフォート、各総合庁舎 1Gbps ベストエフォート）を指す。
NK 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 または接続用 FW で行う。万一、SASE に障害が発生した場合は、接続用 FW で認証を行う。
NK 端末からの通信は、ルート A～D'ともに SASE 経由とするが、SASE との VPN セッションは、別途調達予定の FW（LBO）から確立することで、NK 端末からの VPN セッション数を低減させる。
NK 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 の通信を別途調達予定の FW（LBO）及び接続用 FW 経由でインターネット系へブレイクアウトさせる。

NK 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'の通信を別途

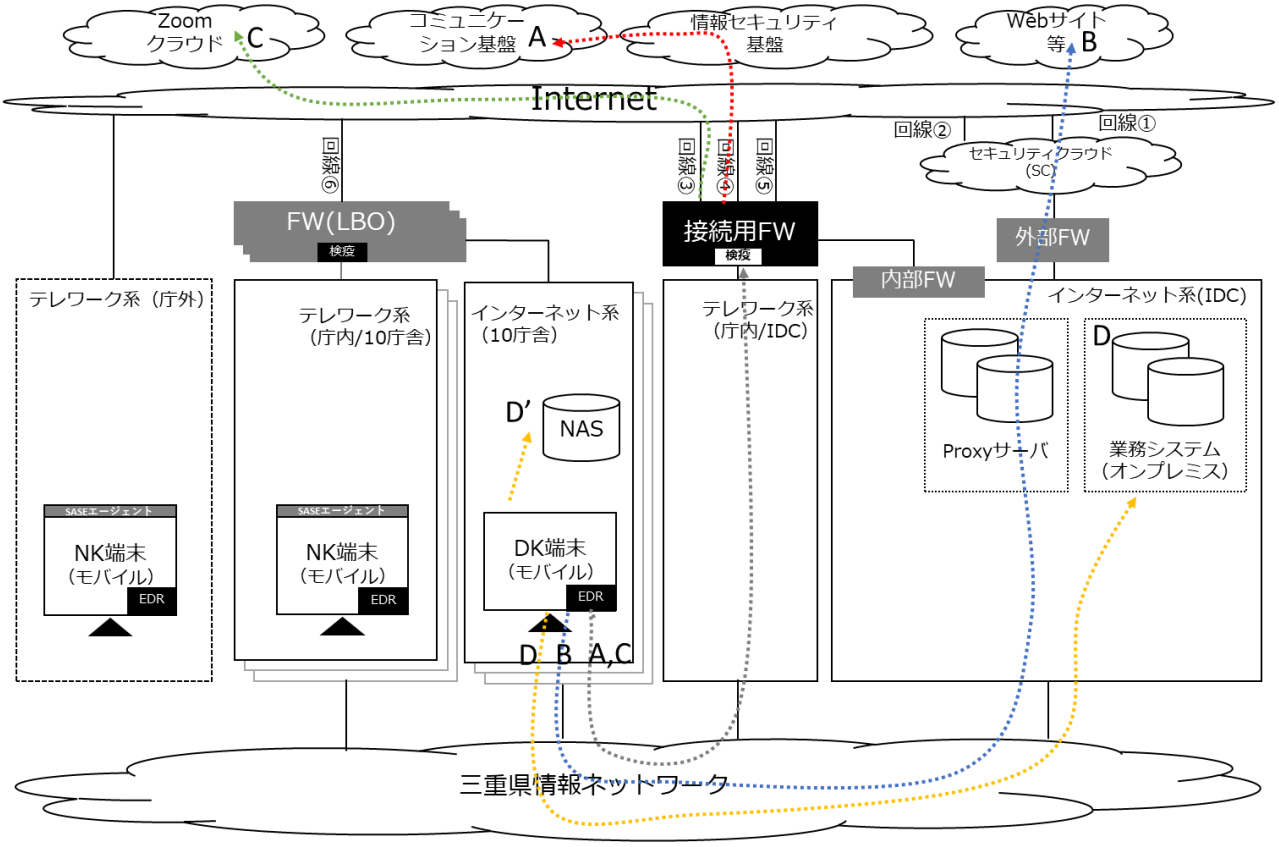
調達予定の FW(LBO)経由でインターネット系へブレイクアウトさせる。

（9） NK 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（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。
ルート D'は、インターネット系の NAS 等へのアクセスルートを示す。
回線①はセキュリティクラウドの接続回線、回線②は、セキュリティクラウドのブレイクアウト回線（3Gbps/1Gbps 帯域保証）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 帯域保証）を指す。
回線⑤は、別途調達予定のインターネット回線（6Gbps ベストエフォート）を指す。
回線⑥は、別途調達予定のインターネット回線（本庁 2Gbps ベストエフォート、各総合庁舎 1Gbps ベストエフォート）を指す。
テレワーク系（庁外）に接続された NK 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、NK 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。
NK 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。

（10）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（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。
ルート D'は、インターネット系の NAS 等へのアクセスルートを示す。
回線①はセキュリティクラウドの接続回線、回線②は、セキュリティクラウドのブレイクアウト回線（3Gbps/1Gbps 帯域保証）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 帯域保証）を指す。
回線⑤は、別途調達予定のインターネット回線（6Gbps ベストエフォート）を指す。
回線⑥は、別途調達予定のインターネット回線（本庁 2Gbps ベストエフォート、各総合庁舎 1Gbps ベストエフォート）を指す。
インターネット系に接続された DK 端末からの通信は、ルート A 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 C は接続用 FW からインターネットへのブレイクアウト通信とする。
ただし、SASE がダウンした場合、ルート A はセキュリティクラウド経由とする。
DK 端末から SASE へのアクセスは、接続用 FW から確立した VPN セッションを利用する。
ルート A と B は、既設のロードバランサ（A10 Networks 社製）でアプリケーション／サービス識別ルーティングによる通信の振り分けを行う。

8-1-4.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「利用者数及び端末台数」に示すとおり（NK 端末及び DK 端末等）とする。

(2) 利用者数

情報セキュリティ基盤の利用者は、「利用者数及び端末台数」のとおりとする。

(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) 接続用 FW 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。

(8) 責任分界

(ア) SASE

本調達の受託事業者は、SASE サービスの提供、SASE 側の接続設定、接続仕様の提示及び接続試験支援を行う。
別途調達予定の第 2 期三重県 DX 推進基盤整備及び運用保守業務（庁内ネットワーク環境の構成変更）の受託事業者は、各拠点のネットワーク設定、FW(LBO)の導入及び各拠点から SASE までの接続設定を行う。
LBO 用回線は別途調達する。
各事業者は、本県の調整のもと、設計、試験、障害切り分け及び移行作業に協力すること。

(イ) その他

本調達の受託事業者は、インターネット系端末に適用する EPP、EDR、UEM その他のセキュリティ機能について、製品及びライセンスの提供、ポリシー設計、管理基盤側の設定並びに運用・監視を行う。
別途調達予定の第 2 期三重県 DX 推進基盤整備及び運用保守業務（庁内ネットワーク環境の構成変更）の受託事業者は、本調達の受託事業者が提示する設計及び手順に基づき、ネットワーク側の設定変更を行う。

8-2. エンドポイントセキュリティ（業務端末）

8-2-1. 機能要件

(1) 端末ネットワーク

指定した通信を除き、NK 端末からの通信は、情報セキュリティ基盤または接続用 FW を通じた通信に限定できること。

NK 端末から外部への通信について、一部を情報セキュリティ基盤を通過しない通信として許可できること。

外部から NK 端末への通信を全て遮断すること。

(2)　ログオン認証

提案 NK 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。
提案 NK 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、ログオン画面で生体認証を行う多要素認証とすること。
提案利便性とセキュリティを両立する多要素認証方式とすること。

(3)　データセキュリティ

提案 NK 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 NK 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。
NK 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

NK 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。
提案 NK 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 NK 端末について、EPP の更新状況の把握が可能であること。
提案 NK 端末について、EPP の強制更新が可能であること。
提案 NK 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。
ドライブ暗号化がなされていない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。
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 NK 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。
NK 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。
提案 NK 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。
NK 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 NK 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 端末に対してゼロタッチデプロイが可能であること。

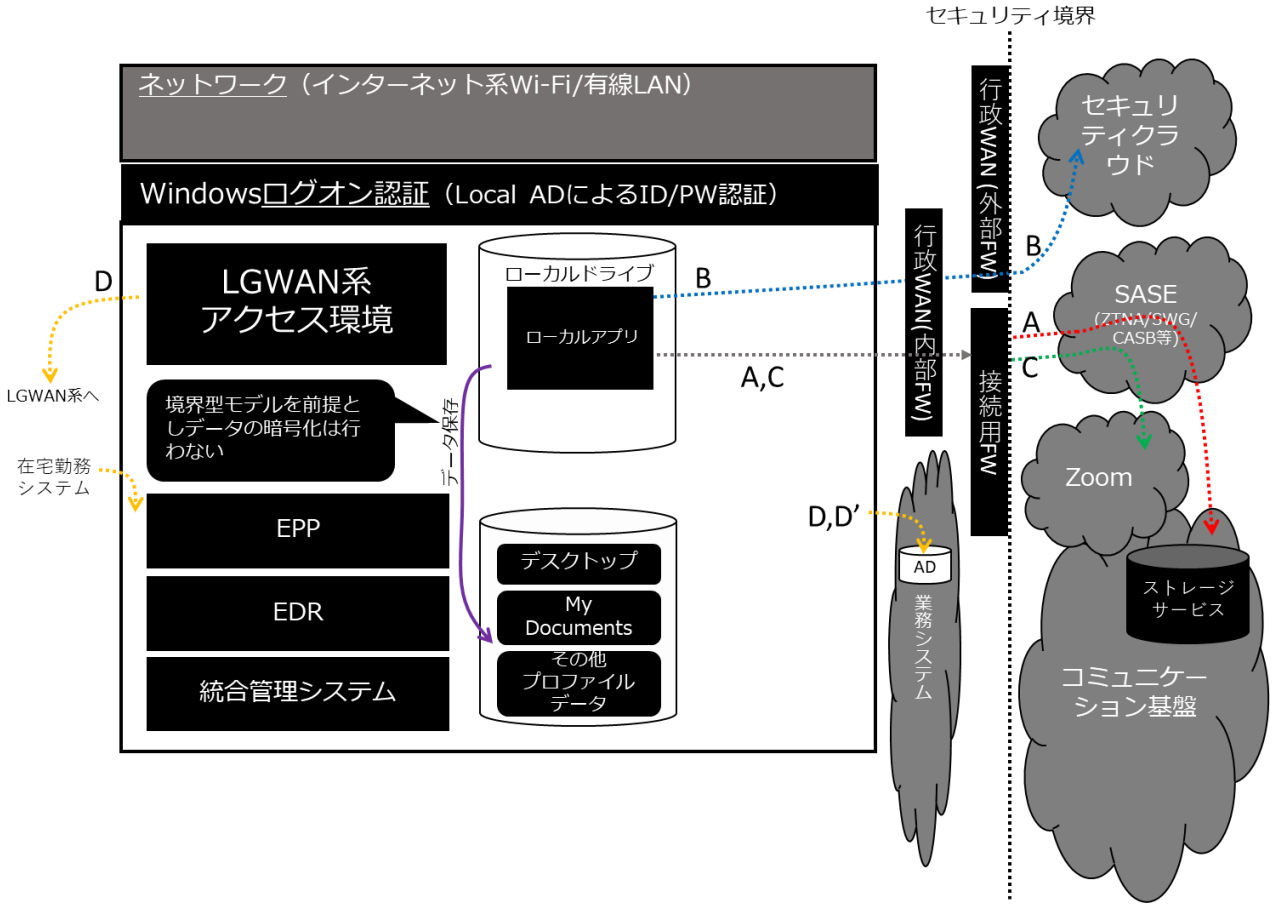
8-2-2. 端末構成

提案 NK 端末及び DK 端末は、「8-1 クラウド・ネットワークセキュリティ」、「8-2 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 NK 端末及び DK 端末の構成例を示す。

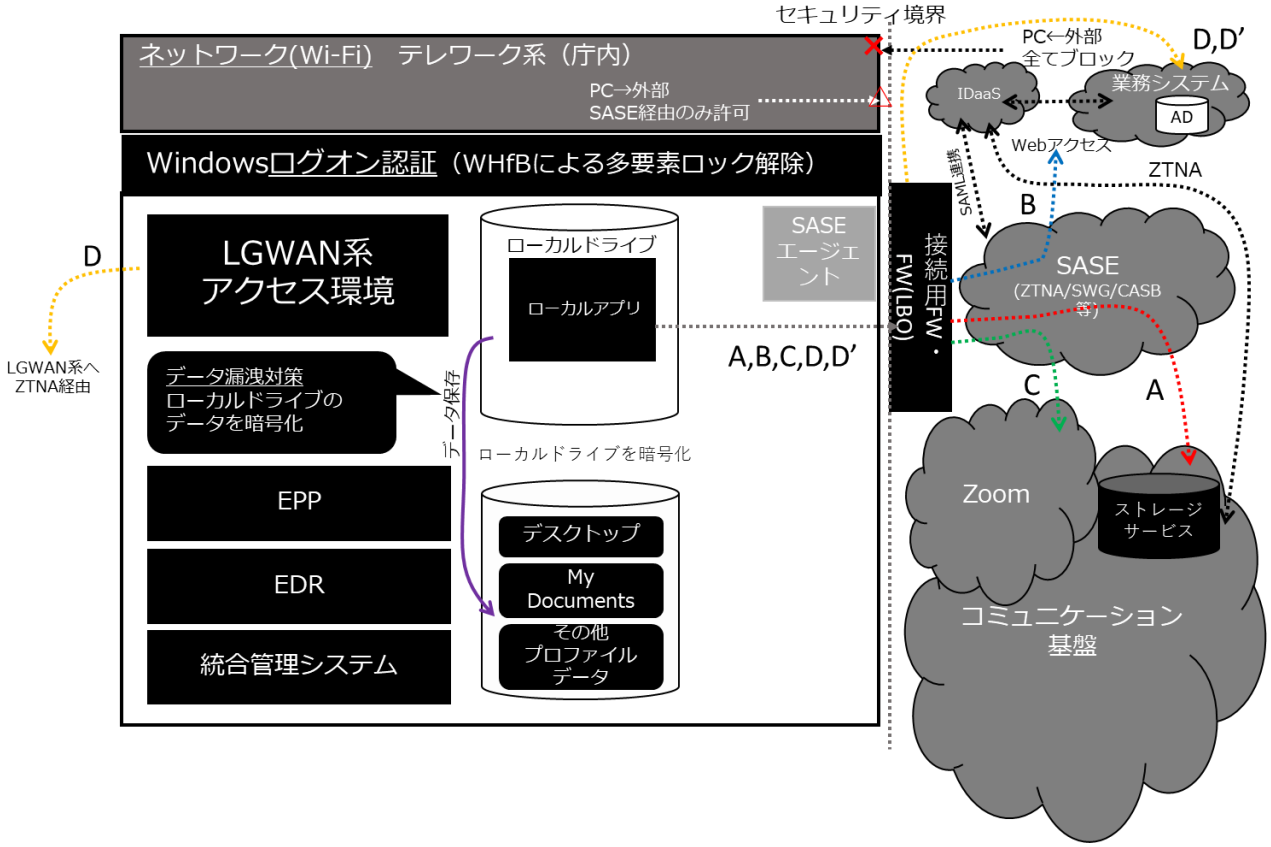
(1) 構成例（DK 端末）

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、セキュアコンテナ方式によるものとする。
以下に DK 端末の構成例を示す。



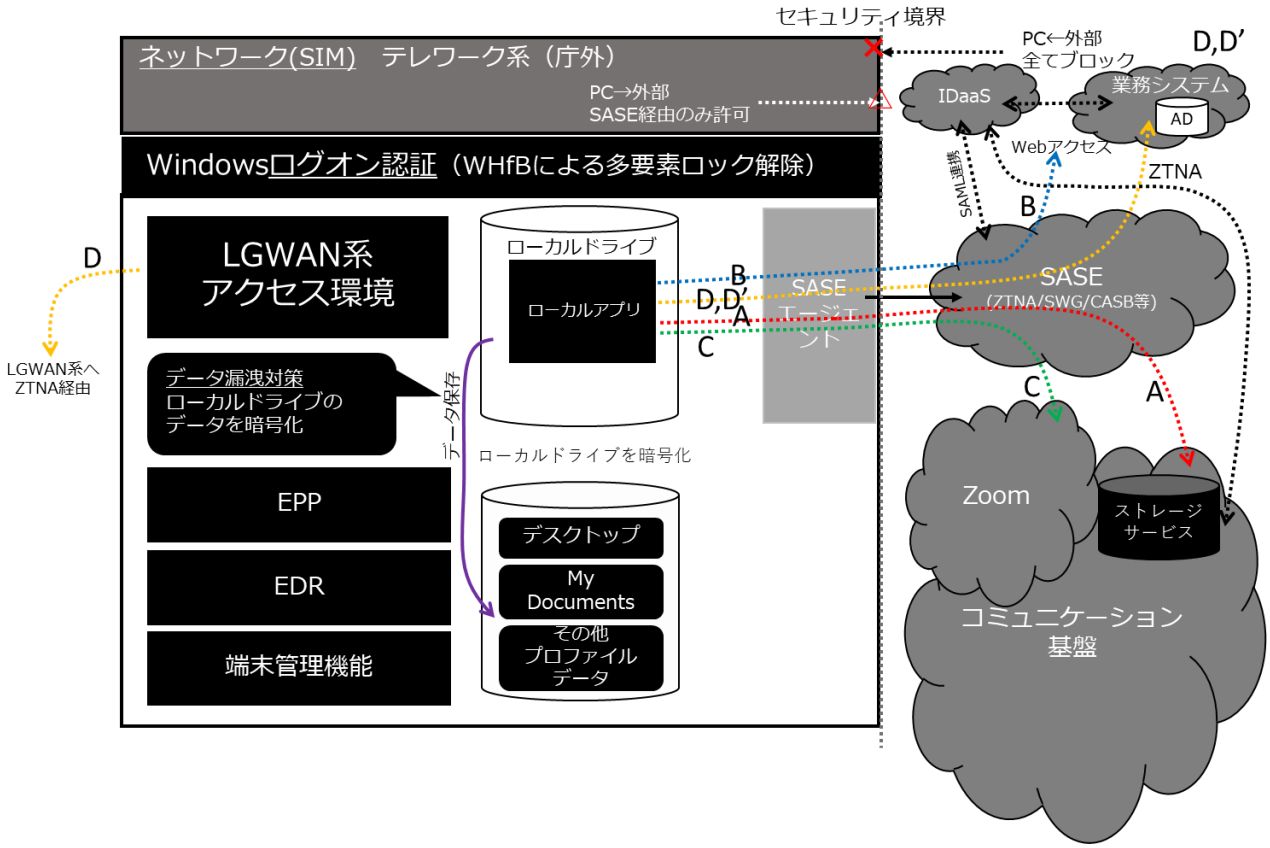
（2） 構成例（テレワーク系（庁内）に接続された NK 端末）

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、接続用 FW 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、接続用 FW 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 NK 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 NK 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 NK 端末の構成例を示す。



8-2-3. 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、「利用者数及び端末台数」のとおりとする。

(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。

8-3. エンドポイントセキュリティ（BYOD 端末）

8-3-1. 対象端末

BYOD の対象端末は、職員個人が所有する Android 及び iOS/iPad 端末とする。

8-3-2. 機能要件

(1) データセキュリティ

業務データを個人データとは論理的に分離して管理できること。
Android では、仕事用プロファイル内に業務アプリおよび業務データを格納すること。
iOS/iPadOS では、管理対象アプリ、管理対象アカウントおよび管理対象データとして識別できること。
業務データを扱うアプリを管理対象として指定し、限定できること。
未承認アプリからの組織リソースへのアクセスを制限できること。
業務データの転送先を、管理対象アプリに限定できること。
管理対象アプリから個人アプリへの「開く」「共有」「送信」を制限できること。
業務上必要なアプリのみ、例外として明示的に許可できること。
業務アプリから個人アプリへのコピーおよび貼り付けを禁止または制限できること。
管理対象アプリ間のコピー・貼り付けは、業務要件に応じて許可できること。
「名前を付けて保存」等による端末の個人領域への保存を禁止できること。
保存先を、組織が承認した OneDrive for Business、SharePoint 等に限定できること。
個人用 OneDrive、個人用クラウドストレージ、SD カード等への保存を制限できること。
暗号化されない領域への業務ファイル保存を禁止できること。
業務データが個人用 iCloud、iTunes バックアップまたは Android バックアップサービスに保存されないよう設定できること。
管理対象アプリの業務データを、個人所有の PC 等へ復元できないこと。
画面キャプチャ、画面録画、画面共有を制限できること。
音声アシスタントや生成 AI 機能への業務データ引き渡しを制御できること。
端末または業務領域が暗号化されていること。
暗号化されていない端末を非準拠として判定できること。
Android では、仕事用プロファイルを含むデバイス暗号化状態を確認できること。
iOS/iPadOS では、端末パスコード設定を通じてデータ保護が有効化なことを確認できること。
管理対象アプリ内の業務データを暗号化できること。
アプリ内暗号化が無効な場合、業務アプリを起動または利用させないこと。
業務データを一時ファイル、キャッシュ等に保存する場合も保護できること。
管理対象アプリの起動時または一定時間経過後に、業務用 PIN または生体認証を要求できること。
業務用 PIN は、端末のロック解除コードと分離できること。
PIN の最小桁数、単純値の禁止、再利用禁止および試行回数を設定できること。
組織リソースへのアクセス時に IDaaS による多要素認証を要求できること。
MDM で「準拠」と判定された端末のみ、組織リソースへアクセスできること。

(2) 端末管理

退職、異動、端末紛失、盗難、利用停止等の場合に、業務データのみを遠隔削除できる

こと。
アプリ単位またはユーザー単位で業務データ削除を実行できること。
個人所有端末として識別して MDM 登録できること。
iOS/iPadOS 端末の脱獄状態を検知できること。
Android 端末の root 化状態を検知できること。
検知した端末を自動的に非準拠とできること。
非準拠端末から組織リソースへのアクセスを遮断できること。
端末のロック解除にパスコードを要求できること。
一定時間操作がない場合に自動ロックできること。
アプリを利用者または端末へ配布できること。
紛失・盗難時に、対応プラットフォームの範囲で遠隔ロックできること。

8-3-3.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、「利用者数及び端末台数」のとおりとする。

(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。

9. 統合認証管理基盤システム（オンプレミス）

9-1. 対象

オンプレミス認証基盤は、インターネット系及びテレワーク系、LGWAN 系の端末を対象とする。

9-2. オンプレミス認証基盤

9-2-1. 機能要件

提案現行の庁内ドメインシステムの機能を継承した認証基盤を構築すること。
インターネット系用の庁内ドメインシステムを構築すること。
LGWAN 系用の庁内ドメインシステムを構築すること。
ドメインシステムは Active Directory によりユーザ認証及びリソース管理を実現すること。
ドメインユーザによるログオン認証機能を提供すること。
グループポリシーにより端末のセキュリティ設定を制御すること。
DNS、DHCP、NTP の各機能を提供すること。
CSV ファイルによるユーザ情報の一括登録・更新・削除を可能とすること。
職員アカウント管理システムの申請結果を反映できること。
既存システムとのシングルサインオン機能を維持すること。

9-2-2. 非機能要件

提案 Active Directory サーバは、最小権限と管理者アカウントの分離、不要な機能・通信の無効化、最新のセキュリティ更新、強固な認証、監査ログの集中監視等により要塞化すること。
提案耐障害性の高い構成とすること。

9-3. パッチ配信サーバ（WSUS）

9-3-1. 機能要件

OS 及びマイクロソフト社製のソフトウェアのパッチ配信を行うこと。
端末ごとのパッチ適用状況を把握できること。

9-3-2. 非機能要件

インターネット系及び LGWAN 系にパッチ配信サーバを導入すること。
約 10,000 台規模の端末へパッチ配信が可能な性能を有すること。

9-4. 資産管理機能

9-4-1. 機能要件

(1)　基本機能

端末のハードウェア、OS、ソフトウェア情報等を収集すること。

ログオン時にインベントリ収集を自動実行すること。
インベントリ情報を一覧表示及び出力できること。

(2) リモート操作

管理端末から業務端末を遠隔操作できること。
複数端末への同時接続及び操作が可能であること。
リモート操作時に、通信帯域を制限できること。リモート操作で画面を受信する際、画質等を落として通信データ量を抑制できること。

(3) ソフト配信

任意の業務端末へソフトウェアを配信できること。
配信対象及びタイミングを指定できること。
セキュリティパッチの配信が可能であること。
大容量データでも確実に配信可能であること。
任意指定端末や検索した資産情報リストを検索グループとして登録し、配布等の操作対象にできること。

(4) パッチ管理

OS 及びソフトウェアのパッチ管理を行うこと。
端末ごとのパッチ適用状況を把握できること。

(5) 脆弱性管理

各端末の脆弱性情報を収集できること。
脆弱性に基づく脅威度の判定を行えること。
優先度に応じた対策を実施できること。
高リスク端末に対する通信制御を実施できること。

(6) デバイス管理

提案 USB 等外部デバイスの利用制御を行うこと。
利用履歴を記録すること。
USB 等外部デバイスの装着日時とログオンユーザ名からデバイスの最終使用者を自動的に特定して表示できること。
提案 定期的な棚卸機能を提供すること。
ユーザ及び端末単位で制御設定が可能であること。

9-4-2. 非機能要件

約 10,000 台規模の端末を管理可能な性能を有すること。
インベントリ収集処理が業務利用に影響を与えないこと。
リモート操作の遅延が少なく実用的な応答性能を確保すること。
リモート操作の同時接続数に応じた性能を維持すること。
ネットワーク負荷を低減したソフト配信方式とすること。

9-5. Apex Central(Trend Micro 統合管理サーバ)

9-5-1. 機能要件

対応する Trend Micro 製品およびエンドポイントを登録し、稼働状態やバージョンを一元管理できること。
管理対象やグループ単位でセキュリティポリシーを設定・配布し、適用状況を確認できること。
管理対象製品が検出した脅威やセキュリティイベントを集約し、ダッシュボードで確認できること。
管理対象製品のログを収集・検索し、CSV 等への出力および外部システムへの転送ができること。
重大な脅威や異常を管理者へ通知し、検出状況や端末状態のレポートを作成できること。
パターンファイル等の更新状況を確認し、対応する管理タスクを実行できること。
管理者の役割に応じて操作権限を設定し、ログインや設定変更等の操作履歴を記録できること。

9-5-2. 非機能要件

必要なサービス提供時間において安定稼働し、障害時に所定時間内で復旧できること。
通信を暗号化し、管理者の認証・権限制御および操作履歴の記録ができること。

9-6. バックアップ

9-6-1. 対象サーバ

本委託業務で構築したオンプレミスサーバーおよび共通機能基盤上のサーバを対象とする。

9-6-2. 機能要件

提案サーバのバックアップを集中管理方式で実施すること。
障害時にデータ復元を可能とすること。
複数世代のバックアップを取得すること。
ファイル単位でリストアできること。

9-6-3. 非機能要件

業務継続に必要な時間内で復旧可能とすること。
定期的にバックアップ処理を実施すること。

9-6-4. 対象データ

対象データは以下のとおりとする。
サーバ上のデータ（業務データ・設定）
システム構成情報
アカウント情報（ID/ユーザ情報）
各種ログ情報（ログオン等）
サーバリソース／システム状態情報

9-7. ログ収集

9-7-1. 対象サーバ

対象サーバは以下のとおりとする。
庁内ドメインシステム（Active Directory）
ウイルス対策システム
運用管理システム（資産管理）
セキュリティパッチ配布システム

9-7-2. 機能要件

ログオン及びログオフの記録を取得すること。
認証失敗等の監査ログを取得すること。
提案任意条件でログ検索・抽出を可能とすること。
提案ログ分析機能を提供すること。

9-7-3. 非機能要件

提案ログを 1 年以上保存すること。
大量ログでも高速検索が可能であること。

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。

10-1. 対象者別研修等

10-1-1. 対象者

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. 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とすること。

(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、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) ライブ方式で実施する研修については、研修内容を録画し、職員が後日視聴することを許諾すること。録画を許諾しない場合は、同等の研修内容をオンデマンドで視聴でき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、1 回 3 時間程度の研修を 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) 加点運用・監視・保守業務は、本庁舎に常駐し、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。
NK 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用作業

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」に記載の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ておらず、かつ、メーカ又は保守委託先と機密保持契約を締結していることを前提として、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

第 3 期三重県 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 15 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 15 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

第 3 期三重県 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
第 3 期三重県 DX 推進基盤の仕様策定時（令和 13 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
第 3 期三重県 DX 推進基盤の調達時（令和 14 年度）	第 3 期三重県 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

対応時期	引継先	対応内容
第 3 期三重県 DX 推進基盤の設計・構築時（令和 14 年度）	第 3 期三重県 DX 推進基盤に関与する設計・構築事業者	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
第 3 期三重県 DX 推進基盤の移行時（令和 14 年度）	第 3 期三重県 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 14 年度に決定が予定される第 3 期三重県 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、第 3 期三重県 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