庁内ネットワーク情報基盤機器等の

賃貸借仕様書

令和6年8月

大阪府 財務部 行政ＤＸ推進課

目次

[第１ 定義 1](#_Toc174961550)

[第２ 概要 3](#_Toc174961551)

[１ 事業概要 3](#_Toc174961552)

[２ 業務範囲 3](#_Toc174961553)

[３ 賃貸借期間 3](#_Toc174961554)

[４ 納入場所 3](#_Toc174961555)

[５ 関係事業者 3](#_Toc174961556)

[６ 想定スケジュール 4](#_Toc174961557)

[７ その他 4](#_Toc174961558)

[第３ 機器等の仕様 6](#_Toc174961559)

[１ 調達機器等一覧 6](#_Toc174961560)

[２ 共通事項 7](#_Toc174961561)

[３ 個別仕様 9](#_Toc174961562)

[第４ 構築及び撤去 34](#_Toc174961563)

[１ 共通事項 34](#_Toc174961564)

[２ 管理 34](#_Toc174961565)

[３ 詳細設計 35](#_Toc174961566)

[４ 移行設計 62](#_Toc174961567)

[５ 配線／設置 64](#_Toc174961568)

[６ 設定 66](#_Toc174961569)

[７ テスト 80](#_Toc174961570)

[８ 移行 93](#_Toc174961571)

[９ 引継ぎ 98](#_Toc174961572)

[１０ 納品 99](#_Toc174961573)

[１１ 撤去 101](#_Toc174961574)

[１２ 役割分担 101](#_Toc174961575)

[第５ 保守及び技術支援 103](#_Toc174961576)

[１ 共通事項 103](#_Toc174961577)

[２ 保守内容 104](#_Toc174961578)

[３ 技術支援内容 105](#_Toc174961579)

[第６ 体制等 106](#_Toc174961580)

[１ 体制 106](#_Toc174961581)

[２ その他 106](#_Toc174961582)

# 定義

本業務における用語については、次の表のとおりとする。

表 １‑１　用語の定義

| **語句** | **定義** |
| --- | --- |
| 府 | 大阪府をいう。 |
| 部局 | 大阪府組織条例（昭和28年大阪府条例第1号）第1項に規定する副首都推進局並びに同条例第2項に規定する部及び局並びに大阪府会計管理者の補助組織設置規則（平成19年大阪府規則第7号）に規定する会計局をいう。 |
| 部局等 | 部局、地方自治法（昭和22年法律第67号）第180条の5第1項に規定する委員会及び委員の事務局、同法第180条の5第2項第2号から第5号に規定する委員会の事務局及び地方自治法第138条第1項に規定する議会事務局をいう。 |
| 室課等 | 部局等における室、課及び出先機関をいう。 |
| ＤＸ推進課 | 大阪府財務部行政ＤＸ推進課をいう。 |
| 教育庁 | 大阪府教育委員会通則（昭和二十四年大阪府教育委員会規則第一号）第一条に規定する大阪府教育庁をいう。 |
| 本館 | 大阪府庁本館をいう。 |
| 別館 | 大阪府庁別館をいう。 |
| 新別館 | 大阪府庁新別館をいう。北館と南館に分かれている。 |
| 大手前庁舎 | 本館、別館及び新別館をいう。 |
| DC | ＤＸ推進課が調達したデータセンターをいう。 |
| SC | 大阪版自治体情報セキュリティクラウドのことをいう。 |
| LGWAN | 地方公共団体情報システム機構が運用する総合行政ネットワークをいう。地方公共団体間を接続する閉域ネットワーク網であり、国の各省庁間を接続する政府共通ネットワークとも相互に接続している。 |
| 個人番号利用事務系ネットワーク | 行政手続における特定の個人を識別するための番号の利用等に関する法律に定義される個人番号利用事務を行うための専用ネットワークをいう。LGWAN接続系ネットワーク及びインターネット接続系ネットワークとは分離された構成である。 |
| LGWAN接続系ネットワーク | LGWANに接続するための専用ネットワークをいう。個人番号利用事務系ネットワーク及びインターネット接続系ネットワークとは分離された構成である。 |
| インターネット接続系ネットワーク | 庁内の情報システム及びインターネット利用等のサービスを提供するためのネットワークをいう。個人番号利用事務系ネットワーク及びLGWAN接続系ネットワークとは分離された構成である。 |
| 庁内ネットワーク | 大阪府の自治体業務を遂行するために、ＤＸ推進課が府の管理する施設内に整備するネットワークをいう。個人番号利用事務系ネットワーク、LGWAN接続系ネットワーク及びインターネット接続系ネットワークを含む。 |
| 庁内ネットワーク機器等 | 庁内ネットワークを構成するスイッチ、ルータ、ファイアウォール、各種サーバ、負荷分散装置、帯域制御装置、監視装置、クラウドサービス、終端装置等をいう。 |
| インターネット接続系端末機 | インターネット接続系ネットワークに接続される端末機をいう。特に指定がない場合は、物理端末機を指す。 |
| 個人番号利用事務系端末機 | 個人番号利用事務系ネットワークに接続される端末機をいう。特に指定がない場合は、物理端末機を指す。 |
| LGWAN接続系端末機 | LGWAN接続系ネットワークに接続される端末機をいう。特に指定がない場合は、物理端末機を指す。 |
| 職員端末機 | ＤＸ推進課が職員に配備する物理端末機をいう。 |
| 独自調達端末機 | 室課等が独自に調達した物理端末機をいう。 |
| 職員端末機等 | 職員端末機及び独自調達端末機をいう。特に指定がない場合は物理端末機を指す。なお、台数は約11,000台ある。 |
| 税務情報端末機 | 個人番号利用事務系端末機のうち、大阪府財務部税務局税政課が調達及び管理し、税所属に配備する独自調達端末機をいう。 |
| AD | Microsoft Active Directoryを用いた庁内の認証基盤をいう｡ |
| Microsoft 365 | Microsoftが提供するOfficeアプリケーション、クラウドサービス、セキュリティサービスを包括して提供するサービスをいう。 |
| 情報基盤 | 庁内共通で利用する職員認証、メール・カレンダーサービス、庁内ポータル、職員端末機の運用管理等を行うための電子計算機及び情報システム並びにこれに類するものをいう。 |
| ICT基盤 | 大阪府における自治体業務を行うためのICT環境を構成するネットワーク、端末機、情報基盤、セキュリティサービス等の、ハードウェア、ソフトウェア及びサービス全般をいう。 |
| 休日 | 大阪府の休日に関する条例（平成元年大阪府条例第2号）第2条第1項各号に規定する休日をいう。 |
| 開庁日 | 休日以外の日をいう。 |
| 夜間 | 18時から翌日の9時までの間をいう。 |
| 調達機器 | 本業務で調達する機器をいう。 |
| 調達ソフトウェア | 本業務で調達するソフトウェアをいう。ファームウェア及びOSを含む。 |
| 調達機器等 | 調達機器及び調達ソフトウェアをいう。 |

# 概要

## 事業概要

府では、行政事務遂行のためのICT環境として、庁内ネットワーク情報基盤機器等を整備している。

本業務は、庁内共通で利用する職員認証、電子メール、庁内ポータルなどの機能を提供する情報基盤、及び個人番号利用事務系情報基盤の賃貸借期間が令和7年9月末に満了することに伴い、当該機器等を更新するものである。

更新対象となる機能は、［別紙１ 大阪府ICT基盤機能配置図］に記載する。Microsoft 365 E3 ライセンスは本業務とは別の調達にて機器更新する。

## 業務範囲

本業務は、庁内ネットワーク情報基盤機器等に必要な機器の賃貸借及びソフトウェア・サービスの調達並びにこれらの詳細設計、設置、設定、移行、保守等を行うものである。

調達機器により更新する庁内ネットワーク情報基盤機器等の概要を［別紙２ 庁内ネットワーク情報基盤機器等構成概要］及び［別紙３ 庁内ネットワーク情報基盤機器等全体概要図］に示す。

## 賃貸借期間

令和7年10月1日から令和13年9月31日まで（72箇月）

## 納入場所

「第３ 機器等の仕様 １ 調達機器等一覧」の設置場所を参照。

## 関係事業者

本業務を行うに当たっては、府及び本業務とは別に契約した以下に示す各事業者（以下「府等」という。）と緊密に連携及び協力して行うこと。

### 設計事業者

調達機器を含むICT基盤の全体設計、基本設計（機器のポートアサイン、機器への詳細な設定値等の設計は除く。）、移行作業（所属用ファイルサーバ、庁内Webサイト、利用者管理システム）、施工管理等の業務を行う。

### 運用事業者

調達機器の運用時における設定変更等の業務を行う。調達機器に係る運用手順等に関して引継ぎが必要となる。

### DCハウジング事業者

調達機器に係るハウジングサービスを提供する。調達機器の設置及び接続を行うに当たり、調整が必要となる。

### 監視事業者

本業務で調達した機器の運用時の死活監視業務を行う。本業務で調達する機器等に係る監視設定に際して調整が必要となる。

## 想定スケジュール

想定スケジュールは、以下のとおり。詳細は、［別紙４ 工程表］に示す。

表 ２‑１　想定スケジュール

|  |  |  |
| --- | --- | --- |
| **項目番号** | **作業項目** | **想定時期** |
| 1 | 契約締結 | 令和7年1月 |
| 2 | 詳細設計／移行設計 | 令和7年2月～4月 |
| 3 | 配線／設置 | 令和7年3月～4月 |
| 4 | 設定 | 令和7年4月～6月 |
| 5 | 移行 | 令和7年6月～9月 |
| 6 | 引継ぎ／納品 | 令和7年8月～9月 |
| 7 | 賃貸借／保守／技術支援 | 令和7年10月～令和13年9月 |

## その他

Microsoft 365利用に必要なライセンスやサービスは本業務の対象外であるが、以下の要件を基に設計、設定、移行を考慮すること。

### 利用するための前提事項は以下のとおりとする。

#### 提供されるサービスの利用対象者は府が調達するMicrosoft 365 E3ライセンスを保有しており、それを利用する。

#### Microsoft 365機能との通信に必要な専用線（ExpressRoute）については、別途調達するクラウド接続閉域網回線サービスにより提供される。

### Exchange Onlineを利用し、メール及び予定表機能を提供できること。また、オンプレミスに構築した庁内メールサーバとハイブリッド環境を構築できること。

### Exchange Onlineを利用し、会議室の作成、予約、更新ができること。

### Teamsを利用し、コミュニケーション機能を提供すること。

### SharePoint Online にて、Web機能を提供すること。

### OneDrive for Businessにて個人ドライブ機能を提供すること。

### Apps for Enterprise にてOffice機能を提供すること。

### Microsoft Entra IDの条件付きアクセスにてアクセス制限ができること。

### 庁内ADと連携し、ディレクトリ同期サーバにより、Microsoft Entra IDの利用アカウントを自動的に登録できること。また、同期間隔を設定可能であること。

### Azure Information Protectionにより、暗号化の機能を提供すること。

# 機器等の仕様

## 調達機器等一覧

以下に、本業務で調達する機器等とその数量を示す。

表 ３‑１　調達機器等一覧

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **項目番号** | **名称** | **数量** | **設置場所** | **保守区分** |
| 1 | 庁内ネットワーク情報基盤仮想基盤サーバ | 10台 | DC |  |
| 2 | ラックコンソール関連機器 | 1式 |  |
| 3 | 庁内ネットワーク統合ストレージ | 1台 |  |
| 4 | 所属用ファイルサーバ | 一式 |  |
| 5 | ファイル送受信サーバ | 6台 |  |
| 6 | サーバ集約スイッチ | 2台 |  |
| 7 | 管理用スイッチ | 4台 |  |
| 8 | 保守用端末 | 4台 | ② |
| 9 | 負荷分散装置 | 2台 |  |
| 10 | 個人番号利用事務系物理端末 | 50台 | 各設置拠点　※ |  |
| 11 | 静脈認証センサー | 2,100台 |  |

※設置場所と台数については［別紙5　個人番号利用事務系関連機器　設置場所一覧］のとおり。

表 ３‑２　仮想サーバ一覧

| **項目番号** | **名称** | **数量** | **設置場所** |
| --- | --- | --- | --- |
| 1 | 庁内ADサーバ | 7台 | DC |
| 2 | LGWAN接続系ADサーバ | 2台 |
| 3 | SC連携用ADサーバ | 1台 |
| 4 | 共通基盤用ADサーバ | 1台 |
| 5 | 検証用ドメインコントローラ | 2台 |
| 6 | ディレクトリ同期サーバ | 1台 |
| 7 | テスト用ディレクトリ同期サーバ | 1台 |
| 8 | 庁内Webサーバ | 1台 |
| 9 | 庁内Web移行用サーバ | 2台 |
| 10 | ターミナルサーバ | 1台 |
| 11 | 利用者管理システムWebサーバ(本番、テスト) | 3台 |
| 12 | 利用者管理システムDBサーバ(本番、テスト) | 3台 |
| 13 | 利用者管理システムサーバ(開発) | 1台 |
| 14 | ジョブ管理サーバ | 1台 |
| 15 | 仮想基盤管理サーバ | 1台 |
| 16 | 職員端末機等中央管理サーバ | 1台 |
| 17 | 職員端末機等サイトサーバ | 2台 |
| 18 | 庁内メールサーバ | 2台 |
| 19 | テスト用庁内メールサーバ | 1台 |
| 20 | 全文検索サーバ | 6台 |
| 21 | 全文検索管理サーバ | 1台 |
| 22 | ファイルサーバ可視化サーバ | 1台 |
| 23 | ファイル無害化サーバ | 1台 |
| 24 | 添付ファイル分離ワークサーバ | 2台 |
| 25 | 添付ファイル分離管理サーバ | 2台 |
| 26 | サーバパッチ管理サーバ[Windows] | 1台 |
| 27 | サーバパッチ管理サーバ[Linux] | 1台 |
| 28 | サーバログ管理サーバ | 1台 |
| 29 | サーバログ保管サーバ | 4台 |
| 30 | ウイルス対策管理サーバ | 1台 |
| 31 | ウイルス対策配信サーバ | 1台 |
| 32 | バックアップ管理サーバ | 1台 |
| 33 | バックアップ転送サーバ | 1台 |
| 34 | バックアップ保護サーバ | 1台 |
| 35 | 運用監視サーバ | 1台 |
| 36 | 議会等Proxyサーバ | 1台 |
| 37 | 庁内ADサーバ(個番・税) | 4台 |
| 38 | 個人番号利用事務系運用管理サーバ | 1台 |
| 39 | 生体認証サーバ | 4台 |
| 40 | Office認証用Pacサーバ | 1台 |

表 ３‑３　調達サービス一覧

|  |  |  |  |
| --- | --- | --- | --- |
| **項目番号** | **名称** | **数量** | **設置場所** |
| 1 | バックアップ用クラウド環境 | 1台 | クラウド |

## 共通事項

### 調達機器は、公告日以降において製品カタログ等に記載されており、かつ、製造を行っているもので、未使用のものであること。

### 数量が2以上のものについては、全て同一機種（製品）であること。

### 大阪府グリーン調達方針に該当する機器は、公告日以降における最新版の「判断基準」に適合したものであること。

【URL】<https://www.pref.osaka.lg.jp/o120020/chikyukankyo/jigyotoppage/greenchotatsu.html>

### 調達機器のOSとしてLinux OSを採用する場合は、導入実績があり、セキュリティパッチや更新プログラムの提供等のサポートが行われている商用のディストリビューターのパッケージから選定すること。また、拡張プラスサポートを採用し、賃貸借期間中のアップデート回数を少なくすること。

### 調達ソフトウェアは、府に使用権があり、賃貸借期間中は適法に使用できること。ライセンス契約のあるものについては、府を契約者とすること。ユーザ登録が必要な場合は、府をユーザとして登録すること。

### OS、サーバ仮想化のハイパーバイザー及び仮想サーバのライセンスは、他のサーバに移動する際においても、制約なく適法に使用できること。

### 調達ソフトウェアは、最新バージョンであること。ただし、機器、他のソフトウェア又は既存環境と整合させるに当たり、最新バージョンでは技術面又はサポート面で問題が生じる場合は、府（以下「設計事業者等」という。）と協議の上、ダウングレードして導入すること。

### 調達機器等は、賃貸借期間中は製造元、販売代理店等の保守を受けることができるものであること。

### 調達機器の設置のために必要な付属物（ラックレール、ラック取付けネジ、ラック用棚板、固定金具等をいう。以下同じ。）及び調達機器の接続のために必要なケーブル類（電源ケーブル、電源タップ、LANケーブル、光ファイバーケーブル、Stackケーブル等をいう。以下同じ。）は、受注者が用意すること。

なお、本業務により新規に敷設するLANケーブルは、カテゴリ6A以上のツイストペアケーブルを使用すること。ただし、詳細設計で拡張性を考慮しても対応速度が1Gbpsで十分と判断された箇所については、カテゴリ6以上でも良いものとする。また、本業務により新規に敷設する光ファイバーケーブルは、シングルモードの場合はOS1、マルチモードの場合はOM4を使用すること。

### 機器構成等の仕様適合を確認するため、仕様適合証明書の添付書類として、以下の資料を開札時に提出すること。

#### 納入機器等構成表

［表 ３‑１　調達機器等一覧］の項目ごとに、対応する納入機器等とその数量が確認できること。

#### 納入機器等仕様適合確認表

［３ 個別仕様］の項目ごとに、製品カタログ等の記載箇所を指し示す等により、納入予定の機器等が仕様を満たしていることを一覧で確認できること。

#### ラック構成図

##### ラックごとの各調達機器の配置及び重量が確認できること。

##### 各調達機器の消費電力が確認できること。

なお、消費電力の単位については、W又はKVAで記載することとし、カタログ値の場合は、その旨を記載すること。

### クラウドサービスは以下の要件を満たすこと。

#### クラウド環境については、利用する環境を国内に設置すること。

#### クラウドサービスにおける情報資産の取扱いについては、日本の法律を準拠するものとし、クラウドサービスに係る争訟においても裁判管轄は国内に限ること。

#### セキュリティ基準の要件として、以下3項目のいずれかを満たすこと。

##### 「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 : ISMAP）」に登録されていること。

##### ICPA（米国公認会計士協会）SOC2又はSOC3 に認定されていること。

##### ISO/IEC 27017:2015を取得していること。

#### クラウドサービス契約期間中、及び利用終了後は情報資産が残留して漏えいすることが無いよう、必要な措置が講じられていること。また、クラウドサービス上のデータを復元不可能な状態にできること。

#### クラウドサービス上に保存した情報資産について、原則としてクラウドサービス提供者が参照、更新等できないこと。また、保存した情報資産を他のクラウドサービスに移行できること。障害調査等において、クラウドサービス提供者が情報資産を参照する必要がある場合は、受注者から府に説明の上で府が承認した場合に限り可能とする。

#### サービス提供は原則年間通じて24時間とする。ただし、受注者又はクラウドサービス提供者の都合により、設備メンテナンス等によるサービスの計画停止が必要となった場合は、運用事業者、設計事業者及び府（以下「運用事業者等」という。）へ停止日時を事前に連絡し、メンテナンス等を実施すること。

### マイクロソフト社製のソフトウェアのライセンス契約、発注方法等は、事前に問合せること。問合せ先は、以下のとおり。

【問合せ先は入札公告時に記載する。】

## 個別仕様

### 庁内ネットワーク情報基盤仮想基盤サーバ

#### ハードウェア

##### 19インチラックにマウント可能であること。

##### 100Vの電圧に対応した機器であること。

##### 動作温度が10℃～35℃に対応していること。

##### 最大消費電力は1,300W以下であること。

##### CPUの動作周波数は、2.10Ghz以上、コア数は64コア以上であること。1基で仕様を満たせない場合は、2基以上搭載することで仕様を満たすこととしても良い。

##### メモリは256GB以上であること。

##### OSが導入できるシステム領域として、M.2 Flashモジュールを実装し、実効容量は240GB以上とすること。

##### DVD-ROMドライブを装備すること。内蔵できない場合は、外付けとしても良い。

##### IEEE 802.3anとして標準化された10GBASE-Tイーサネットのインターフェイスを8ポート以上有していること。

##### ホットプラグ対応の電源ユニットを2基以上搭載し、冗長構成であること。

##### ホットプラグ対応の冷却ファンを2基以上搭載し、冗長構成であること。

##### ハードウェアの故障を検知し、メールで通知できる機能を有すること。

##### 専用のメンテンスポートを搭載し、以下の機能を有すること。

###### サーバ装置に組み込まれたOS環境に依存しない管理ツールにてサーバ管理が行えること。

###### 管理ツールのWeb GUIよりサーバ装置の電源投入等のリモート操作が行えること。

###### 電源ユニットや冷却ファン等の構成表示や障害監視が行えること。

###### バーチャルCD/DVDといったリモートデバイス機能を有すること。

###### NTPサーバとの時刻同期機能を有すること。

#### ソフトウェア

##### ハイパーバイザーはVMware ESXi vSphere、Microsoft　Hyper-V、Nutanix AHVよりいずれかを利用する。

##### 論理仮想スイッチ機能を有すること。

##### ホストの単一障害により停止した仮想マシンを他の正常なホスト上で再稼働する機能を有すること。

##### 再稼働時の仮想マシンの起動順序を設定できる機能を有すること。

##### オペレーションにより、オンラインで他の正常なホスト上へ仮想マシンを移動できる機能を有すること。

##### 仮想マシンの構成変更が必要となった際に、仮想CPU・メモリ・NICの割当量等を変更できる機能を有すること。

##### 仮想マシンに割り当てるCPU及びメモリのリソースは、物理リソースの予約及び上限値設定（制限）並びに複数仮想マシン間での相対値設定（シェア値）の設定ができること。

##### 仮想マシンに対し、ホストに実装されている物理的なCPU及びメモリのリソース量よりも多くのリソースを仮想的に割当可能なオーバーコミット機能を有すること。

##### 論理的なネットワークリソース毎にネットワークI/O性能を制御する機能を有すること。

### ラックコンソール関連機器

#### ハードウェア

##### サーバ装置を設置するラックには、ラックマウント型 17 インチ以上カラー液晶ディスプレイ/キーボード付きを準備すること。また、100Vの電圧に対応した機器であること。

##### 16ポート用KVMスイッチを1台準備すること。また、100Vの電圧に対応した機器であること。

##### 切替えケーブルを10本以上準備すること。

### 庁内ネットワーク統合ストレージ

#### ハードウェア

##### 19インチラックにマウント可能であること。

##### 内蔵記憶装置は、SASディスク以上の性能を持つこと。一つの筐体で要件を満たせない場合は、拡張シェルフを増設することを可とする。

なお、実効容量は圧縮及び重複排除により50%以上の削減が図れることを前提とした上で372TB以上の実効容量を確保すること。また、一部業務用にSSDディスクを実効容量12TB確保すること。

##### 100Vの電圧に対応した機器であること。

##### 動作温度が10℃～35℃に対応していること。

##### 拡張シェルフを含めた最大消費電力が4,000W以下であること。

##### Active/Active構成のストレージコントローラを搭載し、フェイルオーバー構成及びマルチパスI/Oによるデータパスの冗長化が可能であること。

##### メモリは256GB以上、不揮発性メモリは32GB以上であること。

##### 停電が発生した場合、不揮発性メモリの内容をストレージに退避し、データの損失を防ぐ機能を有すること。

##### 内蔵記憶装置はパリティ方式のデータ保護機能を有し、2重障害時にもデータを消失しない機能を有すること。

##### 以下の要件を満たす、IEEE 802.3ccとして標準化された25GBASE-LRイーサネットのインターフェイスを8ポート以上有していること。

###### シングルモードであること

###### 帯域幅は25Gbpsであること

###### LCコネクタ形状であること

###### 伝送距離は10kmであること

##### 3層分離の考え方に基づき、ファイルサーバ機能を論理的に分離する機能を有していること。

##### ADと連携し所属しているユーザ及びグループ単位で、ボリュームに対して容量制限ができるQuota機能を有すること

##### NFSv3、NFSv4 をサポートすること。

##### SMB2.0/2.1/3.0/3.1 をサポートすること。

##### 専用OSであること。Windows、Linux OS などの汎用OSの利用は不可とする。また、１ストレージシステムで複数種のOSが搭載されている製品は不可とする。

##### ボリュームの新規作成や容量変更（拡張及び縮小）がシステム無停止で行える機能を有すること。また、ボリュームの容量縮小で空いた領域を再利用できること。

##### ボリューム、ファイル等に対し、パフォーマンスの上限をIOPS及びスループットで指定可能な QoS 機能を有すること。また、QoS 機能として最低性能保証値について指定できること。

##### ボリュームは、全体ボリュームの空き容量に依存することなく、実際の空き容量を超えたサイズでも作成できる機能を有すること。

##### SMTPベースの監視機能を搭載していること。また、定期的にシステムの状態を送信可能であり、重大な障害が発生した場合に管理者へメール通知が可能であること。

##### 別の専用装置等を必要とせず、ブロック単位での重複排除（Deduplication）及び圧縮（Compression）の機能を有すること。

##### 単一あるいは複数のストレージシステムを一元管理するために日本語対応のWebブラウザベース GUI 管理機能を有すること。

##### 不揮発性メモリを利用してディスク書込みのパフォーマンスを向上できる機能を有すること。

##### システム無停止で、特定の時点でのバックアップイメージを取得できるスナップショット機能を有すること。

##### システム無停止でスナップショット領域の拡張及び縮小可能であること。

##### スナップショットを作成している間もサービスを継続して行えること。

##### スナップショットはスケジュール機能等により自動的に作成できること。

#### 管理機能

##### 障害・閾値超過などをイベントで管理できること。

##### パフォーマンス監視機能とパフォーマンスイベントの根本原因分析機能を有すること。

##### 各種レポートの表示、カスタマイズ、スケジュール設定を可能とするレポーティング機能を有すること。

##### (ｱ)～(ｳ)の機能を実現するためにソフトウェアが必要となる場合は、必要に応じて仮想サーバを仮想化基盤上に構築すること。仮想サーバを追加する場合は、他の仮想サーバに影響がないように仮想化基盤のリソースを調整すること。

### 所属用ファイルサーバ

#### ハードウェア

##### 19インチラックにマウント可能であること。

##### 内蔵記憶装置は、SASディスク以上の性能を持つこと。SSDも可とする。一つの筐体で要件を満たせない場合は、筐体又は拡張シェルフを増設することを可とする。

なお、業務容量は重複排除前・非圧縮状態において令和7年10月時点で400TBの容量を確保すること。令和7年度以降各年度末に16TB以上追加し、令和12年度末で496TB以上を確保すること。

業務容量にはスナップショット用の容量は含まれておらず、別途確保すること。

各年度末において、本機の圧縮機能及び重複排除機能によっても、仕様に定めた業務容量が確保できない場合は、適宜記憶媒体を追加し業務容量を確保すること。追加に要する費用は受注者の負担とする。

階層型ストレージ機能を利用してもよいものとする。階層型ストレージの場合、低アクセス頻度階層はニアラインSASディスク以上の性能を持つディスクで構成し、フラグメンテーション領域を考慮し、必要な業務容量を確保すること。低アクセス頻度階層は、全体の業務容量の70％未満とすること。

##### 100Vの電圧に対応した機器であること。

##### 動作温度が10℃～35℃に対応していること。

##### 拡張シェルフを含めた機器一式の最大消費電力が5,100W以下であること。

##### Active/Active構成のストレージコントローラを搭載し、フェイルオーバー構成及びマルチパスI/Oによるデータパスの冗長化が可能であること。Active/Standby構成も可とするが、この場合フェイルオーバーによるダウンタイムは1秒以内であること。

##### メモリは1筐体あたり256GB以上、不揮発性メモリは32GB以上であること。なお、階層型ストレージ機能を利用し、低アクセス頻度のデータ階層を別筐体にて構成する場合は、低アクセス頻度階層用の筐体は、メモリは64GB以上、不揮発性メモリは8GB以上であること。

##### 停電が発生した場合、不揮発性メモリの内容をストレージに退避し、データの損失を防ぐ機能を有すること。

##### 内蔵記憶装置はパリティ方式のデータ保護機能を有し、2重障害時にもデータを消失しない機能を有すること。

##### IEEE 802.3ccとして標準化された25GBASE-LRイーサネットのインターフェイスを8ポート以上有していること。なお、階層型ストレージ機能を利用し、低アクセス頻度のデータ階層を別筐体にて構成する場合は、低アクセス頻度階層用の筐体はIEEE 802.3anとして標準化された10GBASE-Tイーサネットのインターフェイスを8ポート以上有していること

##### ３層分離の考え方に基づき、ファイルサーバ機能を論理的に分離する機能を有していること。

##### ADと連携し所属しているユーザ及びグループ単位で、ボリュームに対して容量制限ができるQuota機能を有すること

##### NFSv3、NFSv4 をサポートすること。

##### SMB2.0/2.1/3.0/3.1 をサポートすること。

##### 専用OSであること。Windows、Linux OS などの汎用OSの利用は不可とする。また、１ストレージシステムで複数種のOSが搭載されている製品は不可とする。

##### ボリュームの新規作成や容量変更（拡張及び縮小）がシステム無停止で行える機能を有すること。また、ボリュームの容量縮小で空いた領域を再利用できること。

##### ボリューム、ファイル等に対し、パフォーマンスの上限をIOPS及びスループットで指定可能な QoS 機能を有すること。また、QoS 機能として最低性能保証値について指定できること。

##### ボリュームは、全体ボリュームの空き容量に依存することなく、実際の空き容量を超えたサイズでも作成できる機能を有すること。

##### SMTPベースの監視機能を搭載していること。また、定期的にシステムの状態を送信可能であり、重大な障害が発生した場合に管理者へメール通知が可能であること。

##### 別の専用装置等を必要とせず、ブロック単位での重複排除（Deduplication）及び圧縮（Compression）の機能を有すること。

##### 単一あるいは複数のストレージシステムを一元管理するために日本語対応のWebブラウザベース GUI 管理機能を有すること。

##### 不揮発性メモリを利用してディスク書込みのパフォーマンスを向上できる機能を有すること。

##### システム無停止で、特定の時点でのバックアップイメージを取得できるスナップショット機能を有すること。

##### システム無停止でスナップショット領域の拡張及び縮小可能であること。

##### スナップショットを作成している間もサービスを継続して行えること。

##### スナップショットはスケジュール機能等により自動的に作成できること。

#### 管理機能

##### 障害・閾値超過などをイベントで管理できること。

##### パフォーマンス監視機能とパフォーマンスイベントの根本原因分析機能を有すること。

##### 各種レポートの表示、カスタマイズ、スケジュール設定を可能とするレポーティング機能を有すること。

##### (ｱ)～(ｳ)の機能を実現するためにソフトウェアが必要となる場合は、必要に応じて仮想サーバを仮想化基盤上に構築すること。仮想サーバを追加する場合は、他の仮想サーバに影響がないように仮想化基盤のリソースを調整すること。

### ファイル送受信サーバ

#### ハードウェア

##### ファイル送信時においてファイル無害化サーバとの連携が可能であること。

##### 承認者による承認が可能であること。また、承認者は利用者毎に設定可能であること。

##### サーバはハードウェアにて冗長構成とし、システム障害時は残るハードウェアにて機能の継続提供するよう自動で切り替えが可能であること。

##### ユーザ名/パスワードの入力を不要とするよう府にて利用している共通ドメインのアカウントにてシングルサインオンを利用できること。

##### アップロードされたファイルの保持期間が過ぎた場合において、ファイル自動削除機能を有すること。

##### 利用者端末にエージェントをインストールすることなく、ブラウザのみにて利用可能とすること。

##### 庁内の利用者管理システムより出力されたcsvを取り込むことによりユーザ登録及び承認者設定が可能であること。

##### アップロード、ダウンロード、承認、無害化等のログの取得が可能であること。

##### ファイル送受信サーバについて、インターネット接続系、LGWAN接続系、個人番号利用事務系の3層間にサーバを構成し、以下要件を実現すること。

###### インターネット接続系/LGWAN接続系

インターネット接続系、LGWAN接続系の2層間でのファイルの送受信が可能であること。

ユーザ数は3,400以上利用可能であること。

###### インターネット接続系/個人番号利用事務系

インターネット接続系、個人番号利用事務系の2層間でのファイルの送受信が可能であること。

ユーザ数は3,400以上利用可能であること。

###### 個人番号利用事務系/LGWAN接続系

個人番号利用事務系、LGWAN接続系の2層間でのファイルの送受信が可能であること。

ユーザ数は2,000以上利用可能であること。

##### 上記要件を満たす場合は仮想サーバとして、庁内ネットワーク情報基盤仮想基盤サーバ上に構成することも可とする。

### サーバ集約スイッチ

#### ハードウェア

##### 19インチラックにマウント可能であること。

##### 100Vの電圧に対応した機器であること。

##### 動作温度が10℃～35℃に対応していること。

##### 最大消費電力は1,100W以下であること。

##### 400Mpps以上のIPv4パケット転送能力を有すること。

##### 9,000バイト以上のジャンボフレームに対応していること。

##### 専用のスタックポートを有し、2台以上のスイッチを論理的に1台とするスタック接続機能を有すること。

##### スタックされた全ての筐体は1台の論理ユニットとして設定・管理できること。

##### 搭載する全てのインターフェイスを最大速度として利用する場合に、ノンブロッキングで処理できるスイッチング容量を有すること。

##### SFP+インターフェイスを8ポート以上有し、2台のアプリケーションサーバ集約スイッチをスタックした構成で16ポート以上有していること。

##### SFP+インターフェイスは、1000BASE-SX/LX/ZX及び10GBASE-LR/SR/LRMに対応可能であること。

##### 2台のアプリケーションサーバ集約スイッチをスタックした構成で、IEEE 802.3anとして標準化された10GBASE-Tイーサネットインターフェイスを48ポート以上有していること。

##### 2台のアプリケーションサーバ集約スイッチをスタックした構成で、IEEE 802.3aeとして標準化された10GBASE-SRイーサネット用SFP+トランシーバを4個以上搭載すること。

##### VRF-lite機能を有すること。登録できるVRF数は256以上であること。

##### IPv4の静的ルーティングと動的ルーティングプロトコルとしてOSPF及びBGPに対応していること。

##### IPv4ルーティングテーブルのエントリー数が30,000以上であること。

##### IEEE802.1Q VLAN Tagging機能を有すること。

##### 4,000以上のVLAN IDに対応していること。

##### IEEE802.3ad リンクアグリゲーション機能を有すること。

##### 複数のスイッチをスタックした構成で、異なるスタックスイッチ間でリンクアグリゲーション構成が可能であること。

##### IEEE802.1d、IEEE802.1w及びIEEE802.1sに準拠したスパニングツリー機能を有すること。

##### BPDUの受信時にスパニングツリーPortFast対応インターフェイスをシャットダウンして、予期せぬトポロジループを阻止する機能を有すること。

##### ネットワーク管理者の制御下にないエッジデバイスがスパニングツリープロトコルのルートノードになることを阻止する機能を有すること。

##### ポート単位のブロードキャスト、マルチキャスト及びユニキャストのストーム制御機能を有すること。

##### 送信元及び受信元のMACアドレスに基づくパケットフィルタリング機能を有すること。

##### 送信元及び受信元のIPアドレス、ICMP及びTCP/UDPポート番号又はこれらの任意の組み合わせに基づくパケットフィルタリング機能を有すること。

##### 光ファイバーケーブル及びツイストペアケーブルの単一方向リンク（片対障害）検出機能を有すること。

##### ポートにてリンクフラップ等の障害を検知した際、ポートを一時的に使用不可能な状態にし、さらに一定時間経過後、自動的に再度利用可能にする機能を有すること。

##### 学習可能なMACアドレス数は30,000以上であること。

##### トラフィック解析のためのポートのミラーリング機能を有すること。

##### 同一筐体内や他の筐体へVLANを使いミラーリングできる機能を有すること。

##### 設定情報をFTPでアップロード及びダウンロードが可能であること。

##### NTPクライアント機能を有すること。

##### SNMP Trap通知機能を有すること。

##### Syslogサーバにメッセージを送信可能であること。

##### 設定・管理用の通信プロトコルとしてSSHに対応し、ネットワーク上の端末機の端末エミュレータからコマンドライン入力による操作が可能であること。

##### パスワード及び特権レベルの設定により、不正なユーザがスイッチの構成を変更することを阻止できる機能を有すること。

### 管理用スイッチ

#### ハードウェア

##### 19インチラックにマウント可能であること。

##### 100Vの電圧に対応した機器であること。

##### 動作温度が0℃～50℃に対応していること。

##### 最大消費電力は80W以下であること。

##### IEEE 802.3anとして標準化された10GBASE-Tイーサネットのインターフェイスを4ポート以上及びIEEE 802.3anとして標準化された10GBASE-Tイーサネットのインターフェイスを44ポート以上有していること。

##### IEEE802.1Q VLAN Tagging機能を有すること。

##### 4,000以上のVLAN IDに対応していること。

##### IEEE802.1d、IEEE802.1w及びIEEE802.1sに準拠したスパニングツリー機能を有すること。

##### BPDUの受信時にスパニングツリーPortFast対応インターフェイスをシャットダウンして、予期せぬトポロジループを阻止する機能を有すること。

##### NTPクライアント機能を有すること。

##### SNMP Trap通知機能を有すること。

##### Syslogサーバにメッセージを送信可能であること。

##### 設定・管理用の通信プロトコルとしてSSHに対応し、ネットワーク上の端末機の端末エミュレータからコマンドライン入力による操作が可能であること。

##### パスワード及び特権レベルの設定により、不正なユーザがスイッチの構成を変更することを阻止できる機能を有すること。

### 保守用端末

#### ハードウェア

##### ノートブック型であること。

##### 重量は2,100g以下であること。

##### CPUは同一の測定指標として、インテル® Core™ i3-1215U プロセッサー以上の性能を有すること。

##### セキュリティチップは、TCG Ver2.0に準拠したセキュリティチップを搭載すること。

##### メインメモリは、8GB以上を装備すること。

##### 内蔵記憶媒体はSSDとし、容量256GB以上のものを装備すること。

##### IEEE 802.3ab として標準化された1000BASE-Tイーサネットインターフェイスを1ポート以上内蔵すること。

##### USBポートは、3ポート以上を装備すること。また、そのうちType-Aポートを2ポート以上及びType-Cポートを1ポート以上有すること。

##### キーボードは日本語キーボードとし、キーピッチが18.4mm以上であること。

##### 外部ディスプレイ出力端子として、HDMI端子を装備すること。

##### USB Type-Aにて接続できる、有線レーザー式マウスを装備すること。

##### ディスプレイは、15インチ以上16インチ以下とし、ワイドTFT液晶で最大解像度を1920×1080以上とすること。また、ディスプレイには反射防止の処理がされていること。

##### 無線LAN機能を有すること。規格はIEEE802.11ax/ac/a/b/g/n対応、Wi-Fi準拠のこと。

##### 内蔵バッテリーを装備すること。バッテリーでの駆動が8時間以上稼働する性能を有すること。

##### タッチパッドを装備すること。タッチパッド機能は装備するマウスの接続時に自動で停止できること。また、タッチパッド機能単独での、常時使用、常時停止の設定も可能であること。

##### 内蔵マイクを装備すること。

##### 解像度について、フロント及びリア共に有効画素数約92万画素（720P）相当以上に対応したwebカメラを内蔵すること。

##### 100Vの電圧に対応した機器であること。

##### 動作温度が5℃～35℃に対応していること。

#### ソフトウェア

##### Microsoft Windows 11 Enterprise（64bit）相当以上 の 権利 を有すること 。なお、賃貸借期間中にサポートが切れた場合は、後継バージョンにアップグレードする権利を有すること。

##### OSのサービシングモデルは General Availability Channel 相当以上 とすること。

### 負荷分散装置

#### ハードウェア

##### ハードウェアとソフトウェアが一体となったアプライアンス機器であること。

##### 19インチラックにマウント可能であること。

##### 動作温度が10℃～35℃に対応していること。

##### 標準消費電力が 300W 以下であること。

##### Active/Standby 型の HA 構成による冗長化機能を有すること。

##### 設定情報を機器間で同期できる機能を有すること。また、系切り替わり時に設定変更が不要であること。

##### IEEE 802.3abとして標準化された1000BASE-Tイーサネットのインターフェイスを8ポート以上有していること。

##### 機器管理用として1000BASE-Tインターフェイスの独立した管理用ポートを有すること。

##### 管理用ポートに対し、サービス用とは異なるデフォルトゲートウェイが設定可能なこと。

##### 32GB 以上のメモリを搭載していること。

##### L7 スループットは20Gbps 以上であること。

##### SSL スループットは10Gbps 以上であること。

##### L4 CPS の性能は250k CPS 以上であること。

##### 最大 L4 同時接続数は28M 以上であること。

##### 最大 SSL TPS (鍵長 2048 bit)は10k TPS 以上であること。

##### ハードウェアを交換することなく、ライセンス追加によって性能を拡張することが可能なこと。

##### IEEE802.1Q VLAN Tagging 機能を有すること。

##### IEEE802.3ad リンクアグリゲーション機能を有すること。

##### IPv4/IPv6 について静的ルーティングに対応していること。

##### NTP クライアント機能を有すること。

##### Syslogサーバにシステムログを転送可能であること。

##### SNMPv2c エージェント機能を有しており、MIB及びMIB-IIに対応していること。

##### プロキシ機能を提供するポート番号の指定が可能であること。

##### インバウンド/アウトバウンドの通信を終端するフルプロキシ機能を有し、ヘッダ及びペイロード情報を識別し転送先を設定可能なこと。

##### CONNECT メソッドの利用を許可するポート番号の設定が可能なこと。

### 個人番号利用事務系物理端末

#### ハードウェア

##### ノートブック型であること。

##### CPUは同一の測定指標として、インテル® Core™ i3-1215U プロセッサー以上の性能を有すること。

##### セキュリティチップは、TCG Ver2.0に準拠したセキュリティチップを搭載すること。

##### メインメモリは、8GB以上を装備すること。

##### 内蔵記憶媒体はSSDとし、容量256GB以上のものを装備すること。

##### IEEE 802.3abとして標準化された1000BASE-Tイーサネットインターフェイスを1ポート以上内蔵すること。

##### USBポートは、3ポート以上を装備すること。また、そのうちType-Aポート及びType-Cポートをそれぞれ1ポート以上有すること。

##### 外部ディスプレイ出力端子として、HDMI端子を装備すること。

##### キーボードは日本語キーボードとし、キーピッチが18.4mm以上であること。

##### USB Type-Aにて接続できる、有線レーザー式マウスを装備すること。

##### ディスプレイは、15インチ以上16インチ以下とし、ワイドTFT液晶で最大解像度を1920×1080以上とすること。また、ディスプレイには反射防止の処理がされていること。

##### 無線LAN機能を有すること。規格はIEEE802.11ax/ac/a/b/g/n対応、Wi-Fi準拠のこと。

##### 内蔵バッテリーを装備すること。バッテリーでの駆動が8時間以上稼働する性能を有すること。

##### タッチパッドを装備すること。タッチパッド機能は装備するマウスの接続時に自動で停止できること。また、タッチパッド機能単独での、常時使用、常時停止の設定も可能であること。

##### 内蔵マイクを装備すること。

##### 解像度について、フロント及びリア共に有効画素数約92万画素（720P）相当以上に対応したwebカメラを内蔵すること。

##### 100Vの電圧に対応した機器であること。

##### 動作温度が5℃～35℃に対応していること。

#### ソフトウェア

##### 使用権

ソフトウェア等は、府に使用権があり、賃貸借期間中、適法に使用できること。ライセンス契約のあるものについては、府を契約者とすること。ユーザ登録が必要な場合は、府をユーザとして登録すること。

##### 製品保守

ソフトウェア等は、賃貸借期間中は製造元、販売代理店等の保守を受けることができるものであること。

##### サービシングモデル

OSのサービシングモデルはGeneral Availability Channel相当以上とすること。

##### OS

OSは以下の要件を満たすこと。

###### Microsoft Windows 11 Enterprise（64bit）相当以上の権利を有すること。

なお、賃貸借期間中にサポートが切れた場合は、後継バージョンにアップグレードする権利を有すること。

###### ADにおいて管理ができること。

##### オフィスソフトウェア

Microsoft 365 Apps for enterprise相当以上を実装すること。

##### ウイルス対策ソフトウェア

Microsoft Defender相当以上が利用できること。既存の庁内情報基盤内MECMサーバまたは府が調達した資産管理システムにより、常に最新のパターンファイルをダウンロードできるように対応を進めること。

##### 生体認証クライアント

生体認証サーバと連携し、生体認証を行う為のクライアントソフトを実装すること。

##### 府指定ソフトウェア

その他府より提供するソフトウェアを導入すること。

### 静脈認証センサー

#### ハードウェア

##### 非接触型の静脈読取り専用センサーであること。

##### USB Type-Aにて接続できること。また、接続したUSBポートより電源供給を受けることができること。

##### 動作温度が10℃～35℃に対応していること。

##### 外光耐力として、以下の性能を有すること。

###### 認証時の性能は以下とする。

自然光（太陽光） 45,000lux以下

白熱灯・ハロゲン灯 9,000lux以下

###### 登録時の性能は以下とする。

自然光（太陽光） 5,000lux以下

白熱灯・ハロゲン灯 1,700lux以下

##### 生体認証サーバへ導入するソフトウェアとの動作を保証すること。

### 仮想サーバ

#### 共通

##### 各仮想サーバに必要なOS及びソフトウェアのライセンスを準備すること。

##### 各仮想サーバの導入ソフトウェアにて、庁内ネットワーク情報基盤仮想基盤サーバのハイパーバイザー上での動作が保証されていること。カタログ等に記載がない場合は、メーカーもしくは販売代理店に確認を行い、証跡を示すこと。

##### 各仮想サーバにはウイルス対策ソフトウェアを導入し、庁内ネットワークウイルス対策管理サーバ及び庁内ネットワークウイルス対策配信サーバで管理できること。

#### 庁内ADサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Active Directoryドメインサービス相当以上の機能を有すること。

#### LGWAN接続系ADサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Active Directoryドメインサービス相当以上の機能を有すること。

#### SC連携用ADサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Active Directoryドメインサービス相当以上の機能を有すること。

#### 共通基盤用ADサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Active Directoryドメインサービス相当以上の機能を有すること。

#### 検証用ドメインコントローラ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Active Directoryドメインサービス相当以上の機能を有すること。

#### ディレクトリ同期サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Microsoft Entra IDと連携する為のMicrosoft Entra Connect相当以上の機能を有すること。

##### 庁内ADと連携し、同期対象OUを限定する為の機能を有すること。

##### DBソフトウェアとして、SQL Server 2022相当以上の機能を有すること。

#### テスト用ディレクトリ同期サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Microsoft Entra IDと連携する為のMicrosoft Entra Connect相当以上の機能を有すること。

##### テスト用ADサーバと連携し、同期対象OUを限定する為の機能を有すること。

##### DBソフトウェアとして、SQL Server 2022相当以上の機能を有すること。

#### 庁内Webサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Webソフトウェアとして、Internet Information Services相当以上の機能を有すること。

##### ファイル共有の機能として、SMB相当以上の機能を有すること。

#### 庁内Web移行用サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### ソフトウェア開発フレームワークとして、.NET Framework相当以上の機能を有すること。

#### ターミナルサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### PDFドキュメントを閲覧可能なAdobe Acrobat Reader相当以上の機能を有すること。

##### RedHat Enterprise Linuxやアプライアンス製品への接続のため、Tera Term相当以上の機能を有すること。

#### 利用者管理システムWebサーバ(本番、テスト)

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Webソフトウェアとして、Internet Information Services相当以上の機能を有すること。

#### 利用者管理システムDBサーバ(本番、テスト)

##### OSはWindows Server 2022相当以上の機能を有すること。

##### DBソフトウェアとして、SQL Server 2022相当以上の機能を有すること。

#### 利用者管理システムサーバ(開発)

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Webソフトウェアとして、Internet Information Services相当以上の機能を有すること。

##### DBソフトウェアとして、SQL Server 2022相当以上の機能を有すること。

#### ジョブ管理サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Job管理ソフトウェアとして、JP1/Automatic Job Management System 3相当以上の機能を有すること。

##### エージェント導入を行ったサーバのジョブを管理が可能であること。

#### 仮想基盤管理サーバ

##### OSは仮想アプライアンス製品であること。

##### ハイパーバイザー管理ソフトウェアとして、vCenter相当以上の機能を有すること。

##### 庁内ネットワーク情報基盤仮想基盤サーバに導入するハイパーバイザーを一元管理する機能を有すること。

##### Webベースの管理画面を有すること。

#### 職員端末機等中央管理サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### DBソフトウェアとして、SQL Server 2022相当以上の機能を有すること。

##### 端末管理として、Microsoft Configuration Manager相当以上の機能を有すること。

#### 職員端末機等サイトサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### 端末の配信サーバとして、Microsoft Configuration Manager相当以上の機能を有すること。

##### 管理対象をIPの制限等により、制御できること。

#### 庁内メールサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### メールサーバの機能として、Exchange Server 2019相当以上の機能を有すること。

##### メールサーバに必要なサーバ証明書は第三者機関により証明書を発行でき、調達期間終了まで更新に必要な証明書を発行できること。なお、11以上のメールサブジェクト数を設定可能であること。

##### クラウドサービスと連携したハイブリッド構成により、メールの配送、共通のアドレス帳の利用、予定表の相互参照、メールボックスの移行が可能であること。

#### テスト用庁内メールサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### メールサーバの機能として、Exchange Server 2019相当以上の機能を有すること。

##### メールサーバに必要なサーバ証明書は第三者機関により証明書を発行でき、調達期間終了まで更新に必要な証明書を発行できること。なお、4以上のメールサブジェクト数を設定可能であること。

##### クラウドサービスと連携したハイブリッド構成により、メールの配送、共通のアドレス帳の利用、予定表の相互参照、メールボックスの移行が可能であること。

#### 全文検索サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### 全文検索はNeuron ES相当以上の機能を有すること。

##### 3億文書ファイル以上の検索が可能であること。

##### Share Point Online及びInternet Information Services（IIS）で提供されるWEBコンテンツの検索が可能であること。また、Share Point Onlineへ検索用窓を配置するようサンプルのjavascriptが提供されること。

##### 以下に示すファイル形式の検索が可能であること。

###### 拡張子がtxt、text、csvなどのテキストファイル

###### 拡張子がdoc、xls、ppt、docx、xlsx、pptx、ppsx、docm、xlsm、pptm、ppsmなどのOffice文書

###### 拡張子が、vsd、vsdxなどのVisioファイル

###### PDF文書

###### htm、html、xhtml、xhtmなど（HTML Version 1.0, 1.1, 2.0, Atom, RSS 2.0など）のhtmlファイル

###### rtf形式のリッチテキスト

###### odt、ods、odp、odg、ott、ots、otp、otg、sxw、sxc、sxi、sxd、stw、stc、sti、std形式のOpen Document

###### xdw、xbd形式のDocuWorksドキュメント

###### zip、bz2、tar、z、gz、tgz、7zで圧縮された文書

###### mp3, jpeg, mpegなどのマルチメディアファイル

###### 拡張子がmsg形式のメールファイル

###### dwg形式のAutoCADファイル

###### 一太郎ファイル（一太郎Version5以降）

##### 利用者にて任意の文字列やファイルサイズで検索できる機能を提供すること。

##### 全文検索の機能として、以下を有すること。

###### 利用者のアクセス権に応じて検索結果を制御

###### 日本語対応（形態素分析）

###### パス絞り込み

###### ソート

###### 検索結果重複ファイル排除（類似文書グルーピング）

###### 検索ランキング

##### 以下のブラウザを利用した検索が可能であること。

###### Google Chrome 最新版

###### Firefox 最新版

###### Microsoft Edge 最新版

##### 利用ユーザの閲覧権限の無いファイルは、一切、検索結果に表示されず、参照できないこと。また、過去にアクセス権限があり、その後権限がなくなった場合も同様とすること。

##### 文書の情報を収集する際に、所属用ファイルサーバで利用する自動階層によりデータの格納先が変更されないよう、ファイルの実データへのアクセスはせず、メタデータのパラメータを収集すること。

#### 全文検索管理サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### 対象の全文検索サーバを統合的に管理できる機能を有すること。

##### ユーザ名/パスワードの入力を不要とするよう府にて利用している共通ドメインのアカウントにてシングルサインオンを利用できること。

#### ファイルサーバ可視化サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### 可視化はNeuron Smart Repository相当以上の機能を有すること。

##### 全文検索サーバと連携し、ファイルの利用状況を可視化できること。

##### 重複管理されたデータや数年間参照されていないデータ、一定容量を超過したデータ、削除・アーカイブ対象となるデータを抽出及び可視化できること。

##### 分析した結果を定例的なレポートとして出力可能であること。

#### ファイル無害化サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### 無害化はOpswat相当以上の機能を有すること。

##### 特定の事象が発生した際に利用者へ一時的に無害化除外が出来る機能を有すること。

##### 以下の拡張子のファイルを無害化できること。

doc,dot,xls,xlt,ppt,pot,rtf,docx,docm,dotx,dotm,xlsx,xlsm,xlsb,xltx,xltm,csv,tsv,pptx,potx,pptm,potm,pps,ppsm,ppsx,sldx,sldm,vsdx,vssx,vstx,vsdm,vssm,vstm,vsx,vtx,vdx,odt,ods,ott,ots,odp,otp,htm,html,mhthta,pdf,ai,hwp,hwt,hpwx,cell,show,jtd,jtdc,jhd,xml,xml-doc,xml-docx,xml-xls,tbwx,tds,vcs,ics,lnk,jpg,jpx,bmp,png,apng,tiff,tiff64,nef,svg,gif,wmf,emf,ico,cur,webp,wdp,dwg,dwt,dws,sfc,p21,jww,jwc,dxf,dwf,3ds,dae,u3d,drc,rvm,dcm,heic,wmv,wma,mpeg,wav,mp3,mp4,mov,avi,webm,bwf,w64,rf64,m4a,ogg,aiff,opus,eml,msg,oft,pst,txt,json,xdw,crl,spf,7z,gz,gzip,rar,xz,zip,alz,tar,bz2,lzma,lzh,arj,cab,wsp,ace,tse,tsez,tsec,egg

##### OLEファイル等の再帰的な無害化処理ができること。

##### ファイル無害化サーバについて、インターネット接続系、LGWAN接続系、個人番号利用事務系の3層間にサーバを構成し、以下要件を実現すること。

###### インターネット接続系/LGWAN接続系

インターネット接続系、LGWAN接続系の2層間でのファイルの無害化を可能とすること。

###### インターネット接続系/個人番号利用事務系

インターネット接続系、個人番号利用事務系の2層間でのファイルの無害化を可能とすること。

###### 個人番号利用事務系/LGWAN接続系

個人番号利用事務系、LGWAN接続系の2層間でのファイルの無害化を可能とすること。

##### ファイルを無害化できない場合は、承認機能により承認者が承認した場合に無害化を回避できること。

#### 添付ファイル分離ワークサーバ

##### OS は RedHat Enterprise Linux 9 相当以上の機能を有すること。

##### メールのセキュリティとしてGUARDIANWALL相当以上の機能を有すること。

##### RedHatのサブスクリプションを利用する場合は、同一のマイナーリリースを24カ月間使用し続けることができるよう、EUS(Extended Update Support)相当以上の機能を有すること。

##### メール本文から全ての拡張子を対象として添付ファイルを分離する機能を有すること。

##### メール本文に添付ファイルを参照するためのURLを追記する機能を有すること。

##### メールから分離したファイルは、セキュリティが確保されたクラウドストレージに保管すること。ストレージ上のファイルは、メール宛先のユーザのみ参照が可能となるようアクセス制限する機能を有すること。また、送信者がメールから分離したファイルを公開期間が終了する前に削除又は公開停止できること。

##### 添付ファイルの参照は、ワンタイムパスワードまたはソーシャルアカウント(「Microsoft アカウント」または「Google アカウント」)にて認証する機能を有すること。

##### 添付ファイルのストレージ公開期間は、7日以上可能とすること。

#### 添付ファイル分離管理サーバ

##### OS は RedHat Enterprise Linux 9 相当以上の機能を有すること。

##### メールのセキュリティとしてGUARDIANWALL相当以上の機能を有すること。

##### RedHatのサブスクリプションを利用する場合は、同一のマイナーリリースを24カ月間使用し続けることができるよう、EUS(Extended Update Support)相当以上の機能を有すること。

##### 添付ファイル分離ワークサーバの以下設定パラメタを管理できること。

###### メールからの添付ファイル分離

###### メール本文への添付URL付与

###### ストレージへの格納

###### ストレージ格納した添付ファイルの管理

###### メール送受信

###### ログの保存/検索

#### サーバパッチ管理サーバ[Windows]

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Microsoft社より、Service Packs、セキュリティ問題の修正プログラム、重要な更新のダウンロードを行う、本業務で導入したWindows Serverへの配信が可能であること。

#### サーバパッチ管理サーバ[Linux]

##### OS は RedHat Enterprise Linux 9 相当以上の機能を有すること。

##### RedHat社より修正パッチをダウンロードし、本業務で導入したRedHat Enterprise Linux Serverへ適用が可能であること。

##### RedHatのサブスクリプションを利用する場合は、同一のマイナーリリースを24カ月間使用し続けることができるよう、EUS(Extended Update Support)相当以上の機能を有すること。

#### サーバログ管理サーバ

##### OS はWindows Server 2022 Standard相当以上の機能を有すること。

##### ログ管理ソフトウェアとして、Logstorage相当以上の機能を有すること。

##### メニュー、マニュアルが日本語であること。

##### Web ベースのインターフェイスを介し、管理画面の操作が可能な機能を有すること。

##### ユーザ定義の条件により、検索、集計、レポート等が実行できる機能を有すること。

##### 異なる種類のログを統一的に扱う仕組みを持ち、それによりログの追跡が行える機能を有すること。

##### Windows イベントログを収集する機能を有すること。

##### 製品ライセンスの制限により、ログ収集容量の上限を超えたログが欠落するライセンス体系ではないこと。

#### サーバログ保管サーバ

##### OS はWindows Server 2022 Standard相当以上の機能を有すること。

##### ログ管理ソフトウェアとして、Logstorage相当以上の機能を有すること。

##### SYSLOG、SNMPTrap、エージェント、エージェントレス、ファイル共有等の方法でログを収集する機能を有すること。

##### 調達機器等に対して認証に関連するログ、FW に関連するログ、指定されたイベントに関連するログ、SNMP で検知出来ない機器障害に関連するログ等を取得できる機能を有すること。

##### 異なる種類のログを独自形式で一元管理し、収集したログの原本は加工せず保管できる機能を有すること。

##### ログデータを圧縮した状態で保管及び管理できる機能を有すること。

##### ログの改ざんチェックができる機能を有すること

#### ウイルス対策管理サーバ

##### OSはWindows Server 2022 Standard相当以上の機能を有すること。

##### ウイルス対策ソフトウェアとして、Trend Micro Apex One相当以上の機能を有すること。

##### 仮想サーバに導入したウイルス対策ソフトウェアの一元管理が可能であること。

##### リアルタイムスキャン及びスケジュールスキャンが可能な機能を有すること。

##### Windows OSの仮想サーバへパターンファイルの配信を行えること。

##### ウイルスを検知した場合はメールによる通知機能を有すること。

#### ウイルス対策配信サーバ

##### OS はWindows Server 2022 Standard相当以上の機能を有すること。

##### ウイルス対策ソフトウェアとして、Trend Micro Apex One相当以上の機能を有すること。

##### 賃貸借期間中は常に最新のウイルスに対応したパターンファイルをオンラインでダウンロードできる権利を有すること。

##### Linux OSの仮想サーバへパターンファイルの配信を行えること。

#### バックアップ管理サーバ

##### OSはWindows Server 2022 Standard相当以上の機能を有すること。

##### バックアップソフトウェアとして、Veeam Backup & Replication相当以上の機能を有すること。

##### バックアップの保存先として、本サーバに接続されている仮想ディスクを選択できること。

##### バックアップファイルの圧縮及び重複排除の機能を有すること。

##### 庁内Web基盤システムのコンテンツはサイト単位でバックアップ、及びリストアが可能であること。

##### 取得したバックアップからファイル及びフォルダ単位での復元ができる機能を有すること。

##### 取得済みバックアップデータから正常に復元できるよう、定期的に復元テストが行える機能を有すること。

##### バックアップの状況表示、実行等の確認ができるWeb ベースの管理機能を有すること。

##### バックアップの結果をメール通知できる機能を有すること。

##### バックアップの結果をSNMP通知できる機能を有すること。

#### バックアップ転送サーバ

##### OSはWindows Server 2022 Standard相当以上の機能を有すること。

##### バックアップソフトウェアとして、Veeam Backup & Replication相当以上の機能を有すること。

##### バックアップの指示が実行された際、本サーバからバックアップ保存先に書込みができること。

##### 2台以上のサーバを構築した際、バックアップジョブ処理を振分けることで負荷分散が可能であること。

#### バックアップ保護サーバ

##### OS はRedHat Enterprise Linux 9相当以上の機能を有すること。

##### RedHatのサブスクリプションを利用する場合は、同一のマイナーリリースを24カ月間使用し続けることができるよう、EUS(Extended Update Support)相当以上の機能を有すること。

##### バックアップソフトウェアとして、Veeam Backup & Replication相当以上の機能を有すること。

##### ランサムウェア攻撃対策として、取得したバックファイルを第三者によって変更不可とする機能を有すること。

#### 運用監視サーバ

##### OS はWindows Server 2022 Standard相当以上、RedHat Enterprise Linux 9相当以上又は仮想アプライアンス製品であること。

##### RedHatのサブスクリプションを利用する場合は、同一のマイナーリリースを24カ月間使用し続けることができるよう、EUS(Extended Update Support)相当以上の機能を有すること。

##### 監視ソフトウェアとして、Zabbix相当以上の機能を有すること。

##### SNMP マネージャ及びSNMPTrap 機能を有すること。

##### 固有の MIB を読込み可能な機能を有すること。

##### ICMP により指定した機器の死活監視が可能な機能を有すること。

##### ログ監視機能を有すること。

##### 監視対象毎に監視項目及びアラート条件の設定が可能であること。また、条件として閾値を超過した際の設定を含むことができること。

##### アラートを検知した際にメールで通知ができること。

##### 収集したリソース情報のグラフ化が可能な機能を有すること。また、データをcsv形式等で外部出力可能であること。

##### Windows Server 2022 Standard及びRedHat Enterprise Linux 9 に対応したエージェント機能を有すること。

##### グラフ、マップ等を機種や用途ごとに分類できる機能を有すること。

##### Web ベースのインターフェイスを介し、監視画面の操作が可能な機能を有すること。

#### 議会等Proxyサーバ

##### OS はRedHat Enterprise Linux 9相当以上の機能を有すること。

##### リバースプロキシとして、Apache相当以上の機能を有すること。

##### RedHatのサブスクリプションを利用する場合は、同一のマイナーリリースを24カ月間使用し続けることができるよう、EUS(Extended Update Support)相当以上の機能を有すること。

#### 庁内ADサーバ(個番・税)

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Active Directoryドメインサービス相当以上の機能を有すること。

#### 個人番号利用事務系運用管理サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### Windows Server標準機能であるリモートデスクトップ相当以上を実装し、本業務における個人番号利用事務系ネットワーク接続の仮想サーバへの操作を可能とすること。

#### 生体認証サーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### 生体認証サーバはインターネット接続系に接続する職員端末機、個人番号利用事務系に接続する個人番号利用事務系端末機及び税務情報端末機において認証を可能とするようにサーバを構成し、以下の要件を満たすこと。

###### インターネット接続系認証サーバ

インターネット接続系より接続される職員端末機の生体認証ができること。

利用者は同時接続数として約700人、最大利用者約1,000人の認証を可能とすること。

###### 個人番号利用事務系認証サーバ

個人番号利用事務系より接続される個人番号利用事務系端末機及び税務情報端末機の生体認証ができること。

利用者は同時接続数として約1,300人、最大利用者約2,000人の認証を可能とすること。

##### 認証ソフトウェアとして、手のひら静脈認証及び顔認証、指紋認証、ICカード認証に対応していること。

##### 認証を行う対象のアプリケーションを指定できること。

##### 端末の電源起動時において、AD認証前に生体認証にて認証ができること。

##### 管理するユーザアカウントについて、ADアカウントと連携させることができること。

##### 端末がオフラインであっても、一定期間は端末にキャッシュされた情報で端末にサインインできること。

##### 「(12) 静脈認証センサー」と連携して生体情報を認証し、その後ADにてADアカウントのID及びパスワードによる知識情報による認証を組合せた二要素認証方式として構成ができること。

##### デバイスによるライセンスを考慮する場合は、静脈認証センサー台数分の認証を可能とすること。

##### 職員端末機、税務情報端末機及び個人番号利用事務系物理端末へ導入するクライアントと連携し、認証ができること。

#### Office認証用Pacサーバ

##### OSはWindows Server 2022相当以上の機能を有すること。

##### 内ネットワーク内の端末において通信先のドメインに応じて、利用するプロキシサーバの振分けができるよう、Pacファイルの配置ができること。

### 調達サービス

#### バックアップ用クラウド環境

##### 所属用ファイルサーバ及びバックアップ保護サーバのバックアップデータの保管場所として以下の機能を提供すること。

###### Cloud Volumes ONTAP for Azure相当以上のサービスとして、バックアップストレージの機能が提供できること。

###### 所属用ファイルサーバの所属フォルダ領域のバックアップが取得可能であること。

###### バックアップ保護サーバ上のバックアップデータの複製データが取得可能であること。

##### 所属用ファイルサーバ及びバックアップ保護サーバの遠地バックアップは、ストレージの機能により設定とバックアップができること。

# 構築及び撤去

## 共通事項

### 運送、養生、梱包部材の処分、データ消去、原状回復等の付随作業も含めて、本章に示す全ての作業に係る費用は、受注者にて負担すること。

### 構築及び撤去に係る作業は、可能な限り、執務環境及び府の業務に影響を与えない方法で実施すること。やむを得ず影響のある作業が必要となる場合は、当該作業実施の1箇月以上前に府の承諾を得ること。

### 構築及び撤去に係る作業は、開庁日の9時から18時の間に行うこと。ただし、執務環境及び府の業務に影響が生じる作業等については、夜間又は休日に行うこと。

### 構築及び撤去に係る作業に伴う搬入出、工事等に係る各種手続きは、受注者の責任において実施すること。

### 設置場所への入退出に際しては、設計事業者等の指示に従い、必要な手続き等を行うこと。

### 搬入出を行う際は、必要に応じて搬入出の経路を養生すること。

### 機器等を梱包している箱等は、受注者が処分すること。

### 構築に係る作業は、賃貸借期間の開始日までに全ての作業を完了すること。

## 管理

### 受注者は、契約締結後速やかに設計事業者等と打合せを行い、構築に係る作業の内容等について十分に調整した上で業務実施計画書を作成し、府の承諾を得ること。また、作業の途中段階で、計画の修正又は見直しが必要となる場合は、設計事業者等と協議の上、速やかに修正した業務実施計画書を提出し、府の承諾を得ること。

### 業務実施計画書には、以下の内容を含むこと。

#### 作業スケジュール、作業工程、工程の開始・終了条件

#### 各工程における体制、府等との役割分担

#### 会議体、連絡方法

#### リスク及び課題の管理方法

#### 品質方針（品質基準、品質管理保障体制、品質管理プロセス）

### 業務実施計画書に基づき、進捗確認、課題共有、ドキュメントや成果物のレビュー等を行うため、定例会議を開催すること。特に、下記報告内容に関する会議については、開催を必須とする。

#### 進捗管理に関する報告

#### 課題管理に関する報告

#### リスク管理に関する報告

#### 成果物に関する報告

### 定例会議での報告に当たっては、以下の資料を作成すること。

#### WBS（Work Breakdown Structure）

#### 進捗報告書

#### 課題管理表

#### リスク管理表

#### 成果物に関する資料（必要に応じて）

### 設計事業者等から要請がある場合又は府等との協議が必要な事案が発生した場合には、臨時の会議を随時開催すること。

### 会議の開催方式は対面でもオンラインでもどちらでもよいが、これに要する経費は受注者の負担とする。なお、会議を対面実施かつ、大手前庁舎で実施する場合、会場は府から提供可能である。また、会議をオンラインで実施する場合、Microsoft Teamsであれば府にてオンライン会議を主催可能である。

### 会議を開催する日程については、設計事業者等と協議すること。

### 会議での報告内容は、進捗状況や課題を明確に示す等、設計事業者等が今後の対応方針を判断可能なものとすること。

### 会議が開催される都度、原則、3開庁日以内に議事録を提示し、府の承諾を得ること。

## 詳細設計

### 共通事項

#### 設計事業者等が提示する基本設計書及び以下の要件を基に、詳細設計書を作成すること。なお、庁内ネットワーク環境及び本業務以外の機器に影響を及ぼさないように設計すること。

##### 詳細設計書は、調達機器、システム等が性能を十分発揮できるように設定内容を検討すること。

##### 詳細設計書には、調達機器等の設定内容を決定するための考え方や方針を記載すること。

##### 基本設計書等について、十分に内容を確認、理解の上、不明点がある場合は確認事項を一覧にまとめて府と協議を行うこと。協議の結果、設計の追加や修正が必要と判断された場合は受注者の責任において基本設計書等の改版を行うこと。

##### 現行稼働している機器の設定値を実機確認し、基本設計書の記載と異なる設定となっている場合は、設計見直しなどの対応方針を府と協議すること。

#### 詳細設計書、テスト計画書、及びテスト仕様書は受注者にて作成すること。

#### 基本設計書等の要件を満たしていることを検証するため、基本設計書の本文毎に詳細設計書の章番号、及び詳細設計の内容を記載したトレーサビリティを示すこと。

#### マイクロソフト社の製品・サービスの設計にあたり、妥当性を確認できるよう、受注者にてサポートサービス(Premier Support for Partners)を契約すること。

#### バックアップは機能毎の開発元が推奨する方式にてシステム自動取得すること。

#### トレーサビリティを含む詳細設計書は府及び設計事業者へ事前送付し、送付より5営業日以降に受注者にて対面で説明すること。

#### 詳細設計は工程完了判定会議を設け詳細設計書、トレーサビリティの内容を説明し、府及び設計事業者の承諾を得ること。

#### 詳細設計の結果、庁内他システムにおいて設定変更が必要となる場合は、運用事業者又は他所属が実施することを想定している。その際、受注者は運用事業者又は他所属への設定依頼内容を提示すると共に、必要に応じて立会いを行う等、設定変更の支援を行うこと。

#### テスト計画書は、利用者操作、管理者操作、及び非機能の観点でテストシナリオを作成すること。

#### テストシナリオは、基本設計書の本文毎にテスト計画書の章番号及びテスト観点を記載しトレーサビリティを示すこと。

#### テスト仕様書は、テスト計画書を元に府の環境に合わせたテストケースを作成すること。

#### テストケースは、非機能要求グレードの項目を参考に網羅性を示し、またCPU故障など実施が不可能なテストケースを全て明確にすること。

[非機能要求グレード2018]　https://www.ipa.go.jp/archive/digital/iot-en-ci/jyouryuu/hikinou/ent03-b.html

### 仮想基盤

#### ハードウェアの集約化及びリソースの共有化を図るため、庁内ネットワーク情報基盤仮想基盤サーバにハイパーバイザーを導入する設計とすること。

#### 障害時には業務を停止する事なく、異なる庁内ネットワーク情報基盤仮想基盤サーバ間及び異なる個人番号利用事務系情報基盤サーバで仮想マシンを移動する設計とすること。

#### 仮想基盤サーバの予備機は庁内ネットワーク情報基盤仮想基盤及び個人番号利用事務系情報基盤の共通のフェイルオーバーホストとして設定し、HA(High Availability)機能を利用して、仮想基盤サーバの障害時には仮想マシンを予備機上に自動的に移動/起動する設計とすること。

#### 複数台構成の仮想サーバは、可能な限り別々の仮想基盤サーバ上に構築し、耐障害性を高める配置で設計すること。

#### 予備機には通常運用時には仮想マシンを配置しない設計とすること。

#### 運用管理でコマンド操作を想定し、PowerShellなどを利用する設計とすること。導入する仮想サーバについては詳細設計時に決定すること。

### ドメインコントローラ

#### 庁内ADサーバ

##### 現行の庁内ADサーバは共通ドメイン(lan.pref.osaka.jp)を管理するドメインコントローラとなり、本業務で構築する情報基盤の庁内ADサーバにおいても共通ドメインを管理するドメインコントローラとして設計すること。

##### 庁内ADサーバは全台仮想マシンとして動作させるように設計すること。

##### サーバは仮想マシンのレベルにて冗長構成とし、システム障害時は残るサーバにて機能の継続提供するよう自動で切り替えるよう設計すること。

##### 庁内ADサーバは全台仮想マシンとして動作させるので時刻がずれないように設計すること。

##### 現行環境で動作している事業者ドメイン(biz.lan.pref.osaka.jp)で利用している事業者アカウントは共通ドメインに移行済みのため、事業者ドメインは廃止すること。事業者ドメインを削除することにより、共通ドメインに影響のないように設計すること。例として事業者ドメインの利用有無などを確認し、事業者ドメインを廃止することで情報基盤に対して影響がないようにするなど。

##### 現行環境で動作しているLGWAN用ドメイン(lbox.pref.osaka.jp)は、府独自の3層分離β´モデルを採用することでLGWAN用Exchangeサーバが不要となっているため、LGWAN用ドメインは廃止すること。LGWAN用ドメインを廃止することにより共通ドメインに影響のないように設計すること。

##### 現行の共通ドメインでは、用途によりサイトが分かれている。利用しないサイトが実装されているため、不要なサイトを削除するなどサイト構成を見直す設計をすること。

##### グローバルカタログは庁内ADサーバ全台に実装する設計とすること。

##### 庁内ADサーバ間の通信がDCファイアウォールで制御されている場合は、必要な通信ポートをDCファイアウォールで解放するように設計、府に依頼すること。

##### 本業務で構築する情報基盤ではフォレスト機能レベル、ドメイン機能レベルは「Windows Server 2012」から「Windows Server 2016」にアップグレードすること。フォレスト機能レベル、ドメイン機能レベルをアップグレードすることで本業務のミドルウェア、サービスに対しての影響範囲を調査し設計、対処すること。

##### 現行環境は共通ドメインと教育庁ドメインが双方向で信頼関係を設定している。本業務で構築する情報基盤では教育庁ドメインを新規で構成するため信頼関係を設定しない。信頼関係の設定を解除するにあたり、共通ドメインに影響のないように設計すること。

##### 情報基盤の更改に伴い、機能に沿ったGPO/OUの変更が必要となる場合は、現行環境に影響のないように設計すること。例として、WSUSのサーバを指定するGPOを適用する場合は、今回導入する機器のOUを作成して適用し、既存のOUに影響がないようにするなど。

##### Windows OSとOffice製品のKMSホストサーバを設計すること。KMSホストサーバはインターネット接続系と個人番号利用事務系それぞれの系統から接続できる必要があるため、それぞれの系統で配置するように設計すること。

##### インターネット接続系のKMSホストサーバは、認証する機器が多いためKMSホストを複数台で構成できるように設計すること。

##### 現行の情報基盤では庁内ADサーバ上で認証局が動作しているため、本業務で構築する情報基盤でも庁内ADサーバ上で認証局を動作させるように設計すること。

##### 認証局は2種類(SHA1とSHA256)のハッシュ関数を使用すること。

##### ホスト名が大文字/小文字でホスト名が重複しないように設計すること。

##### NetLogonの脆弱性CVE-2022-38023に対処することで、影響範囲を調査し適法方針を検討し、府の了承を得ること。例としてNetAppのDataOntapバージョン、NTLMを利用しているミドルウェアへの影響など。

##### 庁内ADサーバが全損したときにでも復旧できるようにバックアップ設計すること。

#### テスト用ADサーバ

##### 現行のテスト用ADサーバはテスト用ドメイン(testl.lan.pref.osaka.jp)を管理するドメインコントローラとなり、本業務で構築する情報基盤のテスト用ADサーバにおいてもテスト用ドメインを管理するドメインコントローラとして設計すること。

##### 庁内ADサーバはADの機能で冗長化するために複数台で構成する設計とすること。

##### テスト用ADサーバは全台仮想マシンとして動作させるように設計すること。

##### テスト用ADサーバは全台仮想マシンとして動作させるので時刻同期がずれないように設計すること。

##### 本業務で構築する情報基盤ではフォレスト機能レベル、ドメイン機能レベルは「Windows Server 2012」から「Windows Server 2016」にアップグレードすること。フォレスト機能レベル、ドメイン機能レベルをアップグレードすることで本業務のミドルウェア、サービスに対しての影響範囲を調査し設計、対処すること。

##### 情報基盤の更改に伴い、機能に沿ったGPO/OUの変更が必要となる場合は、現行環境に影響のないように設計すること。

##### NetLogonの脆弱性CVE-2022-38023に対処することで、影響範囲を調査し適法方針を検討し、府の了承を得ること。例としてNetAppのDataOntapバージョン、NTLMを利用しているミドルウェアへの影響など。

##### テスト用ADサーバが全損したときにでも復旧できるようにバックアップ設計すること。

### 名前解決

#### 庁内ADサーバ

##### サーバは仮想マシンのレベルにて冗長構成とし、システム障害時は残るサーバにて機能の継続提供するよう自動で切り替えるよう設計すること。

##### 共通ドメインのゾーン(lan.pref.osaka.jp)とExchange Serverを自動検出で

##### 使用するゾーン及び逆引き参照ゾーンを名前解決するDNSサーバを庁内ADサーバで提供するように設計すること。

##### LGWANなど特定のドメインについては、ゾーンを管理しているDNSサーバに条件付きフォワードで問い合わせするように設計すること。

##### 庁内ADサーバ自身、条件付きフォワード先でも名前解決できないドメインは、内部DNSサーバにフォワードするように設計すること。

##### 個人番号利用事務系の庁内ADサーバについては、3層分離の観点から共通ドメインとLGWANドメイン以外の名前解決を実施しないため、内部DNSサーバにフォワーダしない設計とすること。レプリケーションされる条件付きフォワードで共通ドメイン、LGWANドメイン以外のドメインについては、フォワードされる必要がないため、DCファイアウォールで通信を遮断すること。

##### 個人番号事務利用系の庁内ADサーバはLGWAN系のドメインを条件付きフォワードに追加する設計とすること。

##### 業務ネットワークと管理ネットワーク両方のネットワークに接続する場合は、問い合わせするクライアントが業務ネットワークからのみDNSサーバが応答するように設計すること。

##### 条件付きフォワードで不要なドメイン、追加するドメインを検討し、必要に応じて設計すること。

##### 逆引き参照ゾーンで不要なゾーンがあるか検討し、必要に応じて整理、設計すること。

#### テスト用ADサーバ

##### テスト用ドメインのゾーン(testl.lan.pref.osaka.jp)とExchange Serverの自動検出で使用するゾーン及び名前解決するDNSサーバをテスト用ADサーバで提供するように設計すること。

##### テスト用ADサーバ自身で名前解決できないドメインは、内部DNSサーバにフォワードするように設計すること。

##### 業務ネットワークと管理ネットワーク両方のネットワークに接続する場合は、問い合わせるクライアントが業務ネットワークからのみDNSサーバが応答するように設計すること。

##### 条件付きフォワードで不要なドメイン、追加するドメインを検討し、必要に応じて設計すること。

##### 逆引き参照ゾーンで不要なゾーンがあるか検討し、必要に応じて整理、設計すること。

### 時刻同期

#### 庁内ADサーバ

##### サーバは仮想マシンのレベルにて冗長構成とし、システム障害時は残るサーバにて機能の継続提供するよう自動で切り替えるよう設計すること。

##### 時刻同期は庁内ADサーバでサービスを提供するように設計すること。

##### Windows機器はOS標準機能で時刻同期する想定で設計すること。

##### LinuxサーバはOS標準パッケージのChronyを使用する想定で設計すること。

##### ストレージ、アプライアンス、ネットワーク機器は、それぞれの機器で標準に搭載されている時刻同期機能で設計すること。

##### ドメイン参加しているWindows機器はWindowsのデフォルト設定であるいずれかの庁内ADサーバと時刻同期を行う設計とすること。

##### ワークグループに参加しているWindows機器は、PDCが動作している庁内ADサーバ以外の庁内ADサーバの2台と時刻同期を行う設計とすること。

##### 庁内ADサーバはPDCが動作している庁内ADサーバと時刻同期するように設計すること。

##### PDCが動作している庁内ADサーバは別調達にて稼働している内部メール中継サーバと時刻同期できるように設計すること。

##### PDCが動作している庁内ADサーバに障害が発生した場合は他の庁内ADサーバが内部メール中継サーバと時刻同期するように設計すること。

#### テスト用ADサーバ

##### テスト用ドメイン内の時刻同期はテスト用ADサーバでサービスを提供するように設計すること。

##### テスト用ドメインに参加しているWindows機器はOS標準機能で時刻同期するように設計すること。

##### テスト用ドメインにドメイン参加しているWindows機器はWindowsのデフォルト設定であるいずれかの庁テスト用ADサーバと時刻同期を行う設計とすること。

##### PDCが動作しているテスト用ADサーバは内部メール中継サーバと時刻同期できるように設計すること。

##### PDCが動作しているテスト用ADサーバに障害が発生した場合は、他のテスト用ADサーバが内部メール中継サーバと時刻同期するように設計すること。

### サーバパッチ管理

#### サーバはパッチ管理サーバからの適用ではなく、任意のタイミングでサーバ側から取得する必要があるため、パッチ管理サーバはアップデートモジュールのみ提供するプロダクトを選定すること。

#### パッチの適用(詳細な種別、時間帯)については各システムの影響度を考慮したうえで設計すること。

#### Windowsパッチ管理サーバ

##### 管理対象はインターネット接続系と個人番号利用事務系で稼働している全Windowsサーバ（調達機器以外も含む）を対象とし、職員が使用している端末機は対象外とする設計とすること。

##### 対象の製品群はWindows Server 2022と次期バージョンとする設計とすること。

##### ダウンロード対象となるパッチ分類は「Service Pack」、「セキュリティ問題の修正プログラム」、「重要な更新」とする設計とすること。

##### Windowsパッチ管理サーバへの接続はGPOを使用して接続すること。既存環境に影響がないようにOUの配置、GPOの適用を設計すること。

##### 修正プログラムを自動ダウンロードする時間帯は、業務に影響のない時間帯に定期的にダウンロードするように設計すること。

#### パッチ管理サーバ(Linux)

##### 管理対象はインターネット接続系と個人番号利用事務系で稼働している全Linuxサーバ（調達機器以外も含む）を対象とする設計とすること。

##### 対象の製品群はRedhat Enterprise Linux 9のマイナーバージョンまでとする設計とすること。

##### 修正プログラムを自動ダウンロードする時間帯は、業務に影響のない時間帯に定期的にダウンロードするように設計すること。

### 庁内Webサイト(IIS)

#### 庁内Webサイトの構成

庁内Webサイトは、以下に示すサイト区分、ソフトウェア等により構成する。

表 ３‑１　庁内Webサイト構成

| **サイト区分** | **ソフトウェアなど** | **内容** |
| --- | --- | --- |
| 庁内Webページ（ポータル） | SPO | 庁内用のポータルサイト（ブラウザのホームページに指定） |
| 部局等チームサイト | SPO | 各部局等が部局等内の情報共有のために利用するサイト |
| 部局横断チームサイト | SPO | 部局等の枠を超えて情報共有するために利用するサイト |
| 各課ページ（Webページ） | IIS | 各室課等が作成する庁内向けWebページ |
| ダウンロード（Webページ） | 所属ファイル共有ストレージ | ＤＸ推進課が提供するソフトウェア等のダウンロードを行うサイト |

#### 庁内Webサーバ(IIS)

##### 各課ページを庁内に公開するためのWebサービスを設計すること。

##### 庁内ネットワークに公開するサイトと、議会LANに接続する端末機(議会端末、別館 府民お問い合わせセンターの端末機)から議会等Proxyサーバ経由で接続されるサイトを設計すること。

##### 議会Proxy経由の接続は、許可された各課ページのコンテンツが表示される設計とすること。

##### 各課ページサイトへの接続は認証による許可されたユーザに対して許可すること。ただし、利用者に認証を意識させないようにするため、SSOが可能な設計とすること。議会サイトへの接続は議会等Proxyサーバ経由となり、SSOの実現が難しいため匿名認証で設計すること。

##### ログは1日1回ローテーションし、5年間ローカルディスクに保存する設計とすること。

#### 庁内Webサーバ(ダウンロード)

##### ＤＸ推進課が提供するモジュールを庁内に公開するためのダウンロードサイト(以下ダウンロード用フォルダ)を所属用ファイルサーバで動作するように設計すること。

##### 所属用ファイルサーバ上でダウンロード用フォルダのSMB共有を設計すること。

##### 所属用ファイルサーバ上でダウンロード用フォルダの共有フォルダを設計すること。

##### 利用者のファイルの操作ログを保存可能な設計をすること。

##### 所属用ファイルサーバの設計詳細は「ファイル共有(所属)」を参照すること。

### サーバ運用監視

#### 運用監視サーバはインターネット接続系と個人番号利用事務系の2系統のサーバ運用監視を統合管理する構成で設計すること。

#### 運用監視対象は以下として設計すること。

##### 仮想化基盤：死活監視、SNMP監視、リソース監視、ログ監視

##### サーバ：死活監視、アプリケーション・サービス監視、リソース監視、ログ監視

##### ネットワーク機器：死活監視、SNMP監視、リソース監視、ログ監視

##### アプライアンス：死活監視、SNMP監視

##### ストレージ：死活監視、SNMP監視、ログ監視

##### クラウド環境リソース：死活監視

#### ログ監視については、サーバログ管理サーバと連携して実施できるように設計すること。

#### 庁外サイト向けの通信の遅延等の確認のため、Web監視(応答時間の測定)を実施し、レポート作成できるように検討すること。

#### リソース監視については、機器ごとに閾値を設計すること。また閾値に近づいた際に予兆通報を行えるように設計すること。

#### 監視サーバにて障害及び予兆通報を検知した際に、運用監視サーバから管理者へメール通知するように設計すること。

#### 監視サーバ自身の監視を監視サーバ以外から行う仕組みを検討すること。

#### ヒストリデータなどのログ保存期間は3年分とすること。

### ファイル共有(所属)

#### 所属用ファイルサーバ

##### 1台でインターネット接続系、個人番号利用事務系からのファイル共有の接続にあたり、セキュリティ確保のためインターネット接続系からのみ接続可能なボリューム、個人番号利用事務系からのみ接続可能なボリュームを設計すること。

##### ボリューム数は基本設計に合わせて設計すること。

##### セキュリティ確保のため、所属用ファイルサーバはインターネット接続系からのアクセス、個人番号利用事務系からのアクセス、管理用、自動階層/遠地バックアップ用でそれぞれ物理的にNICを分けて設計すること。また、信頼性確保のため各NICはコントローラをまたいで冗長化するように設計すること。

##### インターネット接続系のボリュームは、所属フォルダ用と部局調達NASフォルダ用で構成する設計とすること。ボリューム単位の遠地バックアップは所属フォルダのみとするため、所属フォルダと部局調達NASフォルダは別ボリュームで設計すること。

##### 現行のインターネット接続系の所属フォルダは通常の所属フォルダと作業用(シェアフォルダ)の構成としており、クォータ管理が個別となっている。クォータ管理を統合するため、インターネット接続系の所属フォルダは、現行の所属フォルダと作業用(シェアフォルダ)を統合したフォルダとして設計すること。

##### 5年後の利用容量を想定して以下のユーザ使用容量を確保すること。

###### インターネット接続系所属フォルダ:188TB以上

###### インターネット接続系部局調達NASフォルダ:276TB以上

###### インターネット接続系監査ログ用:2TB 以上

###### 個人番号利用事務系所属フォルダ:24TB以上

###### 個人番号利用事務系監査ログ用:2TB 以上

###### 上記容量はユーザ使用容量のため、容量を算出する際は以下の内容を加味し、容量を算出すること。

スナップショット領域、ボリュームのシステム領域を加味して容量を算出すること。

重複排除を有効化した容量は、各メーカーの推奨値もしくは事例で算出すること。

自動階層を有効化した容量は、フラグメンテーション領域の容量を考慮した容量で算出すること。

##### コントローラに障害が発生した場合でもサービスが継続できるように、正常に動作しているコントローラでサービスが継続できるように設計すること。

記憶領域のRAIDレベルは6とし、ホットスペアを含めて設計すること。

##### 共有フォルダは現行設定を引き継ぐ設計とすること。ただし、組織変更などでフォルダ構成が変更となる場合は、フォルダ構成を見直し、府の了承を得ること。

##### インターネット接続系の所属フォルダのクォータは、現行の所属フォルダ用とシェアフォルダを合算したうえで、利用状況に応じて設計すること。個人番号利用事務系所属フォルダのクォータは現行設定を引き継ぐこと。部局調達NASのクォータは現行使用している容量に対して+5%程度で算出して設定すること。

##### インターネット接続系と個人番号利用事務系の所属フォルダのボリュームは遠地バックアップ保存先にレプリケーションする設計をすること。

##### ローカルのバックアップとしてsnapshot領域を各ボリュームの容量20%以上を確保し、1日1回14世代保持できるように設計すること。

##### 容量確保のために重複排除機能を利用するように設計すること。

##### ランサムウェア対策の機能を利用する設計とすること。ランサムウェア対策のために異常なファイルの保存を制限するよう設計すること。

##### サロゲートペア文字は利用しない方針とする。移行データのファイル名が文字化けする文字列を提示すること。

##### ファイルサーバへのアクセスログをサーバログ管理サーバに保存できるように設計すること。

##### 障害発生時はメーカーと監視サーバに通知するように設計すること。

##### ADのバージョンアップ、修正プログラム適用に伴い所属ファイルサーバへの影響がないことを調査し、影響ない構成、設計とすること。

##### 移行後、運用中に耐えうるiノード数を設計すること。

##### メーカーが推奨する方法でバックアップを取得できるように設計すること。

##### メーカーが推奨する方法でバックアップしたデータでリストアできるよう設計すること。

##### 所属用ファイルサーバで監視できないアラートを検知するために別途管理サーバが必要となる場合は仮想化基盤上に仮想サーバを実装すること。

##### (ﾇ)においてオンプレミス環境に仮想サーバを追加する場合は、他の仮想サーバに影響がないように仮想化基盤のリソースを調整すること。

##### サーバ、ソフトウェアを追加する場合において、調達するバックアップソフトでバックアップが取得できない場合はメーカ推奨の方法でバックアップ/リストアを実施できるよう設計すること。

#### 自動階層化

##### 自動階層化機能を利用する場合は、アクセス頻度の高いファイル(以下ホットデータ)は書き込み速度の速い記憶媒体で構成されたストレージに保存され、特定の期間アクセスのないファイル(以下コールドデータ)を低価格の記憶媒体で構成されたストレージの領域にファイルを移動するように自動階層の設計を設計すること。

##### 自動階層の設定でホットデータの領域は30%以上確保するように設計すること。

### ファイル送受信

#### ファイル送受信

##### 利用するユーザ数は5400名にて設計すること。インターネット接続系：3400ユーザ、LGWAN接続系：3400ユーザ(インターネット接続系と同一ユーザ)、個人番号利用事務系：2000ユーザ

##### インターネット接続系、個人番号利用事務系、LGWAN接続系の3層全てに設置し、各ネットワークの独立性を確保し、セキュリティが担保出来るように設計すること。

##### 基本設計書に記載されている内容をもとに、無害化機能及び承認機能の設計をすること。

##### 冗長構成は各層ごとにActive・Standbyにて設計すること。

##### 利用者管理システムにて作成されたファイル送受信用のCSVデータを自動で取込み、利用ユーザ及び承認者の登録を日次にて一括で実施する設定を詳細設計にて設計すること。

##### 利用ユーザがログインする際に、ログインしている層(インターネット接続系、個人番号利用事務系、LGWAN接続系)が利用画面に表示されるように設計すること。

##### アップロードされたファイルを保持期間及び保持期間を過ぎた場合は自動削除できるように詳細設計にて設計すること。

##### SSOを利用してログインできるように設計すること。

##### 利用者端末にエージェントをインストールすることなく、ブラウザのみにて利用できるよう設計すること。

##### httpsを利用するため、クライアントに設定する証明書の配布設定を設計すること。

##### アップロード、ダウンロード、承認、無害化等のログを取得できるように設計すること。

##### 設計に基づいた期間にてログのローテーションを行い、サーバログ管理サーバへ転送するように設計すること。

##### メーカーで推奨する方法でバックアップを取得する設計とすること。

##### メーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

#### 無害化サーバ

##### 以下の拡張子のファイルを無害化できること。

doc,dot,xls,xlt,ppt,pot,rtf,docx,docm,dotx,dotm,xlsx,xlsm,xlsb,xltx,xltm,csv,tsv,pptx,potx,pptm,potm,pps,ppsm,ppsx,sldx,sldm,vsdx,vssx,vstx,vsdm,vssm,vstm,vsx,vtx,vdx,odt,ods,ott,ots,odp,otp,htm,html,mhthta,pdf,ai,hwp,hwt,hpwx,cell,show,jtd,jtdc,jhd,xml,xml-doc,xml-docx,xml-xls,tbwx,tds,vcs,ics,lnk,jpg,jpx,bmp,png,apng,tiff,tiff64,nef,svg,gif,wmf,emf,ico,cur,webp,wdp,dwg,dwt,dws,sfc,p21,jww,jwc,dxf,dwf,3ds,dae,u3d,drc,rvm,dcm,heic,wmv,wma,mpeg,wav,mp3,mp4,mov,avi,webm,bwf,w64,rf64,m4a,ogg,aiff,opus,eml,msg,oft,pst,txt,json,xdw,crl,spf,7z,gz,gzip,rar,xz,zip,alz,tar,bz2,lzma,lzh,arj,cab,wsp,ace,tse,tsez,tsec,egg

##### OLEファイル等の再帰的な無害化処理が可能となるように設計すること。

##### メーカーで推奨する方法でバックアップを取得できるように設計すること。

##### メーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

### サーバウイルス対策

#### ウイルス対策配信サーバ/ウイルス対策管理サーバ

##### 本サーバはインターネット接続系と個人番号利用事務系の2系統のウイルス対策を統合管理する構成で設計すること。

##### 本業務内のWindowsサーバ及びLinuxサーバの全サーバに対してウイルス対策を実施する設計とすること。

##### 室課等にて独自調達した端末及びサーバについても本サーバにてウイルス対策を実施する設計とすること。

##### インターネットからパターンファイルをダウンロードするサーバとクライアントを管理するサーバの２台構成で設計すること。

##### Linuxサーバについては、ウイルス対策ソフトが対応しているカーネルバージョンで設計すること。

##### アプライアンス機器及びNASに関しては対象外とすること。

##### 本サーバは、導入しているウイルス対策ソフトウェアのバージョン管理、パターンファイルの定期的な自動更新設定、更新状況の監視等を行う設計とすること。

##### ウイルス検知した際は、感染ファイルの隔離・削除等状況に応じた対処を行えるように設計すること。

##### パターンファイルの取得については、ウイルス配信サーバがインターネットから取得可能となるように設計すること。

##### リアルタイムスキャン及びスケジュールスキャンについて設計すること。スケジュールスキャンに関しては週次で実施し、業務影響の無いタイミングで行えるように設計すること。

##### ウイルススキャン除外対象については、サーバに導入しているアプリケーションの推奨除外設定を個別で実施する設計とすること。

##### ウイルスを検知した場合は、運用事業者へメール通知を実施する設計とすること。

##### ログについては定められた期間分を保持し、サーバログ保管サーバに転送する設計とすること。

### ターミナルサービス

#### インターネットなどの庁外からは府で利用中のリモートアクセスシステム経由でターミナルサーバへリモートでログインできるよう設計すること。

#### ターミナルサーバから、調達機器等にログインできるよう設計すること。

#### ターミナルサーバ及びターミナルサーバを経由してログインしたサーバ、機器の一般ユーザでのシャットダウン操作ができないようにすることの要否を検討すること。

#### WEBブラウザとしてEdgeを導入すること。

#### 機器接続用にTera Termを導入すること。

#### ドキュメント閲覧用にOffice/Acrobat Readerを導入すること。

### サーバログ管理

#### サーバログ管理サーバ

##### 仮想化基盤、サーバ、ネットワーク機器、ストレージ、Microsoft 365の監査ログを対象とし、設計すること。

##### サーバのログはWindows、Linux、仮想化基盤を対象とし、イベントログとSyslogを収集する設計とすること。

##### ネットワーク機器及びストレージは、Syslogを収集する設計とすること。

##### Microsoft 365は以下の機能を対象とし、監査ログとメッセージ追跡を収集する設計とすること。

EntraID

Exchange Online

SharePoint / OneDrive for Business

Microsoft Teams

MessageTrace

MessageTraceDetail

##### 管理者向けのログとして、ログイン、ログアウトの状況が把握できるログを保存する設計とすること。

##### 庁内Webサーバ(IIS)、議会等Proxy、全文検索管理サーバはアクセスログを取得する設計とすること。庁内Webサーバ(ダウンロード)、所属用ファイルサーバ、Microsoft 365は利用者の操作ログを取得する設計とすること。

##### 監査ログ収集後、既定の日数をデータベースに保存されるよう設計すること。

##### 既定の期間を超えた監査ログは既定の日数をアーカイブし、保存するよう設計すること。

##### アーカイブした監査ログをリストアし、閲覧できるよう設計すること。

##### 監査ログの収集は複数のサーバで収集し、負荷分散構成として設計すること。

##### ログ管理ソフトウェアはメーカーで推奨する方法でバックアップを取得できるように設計すること。

##### ログ管理ソフトウェアはメーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

#### サーバログ保管サーバ

##### 過去の監査ログが閲覧できるよう設計すること。

##### ログ保管ソフトウェアはメーカーで推奨する方法でバックアップを取得できるように設計すること。

##### ログ保管ソフトウェアはメーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

##### セキュリティを担保するため、庁内ネットワーク情報基盤と個人番号利用事務系情報基盤でサーバを分けるよう設計すること。

##### ログ収集の負荷を分散するため、庁内ネットワーク情報基盤と個人番号利用事務系情報基盤でそれぞれ複数台のサーバで監査ログを収集するよう設計すること。

### サーババックアップ

#### バックアップ管理サーバ/バックアップ転送サーバ

##### バックアップ管理サーバ/バックアップ転送サーバはインターネット接続系と個人番号利用事務系の2系統のバックアップを統合管理する構成で設計すること。

##### 仮想マシンをエージェントレスでバックアップ取得可能であり、インターネット接続系と個人番号利用事務系の系統間における通信が発生しないように設計すること。

##### バックアップ対象は以下として設計すること。

サーバ機器　OS、システム構成、ログ等

ネットワーク機器、ストレージ装置　OS、システム構成、ログ等

##### 仮想化基盤サーバは、オフラインでイメージ取得できるバックアップソフトウェアを選定すること。

##### アプライアンス、ネットワーク機器など選定したバックアップソフトウェアで取得できないプロダクトについては、メーカー推奨の取得方法でバックアップを取得すること。

##### ミドルウェアを含めたバックアップはメーカーが推奨する方法でバックアップを採取すること。例としてサービスを停止して取得、ミドルウェア個別の方法で1次バックアップを取得するなど。

##### バックアップ対象台数を考慮して設計(同時実行数等の考慮等)すること。

##### バックアップ対象のサーバ機器のバックアップ範囲、周期、リストア要件等については、システム、データの重要度、更新頻度等をもとに設計をすること。

##### バックアップ転送サーバについては、バックアップ処理に必要な仮想マシンリソースが適切に分散されるように設計すること。

##### バックアップを取得するネットワークは、業務に影響のないネットワークで取得するように設計すること。

##### バックアップソフトウェアでは取得できない機器、ミドルウェアの個別バックアップを保存する領域をバックアップ管理サーバに1.2TB以上確保すること。

##### バックアップジョブは18時から翌朝の6時に実行し、完了するように同時実行や実行タイミングを設計すること。また、増分バックアップは30分以内に完了するように設計すること。

##### 合成バックアップを取得する場合は、バックアップジョブが18時から翌朝の6時に収まるよう合成フルバックアップの実施タイミングを分散させて設計すること。

##### バックアップ終了及び異常終了時に運用事業者へ通知する設計をすること。

##### バックアップの状況確認については、メール通知、Trap通知、ログ出力、管理画面でのログ確認などで行えるように設計すること。

#### バックアップ保護サーバ

##### ランサム対策を目的としてデータの上書き等が出来ない様に、バックアップデータの保護について講じること。

##### 保護されるバックアップデータは必要世代数保存できる容量を確保すること。必要容量は以下を確保すること。

バックアップ管理サーババックアップ領域:1.2TB以上

バックアップ頻度の高いサーバのバックアップ:270TB以上

バックアップ頻度の低いサーバのバックアップ:36TB以上

バッファ容量:30TB以上

##### 上記容量で容量が不足する場合は必要容量を上記以上で見直すこと。

##### 災害対策を目的としたバックアップデータの遠地保管を可能とすること。

##### バックアップ保護サーバのバックアップデータ領域を遠地保管バックアップ領域にレプリケーションすること。

##### 遠地保管バックアップへのレプリケーションは、圧縮・重複排除された状態で差分ブロック単位の転送が可能であること。

### ジョブ管理システム

#### ジョブ管理サーバはインターネット接続系と個人番号利用事務系の2系統のジョブを統合管理する構成で設計すること。

#### エージェントを導入し、ジョブを管理する対象サーバは以下として設計すること。

##### 利用者管理システムWebサーバ(本番、テスト)

##### 利用者管理システムサーバ(開発)

##### 職員端末構成管理システム

#### 現行のジョブ及びジョブネットの利用状況を精査し、次期のジョブネットを設計すること。

#### エージェントを利用しない他システム向けのバッチ処理に関しては実行ファイルを本サーバ内に配置し、スケジュール実行できるよう設計すること。

#### ジョブ実行時の完了及び異常終了については監視サーバから運用事業者へ通知されるように設計すること。

### 議会等Proxy

#### 議会LANから庁内WEBへアクセスする際は議会等Proxyサーバ上のApacheにて実装するリバースプロキシ機能を設定し、仮想URLにて接続するように設計すること。

#### リバースプロキシ機能により、庁内WEBの特定のフォルダパス（「kihon」という名前のフォルダ）以下のみ参照可能とし、その他フォルダパスは閲覧不可として設計すること。

#### 庁内WEBの所属別コンテンツのURLが変更になる等により、URLリライト先を変更する運用が頻繁に発生するため、Apache全体の設定ファイルとは別にURLリライト設定を別ファイルとして切出して設定できるようにする等の運用工数の軽減検討をおこなうこと。

#### アクセスログを取得できるように設計すること。

#### ログの一定期間でローテーションし、サーバログ管理サーバへ転送するように設計すること。

#### メーカーで推奨する方法でバックアップを取得できるように設計すること。

#### メーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

### ファイル全文検索

#### 全文検索サーバ

##### 文書情報を収集するアカウントを設計すること。

##### 全文検索は庁内ファイルサーバのインターネット接続系の所属フォルダに保存されている文書、並びに庁内Webサーバ(IIS、SharePoint Online)に保存されている文書を対象とし、設計すること。

##### 文書情報の収集は文書数を考慮し、収集による業務への影響を分散するよう組織単位でスケジューリングすること。

##### 文書数は稼動後、５年で合計３億文書まで増加すると想定し、３億文書を超えることが見込まれる場合は、管理者に警告する運用方法を設計し、運用チームに連携すること。また、３億文書を超えた場合の拡張方式を設計すること。

##### ログは、既定の日数をサーバ内に保持するよう設計すること。

##### 庁内WEBの文書情報を収集する方法として、WEBコンテンツをファイルとして情報収集するか、庁内WEBサーバ(IIS、SharePoint Online)にアクセスしてWEBコンテンツとして情報収集するかを設計すること。

##### メーカーで推奨する方法でバックアップを取得できるように設計すること。

##### メーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

#### 全文検索管理サーバ

##### ファイル全文検索ポータル画面へのログインは、共通ドメインのアカウントを使用する利用者がファイル全文検索システムに接続する際に、ユーザ名/パスワードの入力を不要とするSSO機能でログインするよう設計すること。

##### 文書の絞り込み条件として、ファイル種別、最終更新者、ファイルサイズ、ファイル更新日、フォルダ指定が選択できるよう設計すること。

##### 次の文書形式を検索できるよう設計すること。Microsoft Officeファイル、リッチテキストファイル、一太郎ファイル、テキストファイル、PDFファイル、Docuworksファイル、HTMLファイル、XMLファイル、Visioファイル、Open Documentファイル

##### ファイル全件検索のテスト時は、府と調整、合意の上、職員にて作成され移行が完了している実データを用いてテストするよう設計すること。

##### ファイル全件検索のテスト対象を明確化し、テストで必要なアカウントを作成依頼すること。

##### メーカーで推奨する方法でバックアップを取得できるように設計すること。

##### メーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

#### ファイルサーバ可視化サーバ

##### ファイルサーバ可視化は所属用ファイルサーバのインターネット接続系の所属フォルダに保存されている文書、並びにWebサーバ(IIS、SharePoint Online)に保存されている文書を対象とし、設計すること。

##### 文書情報の収集は文書数を考慮し、収集による業務への影響を分散するよう組織単位でスケジューリングすること。

##### 一定期間参照されていないデータや一定容量を超過したデータ等、削除・アーカイブ対象となるデータを分析できるよう設計すること。

##### メーカーで推奨する方法でバックアップを取得できるように設計すること。

##### メーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

### 端末管理

#### 職員端末機等の種類(職員端末機、独自調達端末機及び税務情報端末機)に応じて利用する機能を設計すること。

#### 本業務外の枠組み（AssetView）で管理している職員端末機については、リモートコントロール機能のみ有効として設計すること。

#### 既存のSystem Center Configuration Managerと異なる機能については、有効及び無効の設計と設計理由を明確にすること。

### 生体認証

#### 税務情報端末機及び個人番号利用事務系物理端末機については、端末機起動後にWindowsログオン認証の前に生体認証が起動するように設計すること。

#### 職員端末機にて、個人番号利用事務系仮想デスクトップクライアントを起動時に生体認証が起動するように設計すること。なお、LGWAN接続系仮想デスクトップクライアント起動時は生体認証を起動させない。対象のURLについては、仮想端末基盤クラウドサービス事業者より提示する。

#### インターネット接続系及び個人番号利用事務系へ設置の生体認証サーバは冗長化されており、単体での障害発生時でも継続して機能を提供できること。

#### 登録するユーザ情報については、1時間に一度csvにて情報を取込み、自動で連携されるようにタスクを設計すること。

### バックアップ用クラウド環境

#### 所属用ファイルサーバ(バックアップ)、サーババックアップデータの遠地保管先としてクラウド環境に容量を確保すること。

#### バックアップ用クラウド環境は東日本リージョンで構成する設計とすること。

#### snapshot領域として各ボリュームの容量20%以上を確保すること。

#### 容量確保のために重複排除機能を利用するように設計すること。

#### 自動階層化機能を利用する場合は、アクセス頻度の高いファイル(以下ホットデータ)は書き込み速度の速い記憶媒体で構成されたストレージに保存され、特定の期間アクセスのないファイル(以下コールドデータ)を低価格の記憶媒体で構成されたストレージの領域にファイルを移動するように自動階層の設計を設計すること。

#### 所属用ファイルサーバ(バックアップ)として以下の容量を確保すること。

##### インターネット接続系所属フォルダ

##### 個人番号利用事務系所属フォルダ

##### 容量を算出する際は以下内容を加味し、容量を算出すること。

スナップショット領域、ボリュームのシステム領域を加味して容量を算出すること。

重複排除を有効化した容量は、圧縮率は各メーカーの推奨値もしくは事例で算出すること。

自動階層を有効化した容量は、フラグメンテーション領域の容量を考慮した容量で算出すること。

#### サーババックアップデータの遠地保管領域として、バックアップ保護サーバのバックアップ領域の容量を確保すること。容量を算出する際は以下内容を加味し、容量を算出すること。

##### スナップショット領域、ボリュームのシステム領域を加味して容量を算出すること。

##### 重複排除を有効化した容量は、圧縮率は各メーカーの推奨値もしくは事例で算出すること。

##### 自動階層を有効化した容量は、フラグメンテーション領域の容量を考慮した容量で算出すること。

#### 自動階層化機能を利用する場合は、所属用ファイルサーバ(バックアップ)の自動階層の設定は、ホットデータの領域は30%以上確保するように設計すること。

#### 自動階層化機能を利用する場合は、サーババックアップデータの遠地保管先の自動階層の設定は、すべてコールドデータの領域で保存するように設計すること。

### 個人ドライブシステム

#### 個人ドライブシステムは、E3ライセンスを割り当てる職員が利用できること。

#### 個人ドライブシステムを管理するアカウントを設計すること。

#### コンテンツの共有範囲は可能な限り最小の共有範囲とすること。

#### コンテンツはゲストユーザに共有できないこと。

#### ユーザの利用可能なストレージ容量は本システムの既定値とすること。

#### ユーザに割り当てられた職員個人用のコンテンツ保存領域は、原則当該ユーザのみがアクセスできるように権限を制御すること。

#### 削除されたユーザのコンテンツは定められた期間保持すること。また、保持期間中は管理者が対象のコンテンツを参照できるようにアクセス権を設計すること。

#### 削除されたユーザのコンテンツの完全削除は他システムにて実施するため、本システムとしてのコンテンツの保持期間は最大日数とすること。

#### ユーザの利用可能なストレージ容量が逼迫した場合、ユーザに通知すること。

#### 他のユーザが個人ドライブのコンテンツを外部組織へ共有した場合、所有者に通知すること。

#### 他のユーザが個人ドライブのコンテンツへのリンクを作成した場合、所有者に通知すること。

#### 定められた世代分コンテンツのバージョンを保持し、必要に応じでユーザが任意のバージョンに復元できること。

#### 本システムはブラウザからアクセスするWeb版ではなく、職員端末機にインストールしたクライアントアプリからアクセスすること。

#### 定められた期間のコンテンツが復元可能であること。

#### ランサムウェアに対する影響を考慮し、ウイルス検知されたコンテンツのダウンロードを防止するための警告を表示すること。

#### 個人ドライブシステムの設定はグループポリシーで配布すること。

#### クライアントアプリのアップデートは他システムから配布し適用すること。

#### クライアントアプリで職員端末機に同期されたコンテンツは、ログオフスクリプトを用いてローカル領域から削除すること。

### ディレクトリ同期

以下を満たすパラメータ設計をすること。

#### Microsoft Entra Connectによる機能及び非機能に関するパラメータを設計すること。

#### 本番環境用Microsoft 365テナント向け、及び、テスト環境用Microsoft 365テナント向けのMicrosoft Entra Connectを設計の対象とすること。

#### 本番環境用Microsoft 365テナント向け、及び、テスト環境用Microsoft 365テナント向けの機能として、以下を実現できるよう設計すること。

##### Microsoft Entra Connectの稼働に支障が出ないサーバスペックとすること。

##### Microsoft Entra Connectのインストーラバージョンは原則構築時点の最新版とするが、既存の同期処理に大きな影響が懸念される場合はバージョンを協議の上決定すること。

##### 冗長構成はハードウェアによるHAを採用し、Microsoft Entra Connectはサーバ1台にインストールする構成とすること。

##### Microsoft Entra ConnectのProxy接続要件を整理し、認証除外する場合などプロキシへの変更点を府へ提示すること。

##### データベースは、SQL Server 2022 Standardを利用すること。

##### SQL Server 2022 Standardを利用するうえでパラメータの修正が必要と判明した場合、協議の上パラメータを決定すること。

##### 多数の誤削除を防止するオブジェクト保護機能を利用し、閾値は現行運用を考慮した上で決定すること。

##### シームレスシングルサインオン及びシームレスシングルサインオンの実現に必要なGPOなどの構成見直しの有無を精査し、パラメータを決定すること。

##### ウイルス対策において、ディレクトリ同期に支障を来さないよう除外対象を整理すること。

### Microsoft 365 テナント

以下を満たすパラメータ設計をすること。

#### Microsoft 365 管理センター、及び、Entra ID管理センターによる機能及び非機能に関するパラメータを設計すること。

#### 本番環境用Microsoft 365テナント向け、及び、テスト環境用Microsoft 365テナント向けのMicrosoft 365 管理センター、及び、Entra ID管理センターを設計の対象とすること。

#### 本番環境用Microsoft 365テナント向け、及び、テスト環境用Microsoft 365テナント向けの機能として、以下を実現できるよう設計すること。

##### Microsoft 365 E3ライセンスを活用すること。

##### クライアント端末が、以下URLに記載のURL及びIPアドレスに接続できる。https://learn.microsoft.com/ja-jp/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide

##### クライアント端末の通信先はインターネットプロキシにてExpressRoute、またはインターネットに振り分けしている。Microsoftのアドレス一覧においてExpressRouteがいいえの場合、インターネット接続かつプロキシにて認証除外する必要があるが、運用事業者による手作業追加となっている。Microsoftのアドレスに更新が発生した場合、認証除外のURLをインターネットプロキシに自動登録すること。また、登録した場合は運用事業者に通知すること。

##### Microsoft 365のデータ保護は、以下URLに記載のMicrosoft Cloudにおける暗号化の方針に準拠すること。

https://docs.microsoft.com/ja-jp/microsoft-365/compliance/office-365-encryption-in-the-microsoft-cloud-overview?view=o365-worldwide

##### Microsoft 365で利用する機能は、Exchange Online、SharePoint Online、OneDrive for Business、Microsoft Teamsに必要となる機能を利用すること。

##### (ｵ)以外の機能は原則利用可能とするが、職員利用によるセキュリティリスクが高いと判断できる機能は、可能な限り機能停止すること。

##### 本番環境用Microsoft 365テナント、及び、テスト環境用Microsoft 365テナント共に稼働済み環境における利用ドメインの用途を精査し、過不足が発生しないよう考慮すること。

##### Microsoft 365の監査ログを有効化し、監査ログを取得できる構成とすること。

##### Logstorage Microsoft 365連携パックを利用するにあたり、Microsoft 365 テナントに必要な設定事項を精査し、パラメータを決定すること。

##### 条件付きアクセスポリシーによるアクセス制御は、現行ポリシーの継続利用を原則とし、現行運用などポリシー改善に向けた設定見直しの有無を精査すること。

##### 先行リリース機能によって一部職員アカウントはMicrosoft 365サービスの新機能を先行して利用できるよう構成するが、対象者を府と協議の上決定すること。

##### Microsoft 365のWeb UIとして、府指定の新たなロゴ画像を協議すること。

##### 現行運用を踏まえた上で、Microsoft 365サービス正常性確認、及び、メッセージセンターを確認できる新たなアカウントの追加有無を協議すること。

### 庁内メール及び会議室予約

以下を満たすパラメータ設計をすること。

#### 庁内メール（オンプレ、クラウド共通）

##### 基本設計にて確定した利用機能について、詳細パラメタを決定すること。

##### Exchange ServerとExchange Online間で構成されたハイブリッド構成を継続すること。

##### 現行の電子メールシステムでは、Exchange Server－Exchange Online間の接続にExpressRouteを利用しており、本業務に合わせてExpressRouteが変更となるため、これを考慮した設計とすること。

##### 現行の情報基盤のメール送信サーバのリレー先は、オンプレミスExchangeサーバとしており、本業務以外のその他メールサーバ含め最適なメールルーティングとなるよう見直すこと。

##### 配信不能メールを返す設計に変更すること。

##### 配信不能メールを返す設計に合わせて外部ポストマスターアドレスを設計すること。

##### スパム・ウイルス対策の通知先を設計すること。

##### 庁外より一部の承認済みドメインを利用したなりすましメールを受信する要件があるため、特定のドメインまたはアドレスに対して受信許可できる設計とすること。

##### メールヒントを利用すること。この際、特定ドメイン（教育庁）は内部扱いにすること。

##### 訴訟ホールドを利用し、メールデータを保存すること。またこの機能を有効にした際の影響を調査して問題ないことを確認して設計すること。

##### 上記の他、最新の状況を踏まえ、基本設計から追加や修正が必要と考えられる場合は、設計事業者等と協議の上、速やかに修正した詳細設計書を提出し、府の承諾を得ること。

#### 庁内メール（オンプレミス）

##### サーバは仮想マシンのレベルにて冗長構成とし、システム障害時は残るサーバにて機能の継続提供するよう自動で切り替えるよう設計すること。

##### Exchange Serverは2016から2019にバージョンアップすること。また、Exchange Server 2019は延長サポートが2025年10月14日となっている。この期限より前に次期Exchange Serverにバージョンアップする設計とすること。

##### Exchange Server 2019を構築後、現行の電子メールシステム（Exchange Server 2016）で利用しているメールボックスをExchange Server 2019に移行し、Exchange Server 2016を削除すること。

##### 一部業務メールボックスは、Exchange OnlineにおけるOutlook仕分けルール数を超過している。また、Outlook仕分けルールのアドレスは、府の制度上の制約により配布グループに集約できないためオンプレミスのExchange Serverを継続利用すること。

##### フォレスト及びドメインの機能レベルはWindows Server 2016とすること。

##### Exchange Server上のデータベースについて、可用性を確保し、サーバの単一障害に耐え得る設計とすること。

##### メールデータベース、トランザクションログ、メールキューの3つの領域を考慮したサイジング設計とすること。また、各領域はドライブを分けること。

##### 各データベースに配置するユーザ種別については、利用者管理システムにて指定すること。このため、この配置に合わせたデータベース設計とすること。

##### ミラーリング監視サーバの機能をディレクトリ同期サーバに持たせる設計とすること。

##### サーバ証明書を使用した暗号化通信(SSL)によりサーバ－クライアント間の通信をセキュリティで保護すること。

##### Exchange Serverのデータを定期的にバックアップして保管すること。また、バックアップ取得時はサポートされている方法でのバックアップを行い、バックアップデータを利用した復旧が可能であること。

##### Exchange Serverに対応するウイルス対策ソフトの設計を行うこと。また、必要に応じて除外フォルダの指定等を行うこと。

##### Microsoft 365に対して最低限公開が必要なURLのみ公開すること。また、第三者認証期間から発行された証明書を利用し、通信を暗号化すること。

#### 会議室予約

##### 府における会議室の利用を管理するため、会議室の登録（修正、削除）機能、会議室予約機能を持つシステムを提供すること。

##### 利用者はMicrosoft365 E3ライセンスを保持する常勤職員、または職番なし非常勤職員以外に非常勤職員も利用(予約、変更)するものとする。

##### 会議室の公開範囲は府全体と所属限定の2種類に分類される。

##### 公開範囲が所属限定の会議室は、他の所属の職員が予約できないよう会議室にセキュリティグループのコードによる公開範囲を設定すること。

##### 会議室は予約可能期間の上限を設定すること。

##### 予約承認が必要な会議室は、承認者によりメールにて承認依頼を処理(承認・否認)すること。

##### 会議室の承認者は主任者一覧情報より必要となる会議室のみをcsvファイルにより一括更新すること。

##### 組織替えに伴い会議室情報を年度初めに更新すること。

##### 会議室はExchange Online上に作成すること。また、Exchange Server及びExchange Online上のどちらのユーザでも予約可能であること。

##### 会議室の作成、変更、削除はCSVファイルを読み込んで一括処理できるようPowerShellスクリプトを用意すること。また、作成したPowerShellスクリプトを運用事業者に提供すること。

##### 会議室の命名規則として、会議室名の先頭に管理所課を入れること。

### リアルタイムコミュニケーションシステム

#### リアルタイムコミュニケーションシステムは、チャットや音声通話、音声やビデオによるWeb会議、ファイル送受信等の機能により、職員の業務の円滑化、グループ内コミュニケーション向上の環境を提供すること。

#### 現行のリアルタイムコミュニケーションシステムの設定を確認し、基本設計と差異が生じる場合は、府と記載方針を協議すること。

#### チーム機能は以下の要件を基に、詳細設計書を作成すること。

##### チームの所有者はメッセージの削除ができること。

##### チームで共同作業するためのコンポーネントを利用できること。

##### 共同作業するためのコンポーネントには、箇条書き、チェックリスト等の機能を有していること。

##### 共同作業するためのコンポーネントのメッセージはチャットのすべてのユーザが編集可能であること。

#### チームでのWeb会議機能は以下の要件を基に、詳細設計書を作成すること。

##### トランスクリプト機能を利用できること。

##### ウェビナー機能を利用できないこと。

##### エンドツーエンド暗号化機能を利用できること。

##### エンドツーエンドの暗号化を有効化できること。

#### リアルタイムコミュニケーションシステムへのログインは、シングルサインオンとすること。

#### 外部アクセス方式は以下の要件を基に、詳細設計書を作成すること。

##### 職員による庁外からのアクセス（リモートアクセス）は公用のタブレット端末等や職員個人が所有するモバイルデバイス(iOS/Android)を利用したアクセスが許可されていること。

##### 府立学校のユーザをゲストユーザとして招待するが、庁内Web基盤の利用のみとするため、リアルタイムコミュニケーションシステムの利用は抑止すること。

##### 外部組織かつ他テナントのユーザは、リアルタイムコミュニケーションの利用は抑止すること。

#### クライアント環境は以下の要件を基に、詳細設計書を作成すること。

##### 職員端末機に加え仮想端末機からもWeb会議、資料共有等が実現できること。

##### 庁内からのアクセスにおいて、インターネット接続系端末機をクライアントアプリの導入対象とすること。

##### 庁内からのアクセスにおいて、LGWAN系端末機はクライアントアプリの導入対象としないこと。

##### 庁内からのアクセスにおいて、個人番号利用事務系端末機はクライアントアプリの導入対象としないこと。

#### E3ライセンスを割当る職員に対して、リアルタイムコミュニケーションシステム用のライセンスと庁内Web基盤システム用のライセンスを割り当てること。

#### 年次でチームの利用状況を確認し、棚卸を行うこと。

### 庁内Web基盤システム

#### 庁内Web基盤システムは、情報の共有化、事務処理の効率化を図るポータルサイトを提供すること。

#### 庁内Web基盤システムを管理するアカウントを設計すること。

#### 庁内Web基盤システムは庁内Webサイト、部局サイト、部局横断チームサイトの3種類のサイトで構成されていること。

#### 各課ページはOS標準のWebサーバ(IIS)にて実現すること。

#### サイトのURLは移行設計で検討された値を使用すること。

#### 庁内Webサイト、部局サイト、部局横断チームサイトのライフサイクル及びアクセス方法を設計すること。

#### テスト用のサイトを設計すること。

#### 庁内Webサイト、部局サイト、部局横断チームサイトの容量は現行の利用状況から算出した値を設定すること。

#### 容量による警告有無及び警告の閾値を設計すること。

#### 庁内Webサイトのデザインは現行のデザインを踏襲すること。

#### 庁内Web基盤システムのコンテンツは標準機能で管理するよう設計すること。

#### 庁内Web基盤システムは定められたブラウザからアクセスすること。

#### 庁内Web基盤システムへのログインは、シームレスシングルサインオンとすること。

#### 庁内Webサイト、部局サイト、部局横断チームサイトのアクセス制御を設計すること。

#### 庁内WebサイトはMicrosoft 365 E3ライセンスを保持するユーザであれば全てのユーザが閲覧可能とすること。また、庁内Webサイト以外のサイトは特定のユーザ間の利用を目的とするため、サイト毎にアクセス権を設計すること。

#### 部局サイト、部局横断チームサイトはサイトの管理者がアクセス権を制御可能な設計とすること。

#### 府立学校テナントとテナント間同期することで、府立学校側のユーザ更新(追加、削除)が自動的に反映されること。

#### 府立学校ユーザはゲストユーザとして庁内Webサイトへアクセスできること。

#### ゲストユーザは庁内Web基盤システムへゲストユーザ側のネットワーク経路で接続する設計とすること。

#### 外部アカウントを使用したアクセスを制限すること。

#### サイトの手動削除が可能であること。

#### 庁内Web基盤システムのコンテンツはサイト単位でバックアップが可能であること。

#### 庁内Web基盤システムのコンテンツはサイト単位でリストアが可能であること。

### 添付メール分離

#### サーバは仮想マシンのレベルにて冗長構成とし、システム障害時は残るサーバにて機能の継続提供するよう自動で切り替えるよう設計すること。

#### 府におけるメール送信環境を確認し、利用者に影響しないようメールサイズ上限を設計すること。

#### 外部ストレージ障害時は、2時間以内にメールによる管理者通知を可能とし、また障害復旧までメール配送は保留とすること。

#### ストレージ障害時に管理者通知が不可能な場合は、利用者影響しないようメール配送を設計すること。

#### 製品仕様としてプロキシを利用できない場合は、直接接続が可能となるよう外部FW、外部プロキシ、またはインターネットプロキシに対してプロキシを除外するようFQDN(完全修飾ドメイン名)を提示すること。

#### 賃貸借期間中における開発元のサポートを受けられるよう、稼働後のバージョンアップを設計すること。

#### 稼働後のバージョンアップは、職員のメール送信業務を停止しないよう、負荷分散装置にてサーバ切り離しを基本とすること。

#### メーカーで推奨する方法でバックアップを取得できるように設計すること。

#### メーカーで推奨する方法でバックアップしたデータでリストアできるよう設計すること。

### Officeアプリケーションシステム

#### Officeアプリケーションシステムは、文書作成やメール送受信アプリケーションの機能を提供すること。

#### Officeアプリケーションシステムはサブスクリプション型のライセンスを利用すること。ただし、定期的な更新対応が困難な個人番号利用事務系の税務情報端末機は、買い切り型のライセンスを利用すること。

#### 職員端末機の種類(インターネット接続系、LGWAN接続系、個人番号系 税端末、個人番号系 税端末以外)に応じて展開するアプリケーションを設計すること。

#### ライセンス認証はVDI端末利用時に１台の端末を複数のユーザが利用することを考慮すること。

#### Officeアプリケーションシステムのグループポリシーは現行のグループポリシーの設定を引き継ぐこと。

#### インターネット接続が不可となる職員端末機向けに接続エクスペリエンス機能を無効化するグループポリシーを設計すること。

#### インターネット接続系端末のライセンス認証は、既存プロキシ経由とすること。

#### LGWAN接続系、及び個人番号利用事務系端末は、自治体情報セキュリティ向上プラットフォーム経由でライセンス認証し、Officeアプリケーションシステムを利用できること。

#### LGWAN接続系及び個人番号利用事務系端末は、プロキシサーバを利用しており既存環境変更による影響を回避するため、PacServerを導入し既存プロキシ宛の通信とライセンス認証の通信を振り分けること。

#### 職員端末機の種類に応じた認証経路を設計すること。

#### Officeアプリケーションシステムの初回認証後も継続した日数の認証が必要であること。また、最後の認証から定められた日数が経過した場合、Officeアプリケーションシステムの機能を制限すること。

#### アプリケーションの更新は、本業務とは別の「庁内ネットワークサイバーセキュリティ強化」にて実現することから、対象外とする。

### ファイル暗号化

#### ファイルの分類と秘密度ラベル付けを規定すること。

#### M365 E3ライセンスを保有する府Entra IDの全ユーザのみが暗号化ファイルを参照できるよう設計すること。

#### Officeファイル、及びPDFファイルを暗号化対象文書として設計すること。

#### エクスプローラー操作にてファイル暗号化、復号化処理を設計すること。

#### Azure Information Protection(AIP)クライアント導入を検討すること。

#### AIPクライアントが必要な場合、展開計画を作成しパイロット所管課を対象に展開すること。

## 移行設計

### 共通事項

#### 利用者への影響を与えないよう、以下に記載する機能毎の移行要件に対し移行方法やスケジュールの移行計画を策定し、府の承認を得ること。

#### 移行設計書は、以下項目を含めて作成すること。

##### システム構成図

##### 移行対象データ

##### システム切り替え対象

##### スケジュール

##### 役割分担

##### 切り戻し方針

##### リスク及び対応策

### 個人ドライブシステム

#### 現行NASストレージにて提供している個人ドライブシステム（以下「Mドライブという。」からOneDriveへの移行設計は受注者が設計すること。

#### Mドライブのデータ移行は、所有者本人が移行すること。

#### 休職や派遣者のMドライブのデータ移行(約430人)は、受注者が移行すること。また、正常にデータが移行されたことを確認するためのテストを計画し、実施すること。

#### OneDriveの仕様によるファイル名の変更を防ぐために、Mドライブのファイルをzipファイルに圧縮し、OneDriveにzipファイルをアップロードすることで移行すること。

### ディレクトリ同期

#### ディレクトリ同期を実施するシステムを稼働中のMicrosoft Entra Connectから新規構築するMicrosoft Entra Connectへ切り替える移行設計は受注者が設計すること。

#### 移行要件は、少なくとも以下を満たすこと。

##### ディレクトリ同期切り替えは、受注者が実施すること。

##### 切り替え後に稼働するMicrosoft Entra Connectを構築するために必要なサーバ等は、府等と調整のうえ設置すること。

##### 現行稼働しているMicrosoft Entra Connectは切り替え以降に廃止の上、サーバ停止すること。

##### 職員アカウントによるMicrosoft 365への認証に影響を発生させない手法を選択すること。

### 庁内メール

#### 移行設計における下記の計画・設計及びそれに伴う作業を受注者が実施すること。

#### 稼働中のExchange Server 2016からExchange Server 2019へ移行し、その後次期Exchange Serverへ移行する設計とすること。

#### 基本設計書に定めるオンプレミスに置く必要がある約600個のメールボックスを、最新バージョンのExchange Serverに移行すること。

#### 現在オンプレミスに配置された派遣者(約350ユーザ)をクラウドへ移行すること。移行後にライセンス割当を削除すること。

#### Exchange Onlineとのハイブリッド構成を各新バージョンのExchange Serverで引き継ぐこと。また、移行後、旧バージョンのExchange Serverをアンインストールすること。

#### アドレス帳を含む、各機能をバージョンアップ後も引き継ぐこと。

#### 利用者影響が最も少なく安全確実な移行方法を計画・設計すること。

#### Microsoft 365 だけでなく関連するシステムやサービスへの影響及び運用が滞らないことを考慮した移行計画・設計とすること。

#### バージョンアップに合わせて、適切にバックアップソフトウェア、ウイルス対策ソフトの導入と各種設定を行い、正しく動作する設計とすること。

#### 移行期間中のExchange Serverへのパッチ適用を適切に行うこと。

#### Exchange Server 2019」の次にリリースされる製品についても、延長サポートが切れる前までにバージョンアップすること。

#### 次期Exchange Serverの提供時期などの影響で本賃貸借期間でのバージョンアップが難しい場合は、府と協議、調整の上対応すること。

#### 移行計画は、保有ライセンス数を考慮した移行スケジュールとすること。

### 会議室予約

#### 移行設計における下記の計画・設計及びそれに伴う作業を受注者が実施すること。

#### 会議室予約については、Exchangeとは別の現行会議室予約システムからExchangeのリソースメールボックスを利用した会議室予約に変更すること。

#### 既存の会議室予約システムから各会議室の設定を引き継ぐこと。既存の会議室予約システムと動作が変わる点については府に変更点を説明し了承を得ること。

#### 現在利用している会議室詳細情報（会議室名・最大利用者数・利用期間など）は2025年9月末までに完了するよう計画すること。

#### 会議室予約の切替は、2025年10月を予定しており、一斉切替による混乱を避けるため、会議日付が2025年9月以降の会議について2025年6月から利用者による会議室予約・変更・削除が可能とすること。

#### 会議日付が2025年6月から8月までの会議は、現行会議室予約システムを利用するため、利用者から新システムへ予約はシステム制御にて不可とすること。

#### 会議室の予約データは利用者が再登録するが、上記の期間でスムーズに再登録できるよう、移行スケジュールを含めて計画・設計すること。

### 生体認証

#### 既存の生体認証利用者の静脈データは、受注者にて手順を作成の上で、各拠点で現地作業を行うなど、再登録の支援を行うこと。また、既存の生体認証サーバよりデータを取出し、本業務で構築する生体認証サーバへデータ移行を行う等の効率的にデータを移行することも可とする。その際は、府と協議の上、切替日（移行データ凍結日）を定めること。

#### 切替日以降の生体認証サーバへの生体登録は府にて実施するため、登録に必要な手順書を提供すること。

#### 生体認証サーバの切替時は、利用者影響が最も少なく安全確実な移行方法を計画・設計すること。

### ファイル暗号化

#### 所属ファイルサーバ内の特定のフォルダ（「暗号」というフォルダ）に保管された現行暗号化データは設計事業者にて復号化し次期の所属用ファイルサーバへ移行する。

#### 移行後の復号化されたフォルダ内データを受注者にて一括暗号化を検討すること。開発元への問合せ回答として一括暗号化が難しい場合は、暗号化手順を作成し利用者へ説明すること。

#### 移行時において職員によるファイル操作業務が停止する場合、日中時間帯以外にて移行処理を実施するよう計画すること。

## 配線／設置

### 共通事項

#### 現地環境整備の実施に当たっては、法規等を遵守すると共に、受注者の責任において円滑に進めること。

#### 現地環境整備の実施に当たっては、騒音等に配慮しつつ、建物管理者、DCハウジング事業者、設計事業者及び府（以下「建物管理者等」という。）と十分調整の上、実施すること。

#### 現地環境整備については、既存環境に支障を及ぼさないように実施すること。

#### 現地環境整備のスケジュールは、受注者が各拠点の建物管理者と日程調整を行い、府の承諾を得ること。また、進捗状況については、設計事業者等に随時報告すること。

#### 配線・設置に関しては以下の資料を納品すること。

##### 接続装置の設置場所を示す、府が指定する様式の設置図面

##### ケーブル類の敷設経路を示す、府が指定する様式の施工図面及び経路図面(ただし、受注者が敷設したケーブルに限る。)

##### 各現地環境整備の作業開始前、作業中及び作業終了後の状況が適宜把握できる現場写真

#### 接続装置と接続が必要なケーブル類は、対向の機器が本業務とは別の契約により調達している機器であっても受注者が両方の機器に接続すること。

### 現地環境整備

以下の要件に基づき、調達機器を［第２　４ 納入場所］内の府が指定する位置に設置すること。設置作業には、府が指定するラック、ケーブル類の配線及び接続等の環境整備を含む。

#### 搬入物の仮置き、開梱作業、設置作業等に必要なスペースを十分考慮した上で、安全かつ円滑に進めること。

#### 共用スペース、共用設備等は他の利用者もあり、長期の利用はできないので留意すること。

#### ラックマウント型や専用の取り付け金具が無い機器については、耐震対策を施すこと。

#### 調達機器ごとの設置要件等を［別紙6 機器設置要件］に示す。

#### 接続装置の接続に必要なケーブル類の配線環境整備を実施すること。

#### 既設のケーブルを流用する箇所については、以下の要件に従って引き続き正常に利用できることを確認すること。

##### 接続装置が正常に動作しない等、既設のケーブルに問題があると思われる場合は、ケーブルテスター等にてケーブルの正常性を確認すること。異常が認められた際には設計事業者等に報告した上、該当ケーブルの撤去及び新規ケーブルの敷設を行うこと。

##### 既設のケーブルの取り扱いには、細心の注意を払うこと。受注者が実施する作業の前後で著しく品質の劣化が認められた際には、受注者に該当区間の再敷設を求めることがある。

#### 府の指定する管理用ラベルを用意し、機器の目視できる位置に貼り付けること。ラックに搭載する機器については、正面と裏面の両方に管理用ラベルを貼り付けること。

#### ケーブル類を配線するときは、両端に以下のような旗型ラベルを取り付ける等、接続元及び接続先が明確になるようにすること。ラベルはポリエステル等の柔軟な材質とすること。

 

### その他

#### 現地環境整備に際し、作業又は機器に起因する障害が発生した場合は、速やかに原因を究明し、機器の取替え等の対応を行うこと。

#### 現地環境整備の実施に伴い、施設、設備等に損害を与えた場合は、速やかに建物管理者等に報告すると共に原状回復するものとし、これに要する費用は、受注者が負担すること。

## 設定

### 共通事項

#### 設定は、詳細設計書の内容を実現する内容を調達対象機器等に設定すること。

#### 設定作業の途中段階で、詳細設計の修正又は見直しが必要となる場合は、設計事業者等と協議の上、速やかに修正した詳細設計書を提出し、府の承諾を得ること。

#### 機器設定の作業開始は、府、及び設計事業者による詳細設計の工程完了を条件とすること。

#### 稼働中の機器については、検証環境で事前確認を行うなど、利用中の職員への影響が最小限となるような対策を講じること。

#### 設定にあたり府の業務に影響を与えると想定される作業については、事前に府担当者と調整の上、基本的に夜間または休日に実施すること。

#### 設定に必要なサーバなどがある場合には、その構築も受注者が実施し、その構築にかかる経費、機器等の調達については本業務に含むこと。

#### 調達機器等の設定前に、単体テスト仕様書及び結合テスト仕様書を作成し、府の承諾を得ること。

#### 単体テスト仕様書は、詳細設計書に記載したパラメータが調達機器に設定されていることを確認することとする。

#### 引渡し後、障害発生や不具合発生時において運用事業者からの問合せに対応すること。

### 仮想基盤

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面のログイン・ログアウト手順

##### 仮想化基盤管理ソフトウェアの起動

##### 仮想化基盤管理ソフトウェアの停止

##### 仮想化基盤サーバの正常性確認

##### 仮想マシンの操作手順

##### テンプレートの展開手順

##### 仮想化基盤管理ソフトウェアのアップデート方法

##### 仮想化基盤管理ソフトウェアのバックアップ

##### 仮想化基盤管理ソフトウェアのリストア

### ドメインコントローラ

#### 庁内ADサーバ

##### 詳細設計で不要と判断したサイト、SRVレコードなどを削除すること。

##### 事業者ドメイン廃止に伴い、事業者ドメインを削除すること。

##### NetLogonの脆弱性CVE-2022-38023に対処することで、既存環境に影響がある場合は既存環境に影響がないように対処し設定すること。本番・テスト環境とは独立した環境を構築し、検証可能なテスト環境を作成すること。

#### テスト用ADサーバ

##### NetLogonの脆弱性CVE-2022-38023に対処することで、既存環境に影響がある場合は既存環境に影響がないように対処し設定すること。本番・テスト環境とは独立した環境を構築し、検証可能なテスト環境を作成すること。

##### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

管理画面への接続手順

庁内ADサーバ/テスト用ADサーバの起動

庁内ADサーバ/テスト用ADサーバの停止

庁内ADサーバ/テスト用ADサーバのADサーバ正常性確認

アカウントの追加/削除/変更/無効化/パスワード変更

GPOの追加/変更/削除

組織改編対応(セキュリティグループの追加/削除/メンバー追加)

証明書発行手順

庁内ADサーバ/テスト用ADサーバのバックアップ

庁内ADサーバ/テスト用ADサーバのリストア(部分/全損)

### 名前解決

#### 庁内ADサーバ

##### 詳細設計で不要と判断したゾーン、条件付きフォワードを削除、追加すること。

#### テスト用ADサーバ

##### 詳細設計で不要と判断したゾーン、条件付きフォワードを削除、追加すること。

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面への接続手順

##### 庁内ADサーバ/テスト用ADサーバの起動

##### 庁内ADサーバ/テスト用ADサーバの停止

##### 庁内ADサーバ/テスト用ADサーバのDNSサーバ正常性確認

##### DNS管理画面起動

##### DNSレコードの追加/削除

### 時刻同期

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 庁内ADサーバ/テスト用ADサーバへのログイン/ログアウト手順

##### 庁内ADサーバ/テスト用ADサーバの起動

##### 庁内ADサーバ/テスト用ADサーバの停止

##### 庁内ADサーバ/テスト用ADサーバの時刻同期正常性確認

##### 上位NTPサーバ変更方法

### サーバパッチ管理

#### 運用手順書については以下の項目を含め、記載すること

##### 管理画面のログイン・ログアウト手順

##### サーバパッチ管理サーバの起動

##### サーバパッチ管理サーバの停止

##### パッチ管理サーバの正常性確認

##### Windowsパッチ管理サーバへの接続設定手順

##### Windowsサーバパッチ適用手順

##### Linuxパッチ管理サーバへの接続設定手順

##### Linuxサーバパッチ適用手順

##### サーバパッチ管理サーバのコンテンツ手動アップデート手順

##### Windowsパッチ管理サーバグループ変更手順

##### Windowsパッチ管理サーバ修正パッチ個別承認手順

##### Windowsパッチ適用状況確認手順

##### Linuxパッチ適用状況確認手順

### 庁内Webサイト(IIS)

#### 庁内Webサーバ(IIS)

##### 各サイトのルートフォルダまで作成すること。

#### 庁内Webサーバ(ダウンロード)

##### 共有フォルダを所属用ファイルサーバに作成すること。

##### 所属ファイルサーバの設定詳細は「ファイル共有(所属)」を参照すること。

#### 運用手順書については以下の項目を含め、記載すること。

##### 管理画面のログイン・ログアウト手順

##### 庁内Webサーバの起動

##### 庁内Webサーバの停止

##### 庁内Webサーバ正常性確認手順

##### コンテンツアップロード手順(IIS/ダウンロード)

##### 共有フォルダ作成手順(ダウンロード)

##### 組織改編による各課ページの変更手順

#### 利用手順書については以下の項目を含め、記載すること。

##### コンテンツアップロード手順(IIS)

### サーバ運用監視

#### 運用手順書については以下の項目を含め、記載すること。

##### 管理画面へのログイン・ログアウト手順

##### サーバ運用監視サービスの起動手順

##### サーバ運用監視サービスの停止手順

##### 運用監視サーバの管理画面の表示

##### 監視対象の検索及びステータス確認手順

##### 監視対象の追加設定手順

##### 監視対象の削除設定手順

##### Web監視(応答時間の測定)の確認手順

##### 運用監視サーバのファームアップデート手順

##### 運用監視サーバのバックアップ

##### 運用監視サーバのリストア

### ファイル共有(所属)

#### 所属用ファイルサーバ

##### 部局室課の所属フォルダ、部局調達NASフォルダ、ダウンロード用フォルダに対して共有設定を実施し、適切な共有権限、フォルダ権限を付与すること。

##### 各部局室課のショートカットを職員端末機へ配布すること。また、配布されたショートカットの動作を確認すること。

##### 階層化機能を利用する場合は、自動階層設定を実施すること。部局調達NASフォルダ用のボリュームについては移行完了まではすべてのファイルをコールドデータのボリュームに保存するように設定し、移行完了後に当初設計とおりに変更できるように手順書を作成し、移行部隊に引き継ぐこと。

##### iノードが枯渇しようとした場合の対応手順を作成し、運用事業者に引き継ぐこと。

##### インターネット接続系、個人番号利用事務系それぞれに移行用仮想マシンを各4台以上作成すること。移行用仮想マシンで多重度含めてコピー時間の検証/計測すること。パフォーマンスがでない場合は状況に応じて台数の増減、リソースの調整を府と検討、了承を得ること。

##### サロゲートペア文字は利用を無効化すること。

##### 現行環境から所属用ファイルサーバへのデータ移行時に、ファイルの整合性チェックをするためにファイル名の一覧を比較できる仕組みを提供すること。比較する仕組みはファイルの現行環境と移行先の環境のファイル名を比較し、機械的に可否を判断できる仕組みとすること。ファイル一覧などを出力する際は、Windowsからでは表示されないファイルが存在する可能性があるため、ストレージ上で出力した一覧とすること。

#### 所属用ファイルサーバ(バックアップ)

##### 特定の期間アクセスのないファイルを低価格の領域にファイルを移動するように設定すること。ただし、導入時に一時的にファイルの配置ポリシーを変更する必要がある場合は、運用中に変更できるように手順書を作成し、運用事業者に引き継ぐこと。

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### ファイル共有機器の管理画面接続手順

##### 所属用ファイルサーバのランプチェック

##### ファイル共有機器の起動

##### ファイル共有機器の停止

##### ファイル共有機器の正常性確認

##### ファームウェアアップデート手順

##### HA操作手順

##### 組織改編時対応手順

##### i-node設定変更手順

##### ボリューム容量変更手順

##### 自動階層のポリシー設定変更手順

##### ファイル共有機器のバックアップ

##### ファイル共有機器のリストア(SnapMirror/Snapshot(ボリューム)/Snapshot(ファイル単位))

##### フォルダ利用状況確認

##### クォータ設定変更手順

##### アクセス権限追加/削除/変更手順

#### 利用者手順書については以下の項目を含め、記載すること。

##### 所属ファイル共有利用方針とアクセス制御方針

##### 利用方法

##### データ復旧手順(Snapshotによるファイル単位のリストア)

### ファイル送受信

#### ファイル送受信サーバ

##### 運用手順書については以下の項目を含め、記載すること。

管理画面のログイン・ログアウト手順

利用者アカウントの手動登録手順

利用ユーザのファイル操作履歴の検索手順

ファイル送受信サーバの起動・停止手順

ファイル送受信サービス起動・停止手順

障害発生時の復旧及び正常性確認手順

ファームウェアのバージョンアップ方法

ファイル送受信サーバのバックアップ手順

ファイル送受信サーバのリストア手順

##### 利用者手順書については以下の項目を含め、記載すること。

府における3層間のファイル送受信と承認の考え方

利用者環境要件

ファイル送受信の画面起動方法

ファイルアップロード手順

ファイルアップロードの承認手順

ファイルダウンロード手順

#### 無害化サーバ

##### 用手順書については以下の項目を含め、記載すること。

無害化サーバの起動・停止手順

無害化サービスの起動・停止手順

無害化サービスのバージョンアップ方法

無害化サーバのバックアップ

無害化サーバのリストア

### サーバウイルス対策

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### ウイルス対策ソフトウェアへの接続手順

##### ウイルス対策ソフトウェアの起動

##### ウイルス対策ソフトウェアの停止

##### ウイルス対策ソフトウェアの管理画面の表示(クライアント状態確認とログ確認)

##### ウイルス対策ソフトウェアのアップデート方法

##### ウイルス対策ソフトウェアのパターンファイルの手動ダウンロード

##### ウイルス対策ソフトウェアのパターンファイルの手動配布

##### ウイルススキャン手動実行

##### ウイルス対策ソフトウェアのバックアップ

##### ウイルス対策ソフトウェアのリストア

### ターミナルサービス

#### 利用者手順書については以下の項目を含め、記載すること。

##### ターミナルサービスへの接続手順

##### ターミナルサービスからのログアウト手順

##### ターミナルサーバから各機器への接続手順

#### 利用者手順書については以下の項目を含め、記載すること。

##### リモートアクセス手順

##### リモートデスクトップ接続手順

### サーバログ管理

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面のログイン・ログアウト手順

##### ログ管理ソフトウェアの起動

##### ログ管理ソフトウェアの停止

##### サーバログ管理サーバ、サーバログ保管サーバの正常性確認

##### ログ管理ソフトウェアでのログの表示方法、検索方法

##### ログ管理ソフトウェアのアップデート方法

##### ログのアーカイブ方法

##### アーカイブしたログのリストア方法

##### リストアしたアーカイブログの表示方法、検索方法

##### ログ管理ソフトウェアのバックアップ

##### ログ管理ソフトウェアのリストア

### サーババックアップ

#### 運用手順書については以下の項目を含め、記載すること。

##### 管理画面へのログイン・ログアウト手順

##### バックアップサーバの起動・停止手順

##### バックアップ取得状況の確認手順

##### 遠地保管されているバックアップデータの取得状況確認手順

##### バックアップサービスの正常性確認(データ保護機能を含む)

##### バックアップ対象追加/削除/変更手順

##### バックアップのスケジュール変更手順

##### 手動でのバックアップデータ取得手順

##### バックアップデータからのリストア手順

##### バックアップ管理ソフトウェアのライセンスの更新手順

##### バックアップ管理サーバ・バックアップ転送サーバのバックアップ

##### バックアップ管理サーバ・バックアップ転送サーバのリストア

##### バックアップ保護サーバのバックアップ

##### バックアップ保護サーバのリストア

### ジョブ管理システム

#### 運用手順書については以下の項目を含め、記載すること。

##### 管理画面へのログイン・ログアウト手順

##### ジョブ管理システムの起動、停止手順

##### ジョブ管理ソフトウェアのログ確認手順

##### ジョブネットの状態確認手順

##### ジョブネットの即時実行手順

##### ジョブネットのカレンダー設定確認手順

##### ジョブネットの計画実行及び解除手順

##### 異常終了したジョブネットの再実行手順

##### ジョブ管理システムのバックアップ

##### ジョブ管理システムのリストア

### 議会等Proxy

#### 議会Proxy

##### 議会LANから議会Proxyを経由せず、庁内WEB等へのアクセスが出来ないように設定すること。

#### 運用手順書については以下の項目を含め、記載すること。

##### 管理画面へのログイン・ログアウト手順

##### リバースProxyサービスの起動・停止手順

##### 設定画面の表示方法及び設定内容の確認手順

##### 組織変更時のURLリライト追加設定手順

##### 組織変更時のURLリライト削除設定手順

##### 利用ユーザのアクセスログの確認・取得手順

##### 議会Proxyのバックアップ

##### 議会Proxyのリストア

### ファイル全文検索

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 全文検索ソフトウェアへの接続手順

##### 全文検索ソフトウェアの起動

##### 全文検索ソフトウェアの停止

##### 全文検索ソフトウェアのアップデート方法

##### 全文検索ソフトウェアのバックアップ

##### 全文検索ソフトウェアのリストア

##### ファイル可視化ポータルへの接続手順

##### ファイル可視化の手順

#### 利用者手順書については以下の項目を含め、記載すること。

##### 利用者環境要件

##### 全文検索ポータルへの接続手順

##### 文書の検索手順

##### 絞り込み条件の活用方法

### 生体認証

#### 設定作業に伴い、職員端末機へのクライアントモジュール導入の際は、運用事業者にて、配信サーバ（AssetView）を用いて配信を行っている。設計事業者及び運用事業者と連携し、モジュールの配信・設定における計画及び手順を検討すること。

また、税務情報端末機及び個人番号利用事務系物理端末については、原則として現地に赴き実機に対してインストール及び設定を行うこと。ただし、職員端末機同様に配信サーバにて配信する方法等、他の方法で行うことが効率的かつ支障がないなど合理的と考えられる場合には、府と協議し、府が承認した際に限りその方法で実施することができる。

#### 運用手順書は以下の操作を実施するための手順を作成し、府へ連携すること。

##### 管理画面への接続

##### 生体認証利用者の追加・削除

##### 正常性の確認

##### クライアントソフト配布・設定

##### サポートへの問い合わせ

#### 利用者手順書については以下の項目を含め、記載すること。

##### 生体認証センサー接続手順

##### 生体認証手順

### 端末管理

#### 運用手順書は以下の操作を実施するための手順を作成し、府へ連携すること。

##### 管理画面への接続

##### インベントリダウンロード手順

##### アプリ配信手順

##### 更新プログラム配信・適用

##### リモートコントロール

### バックアップ用クラウド環境

#### 運用手順書については以下の項目を含め、記載すること。

##### クラウド環境機器へのログイン

##### クラウド環境機器の起動方法

##### クラウド環境機器の停止方法

##### クラウド環境機器のアップデート方法

### 個人ドライブシステム

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面への接続

##### ストレージ上限の変更

##### アクセス権限の変更

##### 正常性の確認

##### 利用状況の確認

##### サポートへの問い合わせ

##### 派遣職員復帰後のデータ復旧手順

#### 利用者手順書については以下の項目を含め、記載すること。

##### OneDriveの利用方針(最大容量、共有にて許可する範囲)

##### 利用者環境要件

##### ファイル編集時の格納先とログオフ動作

##### 操作画面への接続(Web/OneDriveアプリ)

##### OneDriveアプリケーション利用時のアイコン一覧

##### ファイル共有(Web/OneDriveアプリ)

##### 旧ファイルの参照方法(バージョン管理)

##### 横断サイト(SPO)のエクスプローラ操作

##### 使用量確認

### ディレクトリ同期

#### 稼働中のMicrosoft Entra Connectとは別に、新規でMicrosoft Entra Connectを構築すること。

#### 稼働中のMicrosoft Entra Connectによるディレクトリ同期処理を妨げないよう、切り替え完了まではステージングモード状態にするなど考慮すること。

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### Microsoft Entra Connectサーバへの接続、管理シェル起動

##### 同期の正常性確認

##### サーバ起動・停止

##### ログ参照・ログ退避

##### Microsoft Entra Connectサーバリソース稼働統計情報取得

##### 監視・通知

##### バックアップ・リストア

##### 更新プログラム適用

##### 障害時運用

##### 同期対象OU追加・削除

##### 手動差分同期実行・手動完全同期実行

##### Microsoft Entra Connectバージョン確認

##### Microsoft Entra Connectバージョンアップ

### Microsoft 365 テナント

#### 新たなMicrosoft 365 テナントは払い出さず、既に稼働済みのMicrosoft 365 テナントに対し運用事業者と設定内容の協議を行い、必要に応じて設定手順書を作成すること。

#### Microsoftの365アドレス更新後にインターネットプロキシにて認証除外のURLを自動登録する処理を実装すること。また登録内容を運用事業者に通知すること。

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面、管理シェル起動

##### サービス正常性確認

##### ログ参照・ログ退避

##### 障害時運用

##### Microsoft 365ライセンス利用状況確認

##### Microsoft 365ライセンス付与・剥奪

##### 先行リリース機能設定変更

##### 管理者ロール付与・剥奪

##### Microsoft 365サポート問い合わせ起票

#### 運用手順書のうち、「ログ参照・ログ退避」はLogstorage Microsoft 365連携パックを利用する前提の手順とすること。

### 庁内メール

#### 稼働中のExchange組織にExchange Server 2019を追加して構築すること。この際、既存のExchange Server 2016－Exchange Online間で構成されたハイブリッド構成をExchange Server 2019で継続できるよう構成すること。

#### 現行の情報基盤のメール送信サーバのリレー先は、オンプレミスExchangeサーバとしており、本業務以外のその他メールサーバ含め最適なメールルーティングとなるよう設定を見直すこと。

#### Exchange Server 2016上のメールボックスをExchange Server 2019に移動すること。

#### その後、稼働中のExchange Server 2016からExchange Server 2019へ必要な機能を引継ぎ、Exchange Server 2016をアンインストールすること。

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。なお、メールボックス削除については訴訟ホールドを保持可能な手順とすること。

##### 管理画面、管理シェルへの接続

##### 正常性確認

##### サーバ起動・停止

##### ログ管理、退避

##### 稼働統計、監視・通知

##### バックアップ・リストア

##### 更新プログラム適用

##### Exchange Server CU適用

##### 障害時運用

##### 派遣職員復帰後のデータ復旧手順

##### データベースアクティブ/パッシブ切替、マウント/マウント解除

##### メールボックス作成・設定変更・削除・無効化、変換、移行

##### 証明書更新

##### ハイブリッド構成ウィザードの実行

##### マルウェア、スパムメール対応、設定変更

#### 利用者手順書については以下の項目を含め、記載すること。

##### Outlook新規接続設定

##### Outlook追加プロファイル作成

##### OWA利用方法

##### メール自動応答設定

##### メール整理

##### 組織メール・業務メール利用方法

##### メールボックス移行後操作

### 会議室予約

#### 会議室予約については、Exchangeとは別の現行会議室予約システムからExchangeのリソースメールボックスを利用した会議室予約に変更すること。

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 会議室作成方法（個別、一括）

##### 会議室設定・変更（個別、一括）

##### 会議室削除

##### 会議室承認者変更

##### 部署変更に伴う会議室予約対象者変更

#### 利用者手順書については以下の項目を含め、記載すること。また、モバイルワーク接続基盤で利用する端末(iPhone端末やAndroid端末等)での手順内容も含めること。

##### 利用対象者

##### 利用者環境要件

##### 会議室の検索

##### 会議室予約の新規作成、変更、キャンセル

##### 承認が必要な会議室の承認

### リアルタイムコミュニケーションシステム

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面への接続

##### チームの作成・削除・復元

##### チームのストレージ上限の変更

##### 利用可能なアプリの制御

##### ポリシーの更新

##### 正常性の確認

##### 利用状況の確認

##### サポートへの問い合わせ

### 庁内Web基盤システム

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面への接続

##### サイトの作成・削除・復元

##### サイトのストレージ上限の変更

##### アクセス権の変更

##### バックアップ・リストア

##### 正常性の確認

##### 利用状況の確認

##### サポートへの問い合わせ

#### 利用者手順書については以下の項目を含め、記載すること。

##### 庁内Web構成とアクセス権の方針(トップサイト、部局サイト、部局横断サイト)

##### 利用者環境要件

##### サイトコレクション容量確認

##### 部局横断チームサイト作成方法

##### サイトコレクション作成、設定方法

##### 教育庁テナントにおける利用可能リソース、接続手順

##### 旧ファイルの参照方法(バージョン管理)

### 添付メール分離

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面への接続

##### アラートログ参照手順

##### アップデート手順

##### サポートへの問い合わせ

#### 利用者手順書については以下の項目を含め、記載すること。

##### 府におけるメール暗号化と添付ファイルの扱い方針

##### 添付メール分離システムが対象とするメール宛先、LGWAN宛、庁内宛メールの扱い

##### 送信可能な最大添付ファイルサイズ、最大添付数量

##### 分離されたファイルの扱い（ストレージ保存期間、アクセス権限）

##### メール添付手順

##### 受信者側の操作手順

#### 必要に応じて内部メールサーバの中継先IPアドレスを変更すること。

### Officeアプリケーションシステム

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面への接続手順

##### Pac Serverの設定変更

##### 正常性の確認

##### サポートへの問い合わせ

#### 利用者手順書については以下の項目を含め、記載すること。

##### ライセンス認証手順(インターネット系端末)

##### ライセンス認証手順(LGWAN/個人番号利用事務系端末)

### ファイル暗号化

#### 必要に応じてインターネット接続が可能な端末にMicrosoft Purview Information Protection(MPIP)クライアントを展開すること。

#### 運用手順書は以下の操作を実施するための手順を作成し、運用事業者へ連携すること。

##### 管理画面のログイン・ログアウト手順

##### Microsoft Purview Information Protection(MPIP)の正常性確認手順

#### 利用者手順書については以下の項目を含め、記載すること。

##### 府におけるファイル暗号の考え方(任意ファイルを手動暗号)

##### 利用者環境要件(クライアント要件など)

##### 暗号化手順

##### 復号化手順

##### 秘密度ラベル設定(Officeファイル、PDFファイル)

## テスト

### 共通事項

#### テスト作業開始は、府、及び設計事業者によるテスト計画書、及びテスト仕様書の承諾を条件とすること。

#### 単体テスト、及び可用性テストは移行作業開始前までに完了すること。

#### 性能・拡張性、運用・保守テストは、ファイルサーバなど全てのデータ移行完了後に実施すること。

#### 稼働済み環境への業務影響が出るテスト作業は、代替手段による実施可否などを検討した上で実施すること。

#### テスト環境向けの機器がある場合、テスト環境向け機器もテスト実施対象とすること。

#### 稼働済み環境から設定を変更した箇所のみテスト対象とするなど、本番環境及びテスト環境のテストケースにおけるテスト実施範囲を府と協議したでテストを実施すること。

### 仮想基盤

#### 仮想基盤管理サーバと仮想化基盤サーバは、メーカーで推奨する方法でバックアップが取得できること。

#### 仮想基盤管理サーバと仮想化基盤サーバは、メーカーで推奨する方法でバックアップしたデータからリストアできること。

### ドメインコントローラ

#### 庁内ADサーバ

##### バックアップリストアのリストアテストは一部障害時と全損障害のリストアテストを実施すること。一部障害はサンプルでFSMOが動作している庁内ADサーバと他のサーバそれぞれで障害が発生した場合のリストアテストを実施すること。全損障害時は全庁内ADサーバが障害発生した場合を想定してリストアテストを実施すること。テストの環境は本番・テスト環境とは独立した環境を構築し、実機をクローンした仮想マシンで実施しても可とする。全損障害時はPDCが動作している庁内ADサーバとPDCが動作していないサーバの一部によるサンプルのテストを可とする。

#### テスト用ADサーバ

##### バックアップリストアのリストアテストは一部障害時と全損障害のリストアテストを実施すること。一部障害はサンプルでFSMOが動作しているテスト用ADサーバと他のサーバそれぞれで障害が発生した場合のリストアテストを実施すること。全損障害時は全テスト用ADサーバが障害発生した場合を想定してリストアテストを実施すること。テストの環境は本番・テスト環境とは独立した環境を構築し、実機をクローンした仮想マシンで実施しても可とする。全損障害時はPDCが動作している庁内ADサーバとPDCが動作していないサーバの一部によるサンプルのテストを可とする。

### 名前解決

#### 疑似的にサーバ障害を発生させ、残るサーバにてクライアントからの名前解決が利用できることを確認すること。

#### LGWANなど特定ドメインに対し条件付きフォワードにて名前解決が利用できることを確認すること。

#### 個人番号利用事務系の庁内ADサーバは、内部DNSサーバにフォワーダしない動作を確認すること。

#### インターネットのサイトなど条件付きフォワード先でも名前解決できないドメインの名前解決が利用できることを確認すること。

#### 条件付きフォワードと逆引きゾーンで不要なドメインが残っていないか確認すること。

### 時刻同期

#### PDCが実行されている庁内ADサーバ、テスト用ADサーバが停止している場合にPDCが動作していない庁内ADサーバ、テスト用ADサーバが内部メール中継サーバと時刻同期可能か確認すること。

#### ドメイン参加しているWindows機器の時刻同期参照先である庁内ADサーバ、テスト用ADサーバが停止している場合に、別の庁内ADサーバ、テスト用ADサーバと時刻動機可能か確認すること。

### サーバパッチ管理

#### 今回導入するWindowsサーバ、Linuxサーバから接続できるか動作確認すること。

#### Windowsサーバ、LinuxサーバそれぞれのOSでパッチを適用できるか確認すること。テスト対象については各OSサンプリングによる動作確認でも可とする。

### 庁内Webサイト(IIS)

#### 庁内Webサーバ(IIS)

##### 各課ページへの接続は庁内の端末機からテスト用利用者アカウントで接続でき、議会端末、別館 府民お問い合わせセンターの端末機からテスト用利用者アカウントで接続できないことを確認すること。

##### 議会LANから議会プロキシを経由して、庁内Webサイト等のコンテンツを閲覧できること確認すること。また、議会LANから直接庁内Webサイトのコンテンツを閲覧できないことを確認すること。

##### 議会等Proxyサーバ経由で接続する場合は、議会等Proxyサーバで指定されたURL以外に接続できないことを確認すること。

##### 利用者と同じ権限のテスト用利用者アカウントでコンテンツがアップロードできるか確認すること。

##### 教育庁の端末機からテスト用利用者アカウントで各課ページ接続できることを確認すること。

#### 庁内Webサーバ(ダウンロード)

##### 庁内の端末機、教育庁の端末機から共有フォルダ、ダウンロードフォルダに設定された権限のみアクセスできるかテスト用利用者アカウントで確認すること。

##### 利用者と同じ権限のテスト用利用者アカウントでコンテンツがアップロードできるか確認すること。

### サーバ運用監視

#### 疑似障害にて各監視項目のサンプリングテストを行い、全監視項目が運用監視サーバにて検知されるか確認すること。

#### 各監視項目のテストはファイルサーバなどの全てのデータ移行完了後に実施すること。

#### Web監視(応答時間の測定)が問題無く行えるか確認すること

#### 監視サーバ自体の監視について正常に監視できていることを確認すること。

#### ログ監視についてサーバログ管理サーバと連携し、異常なログに関して通知が問題無く行われるか確認すること。

#### メーカー推奨の手順でバックアップ・リストアを実施できるか確認すること。

### ファイル共有(所属)

#### 所属用ファイルサーバ

##### 設計事業者にて移行開始するため、受注者にて2025年6月13日までにファイル共有(所属)のテストを完了すること。

##### 冗長化しているすべてのコンポーネントの信頼性を確認すること。確認できないコンポーネントについてはテスト計画で府と協議し、了承を得ること。

##### インターネット接続系のボリュームはインターネット接続系の端末、個人番号利用事務系のボリュームは個人番号利用事務系の端末からのみ接続可能であることを確認すること。

##### ボリュームのバックアップテストを対象のボリュームで実施すること。リストアテストはシステム管理者によるボリューム、ファイルのリストア、利用者アカウントと同じ権限のアカウントによるファイルのリストアを実施すること。なお、リストアテストはサンプルのボリューム単位、サンプルファイルでのリストア実施を可とする。

##### 遠地バックアップテストを対象のボリュームで実施すること。リストアテストについてはサンプルのボリュームでの実施を可とする。

##### 遠地バックアップからのリストアテストで計測した時間をもとに、遠地バックアップからのリストアの想定時間を府に提示すること。

##### 遠地バックアップからのリストア時に自動階層の設定変更などを一時的に実施する必要がある場合は、リストア手順にその旨と付随する手順を記載すること。

##### ボリュームの使用量、iノードが閾値を超えた場合のアラートを確認すること。

##### ランサムウェア対策において、パターンを学習させ、疑似ランサムウェアによる動作を確認すること。

### ファイル送受信

#### ファイル送受信

##### 基本設計書、詳細設計で設計した項目及び設定した項目と以下の要件を基に、テスト仕様書を作成し、テストを実施すること。

##### ファイル送受信は、利用者が使用している系統以外の系統へのアクセスができないことを確認すること。

##### 利用者管理システムにて作成されたファイル送受信用のCSVデータを自動で取込み、利用ユーザ及び承認者の登録を日次にて一括で設定可能かテスト実施すること。

##### 利用ユーザがSSOにて利用が可能かテストを実施すること。

##### クライアントに設定する証明書が配布されているかテストを実施すること。

##### ログの取得及びローテーションが正常に行われているかテストを実施すること。

##### 障害時を想定してActive・Standbyの切り替えが正常に行えるかテスト実施すること。

#### 無害化サーバ

##### 基本設計書、詳細設計で設計した項目及び設定した項目と以下の要件を基に、テスト仕様書を作成し、テストを実施すること。

##### 無害化後の原本保持及び無害化されていることをサンプルファイルやマクロファイル等を利用しテストを実施すること。

##### 無害化できない拡張子のファイルについてはエラーとなり、利用者へ通知されることを確認すること。

### サーバウイルス対策

#### ウイルススキャンテストに関してはリアルタイムスキャンとスケジュールスキャンの両方を実施すること。

#### ウイルススキャン機能にてサンプルファイル等を利用しウイルスを検知した際の隔離、駆除等の動作確認については原則、全サーバにて確認すること。

#### スキャン除外対象設定されたファイルに対してスキャンされないことを確認すること。スキャン除外フォルダについてはサンプルフォルダでの実施を可とする。

#### ウイルス対策対象のサーバ及び端末が全て登録されていることを確認すること。

#### 最新のパターンファイルがサーバに自動配布されていることを確認すること。

#### ウイルスの検知等の情報が管理画面で検索できることを確認すること。

#### 最新のパターンファイルがインターネットから問題無く、ダウンロードされていることを確認すること。

#### 室課等にて独自調達した端末でのテストについては府と調整の上、実施すること。

#### 対象サーバ全台で実施しないテストについては、OS種別(Windows、Linux)ごとに実施すること。

### ターミナルサービス

#### 許可されたユーザが、インターネットなどの庁外からターミナルサーバへ、リモートでログインできること。

#### ターミナルサーバからのログインを許可されている仮想基盤、仮想マシン、ネットワーク機器、ストレージにログインできること。

#### 許可されたユーザ以外が、インターネットなどの庁外からターミナルサーバへ、リモートでログインできないこと。

#### ターミナルサーバからのログインが許可されているサーバ、機器以外へのログインができない事を確認すること。

#### WEBブラウザとしてEdgeが使用できること。

#### Tera Termで機器に接続できること。

#### Office/Acrobat Readerが使用できること。

### サーバログ管理

#### サーバログ管理サーバ

##### 管理者向けのログとして、ログインアカウント、ログイン日時、ログアウト日時、ログインした端末のIPアドレスなどが取得できていること。

##### 利用者のログとして各機能へのログインアカウント、ログイン日時、ログアウト日時、ログインした端末のIPアドレス、操作状況、ファイルダウンロード状況などが取得できていること。

##### 既定の日数分の監査ログがデータベースに保存されていること。

##### 既定の期間を超えた監査ログが既定の日数をアーカイブされていること。

##### アーカイブした監査ログがリストアできること。

##### 監査ログが負荷分散装置で分散されて収集されていること。

##### 監査ログで異常を知らせるログが出力された場合、異常を検知することを確認すること。異常検知の確認は、確認するサーバを府と協議し合意すること。

##### メーカーで推奨する方法でバックアップが取得できること。

##### メーカーで推奨する方法でバックアップしたデータからリストアできること。

#### サーバログ保管サーバ

##### 過去の監査ログが閲覧できること。

##### アーカイブした監査ログをリストアし、閲覧できること。

##### メーカーで推奨する方法でバックアップが取得できること。

##### メーカーで推奨する方法でバックアップしたデータからリストアできること。

### サーババックアップ

#### バックアップ管理サーバ/バックアップ転送サーバ

##### バックアップについては対象となる全サーバにてバックアップを取得できるか確認すること。

##### リストアについては、機能毎にサンプリングで実施すること。

##### 設計された世代数のバックアップを取得できるか確認すること。

##### ミドルウェアはメーカーで推奨する方法でバックアップ及びリストアができることを確認すること。

##### 物理APについては構成情報がバックアップ管理サーバにて取得できていることを確認すること。

##### 遠地保管バックアップデータからのリストアができること。

##### リストア時間のサンプリングを採取し、リストアにかかる想定時間を算出すること。遠地保管バックアップからのリストアについても時間を算出すること。

##### 指定した時間内にバックアップが完了しているかを確認すること。

#### バックアップ保護サーバ

##### バックアップ保護サーバのバックアップデータが更新、編集ができないことを確認すること。

##### リストア時間のサンプリングを採取し、リストアにかかる想定時間を算出すること。遠地保管バックアップからのリストアについても時間を算出すること。

### ジョブ管理システム

#### スケジュール登録されているジョブネットを実行し、エージェントがインストールされているサーバ内のバッチ及びスクリプトが、問題無く実行されているか結果を確認すること。

#### ジョブ管理サーバ内に配置し、実行するバッチ及びスクリプトが、問題無く実行されているか結果を確認すること。

#### ジョブ実行時の完了及び異常終了時にメール通知が行われるか確認すること。

### 議会等Proxy

#### 議会LANから議会等Proxyを経由しない通信が庁内WEBへアクセス出来ないことを確認すること。

#### 議会LANから庁内WEBへアクセスする際は仮想URLにて接続しているか実際に利用される仮想URLを用いてテストを実施すること。

#### 議会LANから庁内WEBサイトへアクセスする際に想定されていない階層やファイルが閲覧出来ないことをテストすること。

#### 正常にアクセスログが取得出来ているかテストを実施すること。

### ファイル全文検索

#### 全文検索サーバ

##### 所属用ファイルサーバの文章情報を収集する際に、自動階層に影響ないことを確認すること。

##### 複数台で構成する全文検索サーバのうち、1台に障害が発生しても他の全文検索サーバに影響なく文書情報が収集できること。

##### 既定の日数分のログが、サーバ内に保存されていること。

##### 職員端末機からのファイル全文検索が、正常に検索されていること。

#### 全文検索管理サーバ

##### 文書の絞り込み条件として、ファイル種別、最終更新者、ファイルサイズ、ファイル更新日、フォルダ指定が選択できること。

##### ファイル全文検索結果に、検索したユーザアカウントの閲覧権限がないファイルが表示されないこと。

##### [別紙２ 庁内ネットワーク情報基盤機器等構成概要]の[(15) ファイル全文検索]で記載されている文書形式を検索できること。

#### ファイルサーバ可視化サーバ

##### 所属用ファイルサーバの文章情報を収集する際に、自動階層に影響ないことを確認すること。

##### 一定期間参照されていないデータや一定容量を超過したデータ等、削除・アーカイブ対象となるデータを分析できること。

### ディレクトリ同期

#### テスト実施時は、新規構築したMicrosoft Entra Connectをステージングモード状態とする等、現行稼働のディレクトリ同期処理に不具合が起きないよう考慮すること。

#### 以下をテスト観点として最低限取り込み、運用作業や業務シナリオ等を踏まえたテストケースを府と協議し、漏れなくテストを実施するよう考慮すること。

##### ディレクトリ同期が自動かつ定期的に実行されることを確認すること。

##### 自動アップグレード機能は、機能として実行されないことを確認すること。

##### 同期オブジェクトの情報が、SQL Server 2022 に蓄積されることを確認すること。

##### オブジェクト保護機能による上限値を超えるオブジェクト削除は、業務利用しているオブジェクトを対象とせず動作確認すること。

##### シームレスシングルサインオン機能は、シングルサインオン先のサービス及び操作するデバイスの網羅性を担保した上で動作確認すること。

##### オンプレミスActive Directoryの同期対象件数とMicrosoft Entra Connectのディレクトリ同期処理の対象件数を確認すること。

##### 有効状態、無効状態などのアカウント状態種別ごとに同期確認及び認証動作確認すること。

##### 同期対象外の条件を満たすアカウントの同期確認及び認証動作確認すること。

##### バックアップテスト及びリストアテストを実施すること。

##### Microsoft Entra Connectの障害を再現した上で、障害テストを実施すること。

##### 上記の他、各設計に従った動作となっていることを確認すること。また設計からの変更点については、変更した設計通りに動作すること。

### 生体認証

#### 全てのテスト項目について妥当性を示すエビデンスを残すこと。

#### 税務情報端末機について、複数台にて起動後に生体認証が行われることを確認する。

#### 職員端末機において、個人番号利用事務系仮想デスクトップを起動時に生体認証が行われ、LGWAN接続系デスクトップ起動時には生体認証が動作しないことを確認すること。

#### 冗長化されているサーバの障害を想定し、片系においても機能が提供できることを確認すること。

### 端末管理

#### 全てのテスト項目について妥当性を示すエビデンスを残すこと。

#### アプリケーション配信においては拠点の端末台数等を想定し、配信サイズや配信数について運用指針となるテストケースを検討及び実施すること。

#### 運用事業者とも連携し、必要なテスト項目を網羅すること。

### Microsoft 365 テナント

#### 以下をテスト観点として最低限取り込み、運用フローや業務シナリオ等を踏まえたテストケースを府と協議し、漏れなくテストを実施するよう考慮すること。

##### 本業務に含まれる機器「利用者管理システム」からの連携によって、Microsoft 365テナント上のユーザアカウントに対するMicrosoft 365ライセンスの付与及び剥奪ができること。

##### Logstorage Microsoft 365連携パックによって、Microsoft 365の監査ログが外部保管できていること。

##### 条件付きアクセスポリシーの各ポリシーによって、意図したアクセス制御をできていること。

##### 府が指定したロゴ画像が、Microsoft 365のWeb UIに表示されていること。

##### 業務利用想定のある端末、クライアントアプリケーション、接続先Microsoft 365サービスを洗い出し、端末とクライアントアプリケーションの組み合わせを基にMicrosoft 365サービスへの接続ができること。

##### 個人用Microsoft 365テナントへのアクセスできないこと。

##### 府外のTeamsへのゲスト参加など、府外の企業用Microsoft 365テナントへのアクセスができること。

##### Microsoftのアドレス更新後にインターネットプロキシにて認証除外のURLを自動登録すること。

##### インターネットプロキシにて認証除外のURL登録後に、運用事業者に登録内容を通知すること。

##### 上記の他、各設計に従った動作となっていることを確認すること。また、設計からの変更点については、変更した設計通りに動作すること。

### 庁内メール

#### 以下をテスト観点として最低限取り込み、運用作業や業務シナリオ等を踏まえたテストケースを府と協議し、漏れなくテストを実施すること。

##### テスト実施時は、既存環境への影響を避けるため、テスト未完了のサーバを使ったメール配送がされないよう構成を考慮すること。

##### 連携している他システムや運用作業へ影響を与えないことを確認した上でテストを実施すること。

##### メールサーバ、会議室予約としての基本的な機能について、正常に動作することを確認すること。

##### メールボックス移行については、移行前にリハーサルを行い、移行の正常性を確認すること。

##### ハイブリッド構成が維持できているか、サーバをバージョンアップするごとに確認すること。

##### 設計上ExpressRoute経由となる通信が、想定通りの通信経路となっていること。

##### ExpressRoute変更後、変更に伴う影響箇所について既存どおり機能していることを確認すること。

##### LGWAN宛の配信不能メールのみ返されること。また配信不能メールの送信者アドレスが設計通りとなっていること。

##### スパム、ウイルス対策の通知メールが設計通り届くこと。

##### 想定しているなりすましメールのみ庁外より受信できること。

##### メールヒントで特定ドメイン（教育庁）が内部扱いになっていること。

##### 訴訟ホールドが有効になっていること。また、退職等となった利用者のメールデータが訴訟ホールドで保持されていること。

##### 派遣となった職員のメールデータがクラウド上に設計した期間保持されていることを確認すること。

##### 派遣となった職員が復帰した場合に、メールの送受信ができることを確認すること。

##### 障害テストを実施し、サーバの単一障害が発生してもサービス停止が発生しないこと。

##### バックアップがエラーなく正常に取得できること。また、リストアテストを実施し、正常復旧すること。

##### テストウイルスによるウイルス検知を確認すること。

##### 上記の他、各設計に従った動作となっていることを確認すること。また設計からの変更点については、変更した設計通りに動作すること。

### 会議室予約

#### 会議室の登録・設定変更・削除で利用するPowerShellスクリプトの動作を確認すること。

#### 作成した会議室が想定通り予約できること。

#### 所属限定の会議室が、想定通り限定された利用者からのみ参照・予約可能となること。

#### 承認が必要な会議室に会議室予約が送信された場合、承認者に電子メールにて通知が届くこと。また、通知を承認者が承認/辞退することでその予約が確定または却下されること。

#### オンプレミス上のユーザからも会議室が予約可能であること。

#### 上記の他、各設計に従った動作となっていることを確認すること。また設計からの変更点については、変更した設計通りに動作すること。

### 個人ドライブシステム

#### 個人ドライブシステムのコンテンツをゲストユーザに共有できないことを確認すること。

#### 個人ドライブシステムのコンテンツを組織内のユーザ間で共有できることを確認すること。

#### アカウントが削除された場合でも、個人ドライブシステムのコンテンツは削除されないことを確認すること。

#### 削除されたアカウントの個人ドライブシステムのコンテンツが利用者管理システムによって削除されることを確認すること。

#### 個人ドライブシステムのクライアントアプリを用いて、外部の個人ドライブシステムとは同期できないことを確認すること。

#### 個人ドライブシステムのコンテンツがバージョン管理されていることを確認すること。

#### 個人ドライブシステムでコンテンツの過去のバージョンを復元できることを確認すること。

#### 派遣となった職員の個人領域データがクラウド上に設計した期間保持されていることを確認すること。

#### 派遣となった職員が復帰した場合に、個人領域のデータを書込、参照できることを確認すること。

#### ユーザが利用できる個人ドライブシステムの容量の90%を超過した場合、ユーザに通知されることを確認すること。

#### 職員端末機の定められた場所にフォルダが作成され、個人ドライブシステムと同期したコンテンツがフォルダ内に保存されていることを確認すること。

#### 職員端末機のディスクの空き容量が50GBを下回った場合、ユーザにディスクの空き容量が不足していることを伝える警告が通知されることを確認すること。

#### 職員端末機のディスクの空き容量が25GBを下回った場合、個人ドライブシステムからコンテンツをダウンロードできなくなることを確認すること。

#### 職員端末機のログオフ時にローカル領域から個人ドライブシステムと同期したコンテンツが削除されることを確認すること。

#### 対象の個人ドライブシステムに対してアクセス権を付与することで個人ドライブシステムのコンテンツを参照できることを確認する。

### リアルタイムコミュニケーションシステム

#### 1対1のチャットを利用できることを確認すること。

#### 3人以上の複数人でチャットを利用できることを確認すること。

#### 外部組織のユーザとチャットできないことを確認すること。

#### リアルタイムコミュニケーションシステム管理者が管理センターからチームを作成できることを確認すること。

#### リアルタイムコミュニケーションシステム管理者が管理センターからチームを削除できることを確認すること。

#### 権限を付与されたユーザがチームのメンバーを追加できることを確認すること。

#### 権限を付与されたユーザがチームのメンバーを削除できることを確認すること。

#### 職員主催のWeb会議で職員が画面共有するとき、外部組織ユーザへ画面制御の譲渡ができないことを確認すること。

#### 職員のSIM端末からリアルタイムコミュニケーションシステムにアクセスできることを確認すること。

#### リアルタイムコミュニケーションシステム向けに展開されているサードパーティー製のアプリケーションが利用できないことを確認すること。

#### リアルタイムコミュニケーションシステム向けに展開されているファーストパーティー製のアプリケーションが利用できることを確認すること。

#### リアルタイムコミュニケーションシステム向けに開発したカスタムアプリケーションが利用できないことを確認すること。

### 庁内Web基盤システム

#### 庁内Web基盤システムのトップページとして庁内Webサイトが設定されていることを確認すること。

#### 庁内Web基盤システムのトップページに配置した各部局サイトのリンクから該当する部局サイトにアクセスすることを確認すること。

#### 庁内Webサイト及び各サブサイトは、サイトごとに表示するコンテンツやサイトカラー等のデザインが設定されていることを確認すること。

#### 庁内Web基盤システムのコンテンツに対して、ユーザごとに閲覧・投稿等の操作が制御されていることを確認すること。

#### ゲストユーザ(府立学校ユーザ)が庁内Web基盤システムにアクセスできることを確認すること。

#### 庁内Web基盤システムのサイトを手動で削除できることを確認すること。

#### サイト単位でバックアップできることを確認すること。

#### バックアップからサイト単位で復元できることを確認すること。

### 添付メール分離

#### メールサイズ上限未満のメールは配送され、サイズ上限を超過するメールは送信者にエラー通知されることを確認すること。

#### 添付ファイルは画像による署名含め添付された100個以上の全ファイルが本文から分離されることを確認すること。

#### 疑似的にサーバ障害を発生させ、利用者からのメール送信はエラーなく相手先に送信されることを確認すること。

#### LGWANを宛先とするメールは、添付ファイルが分離されないことを確認すること。

#### メールの宛先に含まれる全てのメールアドレスを利用し、外部ストレージに格納された添付ファイルを参照できることを確認すること。

#### メールの宛先に含まれないアカウントは外部ストレージに格納された添付ファイルを参照できないことを確認すること。

#### 疑似的に外部ストレージ障害を発生させ、管理者へのメール通知、及びメール配送の保留動作を確認すること。

#### 疑似的に発生させた外部ストレージ障害の復旧後は、メール再配送されることを確認すること。

#### 稼働後のサーババージョンアップ作業を考慮し、負荷分散装置からの単一サーバ切り離し、バージョンアップを実行すること。また、作業時は職員のメール送信業務が停止しないことを確認すること。

### Officeアプリケーションシステム

#### 設計通りにインターネット接続系端末へアプリが展開され、アプリを利用できることを確認すること。

#### 設計通りにLGWAN接続系端末へアプリが展開され、アプリを利用できることを確認すること。

#### 設計通りに税端末(個人番号利用事務系)へアプリが展開され、アプリを利用できることを確認すること。

#### 設計通りに税端末以外の個人番号利用事務系端末へアプリが展開され、アプリを利用できることを確認すること。

#### LGWAN接続系端末及び個人番号利用事務系端末はPac Serverの設定に基づいた通信経路にて認証を行うことを確認すること。

### ファイル暗号化

#### 任意のファイルをエクスプローラの右クリックより暗号化できることを確認すること。

#### 暗号化されたファイルは庁内ユーザにて参照が可能であることを確認すること。

#### 暗号化されたファイルは庁外のユーザは参照が不可能であることを確認すること。

#### ファイル外部持出用に右クリックで復号化し、庁外のユーザに送信し参照可能であることを確認すること。

## 移行

### 移行リハーサル

#### 移行設計にて府の承認を得た移行内容を手順化し実施すること。

#### 調達機器等の移行に当たっては、可能な限り本番移行作業を模した条件下において、移行リハーサルを実施すること。

#### 移行リハーサル開始前に調達機器等のバックアップを取得しておくこと。

#### 移行リハーサルにおいて、移行手順書、テスト仕様書及びタイムチャート（以下「移行手順書等」という。）が適切であることを検証すること。

#### 移行リハーサルにおける検証結果に基づき、移行手順書等の問題点を洗い出し、必要に応じて移行手順書等を修正すること。

### 本番移行

#### 移行手順書に基づき、調達機器等の移行作業を実施すること。

#### 移行開始前に調達機器等のバックアップを取得しておくこと。

#### 調達機器等の移行後、テスト仕様書に基づき調達機器等の動作が、設計した要件を満たしていることを確認すること。

#### 動作確認の結果を速やかに設計事業者等に報告し、移行の判定を仰ぐこと。その結果、切り戻しが必要となった場合は、速やかに対応すること。

#### 動作確認後、テスト成績書を作成し、府の承諾を得ること。

#### テスト成績書の承諾後、リリース版のバックアップを行い、設定情報データ及びバックアップデータを納品すること。

#### テスト成績書の承諾後であっても、賃貸借期間の開始日までに設定の変更が必要となった場合は、府と協議の上、設定対象機器の全てに対して行うこと。

### ドメインコントローラ

#### 庁内ADサーバ

##### 庁内ADサーバに登録されているオブジェクトを次期庁内ADサーバに移行すること。

##### 既存環境や端末機への影響を少なくするために、現行機のホスト名/IPアドレスを引き継ぐこと。

##### FSMOは現行機と同様の庁内ADサーバ#4に引き継ぐこと。

##### 次期庁内ADサーバへの切り替えは2025年９月末までに移行完了すること。また、業務影響が少ない時間帯で実施すること。

##### リハーサルを実施する場合は、本番・テスト環境とは独立したテスト環境を構築し、現行環境をクローンした環境で実施すること。

##### 移行完了後GPOが次期庁内ADサーバに移行されているか、GPOの内容を比較すること。

##### 移行後テスト用アカウントを作成/削除し、オブジェクトの内容がレプリケーションされていることを確認すること。

##### メンバーサーバ、端末機に対してテスト用アカウントでログインできるか確認すること。

##### CAルート証明書を次期庁内ADサーバに移行すること。CAルート証明書を移行するにあたり、有効期限を運用に耐えうる期間に延長すること。

##### 発行済みの証明書を移行すること。

##### 証明書移行後、発行済みの証明書が正常に動作しているか確認すること。確認する証明書は、サーバ証明書、クライアント証明書のサンプリングで確認すること。

##### 現行の庁内ADサーバはFRSからDFSRへの切り替えSTEP2の段階となっている。本番・テスト環境とは独立したテスト環境を構築し、現行環境で稼働している庁内ADサーバのクローンで問題ないことを検証後、DFSRに変更すること。

##### DFSRに切り替え後、LGWAN接続系 ADサーバ(3台)と共通基盤認証用ADサーバ(1台)をWindows Server 2022に移行すること。動作させる仮想化基盤は、情報基盤の仮想化基盤で動作させること。仮想サーバを新規作成する場合はテンプレートを使用すること。

#### テスト用ADサーバ

##### テスト用ADサーバに登録されているオブジェクトを次期テスト用ADサーバに移行すること。

##### 既存環境や端末機への影響を少なくするために、現行機はホスト名/IPアドレスは引き継ぐこと。

##### FSMOは現行機と同様のテスト用ADサーバ#1に引き継ぐこと。

##### 次期テスト用ADサーバへの切り替えは、利用しているサービスに影響がない時間帯で実施すること。

##### リハーサルを実施する場合は、現行環境に影響しない完全に切り離した環境で実施し、現行環境をクローンした環境で実施すること。

##### 移行完了後GPOが次期テスト用ADサーバに移行されているか、GPOの内容を比較すること。

##### 移行後テスト用アカウントを作成/削除し、オブジェクトの内容がレプリケーションされていることを確認すること。

##### メンバーサーバ、端末機に対してテスト用アカウントでログインできるか確認すること。

##### 移行後テスト用アカウントを作成/削除し、オブジェクトの内容がレプリケーションされていることを確認すること。

### 名前解決

#### 庁内ADサーバ

##### 現行の庁内ADサーバから次期庁内ADサーバにレプリケーションされない条件付きフォワードを移行すること。

##### LGWAN接続系ADサーバをWindows Server 2022に移行後、LGWAN DNSサーバを参照しているDNSクライアントがないことを確認し、LGWAN DNSサーバを停止しても問題ないことを確認し、LGWAN DNSサーバを停止すること。

##### 「hq.admix.go.jp」などレプリケーションされた条件付きフォワードを解除し、個別で条件付きフォワードを設定する場合は、LGWAN接続系ADサーバに対しても条件付きフォワードの設定を追加すること。

#### テスト用ADサーバ

##### 現行のテスト用ADサーバから次期テスト用ADサーバにレプリケーションされない条件付きフォワードを移行すること。

### ファイル共有(所属)

#### 現行環境から所属用ファイルサーバへのデータ移行時に、ファイルの整合性チェックをするためにファイル名の一覧を比較できる仕組みを提供すること。比較する仕組みはファイルの現行環境と移行先の環境のファイル名を比較し、機械的に可否を判断できる仕組みとすること。ファイル一覧などを出力する際は、Windowsからでは表示されないファイルが存在する可能性があるため、ストレージ上で出力した一覧とすること。

### サーバログ管理

#### サーバログ管理サーバ

##### 現行の情報基盤から移行した過去のログは、サーバログ管理サーバで表示できる形式で移行すること。

#### サーバログ保管サーバ

##### 庁内ネットワーク情報基盤仮想基盤のサーバのログは、3年分のログを保存するため、現行の情報基盤で保存しているログの過去3年分を、次期のサーバログ保管サーバに移行すること。

##### 個人番号利用事務系情報基盤のサーバのログは、10年分のログを保存するため、現行の情報基盤で保存しているログの過去5年分を、次期のサーバログ保管サーバに移行すること。

### ジョブ管理システム

#### 現行の情報基盤にて利用している再起動ジョブを除くジョブネットを次期にて利用する場合は、次期ジョブ管理サーバへ移行すること。

#### 現行の情報基盤にて利用しているジョブ管理サーバで実行しているバッチ及びスクリプトを移行すること。

#### 移行にあたりジョブネットの変更が発生する場合は、担当ベンダと協議して移行すること。

### 議会等Proxy

#### 組織変更等で庁内WEB上のイエローページなどに変更があった場合は、議会等ProxyについてもURLリライト先の変更を実施すること。

### 生体認証

#### 生体認証データを移行した場合は、移行後に移行元の生体認証データが全て移行できていることをエビデンスとして示すこと。

#### 既存の生体認証システムの認証ログについては、エクスポートを行い府が指定する場所に保存すること。

#### 物理端末機の生体認証クライアントは受注者にてインストールと設定を行い、動作確認を行うこと。インターネット接続系の物理端末機においては、庁内の配信サーバを利用しモジュールの配信及び設定を行うことも可とする。

### 端末管理

#### インターネット接続系物理端末機　約600台と税務情報端末機 約1,300台の端末を移行もしくは再登録し、管理できるようにすること。

#### 移行後、複数台の端末にて以下機能が動作することを確認し、エビデンスとして示すこと。

##### インベントリ

##### 更新プログラム管理

##### アプリケーション配信

##### リモートコントロール

#### エージェントの入替は職員にて実施する為、入替における手順書を提示すること。また、入替におけるモジュールの配信については、運用事業者にて庁内の配信サーバより実施する。

### ディレクトリ同期

#### 受注者が、新規構築したMicrosoft Entra Connectがディレクトリ同期処理の主体となるよう切り替えすること。

#### 切り替え完了後、稼働していたMicrosoft Entra Connectのアンインストール及び機器のシャットダウンを受注者が実施すること。

#### イを実施するにあたり、アンインストールすることでディレクトリ同期に影響が出ないことを受注者者が確認してから着手すること。

### 庁内メール

#### 現在の庁内メール構成にメールボックスサーバを追加登録してメールボックスの移行を行うなど、安全確実な方法で移行すること。

#### オンプレミスExchange Serverは2019に移行し、その後次期バージョンのExchange Serverへ移行すること。

#### オンプレミス側に残す約600個のメールボックスを最新のExchange Serverへ移行するとともに、ハイブリッド構成を維持し、必要な機能を最新のExchange Serverに引き継ぐこと。

#### 現在オンプレミスに配置された派遣者(約350ユーザ)をクラウドへ移行すること。移行後にライセンス割当を削除すること。

#### Microsoft365テナント、Entra ID、Exchange OnlineやTeams等のMicrosoft365サービス、ExpressRoute、AD同期やハイブリッド構成及びその他オンプレミスのサーバを含め、作業順序を考慮した、安全確実な移行方法で移行すること。

#### 利用者管理システムの処理に影響を与えない時間帯に移行作業を実施すること。

#### 可能な限りシステムを停止することなく移行すること。止むを得ずシステム停止が必要な場合は、府と協議し夜間又は休日に移動作業を行うこと。

#### 府の承認を得た移行手順を準備し、検証環境での移行を行った上で手順、スケジュールの見直しを行い、府の承認を得て本番環境の移行を実施すること。

#### 移行に際し、メールサーバに対して必要となるスキーマ拡張作業を行うとともに、本業務期間中に必要となるCU適用作業を適宜実施すること。

#### 新バージョンのExchange Serverへ移行後、旧バージョンのExchange Serverをアンインストールし、AD上に残っている旧サーバの情報を削除すること。

#### 職員による移行作業が発生する場合は、移行手順書を作成・提供し、職員が円滑に作業できるよう支援すること。

### 会議室予約

#### 以下の作業を、特別記載がある場合を除き受注者にて実施すること。

##### 会議室予約については、Exchangeとは別の現行会議室予約システムからExchangeのリソースメールボックスを利用した会議室予約に変更すること。

##### 既存の会議室予約システムから各会議室の設定を引き継ぐこと。具体的な引き継ぐパラメータは基本設計書及び既存会議室予約システムを確認すること。

##### 会議室の作成は一括で実施すること。そのためのPowerShellスクリプトを作成し、リソースメールボックスをExchange Online上に作成すること。

##### リソースメールボックスのアカウントは、オンプレミスのActive Directoryから同期する構成とすること。

##### 変更となる会議室だけCSVファイルを作成して設定変更できるPowerShellスクリプトを用意すること。

##### 会議日付が2025年6月から8月までの会議は、現行会議室予約システムを利用するため、利用者からの新システムの会議室予約は８月末までシステム制御にて予約不可とすること。

##### 2025年9月以降の新システムへの会議室予約は、予約者本人が実施すること。

##### 会議室予約の操作手順書を提供すること。また、操作手順書を運用事業者に引継ぎ、運用事業者による利用者からの問合せを支援すること。

##### 受注者にて現行賃貸借事業受注者及び運用事業者と調整し、現行会議室予約システムで、会議日付が2025年9月以降となる予約を予約禁止できるようにすること。

### ファイル暗号化

#### 移行後の復号化されたフォルダ内データを受注者にて一括暗号化を検討すること。開発元への問合せ回答として一括暗号化が難しい場合は、暗号化手順を作成し利用者へ説明すること。

### Officeアプリケーションシステム

Officeアプリケーションシステムの移行については、職員にて対応するため、移行手順書を作成すること。なお、配信については運用事業者にて庁内の配信サーバより実施すること。

## 引継ぎ

### 以下の要件に基づき、運用事業者等という。）と協議の上、運用引継計画書を作成すること。

#### 手順書、資料等の作成だけではなく、全ての引継事項について一巡することを原則とした操作訓練や説明会を開催する等、十分な引継ぎが行える計画とすること。

#### 操作訓練、説明会等の開催日時は、運用事業者等の要望を十分に反映すること。

#### 引継事項として想定されるものは以下のとおり。

##### 調達機器等の利用方法及び状態確認方法

##### 調達機器等の設定変更方法及び管理方法（ファームウェアのバージョンアップ手順を含む）

##### 障害発生時の切分け及び復旧方法（バックアップの取得及びリストア方法を含む）

##### 保守及び技術支援の利用方法（保守及び技術支援の利用手順、受付窓口の連絡先等を含む）

### 運用引継計画書の作成に当たっては、運用事業者等と十分な連携及び調整を行い、府の承諾を得ること。

### 運用引継計画書及び以下の要件に基づき、調達機器等における運用事項、管理事項等、運用に必要となる手順を記した運用手順書及び管理情報を記した運用管理資料を作成すること。

#### 運用手順書及び運用管理資料の記載内容は、運用事業者等の要望を十分に反映すること。

#### 運用手順書は、調達機器等の操作方法だけではなく、運用業務において実際に必要となる複数の操作を組み合わせた一連の作業を想定した内容とすること。

#### 運用手順書には、以下のドキュメントを含むこと。

##### 調達機器等の操作方法や作業手順を記載した操作手順書

##### 保守及び技術支援の連絡体制や連絡先を記載した保守・技術支援体制図

##### 保守及び技術支援を利用する手順を説明した保守・技術支援利用手順書

#### 運用管理資料には、以下のドキュメントを含むこと。

##### アカウント管理台帳（機器名、ホスト名、管理画面への接続方式、接続先アドレス、管理者ID・パスワード、パスワード変更可否等）

##### 証明書管理台帳（機器名、Common Name（コモンネーム）、使用用途、有効期限、新たな証明書の入手方法・更新手順等）

##### ライセンス管理台帳（機器名、ホスト名、ライセンス名称、ライセンス数量、ライセンスキー等）

##### ライセンス証書、ライセンス体系の説明書等のライセンス関係資料

### 運用手順書及び運用管理資料の作成に当たっては、運用事業者等と十分な連携及び調整を行い、府の承諾を得ること。

### 運用引継計画書に基づき、運用事業者等に対して引継ぎ作業を行うこと。

### 引継ぎ作業が完了した段階で、引継完了報告書を作成し、府の承諾を得ること。引継ぎ内容が不十分と判断された場合は、理由を確認し、説明会等を再度実施すること。

## 納品

### 以下に示すドキュメント、データ等を、紙媒体で１部、電子媒体で1部納品すること。電子媒体の種類は、設計事業者等の指示に従うこと。

なお、設計事業者等が様式及びファイル形式を指定した場合は、当該様式及びファイル形式に従うこと。

#### 管理

##### 業務実施計画書

##### WBS（Work Breakdown Structure）

##### 進捗報告書

##### 課題管理表

##### リスク管理表

##### 会議議事録

#### 詳細設計

##### 詳細設計書

##### 機器構成表

##### ネットワーク物理構成図

##### ネットワーク論理構成図

##### ラック構成図

##### ケーブル結線図

##### ストレージディスク接続構成図

##### ストレージディスク構成表

##### 環境設定書

#### 移行設計

##### 移行設計書

##### 作業体制図

##### 移行日程表

##### 移行手順書

##### テスト計画書

##### テスト仕様書

##### タイムチャート

#### 配線／設置

##### 施工図面（配線）

##### 設置図面（機器）

##### 現場写真（設置）

#### 設定

##### テスト成績書（設定）

#### 移行

##### テスト成績書（移行）

##### 設定情報データ（電子媒体のみ）

##### バックアップデータ（電子媒体のみ）

#### 引継ぎ

##### 運用引継計画書

##### 運用手順書

##### 操作手順書

##### 保守・技術支援体制図

##### 保守・技術支援利用手順書

##### 運用管理資料

##### アカウント管理台帳

##### 証明書管理台帳

##### ライセンス管理台帳

##### ライセンス関係資料

##### 引継完了報告書

上記以外に納品が必要なドキュメント、データ等が発生した場合には、設計事業者等の指示に従い納品すること。

### 調達ソフトウェアのインストール用の電子媒体は、1セット納品すること。

### 取扱説明書等の添付品は、1セット納品すること。

## 撤去

### 賃貸借契約の終了後は、受注者が責任をもって調達機器、ケーブル類等を撤去すること。

なお、撤去方法については設計事業者等が別途指示する。

### 保守交換及び撤去の際、サーバ及びストレージ内の記憶装置については、物理破壊（以下併せて「破壊措置」という。）し、復元不可能な状態にする措置を行うこと。

### 前2項の措置は、原則、府の管理する施設内で行うこと。

### 前3項の規定により措置を実施したときは、機器名、ホスト名、型番、記憶装置のシリアル番号、措置区分、作業結果、作業完了日、作業者氏名等を書面にて設計事業者等に報告すること。参考様式は[別紙7 参考様式]に示す。

なお、物理破壊を実施した記憶装置については、破壊前後の写真も添付すること。また、書面の提出期限は、事前に設計事業者等と協議すること。

### 前各項に係る費用は、受注者の負担とする。また、前各項に必要となるソフトウェア、破壊装置等は受注者が用意すること。

### 保守交換後に破壊し、一時保管場所に保管していた情報記憶媒体について、機器の撤去時に併せて回収すること。

### 機器の撤去後、構築作業により実施した電源工事、配線工事、環境整備等において既存の設備に変更を加えた箇所について、設置前の状態に原状回復を行うこと。ただし、府が指定した箇所は除く。

## 役割分担

調達機器等の構築及び撤去作業において、受注者、設計事業者、運用事業者及び府の役割分担は以下のとおりとする。

表 ４‑１　役割分担表

| **項目番号** | **作業工程** | **作業内容** | **受注者** | **設計事業者** | **運用事業者** | **府** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 基本設計等の確認 | 設計事業者にて作成した基本設計書等を確認すること。 | ◎ | △ |  |  |
| 2 | 詳細設計 | 調達機器等の構築及び設定作業に必要な手順及び設定値を決定し、詳細設計書を作成すること。 | ◎ | ○ |  | ◇ |
| 3 | 移行設計 | 既設機器から調達機器への移行方法、体制、スケジュール等を決定し、移行設計書を作成すること。 | ◎ | ○ |  | ◇ |
| 4 | 配線／設置 | 調達機器に必要な配線等を行い、調達機器の設置及び現地調整を行う。 | ◎ | ○ |  |  |
| 5 | 設定 | 詳細設計書に基づき調達機器等の設定を行う。また、設定した調達機器等が正常に動作することを確認すること。 | ◎ | ○ | △ | ◇ |
| 6 | 移行 | 移行設計書に基づき移行リハーサル及び本番移行（データ移行含む）を行う。また、基本設計書等の要件を満たしていることを検証すること。 | ◎ | ○ | △ | ◇ |
| 7 | 引継ぎ | 運用上必要となる機器操作等について手順書等を作成し、受注者から運用事業者等へ引継ぎ及び操作訓練を行う。 | ◎ | ○ | △ | ◇ |
| 8 | 納品 | ドキュメント、データ等をとりまとめ、納品を行う。 | ◎ | ○ | △ | ◇ |
| 9 | 保守／技術支援 | 調達機器等の保守及び技術支援を行う。 | ◎ |  | ○ |  |
| 10 | 撤去 | 賃貸借期間終了後、調達機器の撤去を行う。 | ◎ |  | ○ |  |

◎：実施主体　　　○：施工管理　　　△：支援又は協力　　　◇承諾

# 保守及び技術支援

## 共通事項

### 調達機器等について、以下の要件を満たす保守及び技術支援を行うこと。

#### 保守及び技術支援を行うに当たっては、運用事業者等と適切に連携すること。

#### 保守及び技術支援に係る作業は、可能な限り、執務環境及び府の業務に影響を及ぼさないように行うこと。

#### 調達機器等に障害が発生した場合（障害が発生したと疑われる場合を含む。）、運用事業者等と協議の上で現地での障害調査が必要と判断した際には、現地で障害調査を行うこと。

#### 障害調査の結果、原因が調達機器等にある場合は、その原因や調査結果を直ちに運用事業者等に報告すること。また、復旧方法について運用事業者等と協議の上で必要な処置を実施し、早期の復旧に努めること。

#### 障害調査の結果、原因が保守対象外の機器等にある場合は、その原因や調査結果を直ちに運用事業者等に報告すること。

#### 障害発生から復旧に至るまで、必要に応じて、速やかに状況を運用事業者等に報告すること。

### 以下の要件を満たす保守及び技術支援の受付窓口を用意すること。

#### 受付窓口は固定とし、導入する全ての製品において受付窓口を一本化すること。

#### 保守の受付時間及び受付方法は、以下のとおりとすること。

受付時間：年間通じて24時間

受付方法：電話及び電子メール

#### 技術支援の受付時間及び受付方法は、以下のとおりとすること。

受付時間：年間通じて24時間

受付方法：

　開庁日の9時から18時まで 電話及び電子メール

　開庁日の夜間及び休日 電話及び電子メール（電子メールのみでも可）

### 調達機器への移行後は、賃貸借期間の開始日より前であっても、賃貸借期間中と同様の保守及び技術支援を行うこと。

### 調達機器の設置場所は、原則として賃貸借期間中には変更しないが、やむを得ず設置場所を変更する場合があっても同様に保守及び技術支援を行うこと。

なお、賃貸借期間中における移設作業は、本契約の範囲外とし、別途契約を行う。

### 保守及び技術支援に係る受付履歴、対応状況、対応内容等について、毎月書面により運用事業者等へ報告すること。また、保守及び技術支援の対応の中で、調達機器等の運用等に改善の余地が見つかった場合は、その改善方策についても報告書に含めること。

## 保守内容

### 調達機器等を常時、正常な状態で使用できるように保守すること。

### 保守対象は調達機器等に加え、以下の要件を満たすこと。

#### 機器の設置に必要な付属物、機器の接続に必要なケーブル類についても保守対象とすること。

#### 機器及びその構成部品が消耗品である場合も保守対象とすること。

#### 機器の設置に必要な付属物、機器の接続に必要なケーブル類についても保守対象とすること。RAIDコントローラ等のバッテリー類も保守対象とすること。

#### 火災を原因とする障害も保守対象とすること

### 保守作業を行う時間は、以下の要件を満たすこと。

#### [表 ３‑１　調達機器等一覧] に示す保守区分①については、保守の受付後4時間以内（ただし、フェイルオーバーが機能していない場合は、2時間以内）に設置場所に到着し、保守作業に着手すること。

#### [表 ３‑１　調達機器等一覧]に示す保守区分②については、開庁日の9時から18時までに保守受付を行った場合は、4時間以内に設置場所に到着し、保守作業に着手すること。また、開庁日の夜間及び休日に保守受付を行った場合は、翌開庁日（翌日（ただし、0時から9時までの間は、翌日を当日に読み替える。）が開庁日の場合は、翌日とし、休日の場合は、休日後初めて訪れる開庁日をいう。以下同じ。）の13時までに設置場所に到着し、保守作業に着手すること。

#### 保守作業が長時間に及び、開庁日の夜間又は休日の時間帯にかかった場合であっても継続して復旧作業を行うこと。

#### 運用に支障のない障害、軽微な障害等の場合、運用事業者等と協議の上、翌開庁日に保守作業を行うことができるものとすること。

#### メール無害化システム、ファイル無害化・送受信システムにおいてクラウドサービスを採用する場合、サービス提供機器側で障害を検知した場合は、開庁日は１時間以内、開庁日の夜間及び休日には3時間以内に府へ通知すること。

### 保守作業は、原則として調達機器の設置場所で行うこと。

### 保守作業における構成部品の交換により調達ソフトウェアの更新が必要な場合は、保守対応の中で調達ソフトウェアの更新作業を実施すること。

### 復旧作業においてリストアが必要な場合は、運用事業者等が用意するバックアップデータにより行うこと。ただし、運用事業者等がリストアを行う場合は、完了までの立会いで良いものとする。

### 復旧作業においてハードディスク等の記憶装置の交換を行った場合は、取り出した記憶装置を［第４　１１ 撤去］第2項から第6項までに準じて復元不可能な状態にする措置を行った上で適法に処分し、その結果を書面にて運用事業者等に報告すること。具体的な方法は、契約締結後に府と協議の上決定する。

### 復旧判断に当たり、運用事業者等によって最終的な動作確認が必要な場合は、当該確認作業が完了するまで現地で待機すること。

### 保守作業終了後は、書面による作業報告を行うこと。

## 技術支援内容

### 調達機器等の操作、設定、チューニング、エラー調査等について、技術支援を行うこと。

### 運用事業者等からの調達機器等の設定、機能等に関する技術的な問合せに回答すること。

### 調達機器等の設定変更、機能追加、調達ソフトウェアのバージョンアップ、チューニング等は、受注者が作成したドキュメントを基に原則として運用事業者が行うが、ドキュメントの不備等受注者の責により運用事業者のみで実施できない場合は、現地での技術支援を行うこと。

### 調達機器等に関する、バージョンアップ情報、脆弱性情報、不具合情報、障害情報等の運用に必要な情報を主体的に運用事業者等に提供すること。特に、調達ソフトウェアの利用バージョンについて、保守サポート終了に関する情報が製造元、販売代理店等から公開された場合には、速やかに運用事業者等へ情報提供すること。

### 調達ソフトウェアの利用バージョンについて、製造元、販売代理店等の保守サポート終了、脆弱性対応、不具合対応、障害対策等のために、賃貸借期間中にバージョンアップ等の対応が必要となり、これに伴う機能追加等の仕様変更により詳細設計の見直しも必要となる場合は、運用事業者等と作業内容、役割分担、スケジュール等について協議し、バージョンアップ等の対応及び詳細設計の見直しを行うこと。また、受注者が対応する費用については、受注者にて負担すること。

### 調達ソフトウェアの更新プログラム等について、追加費用を要することなく入手可能なものはモジュールを入手し、運用事業者等に提供すること（ウェブサイト等で運用事業者等が入手できる場合を除く。）。

### 調達機器等における運用事項、管理事項等、運用に必要となる手順に変更が生じた場合は、その都度、運用手順書を更新し、運用事業者等に提出すること。

# 体制等

## 体制

### 本業務を行うに当たっては、調達機器、ソフトウェア等に精通した者を従事させること。また、調達機器等の製造者から直接的な技術支援を受ける等、効率的な作業が可能となる体制をとること。

### 本契約を確実に履行できるよう受注者の責任と負担において、機器の損害保険に加入する等必要な措置を講じること。

### 受注者の業務範疇の不備に起因して、府等で追加作業（原因調査、作業立会い、打合せ、動作確認等）が発生する場合は、受注者にてその費用を負担すること。

## その他

### 本仕様書に明記されていない細部の事項については、府と協議すること。

### 本仕様書に記載している会社名及び製品名は、各社の登録商標又は商標である。