別紙２　庁内ネットワーク情報基盤機器等構成概要

調達機器等の全体概要は、［別紙3 庁内ネットワーク情報基盤機器等全体概要図］のとおり。調達機器等の構成概要を以下に示す。

なお、以下の内容に関しては、基本設計の概要を示したものであるため、詳細な内容に関しては契約締結後に提示する基本設計書を確認の上で、詳細設計を行うこと。

## 庁内ネットワーク情報基盤仮想基盤サーバ

### 本業務における仮想サーバを稼働させる仮想基盤サーバとして構成する。

### 単一の物理サーバに障害が発生しても、障害が発生したサーバ上で稼働していた全ての仮想サーバを他の物理サーバ上で自動的に再稼働させることでサービスが継続できる構成とする。また、この際にサービスの性能劣化が生じない構成とする。

## ラックコンソール関連機器

庁内ネットワーク仮想基盤サーバと接続し、DC内での構築や保守時に利用する。

## 庁内ネットワーク情報基盤ストレージ

本業務における仮想サーバのディスク領域、ログ保管用領域及びバックアップ用領域として構成する。

## 庁内ネットワーク情報基盤集約スイッチ

### 庁内ネットワーク仮想基盤サーバからDCビルスイッチへのネットワーク接続を集約するスイッチとして構成する。

### 庁内ネットワーク仮想基盤サーバ及び庁内ネットワーク統合ストレージと接続する。

### 各機器との接続はL2接続を行う。

### 物理統合型の仮想化を行い、冗長性、信頼性及び拡張性を確保する。

## 負荷分散装置

庁内メール及び利用者管理システムWebサーバの統合的な負荷分散として構成する。

## クラウドバックアップ領域

#### 所属用ファイルサーバに保存されている所属フォルダのバックアップデータの遠地バックアップ先を提供する。

#### バックアップ保護サーバのバックアップデータ保存ボリュームの遠地バックアップ先を提供する。

#### 災害対策のバックアップデータの保存先となるため、関西圏以外のリージョンのクラウド環境とする。

## 仮想サーバ

仮想サーバの具体的な構成内容、設定時の留意事項等を以下に示す。

### ドメインコントローラ

#### ドメインコントローラは共通ドメインを管理する庁内ADサーバとテスト用ドメインを管理するテスト用ADサーバで構成する。

#### 庁内ADサーバ

##### 庁内ADサーバは、インターネット接続系、個人番号利用事務系に接続している端末機、サーバなどからユーザ認証の要求を受け、認証を行うActiveDirectoryドメインコントローラとする。庁内ADサーバは、既存のドメインコントローラとレプリケーションを行う。

##### 庁内ADサーバは、共通ドメイン(lan.pref.osaka.jp)を管理する。

##### 庁内ADサーバは、すべて仮想マシンで構成する。

##### 庁内ADサーバは、共通ドメインに登録されているユーザ、Windows機器に対して一元管理するためのグループポリシーを配布する。

##### 庁内ADサーバは、DNSサービス、時刻同期サービスと同居する。一部の庁内ADサーバはKMSサーバ、Active Directory証明書発行サービス(ADCS)と同居する。

##### 接続しているネットワークで優先的に認証するドメインコントローラを選択するように複数サイトを構成する。

##### フォレスト機能レベル、ドメイン機能レベルは、Windows Server 2016で構成する。

##### 教育庁との信頼関係は設定しない。

##### KMSはインターネット接続系、個人番号利用事務系の各系統に必要なライセンスを認証する。

##### ADCSは2種類(SHA1、SHA256)のセキュリティレベルの証明書を提供する。

#### テスト用ADサーバ

##### テスト用ADサーバは、インターネット接続系接続しているテスト用の端末機、テスト用サーバなどからユーザ認証の要求を受け、認証を行うActive Directoryドメインコントローラとする。本サーバは既存のテスト用ドメインコントローラとレプリケーションを行う。

##### テスト用ADサーバは、テスト用ドメイン(testl.pref.osaka.jp)を管理する。

##### テスト用ADサーバは、すべて仮想マシンで構成する。

##### テスト用ADサーバは、テスト用ドメインに登録されているユーザ、Windows機器に対して一元管理するためのグループポリシーを配布する。

##### テスト用ADサーバは、DNSサービス、時刻同期サービスと同居する。

##### フォレスト機能レベル、ドメイン機能レベルは、Windows Server 2016で構成する。

### 名前解決

#### 名前解決は、共通ドメインを管理する庁内ADサーバと、テスト用ドメインを管理するテスト用ADサーバで構成する。

#### 庁内ADサーバ

##### 庁内ADサーバは、インターネット接続系、個人番号利用事務系情報基盤の各系統で稼働している機器から 庁内ネットワーク内のすべての機器からの共通ドメイン(lan.pref.osaka.jp)に関する名前解決を行う。

##### 共通ドメインを名前解決するDNSサーバは、ドメインコントローラと同居させる。

##### 庁内ADサーバは、特定のドメイン空間に対しての名前解決は、指定したDNSサーバに条件付きフォワーダで名前解決を行う。

##### インターネット接続系の庁内ADサーバが名前解決できないもしくは条件付きフォワーダに設定されていないドメイン空間については、内部DNSサーバにフォワードし、名前解決を行う。

##### 個人番号利用事務系の庁内ADサーバは、フォワード設定を実施しない。ただし、一部LGWANのゾーンについては条件付きフォワードで名前解決を行う。

#### テスト用ADサーバ

##### テスト用ADサーバは、テスト用ドメインに参加している機器からテスト用ドメイン空間(testl.pref.osaka.jp)に関する名前解決を行う。

##### テスト用ドメインを名前解決するDNSサーバは、テスト用ADサーバと同居させる。

##### テスト用ADサーバは、テスト用ドメイン空間以外の名前解決は内部DNSサーバにフォワードし、名前解決を行う。

### 時刻同期

#### 時刻同期は、庁内ADサーバとテスト用ADサーバで構成する。

#### 庁内ADサーバ

##### 庁内ADサーバは、インターネット接続系、個人番号利用事務系情報基盤の2系統で動作している機器の時刻からの時刻同期問い合わせに応答する。

##### 庁内ADサーバの中でPDC機能を有しているサーバは、別調達で動作する内部メール中継サーバを参照し、時刻同期する。

#### テスト用ADサーバ

##### テスト用ADサーバは、テスト用ドメインに参加している機器からの時刻同期問い合わせに応答する。

##### テスト用ADサーバの中でPDC機能を有しているサーバは、別調達で動作する内部メール中継サーバを参照し、時刻同期する。

### サーバパッチ管理

#### サーバパッチ管理サーバは、インターネット接続系、個人番号利用事務系情報基盤の2系統で動作しているWindows Server、Redhat Enterprise Linuxサーバに対して修正プログラムを提供する。

#### Windows Serverの修正プログラムを提供するサーバとRedhat Enterprise Linuxの修正プログラムを提供するサーバ2台で構成する。

#### サーバパッチ管理サーバは、インターネット接続系、個人番号利用事務系情報基盤共有で構成する。

#### 修正プログラムの適用は、適用する側のサーバの任意のタイミングで適用する。(本サーバ側から適用しない)

### 庁内Webサイト(IIS)

#### 庁内Webサイト(IIS)は、「各課ページ」サイトを提供する庁内Webサーバ(IIS)とダウンロード用モジュールを提供する庁内Webサーバ(ダウンロード)で構成する。

#### 庁内Webサーバ(IIS)

##### 庁内Webサーバ(IIS)は「各課ページ」のWebサイトを提供する。

##### 議会端末、別館 府民お問い合わせセンターの端末機からの接続は、議会等Proxyサーバ経由で特定のサイトのサービスを提供する。

##### 「各課ページ」はサイトへの利用者を特定するために、認証を設定する。利用者は共通ドメインのアカウントでログオンした端末から接続するため、「各課ページ」への接続時には利用者はユーザ名/パスワードを入力させずに認証を行う。

##### 「議会サイト」は共通ドメインに参加していない端末からのアクセスとなるため、ユーザ認証は実施しない。

#### 庁内Webサーバ(ダウンロード)

##### 庁内Webサーバ(ダウンロード)は、ＤＸ推進課が提供するモジュールを利用者がダウンロードするための共有フォルダを提供する。

##### 庁内webサーバ(ダウンロード)は、SMB共有で利用者に共有フォルダを公開する。

##### 庁内webサーバ(ダウンロード)は、利用者を特定するためファイル操作のログを採取する。

### サーバ運用監視

#### インターネット接続系に運用監視サーバを導入し、個人番号利用事務系情報基盤を含めた統合監視を実施する。

#### 仮想サーバに関しては、死活監視、サービス監視、プロセス監視、リソース監視、アプリケーションサービス監視を行う。

#### ネットワーク機器に関しては、各ポートの死活監視、パフォーマンス監視、Trap 監視を行う。

#### アプライアンス機器に関しては、死活監視とSNMPTrap監視を行う。

#### ストレージ機器に関しては、死活監視、Trap監視を行う。

#### 監視サーバにて障害予兆及び障害を検知した際に、運用監視サーバから管理者へメール通知を行う。

#### 定められた期間分の過去履歴を閲覧可能なこと。

### ファイル共有(所属)

#### ファイル共有(所属)は、所属フォルダなどを保存する所属用ファイルサーバ、所属用ファイルサーバを管理するNAS管理サーバ、所属フォルダを遠地保管するための所属用ファイルサーバ(バックアップ)、所属用ファイルサーバ(バックアップ)の管理と所属用ファイルサーバ - 所属用ファイルサーバ(バックアップ)間のレプリケーションを管理するコネクタサーバで構成する。

#### 所属用ファイルサーバ

##### 所属用ファイルサーバは、インターネット接続系、個人番号利用事務系情報基盤の2系統で利用している職員に対して、所属フォルダ(インターネット接続系は旧シェアフォルダ含む)、部局調達NASフォルダ(インターネット接続系のみ)を提供する。

##### 所属用ファイルサーバはセキュリティレベルの違う2系統のデータが同居する為、2系統の各ボリュームは許可された系統からのみ接続できるように論理的にアクセス制御する。

##### 所属用ファイルサーバは、利用者が所属フォルダに接続するためのショートカットを取りまとめたフォルダを提供する。

##### 所属用ファイルサーバは、所属フォルダに必要な権限を付与し、アクセスする職員を制限する。

##### 所属用ファイルサーバは、各所属フォルダ、部局調達NASフォルダの利用容量を制限するためにクォータ機能を使用する。

##### 所属用ファイルサーバは、ファイルの利用頻度で保存する記憶媒体を変更する自動階層機能を使用する。

##### 所属用ファイルサーバは、使用容量を有効活用するために重複排除機能を使用する。

##### 所属用ファイルサーバは、ランサムウェア対策を実施する。

##### サロゲートペア文字を利用できる機能が搭載されている。

##### 所属用ファイルサーバのボリュームはSnapshot機能を使用して筐体内バックアップを提供する。所属フォルダのボリュームは、遠地バックアップとしてクラウド上の所属用ファイルサーバ(バックアップ)にSnapMirrorでバックアップする。

##### インターネット接続系の所属フォルダは全文検索の対象とする。

#### NAS管理サーバ

##### NAS管理サーバは、所属用ファイルサーバを管理/監視する。

#### コネクタサーバ

##### コネクタサーバは、所属用ファイルサーバ(バックアップ)を管理する。

##### コネクタサーバは、所属用ファイルサーバと所属用ファイルサーバ(バックアップ)のSnapMirrorの接続管理を行う。

#### 所属用ファイルサーバ(バックアップ)

##### 所属用ファイルサーバ(バックアップ)は、所属用ファイルサーバの所属フォルダのバックアップ保存先を提供する。

##### 所属用ファイルサーバ(バックアップ)は、ファイルの利用頻度で保存する記憶媒体を変更する自動階層機能を使用する。

##### 所属用ファイルサーバ(バックアップ)は、使用容量を有効活用するために重複排除機能を使用する。

### ファイル送受信

#### ファイル送受信は、系統間でファイルを送受信するファイル送受信サーバと無害化処理を実施する無害化サーバで構成する。

#### 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層間でのファイルの送受信を行う。

#### ファイル送信時において無害化処理の実施および承認者による承認を行う。

#### 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送受信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機能を実装していること。

#### 共通ドメインのアカウントを使用する利用者については、利用者管理システムが配置するCSVを取り込んで、ユーザ管理を一元的に行う。

#### 人事異動や組織改正時にユーザ情報、所属情報の変更が発生した際は、利用者管理システムから出力されたCSVを取り込み、ファイル送受信システムへ反映する。

### サーバウイルス対策

#### サーバウイルス対策は、対象のサーバを管理するウイルス対策管理サーバとパターンファイルなどをダウンロード、配信するウイルス対策配信サーバで構成する。

#### 本サーバにて、本業務で導入する全サーバ(Windows、Linux)のウイルス対策を一元的に管理(パターン更新/配信、ログ管理、アラート通知など)する。

#### 本サーバはインターネット接続系に導入し、個人番号利用事務系のサーバも対象とした統合管理を実施する。

### ターミナルサービス

#### 本サーバは、リモートアクセスシステムとリモート接続対象となるエンドポイントのサーバを中継する踏み台サーバとして構成する。

#### Windows デスクトップ環境への認証は庁内ネットワークの AD と連携して行う。

#### 利用者によるアプリケーションの追加インストールを制限する。

#### 利用者のログインログを収集する。

### サーバログ管理

#### サーバログ管理は、収集したログを保管するログ保管サーバと、収集したログを管理するログ管理サーバで構成する。

#### ログ管理サーバ

##### 本サーバはログ保管サーバとの連携により、ログ保管サーバに収集したログを GUIで検索、集計、レポート出力できるよう構成する。

##### ログの採取方法はsyslog、SNMPTrap、エージェント、エージェントレス、FTP、ファイル共有などの方法でログを収集する。

##### 本サーバは、収集した未加工のログテキストと、解析されたログ双方とも管理画面から分析する。

##### 現行のログ管理サーバで収集したログも参照できるようにする。

#### ログ保管サーバ

##### 本サーバにて収集したログを、既定の期間分保管し、ログ管理サーバからアクセスを行う。

### サーババックアップ

#### サーババックアップはバックアップを管理する庁内バックアップ管理サーバ、ランサムウェア対策としてバックアップデータを一定期間書き込み禁止する庁内バックアップ保護サーバ、バックアップを遠地保管する遠地保管バックアップサーバで構成する。

#### 本サーバはインターネット接続系、個人番号利用事務系の仮想サーバのバックアップについてエージェントレスでの統合管理を実施する。

#### 対象サーバ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定め、OSイメージ、システム構成、ログ等を保存する。

#### ネットワーク機器、ストレージ等のハードウェアについては設定変更作業時に設定ファイルを保存する。

#### 定められた世代管理を実施する。

#### バックアップデータを保護する機能(取得したバックアップの改ざんを防ぐ)を導入し、ランサムウェア対策を実施する。

#### バックアップデータの遠地バックアップは、バックアップ保護サーバのデータ領域をSnapMirrorでクラウド環境に保存する。遠地バックアップ先のクラウド環境は、災害対策となるので関西圏以外のリージョンのクラウド環境にバックアップデータを保存する。

### ジョブ管理システム

#### ジョブ管理システムは、ジョブを管理するジョブ管理サーバとジョブを実行するサーバに導入するジョブ管理エージェントで構成する。

#### インターネット接続系、LGWAN接続系情報基盤、個人番号利用事務系情報基盤において統合的なジョブ管理を行う。

#### バッチ処理、各種スクリプトの実行等について、スケジュール等による自動実行を行う。

#### 利用者管理システム、職員端末構成管理システムおよび利用者管理システムと連携するシステムにおけるバッチ処理及び各種スクリプトの実行等の管理を行う。

#### ジョブ実行の終了および異常終了について、運用者へメール通知を行う。

### 議会等Proxy

#### 議会 LAN などのインターネット接続系とは独立した LAN からの通信は、議会等Proxyを経由し庁内WEB、SSC等の許可された庁内サービスを利用する。

#### 利用者は、議会LAN内の端末から匿名認証にてアクセスを行う。

#### 利用者のアクセスログを取得する。

#### URL変換の機能を備えた議会等 Proxyを導入し、各室課のフォルダ内の閲覧可能となっているファイルにのみアクセスを行う。

#### メーカ保守・メーカサポートが提供されるOSおよびソフトウェアを使用する。

### ファイル全文検索(所属用)

#### ファイル全文検索(所属用)は、利用者が使用するポータル画面、検索の設定などを管理する全文検索管理サーバ、検索対象のフォルダをクローリングする全文検索サーバ、ファイルの利用状況を可視化するファイルサーバ可視化サーバで構成する。

#### 全文検索サーバ

##### 本サーバは、庁内ADサーバで管理するユーザの内、インターネット系の所属フォルダを利用するユーザを対象とする。

##### 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。

##### 全文検索（ファイル内の語句検索）可能なファイル種類は、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ファイルとする。

##### ファイルサーバ（所属用）、庁内Webサイト(IIS)及び庁内Webサイト(SPO)で保存されている文書を巡回し、文書の情報を収集する。

##### 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

##### 本サーバは、全文検索管理サーバの管理を行う。

##### 職員が文書検索するためのポータル画面を提供する。

##### 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機能を実装していること。

#### ファイルサーバ可視化サーバ

本サーバは、ファイル数や使用頻度などの状況を把握するために使用する。

### 生体認証

#### 個人番号利用事務系の業務を利用する際の二要素認証として、生体認証を行う。

#### 生体認証は静脈認証とする。可能な限り、既存利用者のデータを再登録することなく移行を実現する。

#### インターネット接続系に配置される職員端末機及び個人番号利用事務系に設置される税務情報端末機、個人番号利用事務系端末機より生体認証を行う。また、それぞれの同一セグメント内で認証ができるように、サーバを配置する。

#### インターネット接続系及び個人番号利用事務系ネットワークに構築する各サーバは冗長されており、主系サーバに障害が発生しても生体認証を継続する。

#### 生体認証サーバに登録されるアカウントは、利用者管理情報を自動で取込むことで登録を行う。

### 端末資産管理

#### インターネット接続系と個人番号利用事務系に設置の物理端末機を管理する。

#### 管理サーバと配信用サーバは役割を分けて構成する。

#### 以下の機能を利用する。

##### インベントリ

ハードウェア及びソフトウェアのインベントリを行う。

##### 更新プログラム管理

セキュリティパッチを含む更新プログラムの適用及び適用確認を行う。

##### アプリケーション配信

バッチやWindows関連アプリの配信を行う。

##### リモートコントロール

物理端末機へリモートコントロールにより、画面の共有、リモート制御を行う。

## コミュニケーションシステム

コミュニケーションシステムの具体的な構成内容、設定時の留意事項等を以下に示す。

### 個人用ドライブ

#### Microsoft365 E3ライセンスを保持する職員が個人用のファイル保存環境を提供する。

#### 職員端末機等のExplorerから利用できるようにOneDriveアプリケーションを利用する。

#### ユーザに割り当てられた職員個人用のファイル保存領域は、当該ユーザのみがアクセスできるよう基本的な共有範囲は職員自身のみとする。

#### ユーザが、自身のファイル保存領域内にあるフォルダ及びファイルについて、他のユーザにアクセス権を付与することができる機能を提供する。

#### OneDriveアプリケーションで同期されたファイルは、グループポリシーのログオフスクリプトを利用しログオフ時に同期済みファイルをローカル領域から削除するものとする。

#### アカウントやライセンス削除後も、個人用ドライブのデータを参照する場合があるため、管理者が対象の職員サイトに対してPowerShellにてアクセス権限を付与し、データ保持期限内の範囲でブラウザからデータを参照可能とする。

### ディレクトリ同期

#### Microsoft EntraIDと連携し、オンプレミスのADドメインコントローラからディレクトリ情報を同期する環境を提供する。

#### 職員はID入力のみでMicrosoft 365にサインイン可能となるよう、シームレスシングルサインオンを利用する。

#### 退職者・派遣(出向)者は同期対象外とするなど一時的にM365ライセンスをはく奪するため、拡張属性を利用しディレクトリ同期の対象外とする。

### Microsoft365テナント

#### Microsoft 365 E3ライセンスにて提供されるサービスを利用する。

#### 庁外からのMicrosoft365テナントへのアクセスを許可するため、IPアドレスベースでの制御、または特定セキュリティグループからのアクセス制御を利用する。

#### Microsoft365テナントはMicrosoft365のギャラリーアプリケーション、または非ギャラリーアプリケーション(独自開発など)の認証する環境を提供する。

#### 府立学校テナントは、教育庁管轄にて学校の教職員などのアカウントを保持している。本業務にて利用するテナントと府立学校テナントは双方向で職員情報の連携が必要なため、Entra IDのB2B コラボレーション（テナント間同期）を利用する。

### 庁内メール

#### 庁内メールは、情報伝達可能なメール送受信機能並びにユーザ単位のカレンダー機能により、事務処理の効率化、情報共有等のコミュニケーション強化を実現する環境である。

#### 庁内メールは、Microsoft365のExchange Onlineによる提供を基本とする。

#### 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。

#### 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ExchangeServerを継続利用する。

#### オンプレミスのExchangeServerを利用するメールボックス数は625、必要ディスク容量は1.2TBとする。

#### Exchange Onlineを利用するユーザメールボックスの容量は、Exchange Onlineユーザの場合E3ライセンス上限の100GBに変更する。

#### メールサイズがサーバの制限値を超過するメールまたは、配送先のアドレスが存在しないメールは、配信不能レポート(NDR;Non-Delivery Receipt)により、メールの送信者に対してメールの配送状態を通知する。

#### LGWAN宛のNDRのみ配送するため、ヘッダー情報「X-MS-Exchange-Message-Is-Ndr」によりインターネット向けのNDR配送は破棄する。

#### 退職者・派遣(出向)者はMicrosoft 365 E3ライセンスをはく奪し、かつメールボックスのデータを保持する。

### 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。

#### 利用者はMicrosoft365 E3ライセンスを保持する職員も利用(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。

#### 会議室は予約可能期間の上限を設定する。

#### 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。

#### 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。

#### 組織替えに伴い会議室情報を年度初めに更新する。

### リアルタイムコミュニケーション

#### リアルタイムコミュニケーションサービスは、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。

#### 庁内のADと連携し、シングルサインオンを提供すること。

#### 職員端末機に加え仮想端末機環境からもWeb会議、資料共有等が実現できる構成とする。

#### 庁外からのアクセスは特定の端末機や利用者を限定するためMicrosoft の条件付きアクセスを利用する。

#### 府立学校テナントのユーザは、ゲスト扱いとし、セキュリティの観点から外部組織かつ他テナントのユーザもしくはMicrosoft365以外のユーザとのチャット、チームは利用制限する。

### 庁内Webサイト(SPO)

#### 庁内Webサイトは、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。

#### 庁内Webページ、部局等チームサイト、部局横断チームサイトを、Microsoft365 E3ライセンスで利用できるSharePoint Onlineに配置する。

#### 利用目的に応じて、庁内Webサイト、部局サイト、部局横断チームサイトの3種類でサイトを構成する。

#### 各課ページはOS標準のWebサーバ(IIS)にて実現する。

#### 利用者は、庁内Webサイト(SPO)を利用するために、Microsoft Edgeからアクセスし、Entra ID上のアカウントに対してログインする。

#### ログインは、シームレスシングルサインオンを利用する。

#### オンプレミスActive Directoryにのみ存在するユーザは庁内Webサイトを参照しない。

#### サイト、コンテンツごとにアクセス権の制御を実施する。

#### 部局横断チームサイトのアクセス権限の付与は、サイト管理者にて設定変更する。

#### 府立学校テナントのユーザはクロステナントを利用し招待する。

#### ユーザ招待の単位は府立学校側のユーザ更新(追加、削除)が自動で反映される「テナント間同期」を利用する。

#### 府立学校ユーザはゲストユーザとしてアクセス権限を付与する。

#### 庁内WebサイトおよびSharePoint Onlineの全体管理を行うアカウント利用する。

#### 現行庁内Web基盤からのデータ移行を考慮し、サイト毎のストレージ上限を設定できること。

#### サイトの利用サイズによる警告の有無および閾値を設定できること。

#### 庁内Web(SPO)サイトは、標準機能のリスト、ライブラリ単位のバージョン管理とは別にサイト単位でバックアップおよびリストア機能を提供する。

#### 庁内Web(SPO)サイトは、サイト毎にバックアップ可否を設定する。

#### 庁内Web(SPO)サイトは、手動により削除を利用する。

### 添付メール分離

#### 府はメール送信におけるPPAPの課題対応(※)のため、メールから添付ファイルを分離する。※ウイルスチェックができない。また、パスワードが添付ファイルと同じ通信経路で送られるため、情報流出のリスクが高い

#### メール全体がHTML化により暗号化される方式は、職員の操作環境に大きな影響を与えるため採用しない。

#### 添付ファイルを分離する対象メールはLGWAN宛を除くインターネット向けとする。

#### 添付ファイルは、メール受信者のみが参照できるストレージに格納する。

#### 添付ファイルのストレージ公開期間は、7日以上とする。

#### 添付ファイルの参照はワンタイムパスワード入力、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。

#### 添付ファイルは全てのファイルを対象とし、分離除外する拡張子は設けない。

#### 1通あたりのメールに添付可能な最大ファイル数は100以上とする。

#### 添付ファイルを分離は、LGWAN宛先を除外する必要があるため、内部メール中継サーバにてメール配送先を変更する。

#### 受信者によるダウンロードのログは、サーバログ管理機能に連携する。

### Officeアプリケーション

#### Officeアプリケーションは、文書作成やメール送受信機能を提供する。

#### Officeアプリケーションは、Microsoft 365 E3ライセンスにて利用可能なApps for Enterpriseとする。

#### アプリケーションの定期的な更新対応が困難な個人番号系の税務情報端末機は、Office LTSC 2021を利用する。

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

#### LGWAN接続系、および個人番号利用事務系端末のAppsライセンス認証は、自治体情報セキュリティ向上プラットフォームを利用する。

#### LGWAN接続系、およ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Appsライセンス認証の通信を振り分ける。

#### 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。

#### Officeのグループポリシーは、Office2016を利用し現行と同様のセキュリティ設定を利用する。

### ファイル暗号化

#### 庁内のインターネット接続が可能な端末よりM365 E3ライセンスを保有する職員にて任意のファイルを暗号化する。

#### ファイル暗号処理はパスワード設定や他のユーザへのファイル送信時にパスワード通知が不要となるよう庁内共通ドメインを利用する。

#### 庁外の他者にてファイル参照が不可能となるよう、暗号化ファイルのアクセス権は、庁内の利用者のみファイル参照可能とする。

#### 情報公開請求など庁外へのファイル送信時は、職員にて復号処理後に送信する。

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

#### 暗号化対象文書はOfficeファイル、およびPDFファイルとする。

#### 現行環境では、特定フォルダにファイルを配置することによりファイルが自動で暗号化される。次期システムでは、ファイルは職員にて暗号処理するため、特定フォルダへのコピーによる自動暗号化処理は不要とする。