平成 26 年度三重県行政 WAN ユーザ認証システム

設計・機器調達・構築・保守業務委託

詳細仕様書

三重県地域連携部 IT 推進課

目　次

1. 現行システムの概要

1.1. 庁内ドメインシステム

1.1.1. システムの概要

マイクロソフト製 Windows Server 2003 の Active Directory によるドメイン環境であり、主にクライアント(庁内端末)の認証処理とドメイン内のリソース管理を行うシステムである。また、グループポリシー等にてユーザ及びクライアントのセキュリティ管理も行っている。

1.1.2. サーバ構成

庁内ドメインシステムにて使用しているサーバの設置場所及び用途は下表の通りであり、一部のサーバは他サブシステムと兼用している。

なお、各サーバの詳細については別紙 4「現行システム機器一覧」を参照のこと。

設置場所	用途	兼用	台数
本庁	DC/DNS/NTP/DHCP		3
	DC/DNS/NTP/DHCP/ウィルス対策	○	2
総合庁舎	DC/DNS/NTP/DHCP		10
IDC1	DC/DNS/NTP/WINS/FSMO/ウィルス対策	○	1
	DC/DNS/NTP/ウィルス対策/運用管理	○	1
IDC2	DC/DNS/NTP/WINS/ウィルス対策	○	1
	DC/DNS/NTP/ウィルス対策/運用管理	○	1
合計			19

1.1.3. システム設定、設計内容

1.1.3.1. Active Directory 構造

ア．フォレスト構造

シングルフォレスト・シングルドメインである。

イ．サイト構造

シングルサイトである。

ウ．OU 構造

ユーザ、コンピュータともに数個の OU に振り分けている。

エ．グループ構造

セキュリティグループを所属毎に作成しており、所属の階層にあわせてネスト化されている。

オ．機能レベル

フォレスト：Windows Server 2003

ドメイン：Windows Server 2003

カ．信頼関係

信頼関係を結んでいる外部ドメインは存在しない。

1.1.3.2. ネットワークサービス構造

ア．DHCP

行政 WAN のセグメントは、本庁(吉田山会館等含む)はフロアまたは建物毎(13 個)、総合庁舎は庁舎毎(計 10 個)に分かれており、本庁設置の DC のうち 5 台及び各総合庁舎に設置の DC が DHCP サービスを提供している。

本庁では、下表の通り、1 台の DC がセグメントをまたいで 2 フロア以上にサービスを提供している。また、冗長性確保のため、同一スコープを 2 台のサーバに持たせる構成となっている。

	設置セグメント	スコープ(主)	スコープ(副)
DC 1	吉田山会館	吉田山会館等(5セグメント)	1 階、2階
DC 2	2階	1階、2階	3階、4階
DC 3	4階	3階、4階	5階、6階
DC 4	6階	5階、6階	7階、8階
DC 5	8階	7階、8階	吉田山会館等(5セグメント)

各総合庁舎では、庁舎に設置された DC がその庁舎内にサービス提供しており、冗長構成とはなっていない。

イ．DNS

全 DC にて DNS サービスが稼働しており、全クライアントは、原則各 DC を規定の DNS サーバとして利用している。

同一ドメインの名前解決は DC が解決、それ以外のドメイン名については既設の DNS サーバ(BIND)へのフォワーダにより解決する。

ウ．NTP

本庁設置の DC のうち 1 台が行政 WAN 上に別途構築した NTP サーバと時刻同期をし、他の DC サーバはこの 1 台と時刻同期を行う。全 DC は NTP サービスを提供しており、全クライアントはいずれかの DC を NTP サーバとして利用している。

エ．WINS

IDC1 及び IDC2 設置の DC のうち 2 台が WINS サービスを提供しており、全クライアントはこの 2 台を WINS サーバとして利用している。

1.1.3.3. ログオンスクリプト

ドメインに接続するクライアントに対し、ログオンスクリプトを使用して、必要なアプリケーションのインストール及び設定変更等を自動で行うよう設定している。

1.1.3.4. CSV インポート機能

CSV データをインポートすることにより、ユーザの新規追加、有効化、変更、無効化、削除を VBScript により実施している。

また、セキュリティグループの登録、メンバ変更、削除も同様に行う。

1.1.3.5. ログ管理

ア．Windows 標準のイベントビューアでは、ログオン及びログアウトの状況が正確に把握できないため、ログオン及びログアウトを行ったユーザ、コンピュータの情報を自動取得する仕組みを構築し、そのログを 1 年間以上保存している。

イ．ログオンに失敗したユーザ、コンピュータの監査ログを 1 年間以上保存している。

ウ．保存したログを任意に抽出し分析できる仕組みが整備されている。

1.1.3.6. 他システムによる利用

庁内ドメインシステムはログイン時のユーザ認証だけでなく、他システムにて認証等に利用されている。

1.2. 庁内メールシステム

1.2.1. システムの概要

マイクロソフト製 Exchange Server 2007 を用いて構築した、三重県行政 WAN 内部でのみ利用できるメールシステムである。

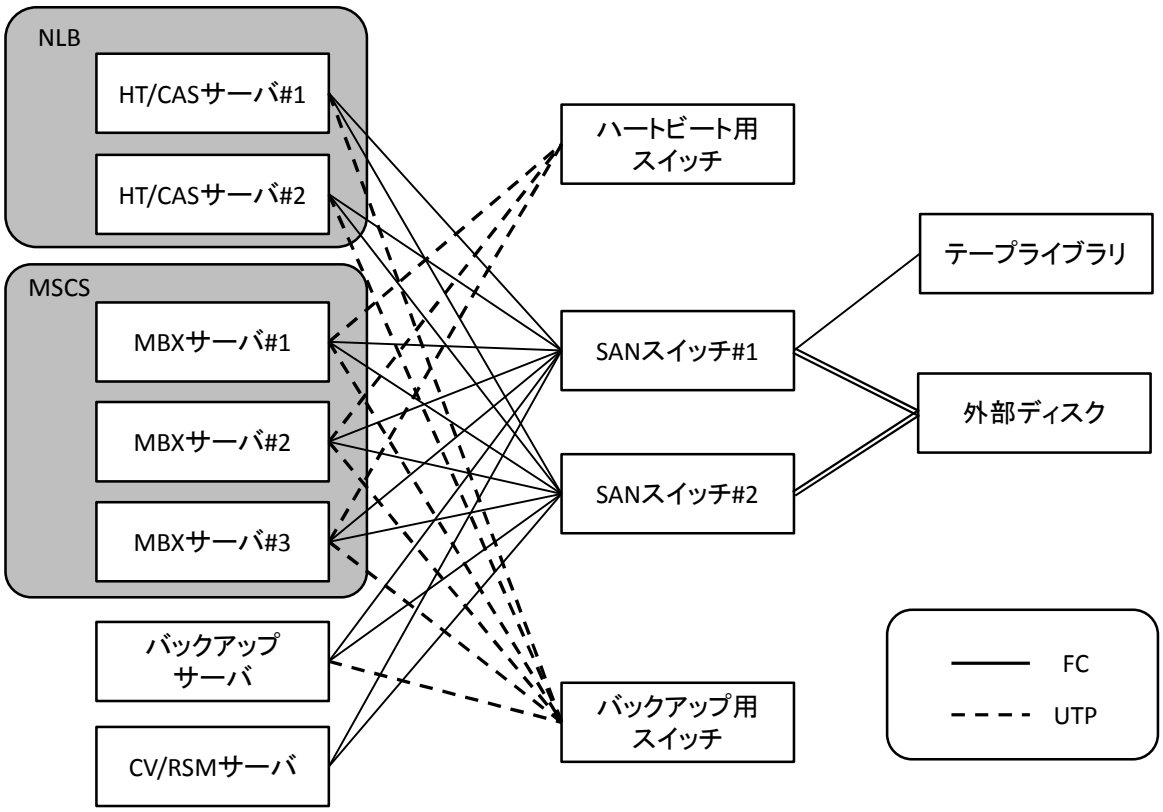
1.2.2. サーバ構成

ア．庁内メールシステムの機器は全て IDC2 に設置されている。

イ．メールサービスを提供するサーバは、ハブトランスポートサーバとクライアントアクセスサーバを共存させたサーバ(HT/CAS サーバ)2 台を負荷分散(NLB)構成、メールボックスサーバ(MBX サーバ)を MSCS で稼働する 3 ノードクラスタ(2Active＋1Passive)構成としている。

ウ．ファイバーチャネルによる SAN 構成をとり、メールデータは外部ディスクに格納している。外部ディスクにはメールボックス用ディスクグループ（RAID1+0、実効容量 1.55TB）及びオフラインバックアップ用ディスクグループ（RAID5、実効容量 1.65TB）が設定されており、専用のサーバ（CV/RSM サーバ）にて管理している。

エ．バックアップ用に LAN が構成されており、バックアップサーバにより LTO テープライブラリに対して各バックアップを行っている。



1.2.3. システム設定、設計内容

1.2.3.1. メールボックス設定

1 通あたりの最大容量は 500kB(一部ユーザは 2MB)である。

1 ユーザあたりのメールボックス容量は 100MB である。

全ユーザ(約 7,700 ユーザ、無効となっているユーザも含む)のメールボックスは 15 個のメールボックスストアに格納されており、1 サーバあたり 4 個(1 台のみ 3 個)のメールボックスストアを保有している。また、パブリックフォルダ用のストアが 1 個整備されている。

1.2.3.2. その他サービス設定

クライアントはマイクロソフト製 Microsoft Outlook を使用してアクセスしており、利用する機能はメール、予定表、仕事、連絡先、メモ、履歴である。

年間、約 3,500 万通のメールを送受信している。

庁内のサーバからの SMTP 接続を受け付けているが、外部メールとの連携は行っていない。

1.2.4. 現行システムの課題

Exchange Server を導入しているが、本県では別途グループウェアシステムを導入しており、機能を有効に活用できていない。

1.3. ウィルス対策システム

1.3.1. システムの概要

三重県行政 WAN に接続されている Windows 及び Linux のサーバ機器、及び庁内端末へウィルス対策ソフトウェア(トレンドマイクロ製ウィルスバスターCorp.もしくは Server Protect for Linux)のプログラムやパターンファイルの配布、管理を行っている。

また、ウィルスの検出状況やパターンファイルの更新状況についての情報を集約し、レポート出力を行っている。

さらに、集中管理サーバ(トレンドマイクロ製 Trend Micro Control Manager)を構築し、各ウィルスバスターCorp.サーバの一元管理や、本県が別途構築しているメール用ウィルス対策サーバへのパターンファイル等の配付を行っている。

1.3.2. サーバ構成

ウィルス対策システムにて使用しているサーバの設置場所及び用途は下表の通り。

なお、各サーバの詳細については別紙 4「現行システム機器一覧」を参照のこと。

設置場所	セグメント	用途	台数	備考
本庁	業務系	Trend Micro Control Manager	1	DC兼用
本庁	業務系	ウィルスバスターCorp.	1	DC兼用
IDC1	業務系	Trend Micro Control Manager ウィルスバスターCorp.	1	DC兼用
IDC1	業務系	ウィルスバスターCorp.	1	DC兼用
IDC2	業務系	ウィルスバスターCorp.	2	DC兼用
IDC1	Proxy	Trend Micro Control Manager ウィルスバスターCorp.	1	
IDC2	Proxy	Trend Micro Control Manager ウィルスバスターCorp.	1	

1.3.3. システム設定、設計内容

1.3.3.1. 配信設定

ア．インターネットよりパターンファイル等をダウンロードするサーバは Proxy セグメントに設置する Trend Micro Control Manager(TMCM)のみである。

イ．Proxy セグメントに設置の TMCM は他の TMCM 及びウィルスバスターCorp.サーバに配信を行っている。

ウ．Proxy セグメント及び DMZ に接続されている Windows クライアントは Proxy セグメントに設置のウィルスバスターCorp.サーバから配信を受ける。Proxy セグメントの 2 台のウィルスバスターCorp.サーバを冗長構成とし、クライアントは通常接続するサーバに障害が発生した場合は他のサーバからパターンファイル等の提供を受けるよう設定されている。

エ．業務系に接続されている Windows クライアントは業務系のいずれかのウィルスバスターCorp.

サーバから配信を受ける。業務系の全てのウィルスバスターCorp.サーバを冗長構成とし、クライアントは通常接続するサーバに障害が発生した場合は他のサーバからパターンファイル等の提供を受けるよう設定されている。また、全てのウィルスバスターCorp.サーバと疎通が取れない場合は既存のプロキシサーバ経由でインターネットよりパターンファイル等をダウンロードするよう設定されている。

オ. 業務系の TMCM は業務系の Linux サーバ、Proxy セグメントの TMCM は Proxy セグメント及び DMZ の Linux サーバに対して、パターンファイル等の配信を行っている。

カ. Proxy セグメントに設置の TMCM は別途構築しているメール用ウィルス対策ソフトへパターンファイル等の配信を行う。

1.3.3.2. レポート機能

各クライアントのウィルスバスター、エンジン、パターンファイルのバージョン及び過去に検出されたウィルスの確認を行うことができる画面を整備している。

ウィルスが発見された場合は、ウィルス名・コンピュータ名・パス名及び対処結果を記載したメールをシステム管理者へ送付する設定を行っている。

1.3.4. 現行システムの課題

サーバによっては、DC サーバ等と兼用しているため、サーバリソースが不足する時がある。

1.4. 運用管理システム

1.4.1. システム概要

大塚商会製 QND α を用いて、三重県行政 WAN に接続されている全サーバ機器、庁内端末のハードウェア及びソフトウェア情報を収集する。また、端末へのリモート接続やソフトウェアの強制配付など、端末管理も行う。

さらに、マイクロソフト製 Windows Server Update Services(WSUS)を用いて、クライアントへのセキュリティパッチ等への配信を行っている。

1.4.2. サーバ構成

運用管理システムにて使用しているサーバの設置場所及び用途は下表の通り。

なお、各サーバの詳細については別紙 4「現行システム機器一覧」を参照のこと。

設置場所	用途	台数	備考
IDC1	マスタサーバ	1	
IDC1	スレーブサーバ	1	DC兼用
IDC2	スレーブサーバ	1	DC兼用
IDC1	パッチ配信	1	

1.4.3. システム設定、設計内容

1.4.3.1. インベントリ取得・出力機能

毎日、各クライアントのログオン時に以下の項目を全て取得している。

取得したインベントリ情報は管理コンソールによりリアルタイムで確認可能であり、また、週に 2 回各項目の情報を CSV で出力し、保存している。

ア．ハードウェア情報(CPU、メモリ、HDD 容量等)

イ．ウィルス対策ソフト情報(種類、パターンファイル等)

ウ．OS 情報(バージョン、適用パッチ等)

エ．アプリケーション情報(インストールされているアプリケーション名)

オ．ソフトウェア情報(保存しているプログラムファイル名等)

カ．レジストリ情報(指定した任意のレジストリ値)

キ．その他(ログオンユーザ名、IP アドレス等)

1.4.3.2. リモート操作機能

リモート操作用のコンソールにより、クライアントのリモート操作を行っている。

リモート操作用のコンソールは複数のコンピュータにて起動することができるため､複数の操作者による複数のクライアントへの同時リモート操作が可能である。

なお、クライアントの画面は操作者及び被操作者双方で閲覧及び操作が可能である。

1.4.3.3. プログラム配信機能

任意のクライアントへセキュリティパッチ等の任意のプログラムの配付を行うことができる機能を整備している。

1.4.3.4. セキュリティパッチ配信機能

WSUS にて､Windows クライアント(約 8,000 台)にマイクロソフトのセキュリティパッチ、サービスパック等を配信している。

また、各クライアントのパッチ適用状況の出力を行っている。

1.4.4. 現行システムの課題

WSUS サーバにあっては、導入当初から配布対象となるプログラムが増加しており、サーバのディスク容量を逼迫している。

1.5. 障害監視

1.5.1. 概要

本県が別途構築した障害監視システムを利用している。

1.5.2. 障害監視対象

本システムにて導入する全てのサーバ及び庁内メールシステムの外部ディスク、スイッチに対し、必要に応じてエージェントをインストールのうえ障害監視の対象としている。

1.5.3. 設定

障害や異常な状態を検知した場合は、運用管理担当者へメール送信される。

1.5.4. 監視項目

以下の項目の監視を行っている。

ア．ネットワーク障害

イ．サービス稼働

ウ．OS パフォーマンス

エ．ログ

オ．バックアップ状況

カ．庁内メールシステム共有ディスク稼働状況

1.6. バックアップ

1.6.1. 全サブシステム共通

障害等に備え、各サーバにて夜間にデータのバックアップを取得している。

1.6.2. 庁内メールシステム

以下のとおり 3 種類のバックアップを行っており、バックアップ先は全て LTO ライブラリである。

なお、オフラインバックアップでは、オフライン時間が最小となるようスナップショット機能を利用し、一旦ハードディスクにミラークローンを作成する設定となっている。

種類	対象データ	スケジュール
オンラインバックアップ （サービス無停止）	メールデータ （データベース単位）	フル：週1回 差分：週6回
オフラインバックアップ （10分間程度サービス停止）	Exchangeデータベース トランザクションログ	フル：月1回
ローカルディスク フルバックアップ	システム領域	フル：随時 （設定変更時等）

1.6.3. 庁内メールシステム以外

庁内メールサーバ以外の各サーバについては、各サーバに内蔵の DAT72 オートローダへバックアップをとっている。

バックアップスケジュールは、週 1 回フルバックアップ、その他の日に増分バックアップと

している。

1.6.4. 現行システムの課題

庁内メールサーバ以外の各サーバでは、DAT ドライブ不良や DAT テープ詰まり等によりバックアップエラーが頻発している。

1.7. 電源管理

1.7.1. 概要

本庁及び総合庁舎に設置のサーバには停電に備えて、UPS を設置し、電源管理ソフトにて管理している。

IDC1 及び IDC2 はデータセンターとして停電対策が取られているため、設置するサーバでは個別の停電対策は行っていない。

1.7.2. 設定

本庁及び総合庁舎に設置のサーバは、電源障害時に自動シャットダウンし、復電時に自動起動するよう設定している。

庁舎の計画停電時にはシャットダウン及び起動の日時を事前設定する機能も有している。

2. システム更新要件

2.1. 基本的な考え方

ア. 本項目では、現行システムから本システムへの更新にかかる方針及び、本システムの最終的な構成、機能を定義する。具体的な手順に関しては、「4. システム更新方法」に記載する。

イ. 本システム構築に必要な調査から設計・テスト・稼働までのすべての工程および作業を本システム構築業務の範囲とする。また、本システム構築に伴い、現行システムにおいて再インストール等大幅な設定変更が発生する場合、その設定作業についてもシステム構築の業務範囲とする。

ウ. 行政 WAN のネットワーク構成を変更することは認めない。

エ. 構築を進めていくうえで必要となる関係部局、関係機関との調整用資料等を作成し、必要に応じて打合せ等に出席すること。

オ. 必要に応じ、本県に関わる現行システムおよび、その他関連するシステムの委託業者もしくは保守業者等と調整、確認を行うこと。

2.2. 庁内ドメインシステム

2.2.1. 概要

原則として、現行の Windows Server 2003 の Active Directory の構成を引き継ぎ、必要な設定変更を行う。

ただし、総合庁舎に設置するサーバを廃止するなど、サーバ構成を見直すこととする。

2.2.2. サーバ構成

想定するサーバ構成は下記の通りであるが、性能要件、設置要件等を踏まえたうえで、サーバ構成を決定すること。

設置場所	用途	台数
本庁	DC/DNS/NTP/DHCP(本庁、吉田山会館用)	3
IDC1	DC/DNS/NTP/WINS	1
	DC/DNS/NTP/DHCP(総合庁舎用)	1
IDC2	DC/DNS/NTP/WINS	1
	DC/DNS/NTP/FSMO/DHCP(総合庁舎用)	1
合計		7

2.2.3. 現行システムの設定変更を行う項目

2.2.3.1. 機能レベルの変更

ア. ドメイン及びフォレストの機能レベルについて、引き上げ可能である最新のレベルに変更すること。

イ. 機能レベルの変更に際し、Active Directory 構造等において修正が必要となる場合は、その修正

を行うこと。

2.2.3.2. 総合庁舎 DC の廃止

ア．各総合庁舎に設置している DC は廃止することとする。

イ．各総合庁舎の DHCP サーバとして、IDC1 及び IDC2 に設置するサーバから IP アドレスの配付を行うこととする。

2.2.3.3. WINS の廃止検討

ア．WINS について、廃止可否の検討を行い、廃止可能であれば廃止の措置を行うこと。

イ．廃止不可能である場合は、不可能である理由を本県に説明し、承認を得たうえで、引き続き IDC に設置のサーバにて WINS サービスを提供すること。

2.2.4. 現行システムの設定を引き継ぐ項目

2.2.4.1. Active Directory 構造

機能レベル以外の構造については現行の構造を引き継ぐこと。ただし、現行よりセキュリティ等が向上する構成があれば、本県の承認を得たうえで変更を行うこと。

2.2.4.2. DHCP 設定

本庁（吉田山会館、合同ビル、勤労者福祉会館、栄町庁舎を含む）の 13 セグメント及び各総合庁舎のセグメントにおいては、現行システム同様、1 セグメントに 2 台以上のサーバから IP アドレスの配付を行うこと。

2.2.4.3. ネットワークサービス構造

ア．本庁及び IDC に設置の DC について、DNS、NTP に関する現行の機能・設定を引き継ぐこと。ただし、現行より可用性・セキュリティ等が向上する構成があれば、本県の承認を得たうえで変更を行うこと。

イ．本庁及び総合庁舎 DC の削減を除き、サーバの IP アドレス等の構成情報を変更する場合は、その影響範囲を本県に説明し、承認を得ること。また、利用者にて設定変更が必要な事項があれば、マニュアル等を作成すること。

2.2.4.4. ログ管理

ア．Windows 標準のイベントビューアでは、ログオン及びログアウトの状況が正確に把握できないため、ログオン及びログアウトを行ったユーザ、コンピュータの情報を自動取得する仕組みを実装し、そのログを 1 年間以上保存すること。

イ．ログオンに失敗したユーザ、コンピュータの監査ログを 1 年間以上保存すること。

ウ．保存したログを任意に抽出し分析できる仕組みを提供すること。

エ．本機能は運用管理システムでの実装でも可とする。

2.2.4.5. ログオンスクリプト設定

ログオンスクリプトにて、運用管理システムのクライアント等必要なアプリケーションのインストールや設定変更ができること。

2.2.4.6. 他システムによる利用

現行システムにて認証等に庁内ドメインシステムを利用している他システムと継続して連携できること。

2.2.4.7. CSV インポート機能の実装

ア．本県が指定する CSV フォーマットにより、ユーザの新規登録、有効化、変更、無効化及び削除、セキュリティグループの登録、メンバ変更及び削除について一括で行える機能(スクリプト)を提供すること。

イ．CSV データ作成については委託業務の範囲外とする。

2.3. 庁内メールシステム

2.3.1. 概要

新規のハードウェアを用いて、WEB メールシステムを構築すること。

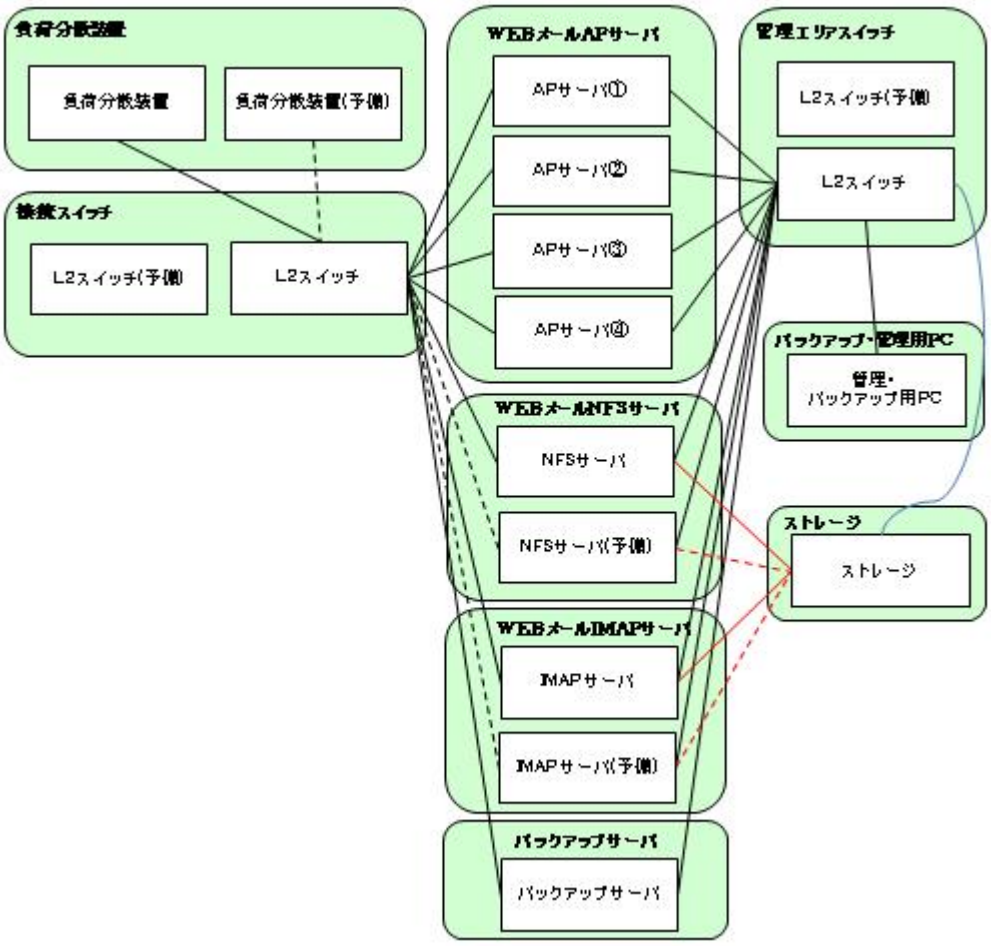
また、現行システムを踏襲して Exchange Server 2013 による環境を構築することも可能とするが、その場合は、現行の Exchange Server 2007 から設定を引き継ぐこととする。

なお、現行システムからのメールデータの移行は原則不要とするが、データ移行の手法や各ユーザが保存しているメールデータ（pst ファイル等）の閲覧方法等を検討し、本県に提案すること。

2.3.2. サーバ構成

サーバは IDC2 に設置することとする。

想定する WEB サーバ構成は下記の通りであるが、性能要件、設置要件等を踏まえたうえで、サーバ構成を決定すること。



- AP サーバ

  WEB メール機能を提供する。クライアントからは、HTTPS にて接続を行う。4 台構成とし、下記負荷分散機能により、負荷を分散し、障害時には、自動的に縮退運用を行う。

- 負荷分散装置

  WEB メール AP サーバ 4 台へのアクセスを分散させる。2 台での、Active-Standby 構成とし、障害時に予備機への自動切替を行う。

- NFS サーバ

  WEB メールのアカウント情報やその他設定管理情報の保存を行う。但し、実データは、ストレージに保存する。接続は、AP サーバからのみとする。2 台でのホットスタンバイ成とし、障害時には予備機への自動切替を行う。

- IMAP サーバ

  メールサーバ機能を提供し、WEB メールの各ユーザデータの保存を行う。但し、実データは、ストレージに保存する。2 台でのホットスタンバイ成とし、障害時には予備機への自動切替を行う。

- ストレージ

  WEB メールの管理データや、メールデータの格納を行う。主要コンポーネントは冗長

化されており、障害時には、自動切替を行う。

- バックアップサーバ
  ストレージ内のデータバックアップの管理を行う。また、各サーバのハード情報の監視などを行う。
- 接続スイッチ
  2 台での、コールドスタンバイ構成とし、障害時には、手動で LAN ケーブルの差替えにより切替を行う。
- 管理エリアスイッチ
  2 台での、コールドスタンバイ構成とし、障害時には、手動で LAN ケーブルの差替えにより切替を行う。
- バックアップ・管理用パソコン
  各サーバのシステムフルバックアップを行う。また、メンテナンス時等に、コンソールパソコンとして利用する。

2.3.3. 必要とする機能

本項では庁内メールシステムを WEB メールシステムにより構築する場合に必要とする機能について記載しているが、現行システムを踏襲して Exchange Server 2013 による環境を構築する場合は現行システムの機能を引き継ぐものとする。

2.3.3.1. 全般

ア．SMTP、POP3 及び IMAP プロトコルに対応すること。

イ．メールアカウント数が 8,000 以上利用できるように必要なライセンス等を提供すること。

ウ．100KB のメールを 1 秒間に 20 通以上送受信できること。また、6,000 アカウントへ同報配信が可能であること。

2.3.3.2. 言語

ア．全ての機能が日本語に対応していること。

イ．UTF-8 及び S-JIS に対応していること。

2.3.3.3. ログイン

ア．Active Directory を利用してシングルサインオンでログインが可能なこと。

イ．ID・パスワードを直接入力するログイン画面をシングルサインオンとは別に用意すること。この場合、Active Directory サーバへ認証情報を問合せることとなる。

ウ．マルチドメインに対応し、「mieken.jp」ドメイン以外のドメインを管理運用できること。また、ドメイン単位で各種設定を変更できること。

エ．マルチアカウントに対応し、各ユーザが既定のアカウント（個人アカウント）以外に所属メールアカウント等を複数管理できること。また、複数ユーザが同一のアカウントを共有できること。

オ．本県にて運用しているグループウェアシステムと連携するAPIを提供すること。同APIにより、グループウェアシステム上で新着メールの件数、送信者、タイトル及び送信日時等が表示できること。また、グループウェアシステムからWEBメールシステムが起動できること。
なお、連携方法として、http又はhttpsによりグループウェアシステムのWEBサーバポータル画面から必要なパラメータを渡し、生成された結果を表示させる方法を想定しているが、グループウェアシステム側の改修費用が発生する場合は、受託事業者にて負担すること。

2.3.3.4. 画面レイアウト

ア．フォルダ、メール一覧、メール本文が表示可能であり、各表示エリアの表示・非表示をユーザが選択できること。
イ．ユーザフォルダの使用容量表示が可能であり、しきい値を設定することでユーザに警告メッセージを表示できること。

2.3.3.5. フォルダ操作

ア．フォルダの新規作成、名称変更、削除が可能なこと。また、フォルダペインを右クリックすることでも操作できること。
イ．フォルダは階層化することが可能であり、5階層以上階層化できること。
ウ．フォルダ内のメール件数（未読／既読）を表示できること。
エ．フォルダ内メールを一括で既読化できること。
オ．フォルダ内メールを一括で削除できること。
カ．フォルダ内メールをtxt／eml形式により一括でエクスポートできること。
キ．ドラッグ&ドロップでメールのフォルダ間移動・コピーできること。
ク．ドラッグ&ドロップでフォルダの移動・コピーができること。
ケ．受信メールの自動振分が可能であり、複数の振分ルールが作成できること。

2.3.3.6. メール一覧表示

ア．メールの一覧表示ができること。
イ．一覧表示件数を設定でき、別途管理者が上限値を設定できること。
ウ．メールの未読・既読表示ができること。また、未読については強調表示等ができること。
エ．メールの未読・既読の変更ができること。
オ．メールのソートが可能であり、件名、送信者、受信日時、サイズでソートが可能なこと。
カ．メールの検索が可能であり、件名、送信者、本文検索ができること。また、and検索ができること。
キ．メールにマーキングができること。なお、フラグ設定でも可とする。
ク．メール一覧にて右クリックでのメール操作が可能であり、返信、全員への返信、転送、削除、未読・既読の変更及びマーキングができること。
ケ．メール一覧にてダブルクリックにより別画面でメール本文を表示できること。

2.3.3.7. メール本文表示

ア．メール一覧と同一画面でメール本文を表示できること。

イ．HTML メールの表示が可能であり、HTML／テキストの表示を選択できること。

ウ．添付ファイルをダウンロードできること。

エ．添付ファイルのみの削除が可能であり、メール本文表示画面にて添付ファイルを削除していることが分かること。

オ．メールデータを txt／eml 形式にてエクスポートできること。

カ．メール本文内の URL リンクをクリックすると、Web ブラウザにてリンク先サイトが表示できること。

キ．開封通知確認への対応選択が可能であり、開封通知を返送するか無視するかを選択できること。

2.3.3.8. メール作成・送信

ア．署名の入力、編集、選択挿入が可能であり、1 アカウントに複数の署名が登録できること。

イ．アドレス入力補助機能（オートコンプリート）が利用可能であり、アドレス帳からの選択入力もできること。

ウ．宛先欄で To、Cc、Bcc を表示できること。

エ．HTML メールを作成できること。

オ．ファイルの添付が可能であり、複数ファイルを添付できること。

カ．下書き保存ができること。

キ．開封確認の要求ができること。

ク．重要度の設定ができること。

2.3.3.9. アドレス帳

ア．個人用アドレス帳の作成、編集、削除ができること。

イ．共有アドレス帳の参照が可能であり、以下の作業が行えること。

・作成・編集・削除は管理者のみが行えること。

・共有アドレス帳への登録は CSV ファイルにより一括で行えること。

・人事異動等の際に、CSV ファイルにより一括登録変更ができること。

・共有アドレス帳から個人用アドレス帳への登録ができること。

・共有アドレス帳は所属単位での階層表示が可能であり、4 階層以上表示できること。

・アカウント単位で共有アドレス帳への掲載・非掲載を設定できること。

ウ．受信メールからアドレス帳への登録が可能であり、送信者・受信者どちらも登録できること。

エ．アドレスグループの作成、編集、削除が可能であり、右クリックやドラッグ&ドロップにより操作できること。また、宛先へのアドレスグループ設定ができること。

オ．アドレス帳からメール作成ができること。

カ．アドレス帳から To、Cc、Bcc を指定してメール作成が可能であり、右クリックやドラッグ&ド

ロップにより指定ができること。

キ．アドレス帳フォルダの階層表示が可能であり、5 階層以上表示できること。

ク．アドレス帳のソートができること。

ケ．アドレス帳の検索が可能であり、個人用アドレス帳と共有アドレス帳ともに検索できること。

2.3.3.10. その他

ア．ユーザ自身でメールの自動転送設定が可能であり、転送メールをメールボックスに残す・残さないの設定ができること。また、条件付き転送設定や転送期間の設定ができること。

イ．ユーザ自身でメールの自動応答設定が可能であり、不在時等にメール送信者に対して各ユーザがそれぞれ指定したメッセージを自動で送信できること。

ウ．各種機能の有効・無効設定は管理者のみが設定変更可能であり、アカウントをグループ分けし、グループ単位で各種機能の有効・無効設定ができること。

エ．WEB メール以外の機能（例えばスケジュール機能等）について、管理者が不要と判断する機能については表示しないこと。

オ．ユーザが直感的に操作可能な画面構成となっていること。

カ．オンラインヘルプが利用できること。また、エにて非表示になっている機能については、ヘルプでも表示しないこと。

2.3.3.11. アカウント管理

ア．アカウントの作成、変更、削除、停止、再開が可能であり、管理者のみが操作できること。また、以下の作業が行えること。

・アカウントの新規作成については、既定のルールに従った運用が行えること。既定のルールについては、別紙「ログイン／アカウント」を参照すること。

・既定のルールに依らないアカウントを新規作成が可能であり、以下の作業が行えること。

・氏名変更等によるアカウント変更ができること。

・退職等によるアカウントの削除ができること。

・休職等によるアカウントの停止ができること。

・復職等によるアカウントの再開ができること。

イ．アカウントのパスワード管理が可能であり、管理者のみが操作できること。また、パスワード通知書類の発行ができること。

ウ．アカウントの運用については、「職員番号」や「所属コード」等と紐付けて管理できること。また、アカウント管理画面をシステム上に作成し、GUI により各種操作が行えること。

2.3.3.12. メール機能管理

ア．一度に送信できるメールの数を制限できること。制限値を超える場合は送信せず、ユーザにその旨が通知されること。

イ．添付ファイルの容量制限が可能であり、制限値を超える場合は送信せず、ユーザにその旨が通

知されること。

ウ．メール設定の一括設定ができること。

2.3.3.13. メーリングリスト

ア．メーリングリストの作成・変更・削除が可能であり、管理者のみが操作できること。

イ．全登録アカウントへの一斉メール送信ができること。

2.3.3.14. ログ管理

ア．ユーザのログイン・ログアウトのログが取得できること。

イ．メールの送受信のログが取得できること。

ウ．管理者の操作ログが取得できること。

エ．サーバイベントのログが取得できること。

2.4. ウィルス対策システム

2.4.1. 概要

現行システムに引き続きクライアントに対してウィルスの検出､パターンファイルの配信等のウィルス対策を行う。また、ウィルスの検出状況等の統計情報を出力する。

2.4.2. サーバ構成

想定するサーバ構成は下記の通りであるが、性能要件、設置要件等を踏まえたうえで、サーバ構成を決定すること。

設置場所	セグメント	用途	台数
本庁	内部	本庁への配信サーバ	1
IDC1	内部	本庁以外への配信サーバ	1
	Proxy	パターンファイル等ダウンロードサーバ(正) Proxyセグメント､DMZへの配信サーバ	1
IDC2	内部	本庁以外への配信サーバ	1
	Proxy	パターンファイル等ダウンロードサーバ(副) Proxyセグメント､DMZへの配信サーバ	1

2.4.3. 必要とする機能

2.4.3.1. ウィルス等の検出、駆除

ア．三重県行政 WAN に接続された Windows 及び Linux クライアントのウィルス等について検出を行うこと。また、検出されたウィルス等について、管理者にてあらかじめ隔離、駆除等の設定ができること。

イ．ウィルス等の検出はパターンファイルによるものだけでなく、未知のウィルス等にも対応できるようファイルの内容を基にした検出も可能であること。

ウ．クライアントにて、任意のファイル、フォルダ及びドライブ（ネットワークドライブを含む）

に対し、手動スキャンができること。

エ．管理者もしくはクライアントにて、任意の日時にスキャンを実行するよう設定ができること。

2.4.3.2. レポート機能

ア．各クライアントのエンジン、パターンファイルのバージョン及び過去に検出されたウィルス等の確認を行うことができること。

イ．ウィルス等が発見された場合は、ウィルス名・コンピュータ名・パス名及び対処結果を記載したメールをシステム管理者が指定する送付先へ送付すること。

2.4.3.3. パターンファイル等配信機能

パターンファイルやプログラムのアップデートが発生した際は、速やかに全クライアントに配信を行うこと。

2.4.3.4. 配信経路の設定

パターンファイル等の配信経路は以下のとおり設定することを想定しているが、より効率的で可用性等が向上する配信方法があれば、本県の承認を得たうえで設定を行うこと。

ア．インターネットよりパターンファイル等をダウンロードするサーバは Proxy セグメントに設置するサーバのみとする。なお、インターネットへの接続は IDC1 に設置のプロキシサーバを経由すること。

イ．Proxy セグメントに設置のサーバは他の配信サーバに配信を行うこと。

ウ．内部セグメントに接続されている Windows 及び Linux クライアントは内部セグメントのいずれかの配信サーバから配信を受けること。なお、本庁設置の配信サーバは本庁設置のクライアント、IDC 設置の配信サーバは本庁以外のクライアントへ配信することを想定している。

エ．Proxy セグメント及び DMZ に接続されている Windows 及び Linux クライアントは Proxy セグメントに設置の配信サーバから配信を受けること。なお、各 IDC の配信サーバは同一 IDC のクライアントへ配信することを想定している。

オ．内部セグメントの全ての配信サーバを冗長構成とし、内部セグメントのクライアントは通常接続するサーバに障害が発生した場合は他の配信サーバからパターンファイル等の提供を受けるよう設定を行うこと。また、全ての配信サーバと疎通が取れない場合は既存のプロキシサーバ経由でインターネットよりパターンファイル等をダウンロードするよう設定を行うこと。

カ．Proxy セグメントの 2 台の配信サーバを冗長構成とし、Proxy セグメント及び DMZ のクライアントは通常接続するサーバに障害が発生した場合はもう一方の配信サーバからパターンファイル等の提供を受けるよう設定を行うこと。

2.5. 運用管理システム

2.5.1. 概要

各クライアントに対して、インベントリの収集、プログラムの配信等を行う。

2.5.2. サーバ構成

想定するサーバ構成は下記の通りであるが、性能要件、設置要件等を踏まえたうえで、サーバ構成を決定すること。

設置場所	用途	台数
IDC1	インベントリ収集等サーバ（正）	1
IDC2	インベントリ収集等サーバ（副）	1
IDC1	パッチ配信サーバ（正）	1
IDC2	パッチ配信サーバ（副）	1

2.5.3. 必要とする機能

2.5.3.1. インベントリ取得・出力機能

ア．ハードウェア情報(CPU、メモリ、HDD 容量等)任意のタイミングに任意のクライアントに対してインベントリの取得が行えること。

イ．インベントリ取得のタイミングは、スケジュール設定できること。

ウ．取得するインベントリの種類は取得タイミング毎に設定でき、インベントリ取得に際してクライアントへの通知有無を選択できること。

エ．取得したインベントリ情報をリアルタイムで確認でき、任意の項目について、CSV 形式でエクスポートできること。

オ．各クライアントのインベントリ情報は 3 世代以上保有すること。

2.5.3.2. 取得するインベントリの種類

以下のインベントリ情報が取得できること。

ア．ハードウェア情報(CPU、メモリ、HDD 容量等)

イ．ウィルス対策ソフト情報(種類、パターンファイル等)

ウ．OS 情報(バージョン、適用パッチ等)

エ．アプリケーション情報(インストールされているアプリケーション名)

オ．ソフトウェア情報(保存しているプログラムファイル名等)

カ．レジストリ情報(指定した任意のレジストリ値)

キ．外部接続機器情報（USB にて接続されているデバイスの種類等）

ク．その他(ログオンユーザ名、IP アドレス等)

2.5.3.3. クライアント管理機能

取得したインベントリ情報等を基にクライアントのグループ分けが行えること。その際、クライアントは複数のグループに含めることができること。

2.5.3.4. プログラム配信機能

任意のクライアントもしくはグループに対し、任意のタイミングにてプログラムの配信ができること。また、プログラムの配信に際してクライアントへの通知有無を選択できること。

2.5.3.5. プログラム制御機能

管理者が指定する任意のプログラムについてクライアントにて起動不能とする設定ができること。

2.5.3.6. リモート操作機能

ア．クライアントのリモート操作ができること。なお、リモート操作時は操作者・被操作者双方でクライアント画面の閲覧・操作ができること。また、リモート操作開始時はクライアント側での操作は不要であること。

イ．リモート操作は複数の操作者が同時に行えること。

2.5.3.7. マイクロソフトセキュリティパッチ等配信機能

ア．全クライアントにマイクロソフトの任意のセキュリティパッチ、サービスパック等を配信することができること。なお、対象とするプログラムはマイクロソフトの分類で下表のとおりとし、今後新たな製品、クラスが追加された場合は、その都度配信対象とするか検討を行うものとする。

製品	Office(全てのバージョン) Silverlight Windows(全てのバージョン)
クラス	Service Packs セキュリティ問題の修正プログラム 更新 修正プログラム集 重要な更新

イ．各クライアントのパッチ適用状況の出力ができること。

ウ．Office365 等のクイック実行製品にも対応できるように配信領域等を別途設けること。

2.6. 障害監視

2.6.1. 概要

本県にて別途準備する障害監視ソフト（NTT 製 Crane）を用いて別途構築した障害監視システムを利用する。

2.6.2. 障害監視対象

本システムにて導入する全てのサーバ及び庁内メールシステムの外部ディスク、スイッチを障害監視の対象とする。

2.6.3. サーバの設定

障害監視システムは、本県が別途運用を委託している業者（以下、障害監視システム運用業者という。）が運用しているため、サーバの設定は本県及び障害監視システム運用業者と調整のうえ行うこと。

なお、障害監視システムの監視サーバ側の設定は障害監視システム運用業者が行う。

2.6.4. 監視項目

以下のような項目を監視する。

ア．ネットワーク障害

イ．サービス稼働

ウ．OS パフォーマンス

エ．ログ

オ．バックアップ状況

カ．庁内メールシステム共有ディスク稼働状況

2.7. バックアップ・リストア

2.7.1. 全サブシステム共通

ア．システム障害等に備え、データのバックアップを取得すること。

イ．バックアップは自動で取得するよう設定を行うこと。なお、バックアップは業務に影響のない夜間に行うこと。

ウ．バックアップ媒体は適宜交換を行うこと。なお、テープ交換はオートローダにより自動化すること。

2.7.2. 庁内メールシステム

ア．メールデータはシステムを停止せずに土曜日もしくは日曜日の夜間にフルバックアップ、フルバックアップを行わない日は差分もしくは増分バックアップを行うこと。

イ．ログやデータベースのバックアップ時にはシステムを停止することも可能とするが、その際の停止時間は 10 分以内とすること。

ウ．システム変更の都度、システムのフルバックアップを取得すること。

エ．システム停止を伴わず、ユーザ単位でメールデータのリストアが行えること。

2.7.3. 庁内メールシステム以外

ア．各サーバでの個別バックアップは行わず、IDC1 に集中バックアップサーバを構築し、各サーバのバックアップを取得すること。

イ．バックアップはテープ等の外部媒体に取得することとする。また、各サーバからのバックアップ時間短縮のため、一旦バックアップサーバにおいてディスク間バックアップを活用することを想定している。

ウ．週に一度フルバックアップを行うこととし、必要に応じてそれ以外の日に差分もしくは増分バックアップを行うこと。

エ．データのバックアップは複数世代の管理を行うこととし、4 週間分のデータを常に保持すること。また、上記とは別にフルバックアップのデータを毎月 1 回取得し、1 年間以上保存すること。

オ．ログデータを 1 年間以上保存すること。

カ．サーバ単位でのリストアが行えること。

2.8. 電源管理

2.8.1. 概要

本庁に設置のサーバについては無停電電源装置を整備したうえで停電対策を行う。

データセンターに設置のサーバについてはデータセンター自体に停電対策が施されているため、個別の停電対策は必要ない。

2.8.2. 設定

ア．本庁に設置のサーバは、電源障害時に自動シャットダウンし、復電後に自動起動するよう設定できること。

イ．シャットダウン及び起動時間の事前設定ができること。

3. ハードウェア・ソフトウェア要件

3.1. 基本的な考え方

ア．本システムの設計、構築、導入及び運用に伴い必要となる全てのハードウェア、ソフトウェア等の物品（以下、納入物品という。）の取得、設定に関することを業務範囲とする。

イ．納入物品の設置に伴って必然的に必要となる物品（ラック取り付け金具や、ケーブル等の接続部品等）についても提供すること。

ウ．落札決定後速やかに業務計画書の一部として納入物品の一覧を提出することとするが、納入時点での製品状況が業務計画書提出時点より変わった場合は、本県の承認を得たうえで最新の製品状況に従い最適な物品を納入すること。

エ．納入物品は「国際エネルギースタープログラム」に適合するものであることが望ましい。

オ．納入物品は、買い取りで提供すること。また、中古品であってはならない。

カ．納入物品等に伴うマニュアル、技術資料等については、必要部数を提供すること。

キ．納入に際して、梱包材、本県が不要と判断する付属品、マニュアル等を撤去すること。

ク．バックアップ及びクリーニングに必要な磁気媒体については、委託期間内において必要な量を見積り、確保するとともに、本県の要請に応じ納入すること。

ケ．本業務終了後、本業務範囲に係る物品（本業務で導入したハードウェア等）については、本県が指示するものを除き、受託事業者側で撤去（データの完全な消去を含む）を行うこととし、データの消去と機器の廃棄を証明する書類を提出すること。

コ．納入したソフトウェアは業務終了後も本県にて利用できるものとすること。

サ．納入物品のすべてを保守対象とし、一つの窓口で対応すること。

3.2. 性能要件

3.2.1. 全サブシステム共通の要件

本システムの使用環境は以下のとおりであり、この環境にて業務が円滑に行えるような機器の構成・性能とすること。

ア．ユーザ数

約 6,600 ユーザが登録されているが、10,000 ユーザまでの利用が可能であること。なお、ユーザが増加した場合の Windows CAL の追加は、本業務には含まない。

イ．クライアント数

約 8,800 台が接続されているが、12,000 台までの利用が可能であること。

ウ．クライアント端末

平成 26 年 11 月時点のクライアント環境は下表の通りであるが、下表に関わらず OS、ブラウザ、Office ソフトにおいてサポート期間内であるものであれば利用可能とすること。

OS	Windows 7 Professional SP1
ブラウザ	Internet Explorer 8
Officeソフト	Microsoft Office 2010 Professional Plus

エ．ネットワーク

2Gbps の幹線に 1Gbps の支線で本庁、各総合庁舎及びデータセンター、1Gbps もしくは 100Mbps の支線で大規模単独地域機関が接続されたネットワークを構築している。また、上記以外の単独地域機関については、ベストエフォートで下り 100Mbps 程度（数拠点のみ 30Mbps 程度）のインターネット VPN 接続を行っている。

3.2.2. 各システムにかかる要件

3.2.2.1. 庁内ドメインシステム

同一セグメント上にて、ログオン時にユーザ名、パスワードを DC に送信してから、DC が応答するまでにかかる時間を 5 秒以内とすること。

3.2.2.2. 庁内メール

ア．メール 1 通あたりの最大容量は約 1MB（一部ユーザについては 2MB）とすること。

イ．1 アカウントあたり、300MB 以上のメールデータ保存領域を確保すること。

ウ．メール送信後相手のメールボックスに到着するまでの時間を 5 秒以内とすること。

3.2.2.3. ウィルス対策システム

パターンファイル、検索エンジン等の全クライアントへの一斉配付が安定的に行えること。

3.2.2.4. 運用管理システム

ア．インベントリ収集に関して、400 台の同時アクセスが行えること。

イ．20 台のリモート接続が同時に行えること。

ウ．全クライアントに対して、任意のプログラムの一斉配信が安定的に行えること。

エ．全クライアントに対して、セキュリティパッチ等の一斉配信が安定的に行えること。

オ．マイクロソフトセキュリティパッチ等配信サーバについては、運用期間における十分なディスク容量を確保すること。

3.3. ハードウェア要件

3.3.1. 共通

ア．本県が提示する構成にて不足するハードウェアがある場合は、受託事業者にて追加を行うこと。なお、追加するハードウェアの納入、設定、保守も本業務に含むものとする。

イ．メモリ、ディスク容量等に関しては、性能要件を満たす構成とすること。また、要件の 2 割程度の拡張性を確保すること。なお、性能の拡張を行う際は、ハードウェアの増設等の単純な作業により対応可能な構成とすること。

3.3.2. 設置場所及び構成

3.3.2.1. 庁内メールシステム以外のサブシステム

ア．サーバの設置場所及び用途は下表のとおり想定しているが、性能要件、設置要件等を踏まえたうえで、サーバ構成を決定すること。

No.	設置場所	利用用途						備考
		庁内ドメイン			ウィルス対策	運用管理	バックアップ	
		DNS	DHCP(主)	DHCP(副)				
1	本庁	○	1-4階	吉田山等				
2		○	4-8階	1-4階				
3		○	吉田山等	4-8階				
4					○			
5	IDC1	○	5庁舎					
6		○						
7					○			
8					○			Proxyセグメント
9						収集(正)		
10						パッチ(正)		
11							○	
12	IDC2	○	5庁舎					
13		○						
14					○			
15					○			Proxyセグメント
16						収集(副)		
17						パッチ(副)		

イ．1 台のサーバで複数のサブシステムを兼用させてはならない。

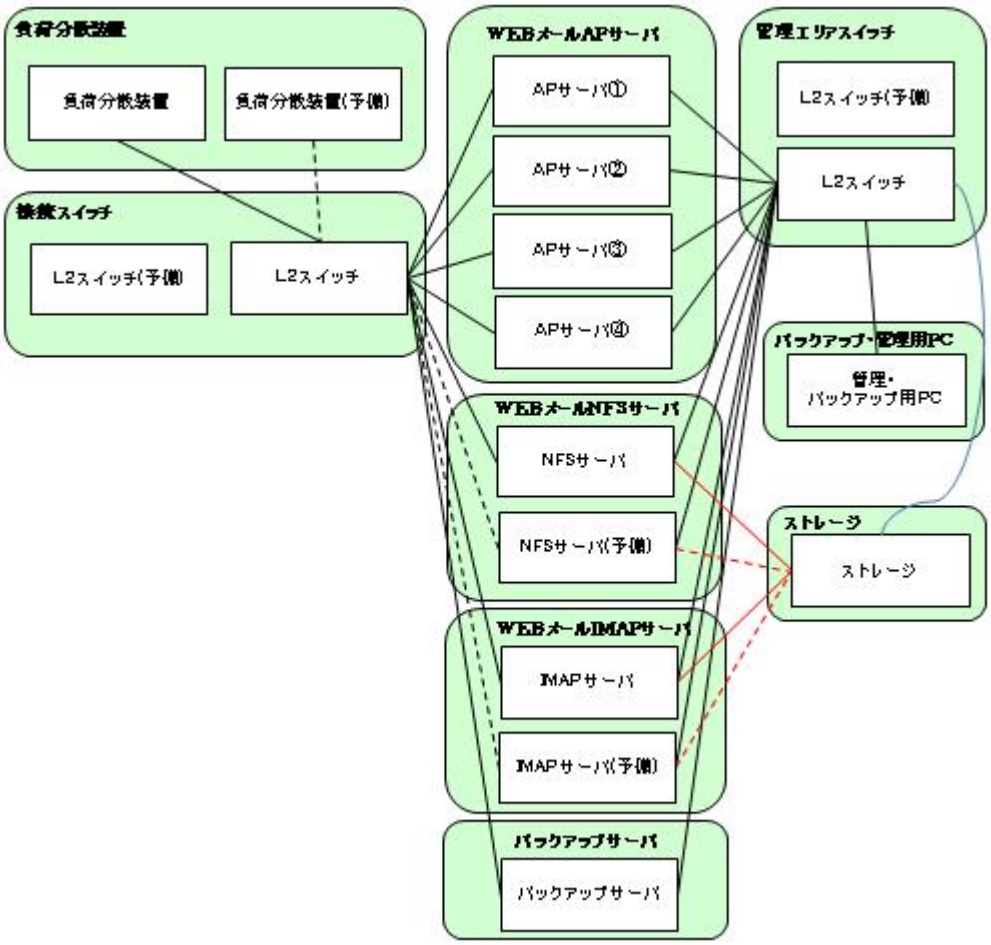
ウ．IDC1 及び IDC2 に設置するサーバのうち、2 つのサーバ（IDC1 設置のバックアップサーバと DC サーバの内の 1 つ）以外の内部セグメントのサーバについては、本県にて別途構築している統合サーバの利用を想定しているが、統合サーバの利用が不可能な場合は個別にサーバを設置することも可とする。統合サーバについての仕様等の詳細については、別紙 3「統合サーバの利用について」を参照のこと。

エ．独自でサーバを設置する場合、ディスクは RAID による冗長化を行い、1 つのディスクドライブに障害が発生してもサービスを継続できるような構成とすること。また、電源の二重化を行うこと。

オ．集中バックアップ装置は LTO ライブラリを想定しているが、運用要件を考慮し、メディア、カートリッジ数等を決定すること。

3.3.2.2. 庁内メールシステム

ア．サーバ構成は下図のとおり想定しているが、性能要件、設置要件等を踏まえたうえで、サーバ構成を決定すること。



イ．ディスクは RAID による冗長化を行い、1 つのディスクドライブに障害が発生してもサービスを継続できるような構成とすること。また、電源の二重化を行うこと。

ウ．バックアップ装置は LTO ライブラリを想定しているが、運用要件を考慮し、メディア、カートリッジ数等を決定すること。

3.3.3. 周辺機器

ア．ディスプレイは LCD ラックマウントタイプであり、1,024×768 ドット以上の解像度を持つものとすること。

イ．キーボードは日本語キーボードとすること。なお、ディスプレイと一体型のものも可とする。

ウ．ポインティングデバイスは 2 ボタンマウス、もしくはキーボード一体型のトラックパッドとすること。

エ．必要となる KVM スイッチを用意すること。

3.4. ソフトウェア要件

3.4.1. 共通

ア．新規に納入するソフトウェアは、契約時の最新バージョンの使用権を確保すること。なお、最新バージョンを使用しない場合は、最新バージョンの使用権を確保したままダウングレードを行うこと。

イ．使用するソフトウェアはシステムへの影響がない限り、最新のセキュリティパッチの適用を行ったうえで納入すること。

3.4.2. 使用ソフトウェア

要件を満たすソフトウェアを選定し、納入すること。

以下に示す保有ライセンス等以外のライセンスが必要となる場合は、全て受託事業者にて準備すること。

なお、ウィルス対策ソフト及び運用管理ソフトに関して、平成 27 年 9 月 1 日以降のライセンスは別途、本県にて調達することとし、本調達には含めないものとする。ただし、ウィルス対策ソフトは年間ライセンス費用 7,620,000 円（税抜）、運用管理ソフトは年間ライセンス費用 5,000,000 円（税抜）以内のソフトとすること。このライセンス費用は使用権のみでなく、バージョンアップ権も含まれるものとする。

3.4.3. 保有ライセンス等

3.4.3.1. マイクロソフト製品のライセンス

本県では行政 WAN を利用する全職員分の Windows Server 2012 のクライアントアクセスライセンス(CAL)を保有しており、本システムにおいても利用可能である。

また、マイクロソフト製品を新規で導入する場合、以下に示すライセンスプログラムを利用することができる。

製品の種類	ライセンスプログラム
全ての製品群	地域Select Plus for Government Partnars

3.4.3.2. ウィルス対策ソフトのライセンス

ウィルス対策ソフトについて、本県では平成 27 年 8 月 31 日まで以下のトレンドマイクロ社ライセンス（クライアントライセンス）を保有しており、本システムにおいて利用可能である。

製品の種類	数量
Client/Server Suite Premium	10,000
Server Protect for Linux	10,000
External Access Pack Server Protection 基本パック(100CPU)	1

3.4.3.3. 運用管理ソフトのライセンス

運用管理ソフトについて、本県では平成 27 年 8 月 31 日まで以下のライセンス（年間バージョンアップ保証サービス）を保有しており、本システムにおいて利用可能である。

製品の種類	数量
QNDα Standard	9,450

3.4.3.4. 障害監視ソフトのライセンス

障害監視ソフトについて、本県では Windows もしくは Linux(RHEL)サーバにインストールするエージェント 30 台分のライセンスを保有している。

エージェントライセンスの追加は不可であるため、上記ライセンス数に収まるサーバ構成とすること。

3.5. 設置要件

3.5.1. 共通

ア．機器の導入にあたり、各機器の搬入、設置、設定作業は基本的にすべて受託事業者が行うこと。

イ．サーバ及びその付属機器は全て、本県が指定する 19 インチラックに搭載すること。

ウ．サーバのディスプレイ、キーボード等に関しては複数サーバ間で共用するなどの省スペースに配慮した構成とすること。

エ．ラックに機器をマウントする際には、空調・ファンの稼動など、ラック内の温度に考慮した設置を行うこと。

オ．ラックの設置位置においては、ブランクパネル等を使用し通気通路を考慮すること。

カ．ラックにマウントできない機器に関しては耐震バンド等により耐震・免震措置を施すこと。

キ．機器・ラック・分電盤・電源ケーブル・通信ケーブルにラベル表記すること。

ク．通信ケーブルに負荷の掛からないケーブリングを施すこと。

ケ．各機器を設置場所へ直接納入し、本県指定のラックに収納し、設定作業およびソフトウェアのインストール作業を行うこと。

コ．設置場所への納入および設置作業、電源工事、配線工事ならびにネットワークへの接続作業の実施においては、必要に応じて実施日時を本県と調整すること。また、搬入時は本県が別途指示する搬入口およびエレベータを使用し、設備、器物破損を防止するための措置を講じること。

サ．ハードウェアの納入を円滑に進めるため、本県に事前に説明し、協議のうえ本県の指示に従い実施すること。

3.5.2. 本庁

ア．ラックに搭載する機器は 1 ラック以内とすること。なお、現行機器が設置されているラックは本システム用のラックとは別ラックであり、本庁においては新旧機器の併設が可能である。

イ．ラック単位に無停電電源装置を設置し、同一ラック内のサーバ等の機器へ電源供給を行うこと。
ウ．現行システムの機器の一部は 100V, 60A 分の非常用電源に接続されており、機器更新後は可能な限りこの非常用電源への接続を行うこと。
エ．ラックの規格は H2,000mm×W600mm×D1,000mm(41U)である。
オ．必要に応じて本県が指定する分電盤コンセントから各機器用コンセント等の電源ケーブルの敷設を行うこと。
カ．本県が準備するスイッチのポートからの UTP ケーブル敷設作業および接続作業を行うこと。なお、スイッチと本システムのサーバは別ラックである。
キ．本庁のラックは本県が用意する。

3.5.3. IDC1

ア．平成 27 年 6 月末までは受託事業者にてハウジング費用を負担し、平成 27 年 7 月以降は本県にて負担することとする。
イ．必要スペースとしては 10U 程度を想定しているが、それ以外のスペースが必要である場合は受託事業者にてハウジング費用を負担すること。
ウ．電源容量については各ラック 100V, 30A ずつ準備するが、それ以上に必要な場合は受託事業者にて追加電源の費用を負担すること。
エ．ラックの規格は H2,000mm×W700mm×D1,000mm(42U)である。ただし、各ラックにパッチ盤及び電源盤が設置されているため、実質的に利用できるのは 35U 程度である。
オ．同一ラック内のパッチ盤までの UTP ケーブル配線及びラック内の UTP ケーブル敷設、接続作業を受託事業者の作業とする。ただし、ラック間配線については IDC 事業者に依頼する必要があるため注意すること。
カ．センターでのラック間配線の申請から接続までは 2 週間程度を要するため、余裕をもって設置計画を立てること。

3.5.4. IDC2

ア．平成 27 年 6 月末までは受託事業者にてハウジング費用を負担し、平成 27 年 7 月以降は本県にて負担することとする。
イ．必要ラック数としては 1 ラックを想定しているが、それ以外のスペースが必要である場合は本県と調整のうえ、必要に応じ受託事業者にてハウジング費用を負担すること。
ウ．ラックの規格は H2,000mm×W700mm×D900mm(41U)である。ただし、各ラックにパッチ盤が設置されているため、実質的に利用できるのは 39U 程度である。
エ．同一ラック内のパッチ盤までの UTP ケーブル配線及びラック内の UTP ケーブル敷設、接続作業を受託事業者の作業とする。ただし、ラック間配線については IDC 事業者に依頼する必要があるため注意すること。
オ．センターでのラック間配線の申請から接続までは 2 週間程度を要するため、余裕をもって設置計画を立てること。

3.6. テスト要件

3.6.1. テスト計画

各設計書の内容が本番環境において有効であることを実証するための適切な試験を行い、発見された問題について対応し解消すること。

ア．試験計画を立案、ならびに試験計画書を作成し、本県の承認を得ること。

イ．.試験計画書に基づき、本番稼動前に試験を実施すること。

ウ．.本番稼動環境と同等の利用環境下において、構築したシステムの操作作業を行い機能、性能、セキュリティ面を含めて、目的の用途として利用可能な状態が保たれているか、十分な確認作業を行うこと。

エ．.本番稼動環境下において、障害発生時を想定したリストアを含む一連の復旧作業を試験し評価すること。

オ．.構築したシステムが既存の三重県情報ネットワークに影響を与えないこと等に留意した、信頼性に関する確認作業を行うこと。

3.6.2. テスト結果と判定

全ての試験が問題なく終了したことを記録した試験結果報告書を作成、報告し、本県の承認を得ること。

4. システム更新方法

4.1. 基本的な考え方

ア．平成 27 年 6 月 30 日までに「2. システム更新要件」に記載の事項を全て満たすよう、本システムへの設定変更作業を完了させること。

イ．システム更新作業において必要となる現行システムに関する調査、現行システムの保守業者等との調整、移行の際に必要となる全ての作業を本業務の範囲とする。

ウ．システム更新作業に際して、移行計画を作成し、本県の承認を得たうえで作業を実施すること。

エ．システム更新作業は休日もしくは夜間を基本とすること。ただし、サービスに影響がないと認められる場合は平日日勤帯での作業も可とするが、必ず本県の承認を得たうえで作業を行うこと。

オ．休日、夜間の作業であってもサービス停止時間を極力短縮するよう努めること。

カ．本番稼動前に、事前テストを実施し、テスト結果について本県の承認を得ること。

キ．システム更新作業は、機器設置場所内での作業とし、外部へのデータの持ち出しは不可とする。

ク．各サーバのサーバ関連 OS、アプリケーションについては、システムへの影響がない限り、納入時点での最新のパッチファイルもインストールすること。

4.2. システム更新作業

4.2.1. 全サブシステム共通

ア．システム更新に関して必要となる機器および媒体等の取得については本業務の範囲とする。

イ．作業にあたっては、本番環境の利用も可とするが、現行システム、各種テストに支障がないようにすること。

ウ．本システムの本番移行前にバックアップデータからのリストア試験を実施し、問題なくリストアができることを確認すること。

エ．移行にあたっては事前に現行システムのバックアップを取得することとし、また、万一に備え必ず切り戻しが可能であることを前提とした移行方法を採用すること。

オ．移行作業に伴い使用するバックアップ媒体について、移行作業終了後に必要となる媒体は書込み禁止処置を行い、機器設置場所内に保管すること。移行完了により不要となる媒体はデータの消去を行い、物理的に破壊すること。

カ．クライアント側で設定変更が必要となる場合は、その設定用のマニュアルを作成すること。

4.2.2. 庁内ドメインシステム

ア．新規にドメインを構築するのではなく、既存の Windows Server 2003 Active Directory ドメインを引き継ぐ形で更新を行うこと。

イ．ドメインコントローラの IP アドレスは可能な限り現行ドメインコントローラのものを引き継ぐこと。また、IP アドレスが変更となる場合は、その影響範囲及び対応策を本県に説明のうえ、了承を得ること。

ウ．更新に際して Active Directory の構成等を変更する必要が生じる場合は、その影響範囲及び対

応策を本県に説明のうえ、了承を得ること。

4.2.3. 庁内メールシステム

ア．新規に WEB メールシステムを構築する場合にあっては、現行システムからのメールデータ移行は原則不要とするが、各ユーザが保存しているメールデータ（pst ファイル等）の閲覧方法を検討し、本県に説明すること。

イ．現行システムを踏襲して Exchange Server 2013 による環境を構築することも可能とするが、その場合は、現行の Exchange Server 2007 から設定を引き継ぐこととする。また、メールデータの移行は原則不要とするが、データ移行の現実的な手法等を提案すること。

4.2.4. ウィルス対策システム

ア．可能な限りクライアントへのパターンファイル等の配信が継続できる方法とすること。

イ．ウィルス対策ソフトを変更する場合は、各クライアントの既存のウィルス対策ソフトのアンインストール及び更新後のウィルス対策ソフトのインストールを行うこと。

4.2.5. 運用管理システム

ア．可能な限り既存クライアントのインベントリ収集が継続できる方法とすること。

イ．運用管理ソフトを変更する場合は、各クライアントの既存の運用管理ソフトのアンインストール及び更新後の運用管理ソフトのインストールを行うこと。

4.2.6. 障害監視

2.6.に記載の要件を満たすよう設定を行うこと。

4.2.7. バックアップ

2.7.に記載の要件を満たすよう設定を行うこと。また、本運用開始までにバックアップデータからのリストアテストを実施すること。

4.2.8. 電源管理

2.8.に記載の要件を満たすよう設定を行うこと。

4.2.9. 開発用 ID 等の取扱い

ア．構築用及び試験用の ID 及びアカウントは、システム更新時に可能な限り削除すること。

イ．管理者権限を有する ID は使用者を限定し定期的に変更すること。管理者権限を有する ID を運用管理担当者に引き継ぐときには、ただちに運用管理担当者がパスワードを変更すること。

5. システム更新にかかる付帯作業

5.1. 研修

本システムにおいては、運用管理業務を運用管理担当者が行うことを前提としている。そのため、システム移行時に運用管理担当者に対する研修を行うこと。

なお、本番環境の運用が運用管理担当者に引き継がれるまでの期間における運用管理業務は全て受託事業者にて行うこと。

5.1.1. 運用管理担当者に対する教育

本システムについての運用管理担当者に対する操作マニュアルを作成し、稼動前および稼動後に本県、及び運用管理担当者に対して運用業務についての説明、ならびに各機器の操作教育を行うこと。

5.1.2. 運用管理担当者に対する再教育

運用管理担当者が変更となった場合、再研修を委託期間内に 2 回を限度として実施すること。その際には、本県に対しても同様の研修を行うこと。

5.2. 利用者向けマニュアルの作成

ア. 本県としては、移行に際し利用者の端末変更操作が極力必要のない運用形態を前提としているが、それらが必要となる場合は、利用者が容易に作業できるようマニュアルを作成すること。また、利用者にて必要となる端末変更操作及びマニュアルの内容について、本県及び運用管理担当者へ説明を行うこと。

イ. システム移行後に行政 WAN へ新たに接続する端末へ各種ソフトウェアインストールが必要となる場合は、職員が容易にインストールできるようなインストーラー等を作成するとともに、インストールマニュアル等を作成すること。

ウ. 本県が利用者を対象としたマニュアルの説明会を開催するときには、会場にて利用者からの質問等に対応すること。また、説明会後、質疑応答の内容を利用者向けマニュアルに反映し改版すること。

6. 運用保守要件

6.1. 基本的な考え方

ア．運用保守に必要なハードウェア、ソフトウェア等の準備は全て受託事業者の作業範囲とする。

イ．各サーバは行政 WAN 内の特定の管理端末から操作することを前提とする。

ウ．委託期間中にハードウェア、ソフトウェアのサポートが終了する場合、速やかに代替機、バージョンアップ版ソフトウェアの取得を行い、継続してサポートが受けられるように対応を行うこと。また、その際に発生する全ての作業については受託事業者の業務範囲とする。

エ．システム安定稼働後は、システム運用を運用管理担当者が行う。そのため、システム運用開始までに受託事業者はマニュアル等を整備し、運用管理担当者に業務の引き継ぎを行うこと。

オ．障害及び復旧作業により業務への影響が考えられる場合、速やかに関係者へ連絡を行うこと。

カ．機器保守に必要な体制を整えること。なお、保守を行う機器の範囲は、納入した全ての機器とする。

キ．納入物品のすべてを保守対象とし、一つの窓口で対応すること。

6.2. システム運用

6.2.1. 受託事業者の業務範囲

システム運用における受託事業者と運用管理担当者の業務分担は以下のとおりとする。

作業内容	受託事業者	運用管理担当者
日常の設定変更		○
バックアップテープ交換		○
データバックアップ、リストア		○
稼働監視		○
性能・構成管理		○
ログ管理		○
セキュリティ管理		○
日常運用業務に対する支援	○	
パッチによる影響等の情報提供	○	
パッチインストール		○
バージョンアップによる影響等の情報提供	○	
バージョンアップ作業	○	
庁舎停電対応		○
障害一次切り分け		○
障害対応	○	
障害後予防措置・是正措置	○	
運用マニュアルの改訂	○	

6.2.2. 運用管理担当者が行うもの

以下の業務については、運用管理担当者が行うことを想定しているが、そのマニュアルについては受託事業者にて作成し、運用管理担当者に業務の説明を行うこと。

また、運用期間中において、運用管理担当者の技術支援を行うこと。

ア．日常の設定作業

アカウントの登録、削除等、運用マニュアルに基づき日常の設定作業を行う。

イ．バックアップテープ交換、管理

月に 1 回程度のバックアップテープ交換を行う。

バックアップテープの管理を行う。

ウ．データバックアップ・リストア

システムに変更を加える際にデータのフルバックアップを取得する。

また、必要に応じてデータのリストアを行う。

エ．稼働監視

障害監視システムにより、各サーバの死活監視及びリソース監視を行う。

オ．性能・構成管理

サーバのリソースについて、不足がないか定期的にチェックを行う。

また、本システムにて導入される、ハードウェア及びソフトウェアの構成を管理する。

カ．ログ管理

各種ログ（ログオン、メール送受信、DHCP 等）について異常がないかチェックし、定期的に報告する。

キ．セキュリティ管理

ウィルス検出件数等をチェックし、定期的に報告する。

ク．パッチインストール

受託事業者により本システムへの影響がないと判断されたパッチのインストールを行う。

ケ．庁舎停電対応

本庁及び総合庁舎について、電気設備点検等で停電が発生する際、スケジュール機能を用いて機器の停止・起動の設定を行う。

コ．障害一次切り分け

障害が発生した場合、運用マニュアルに基づき、障害の一次切り分けを行う。

6.2.3. 受託事業者が行うもの

6.2.3.1. 日常運用業務に対する支援、提案

ア．運用管理担当者による本システムの運用業務全般を実施するための技術支援を行うこと。定常運用に伴う技術支援も範囲とする。

イ．必要に応じて性能を改善するための計画策定・対策を立案し、本県と協議のうえ対策方法の提案を行うこと。また、運用を効率的に行うためのスクリプト等の作成の支援を行うこと。

ウ．運用管理担当者が各種報告を行うための支援を行うこと。

6.2.3.2. パッチによる影響等の情報提供

ア．本システムで使用するソフトウェア製品に関するバグフィックス、セキュリティ対応等のパッチがリリースされた場合、速やかにその内容の調査を行い、適用の可否を本県に報告すること。また、適用できない場合は、適用するためのシステム改修の内容を本県に報告すること。なお、パッチリリースから情報の提供までの期間はマイクロソフトのパッチは 2 開庁日以内、その他の製品のパッチは 1 週間以内とする。

イ．本システムで影響を及ぼす恐れのあるパッチの提供がある場合、運用管理担当者が影響の有無についての確認作業を短時間に行えるように支援を行うこと。もしくは受託事業者がパッチ適用に立ち会い、本システムへの影響の有無を確認すること。

ウ．パッチの適用作業は運用管理担当者が行うものとするが、パッチ適用による障害が発生した場合は、受託事業者にて障害対応を行うこと。

6.2.3.3. バージョンアップによる影響等の情報提供

本システムで使用するすべてのソフトウェア製品のバージョンアップ製品がリリースされた場合、その内容の調査、本システムに対する影響の調査、適用の検討、本システムの改修が必要な場合はその内容に係る情報の提供を行うこと。

6.2.3.4. バージョンアップ作業

契約期間中に本システムで利用しているソフトウェアのバージョンのサポートが終了する場合、速やかにバージョンアップ版ソフトウェアの取得を行い、継続してサポートが受けられるように対応を行うこと。その際に発生する全ての作業については受託事業者の業務範囲とする。

また、サポート切れとなるソフトウェアのバージョンアップに伴い、他のソフトウェアのバージョンアップが必要となる場合は、そのソフトウェアのバージョンアップ版の取得及びバージョンアップ作業も本業務の範囲とする。

なお、ソフトウェア製品に対してパッチが適用されない、または、セキュリティホールの有無をそのソフトウェア開発業者が確認しなくなった時点でサポートの終了とする。

6.2.3.5. 障害対応

ア．運用管理担当者にて障害の発生原因の切り分けが困難である場合は、本県もしくは運用管理担当者からの連絡に基づき、障害の切り分け支援を行うこと。

イ．障害発生拠点へ駆けつけ、不良部位の切り分け及び修理・修正・交換を行うこと。

ウ．障害によりソフトウェア、データが破損した場合、バックアップデータ等より速やかに復旧を行うこと。また、必要に応じて、システムの再セットアップを行うこと。

6.2.3.6. 障害後是正措置・予防措置

障害が発生した場合、障害に関する情報を収集したうえで、その障害情報をもとに原因を分析し、同様の障害が発生しないように是正措置・予防措置を講じること。また、直ちに障害原因が判明しない場合は、本県の了承を得たうえで、継続して調査を行い、障害原因の特定に努めること。

障害情報、是正措置・予防措置の内容は障害記録として体系的に記録し、常に活用できるように保存すること。

6.2.3.7. 運用マニュアルの改訂

運用作業により、ドキュメント等の修正が発生した場合には履歴管理を行った上で速やかに各種ドキュメントを修正すること。尚、ドキュメントの修正にあたっては本県へ説明を行った上で、承認を受けること。

6.3. 保守体制

6.3.1. 保守対応時間

ア. 保守対応時間は、庁内メールシステムは 365 日 24 時間、それ以外のサブシステムは開庁日の 7 時 30 分から 20 時までとする。

イ. 上記とは別に、年度末の異動処理を行う 3 月 31 日 20 時から 4 月 1 日 7 時 30 分までは庁内ドメインシステムの保守対応時間とし、アカウント登録時のトラブルに備えること。

ウ. メール及び電話による障害連絡を 24 時間受け入れられることとし、保守対応時間外に障害が発生した場合は、翌開庁日の 7 時 30 分より対応を行う体制をとること。

6.3.2. 障害対応要件

ア. 保守対応時間内において、対応依頼から初期対応を開始するまでの時間を、概ね 30 分以内とすること。大規模災害発生時においては可能な限り当該時間を目標に対応すること。なお、初期対応とは、障害発生箇所・原因の確認作業への着手、本県などの関係者への連絡等を指す。

イ. 駆けつける必要があると判断してから、駆けつけ完了までの時間を開庁日の 8 時から 17 時 30 分までは 2 時間以内、上記以外の時間帯は 4 時間以内とすること。大規模災害発生時においては可能な限り当該時間を目標に対応すること。

ウ. 復旧方法が明らかになり、かつ復旧作業が必要な場所へ到着してから、復旧するまでを概ね 2 時間以内とすること。また、2 時間以内の復旧が困難と判明した場合は、2 時間以内に進捗状況と以降の対応スケジュールを報告すること。ただし、大規模災害発生時においては可能な限り当該時間を目標に対応すること。

エ. 障害によりサービスが停止している場合は、可能な限り速やかに復旧作業を行うこと。

オ. サービス停止を伴わない障害発生時において、サービス停止を伴う対応は開庁日の 8 時から 17 時 30 分以外の時間帯に行うこと。ただし、障害箇所が冗長化されておりサービスへの影響がない場合、本県の承認を得たうえで上記時間内に作業を行うことができるものとする。

6.3.3. 保守部品・消耗品

ア．オンサイトでの保守対応が不可能な部位がある場合については、予備品の保有等により迅速な復旧を実現すること。

イ．保守部品（付属品、ソフトウェアを含む。）を常時保有するとともに、契約期間における供給が可能なこと。なお、製造中止等に伴いこれらの対応ができなくなった場合は本システムに影響がないと本県が判断した部分に限り、代替品等による提供も可とする。

ウ．バックアップおよびクリーニングに必要な磁気媒体については、委託期間内において必要な量を見積り、納入すること。

6.3.4. リモート保守環境

ア．インターネット回線を介し三重県行政 WAN へ接続することにより、遠隔地でのリモート監視やリモート保守ができるリモート保守環境が利用可能であるので、必要に応じて利用することができるものとする。

イ．リモート保守環境の利用には、技術的、セキュリティ的な制限事項等があるため、別紙 5「リモート保守環境の利用について」を参照のうえ、利用可否の判断を行うこと。

ウ．リモート保守環境を活用する場合、受託事業者側にて必要となる回線費用等については、受託事業者が負担すること。

エ．リモート保守環境以外の方法での、三重県行政 WAN 外から本システムへのリモートアクセスは一切認めない。

7. その他

ア．履行期間終了時には受託事業者にて納入した機器について、本県が指定したものを撤去すること。

イ．機器撤去時期については、本県と調整の上、対応を行うこと。

ウ．機器撤去においては、機器内のデータは全て削除することとし、データの消去と機器の廃棄を証明する書類を提出すること。