インターネットメールシステム再構築及び
運用保守業務委託仕様書

平成 30 年 6 月

三重県

目次

1.業務の概要

1.1. 業務名

インターネットメールシステム再構築及び運用保守業務

1.2. 目的

現行のメールサーバ及びウイルスチェックサーバの老朽化に伴い、メールサーバ、ウイルスチェックサーバ及びそれらに付帯する装置の更新及び保守サービスを調達することを目的とする。

また、インターネットメールについて、危険な添付ファイルの分離等の新たなセキュリティ対策を実施することを目的とする。

1.3. 調達範囲

1.3.1. 調達内容

本業務の内容は以下のとおりである。

各業務の詳細については、2.2 調達内容を参照すること。

ア　メール送受信環境の再構築

イ　添付ファイルの分離機能の構築

ウ　添付ファイルの原本保管及び抽出機能の構築

エ　システム・データ移行

オ　運用引継ぎ

カ　保守サービス

1.3.2. 機能

本業務で調達する機能は以下のとおりである。

各機能の詳細については、6.個別要求事項を参照すること。

ア　内部メールサーバ機能

イ　ウイルスチェック機能

ウ　危険な添付ファイルの分離機能

エ　添付ファイルの原本保管及び抽出機能

オ　メールクライアントのアップデート機能

1.4. 履行場所、機器設置場所

履行場所及び納入する機器の設置場所は次のとおりである。

ア　三重県本庁舎(津市広明町 13)（以下「本庁」という。）

イ　三重県津市内データセンター（以下「津 DC」という。）もしくは三重県伊勢市

内データセンター（以下「伊勢 DC」という。）

1.5. 契約期間

表 1-1 契約期間

	期間	開始	終了
1	契約期間	契約日	平成 36 年 3 月
2	準備期間	契約日	平成 31 年 1 月
3	運用開始	平成 31 年 1 月	－
4	運用期間	平成 31 年 1 月	平成 36 年 2 月

1. 契約期間は、平成 30 年度の契約締結日から平成 36 年 3 月 31 日までとする。
2. 準備期間は、契約日から平成 31 年 1 月までとする。
   準備期間において、設計（基本、詳細）、構築・移行を完了すること。
3. 本業務で構築するシステム（以下、「本システム」という。の運用期間は、平成 31 年 1 月から平成 36 年 2 月末までとする。

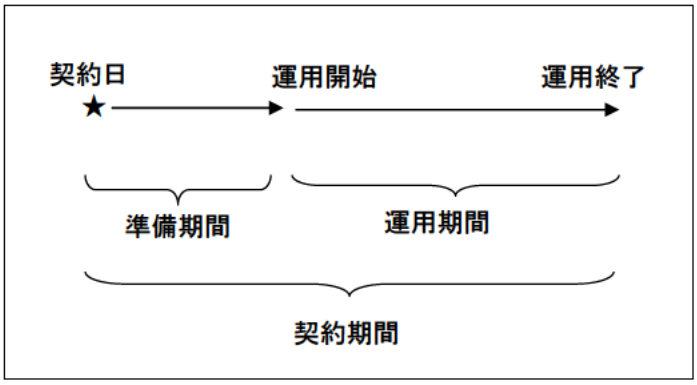

図 1-1 契約期間

1.6. 支払

1.6.1. 支払条件

本業務の利用にかかる費用の支払条件は以下のとおりである。

ア 各年度の支払額

各年度の支払額（税抜額）は、以下の割合を目安として、契約時に協議するものとする。

平成 30 年度 総契約額の○○%
平成 31 年度 総契約額の○○%
平成 32 年度 総契約額の○○%
平成 33 年度 総契約額の○○%
平成 34 年度 総契約額の○○%

平成 35 年度　総契約額の○○％

イ　保守費用は年度毎に業務完了分を支払うこととする。

ウ　業務の未完了分を前倒しで支払いすることはできない。

1.6.2.　内訳資料の提出

上記支払いの範囲内で入札額の内訳資料を作成し、提出すること。特に初年度の初期費用分と保守費用については明確に分離した資料を作成すること。また、内訳項目とその金額が明確な資料を作成し提出すること。

1.7. 本県からの提供資料

現行システム構成の詳細については、競争入札参加資格確認申請により有資格者であることが確認され、守秘義務の遵守に関する誓約書を提出した者に対して開示することが可能である。

ア　現行システムの設計構成情報、ハードウェア・ソフトウェア構成にかかる情報

イ　現行システムの監視・運用・保守にかかる情報

1.8. 機密保持

ア　本業務は、三重県電子情報安全対策基準（三重県情報セキュリティポリシー）を遵守して行うこと。当該ポリシーに抵触する行為または事象が発生した場合、そのようなおそれがある場合は、本県に報告を行い、本県の指示のもと速やかに対応すること。なお、三重県電子情報安全対策基準については、契約後に開示する。

イ　業務遂行上知り得た個人情報及び三重県の機密事項については、本業務のみに利用するものとし、契約期間中または契約終了後を問わず第三者に漏えいしないこと。

ウ　本業務における個人情報の取扱いについては、契約書（案）別記「個人情報の取扱いに関する特記事項」を守らなければならない。

1.9. 注意事項

1.9.1.　注意事項

ア　本業務について、契約書及び仕様書に明示されていない事項でも、その履行上当然必要な事項については、受託事業者が責任を持って対応すること。

イ　受託事業者は、運用開始までの作業スケジュールを本県と協議の上、決定すること。

ウ　本仕様書に記載されている全ての業務について、いかなるケースにおいても

本県に対して別途費用を請求することはできない。ただし、本県の要求仕様変更による追加費用については別途協議を行うこととする。

エ　本仕様書に定めのない事項が発生した場合及び疑義が発生した場合は、本県と協議の上、定めるものとする。

オ　現行システムまたはネットワークの停止を伴う作業は、閉庁日もしくは夜間での実施を前提にすること。

カ　受託事業者は、業務の履行にあたって暴力団、暴力団関係者又は暴力団関係法人等（以下暴力団等という。）による不当介入を受けたときは、次の義務を負うものとする。

受託事業者が(2)又は(3)の義務を怠ったときは、三重県の締結する物件関係契約からの暴力団等排除要綱第７条の規定により三重県物件関係落札資格停止要綱に基づく落札資格停止等の措置を講じる。

(1) 断固として不当介入を拒否すること。

(2) 警察に通報するとともに捜査上必要な協力をすること。

(3) 委託者に報告すること。

(4) 業務の履行において、暴力団等による不当介入を受けたことにより工程、納期等に遅れが生じる等の被害が生じるおそれがある場合は、委託者と協議を行うこと。

1.9.2.　関連事業者との調整

本業務の契約期間中、次期三重県情報ネットワークにかかる各システムの構築事業者ならびに運用管理事業者を決定する予定となっている。本業務の履行上、次期三重県情報ネットワークにかかるその他の調達の関連事業者との調整を行うこととなるため、留意すること。

ア　本業務の履行上、現行の三重県情報ネットワークの運用保守事業者（以下、「ネットワーク運用管理事業者」という。）との調整等は、本業務の範囲内とする。なお、調整にかかる費用を本県に請求することはできない。

イ　本業務の契約期間中（平成 30 年度～平成 35 年度）にネットワーク運用管理事業者が交代する場合、交代後のネットワーク運用管理事業者との調整等は本業務の範囲内とする。なお、調整にかかる費用を本県に請求することはできない。

ウ　本業務の契約期間中にファイアウォールシステム（以下、「FW システム」という。）の更新等により FW システム保守事業者が交代する場合、交代後の保守事業者との調整等 は本業務の範囲内とする。なお、調整にかかる費用を本県に請求することはできない。

エ　本業務の契約期間中にインターネットメール誤送信対策システム（以下、「誤送信対策システム」という。）の更新等により誤送信対策システム保守事業者が交代する場合、交代後の保守事業者との調整等 は本業務の範囲内とする。なお、調整にかかる費用を本県に請求することはできない。

2. 調達概要

2.1. 前提条件

2.1.1.　三重県行政 WAN の各セグメントについて

三重県行政 WAN は本県が利用している全庁的な行政事務用ネットワークである。三重県行政 WAN の論理ネットワーク概要図は別紙１のとおりである。

ア　業務系セグメント（①、⑩、⑪、⑳）
職員が通常利用する端末（以下、「利用端末」という。）や業務システムが接続されているセグメントであり、全ての拠点に存在する。拠点間は後述の業務系 WAN セグメントにて接続されている。

イ　Mail/DNS セグメント（②）
メールボックスを保有する内部メールサーバやドメインコントローラが接続されているセグメントであり、津 DC のみに存在する。

ウ　FW 接続用セグメント（③、⑬）
業務系セグメントと内部ファイアウォールの間のセグメントであり、津 DC 及び伊勢 DC に存在する。

エ　インターネット接続セグメント（④）
インターネット接続環境の仮想端末群が接続されているセグメントであり、津 DC のみに存在する。業務系セグメントとインターネット接続セグメント間においてファイルのやり取りを行う際は、専用のファイル転送サーバを通じて行う必要がある。

オ　Proxy セグメント（⑤、⑮）
内部ファイアウォールと外部ファイアウォールの間にあるセグメントであり、津 DC 及び伊勢 DC に存在する。メール用ウイルスチェックサーバ及びメール誤送信対策システムサーバは Proxy セグメントに接続されている。また、津 DC と伊勢 DC の Proxy セグメント間は、後述の Proxy-WAN セグメントにより相互接続されている。

カ　DMZ（⑥、⑯）
インターネット及び LGWAN とメール送受信を行う外部メールサーバやインターネットに公開しているサーバが接続されているセグメントであり、津 DC 及

び伊勢 DC に存在する。

キ　LGWAN 接続セグメント（⑦）

LGWAN に接続しているセグメントであり、津 DC のみに存在する。

ク　バリアセグメント（⑧、⑱）

三重県及び三重県内市町共通のインターネット接続基盤である三重県自治体情報セキュリティクラウドに接続しているセグメントであり、津 DC 及び伊勢 DC に存在する。

ケ　Proxy-WAN セグメント（ｉ）

津DC、伊勢DCのProxyセグメント同士を接続するセグメントであり、幹線である三重県情報ネットワーク上に存在する。

コ　業務系 WAN セグメント（ⅱ）

各拠点の業務系セグメント同士を接続するセグメントであり、幹線である三重県情報ネットワーク上に存在する。

2.1.2.　利用者

本県職員等(約 6,600 名)である。

ただし、メールアカウントは 7,000 アカウントまで利用できること。

2.1.3.　利用端末

メール受信に使用する主な庁内端末（以下、「利用端末」という。）の仕様は以下のとおりである。

OS：Windows 7 Professional SP1(32bit)もしくは Windows 10 Pro(64bit)

CPU：Intel Core i3

メモリ：2GB もしくは 4GB

ブラウザ：Internet Explorer 11

メールクライアント：Mozilla Thunderbird

台数：約 8,000 台

本業務にて提供する機能は、上記端末の他、マイクロソフトのサポート期間中である全ての Windows OS の機器にて利用できること。

2.1.4.　インターネット接続環境の仮想端末

インターネット接続環境の仮想端末群（以下、「仮想端末」という。）の仕様は以下のとおりである。

OS：Windows Server 2012 R2(64bit)

CPU：Intel Xeon E5-2697A（30 人あたり 5 コアを割り当て）

メモリ：32GB（最大 30 人で共用）

ブラウザ：Internet Explorer 11 または Google Chrome
同時接続数：1,500 セッション

2.1.5.　運用管理について

本業務の運用の一部は本県が別途契約しているネットワーク運用管理事業者のSE（以下、「運用管理担当者」という。）が行うことを想定しており、その駐在場所、時間及び契約期間は下表のとおりである。

なお、運用管理担当者について、契約期間終了後も同様の契約を行う予定である。

表 2-1 運用管理担当者駐在場所等

駐在場所	駐在時間	契約期間
本庁	開庁日 7:30～20:00	平成 31 年 12 月 31 日まで
津 DC	開庁日 8:30～17:00	

2.2. 調達内容

本業務における調達内容は以下のとおり。

ア　メール送受信環境の再構築

本システムで使用する機器及び付帯設備機器の調達・設計・納入・設定・構築・導入試験、ドキュメント等の作成、関係者との調整等を行うこと。

イ　添付ファイルの分離機能及び原本保管機能の構築

危険な添付ファイルを含むインターネットメールを受信した際に、当該添付ファイルを分離したメールを内部メールサーバに転送するとともに、添付ファイルを分離する前の原本を原本保管サーバに保管する機能を新たに構築すること。

ウ　添付ファイルの原本保管及び抽出機能の構築

添付ファイルを分離する前の原本を保管し、利用者からの要求に応じて分離された添付ファイルを抽出するための機能を新たに構築すること。

エ　システム・データ移行

既存システムから新システムへのデータ移行における計画策定、移行試験、移行作業、移行にかかる報告書等の作成、関係者との調整等を行うこと。

オ　運用引継ぎ

本システムで使用する機器及び付帯設備機器の操作説明書・運用手順書・関連資料の作成、運用管理担当者へのトレーニング等の運用引継ぎ、関係者との調整等を行うこと。

カ　保守サービス

本システムで使用する機器及び付帯設備機器の保守メンテナンス（ソフトウェア更新など）やシステム異常時における保守サービスの設計、保守サービスの実施にかかる報告書等の作成、関係者との調整等を行うこと。

2.3. 責任分界点

本県が指定するラック内のスイッチまたはパッチパネルの接続インタフェースまでを受託事業者の責任分界点とする。責任分界点までの全ての機器の準備及び配線を受託事業者の責任で行うこと。なお、ラック間の配線についても範囲内とする。

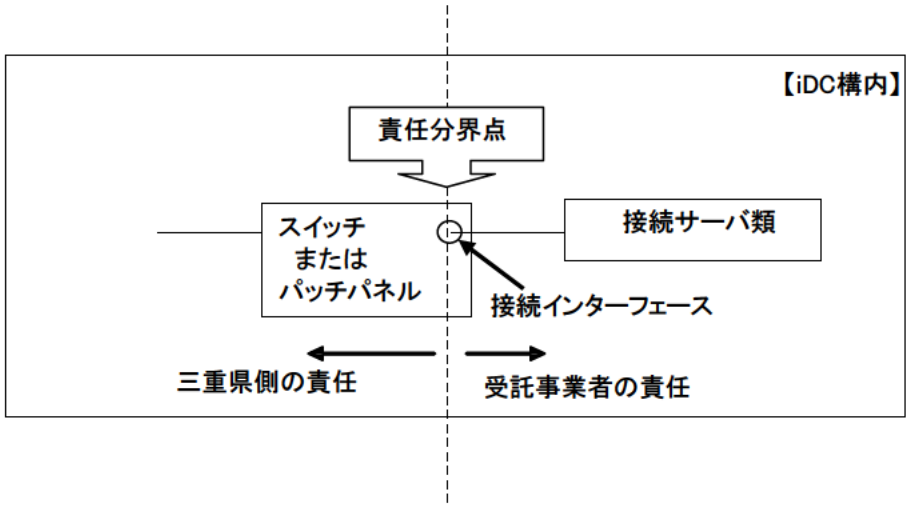

図 2-1 責任分界点

物品調達から保守における責任範囲を以下に示す。

表 2-2 受託事業者の責任範囲

作業内容	受託事業者	ネットワーク運用管理事業者（運用管理担当者）
物品調達	○	
設計	○	△
構築	○	
移行	○	
運用引継ぎ	○※1	○※1
運用	△	○
保守	○	△

［凡例］ ○：実施責任、△：支援

※1．ネットワーク運用管理事業者が契約期間中に交代する場合、変更後の次期ネットワーク運用管理事業者に対しても運用についての引継ぎを行うこと。

2.4. 想定スケジュール

本業務における想定スケジュールは以下のとおり。

① 基本設計 ： 契約日 ～平成 30 年 9 月
② 詳細設計 ： 平成 30 年 10 月 ～平成 30 年 11 月
③ 構築・移行 ： 平成 30 年 12 月 ～平成 31 年 1 月
④ 運用 ： 平成 31 年 1 月 ～平成 36 年 2 月（5 年間）

年 / 月	平成 30 年					平成 31 年				～	平成 36 年
	8	9	10	11	12	1	2	3	4		2
①基本設計		■									
②詳細設計			■	■							
③構築・移行					■	■					
④運用						■	■	■	■	■	■

図 2-2 想定スケジュール

3. 納品物件

3.1. 共通

ア 本業務の設計、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、「納品物件」という。）の取得、設置、設定を行うこと。
イ 納品物件は、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。
ウ 納品物件のすべてを保守対象とし、運用期間において一つの窓口で対応すること。

3.2. ハードウェア・ソフトウェア

本業務に必要な全てのハードウェア・ソフトウェアを納入すること。

3.3. ドキュメント

受託事業者は以下のドキュメントを指定された期日までに、本県に納品すること。納品方法は、電子媒体と紙面での納品を各 1 部とする。

なお、電子媒体のファイル形式については、本県と事前に協議を行い決定すること。

3.3.1. 業務計画書

受託事業者は契約締結後、速やかに業務計画書を作成の上、本県に提出し、本県の承認を得た上で業務に取りかかること。なお、業務計画書の内容は以下のとおりとする。

ア　業務スケジュール

イ　業務遂行体制・業務従事者名簿

ウ　納入予定物件一覧

3.3.2. 各種設計書、完成図書及び報告書

受託事業者は各工程の計画、成果を示すドキュメントを作成すること。

想定するドキュメントは以下のとおりである。

ただし、各工程に着手する前に、当該工程において作成するドキュメントに関し、本県と協議すること。また、内容に関しては、レビュー会を設けて本県に対し十分な説明を行い、内容の承認を得てから納品すること。

表 3-1 納入ドキュメント一覧

No.	成果物	提出期限
1	基本設計書	平成 30 年 10 月
2	詳細設計書	平成 30 年 12 月
3	構築手順書	平成 30 年 12 月
4	移行設計書	平成 30 年 12 月
5	試験計画書	平成 30 年 12 月
6	サーバ設定書	平成 30 年 12 月
7	付帯装置設定書	平成 30 年 12 月
8	試験報告書	平成 30 年 12 月
9	ラック配置図	平成 30 年 12 月
10	物理配線図	平成 30 年 12 月
11	納品物一覧（構築完了後）	平成 31 年 1 月
12	運用手順書	平成 31 年 1 月
13	操作説明書	平成 31 年 1 月
14	保守体制表	平成 31 年 1 月
15	保守作業報告書	保守作業対応の都度、提出

16	保守報告書	保守開始後から契約終了まで、年次で提出
17	議事録　※契約期間中の全ての会議体	１週間以内に提出

3.3.3.　手順書

システム運用前に以下の手順書等を作成すること。手順書等の内容に関しては、レビュー会を設けて本県及び運用管理担当者に対し十分な説明を行い、本県の承認を得てから納品すること。

ア　運用手順書

本システムについて、運用管理担当者が円滑に運用できるよう、運用手順書を作成すること。なお、障害時の緊急対応方法について必ず明記すること。

イ　操作説明書

本県及び運用管理担当者向けに、本システムについての操作説明書を作成すること。

また、利用者（一般県職員利用者）による端末操作については必要最小限にとどめることを前提としているが、利用者による操作が必要となる原本保管サーバからの添付ファイルの抽出方法等について、利用者が容易に作業できるよう操作説明書を作成すること。

3.3.4.　業務従事者名簿

業務に従事する者に変更がある場合は、その都度業務従事者名簿を提出し、本県の承認を得ること。

3.3.5.　議事録

本業務の遂行に伴う会議・打合せの議事録は受託事業者がその都度作成し、本県に提出すること。

3.4. 消耗品

3.4.1.　消耗品

本業務の遂行に必要となる消耗品等のすべてについて、契約期間内において必要な量を見積もり、納入すること。

4. 基本要件

4.1. 設計にかかる基本要件

ア　インターネットメールシステムを更新する際には、原則として現行のセキュリティポリシー等を踏襲するものとし、現行のメールサーバ・ウイルスチェックサーバなどの設定及び構成を参考に設計を行うこと。

イ　ウイルスチェックサーバにおいては、最新のウイルス定義ファイルでウイルスチェックができること。

ウ　保守・運用管理やセキュリティ面の向上を見据えた設計を行うこと。

4.2. 構築にかかる基本要件

ア　本システムに必要なOSのインストール、ソフトウェアのインストール・設定を行うこと。

イ　各サーバに使用するOSやソフトウェアは、納入時点での最新のパッチファイルをインストールすること。

ウ　本県が不要と判断するソフトウェアはインストールしないこと。

エ　仕様を満たすために必要なその他付帯設備装置（ロードバランサ等）については、導入における懸念事項を整理し、その対策を行うこと。必要ならば、関係する事業者等と調整を行うこと。

オ　本システムで利用するハードウェア及びソフトウェア（アプリケーション、ミドルウェア、ファームウェア等を含む）は、契約期間中に製品サポートの終了が予定されていない製品を選定すること。なお、契約期間中に本システムで利用している製品のサポートが終了する場合は、受託事業者の責任で後継製品や更新版の製品への移行を行い、継続してサポートが受けられるように対応を行うこと。ただし、サポートを受けなくても十分な品質を維持できることが事前に確認できた製品は移行しなくてもよい。

4.3. 移行にかかる基本要件

ア　データ移行においては、既存のメールデータやユーザ認証データを漏れなく移行すること。

イ　移行後のシステムが問題なく稼動すること。

ウ　システム切り替え作業中にメール通信が計画外に途切れないようにすること。

エ　外部メールシステム、誤送信対策システム等メール送受信に関連したシステムにも注意を払うこと。

オ　外部ロードバランサについては、別途構築している誤送信対策システム及びキャッシュサーバと共用となっているため、移行にあたっては既存システム

に影響を及ぼさないよう留意すること。

5.現行システム構成

5.1. 全体構成

現行システムは内部メールサーバ、ウイルスチェックサーバによって構成されている。

また、別途構築している誤送信対策システム、外部 DNS/メールサーバと連携して、本県内と外部とのメール送受信を行っている。

5.1.1. 概要

ア　メールボックスを保有する内部メールサーバ、ウイルス対策を行うメール用ウイルスチェックサーバ、送信時に添付ファイルの暗号化や宛先の BCC 化を行う誤送信対策システム、インターネット及び LGWAN とメールの送受信を行う外部メールサーバを整備している。

イ　利用者は、利用端末にインストールされたメールクライアントソフトウェア（Mozilla Thunderbird）を利用してメールの送受信を行っている。

ウ　各サーバにてメール送受信の履歴を記録している。

エ　メール送受信の処理の流れは別紙２－１～２－５のとおりである。

オ　メールの過去１年間の状況として、受信件数は 1 ヶ月あたりピーク時で約 103 万通、平均で約 73 万通、送信件数は 1 ヶ月あたりピーク時で約 28 万通、平均で約 24 万通である。

5.1.2. 機器構成

ア　内部メールサーバは津 DC に設置されており、2 台の物理サーバにて負荷分散を行っている。また、メールボックスは共有ストレージに保存されている。内部メールサーバの負荷分散は専用のロードバランサにて行われており、ロードバランサ自体もアクティブ/アクティブの冗長構成となっている。

イ　誤送信対策システムサーバは津 DC に設置されており、2 台の物理サーバにて負荷分散を行っている。なお、ロードバランサはメール用ウイルスチェックサーバ及び別途整備しているキャッシュサーバと共用している。

ウ　メール用ウイルスチェックサーバは津 DC に設置されており、2 台の物理サーバそれぞれに仮想アプライアンスサーバを搭載し、負荷分散を行っている。

エ　外部メールサーバは津 DC 及び伊勢 DC にそれぞれ 1 台設置されている。

オ　内部メールサーバ（共有ストレージを含む）、メール用ウイルスチェックサーバにおいては、共用のバックアップサーバ及びテープ装置を整備している。

カ　誤送信対策システムサーバについては、専用のバックアップサーバを整備している。外部メールサーバについては、個々のサーバに内蔵されたテープ装

置によってバックアップを取得している。

5.2. システム設定、設計内容

5.2.1. メール配送設定

ア　内部メールサーバは利用端末から送信されたメールを受け付け、外部宛のメールであればメール用ウイルスチェックサーバに転送し、内部宛のメールであれば該当のメールボックスに格納する。また、メール用ウイルスチェックサーバから転送された本県宛のメールを該当のメールボックスに格納し、利用端末からの POP アクセスにより各利用端末へ配送する。

イ　メール用ウイルスチェックサーバは、内部メールサーバから転送された外部宛のメール及び外部メールサーバから転送された本県宛のメールに対し、ウイルスチェックを行った後、外部宛のメールは誤送信対策システムサーバ、本県宛のメールは内部メールサーバに転送する。

ウ　誤送信対策システムサーバはメール用ウイルスチェックサーバから転送された外部宛のメールに対し、複数宛先の BCC 化や添付ファイルの暗号化等の措置を行った後、外部メールサーバに転送する。

エ　外部メールサーバは、メール用ウイルスチェックサーバから転送された外部宛のメールをインターネット/LGWAN へ転送する。また、インターネット/LGWAN から転送された本県宛のメールをメール用ウイルスチェックサーバへ転送する。

オ　内部メールサーバ、メール用ウイルスチェックサーバ、誤送信対策システムサーバ、外部メールサーバ間の配送方法は、スタティック配送である。

カ　インターネット/LGWAN から外部メールサーバへの配送方法は MX 配送を行い、津 DC 側の外部メールサーバについて、伊勢 DC 側より優先順位を高く設定している。

キ　外部メールサーバにて、宛先に応じて転送先をインターネットと LGWAN に振り分けている。また、LGWAN へメールを送信する場合、送信元ドメインやあて先ドメインが「pref.mie.jp」の場合は「pref.mie.lg.jp」に付け替えを行っている。

ク　後方散乱メール(Backscatter)対策のため、添付メールの件名に特定の文字列を含むメールを、外部メールサーバにて破棄している。

ケ　津 DC バリアセグメントの障害等で津 DC の外部メールサーバからメール送信ができない場合は、伊勢 DC の外部メール/DNS サーバにメールを転送したうえで、伊勢 DC の外部メールサーバからメール送信を行う。

コ　メールアドレスにおいて、「@」の直前にピリオドがある場合等、RFC(2821/2822)非準拠のメールであっても配送を行っている。

サ　メールキューの保持期間は 5 日間である。

シ　メール転送を行ったログを 1 年間保存している。

5.2.2.　ウイルスチェック

ア　メール用ウイルスチェックサーバにて以下のとおりメールのウイルスチェックを行っている。

イ　外部宛のメールにてウイルスが検出された際は、メールの配送を停止し、管理者及び送信者宛にウイルスが検出された旨のメールを送信する。

ウ　本県宛のメールにてウイルスが検出された際は、ウイルスを駆除し、本文にウイルスの駆除を行った旨のメッセージを挿入したうえで内部メールサーバに転送する。また、管理者にウイルスが検出された旨のメールを送信する。

エ　暗号化等によりウイルスの検索ができなかった場合は、本文にウイルス検索を行っていない旨のメッセージを挿入したうえで転送先のサーバにメール転送を行う。

5.2.3.　誤送信対策

ア　誤送信対策システムにて以下の通りメールの誤送信対策を行っている。

イ　宛先､CC､BCC に複数の外部のアドレスがある場合､宛先を送信者のアドレス、全ての送信先を BCC に変換し、本文に宛先の BCC 化を行った旨のメッセージを挿入したうえで外部メールサーバに転送する。また、送信者に対し、BCC 化を行った旨のメールを送信する。

ウ　暗号化されていないファイルが添付されている場合、パスワード付きの ZIP ファイルに変換する。また送信者に対し、ファイルのパスワード通知を行う。

エ　メールを一定時間保留し、保留時間内に送信者からの取り消し要求があればメールの削除を行う。また、送信者からの即時送信要求があれば、即時送信を行う。

オ　取り消し要求、即時送信要求を行うための利用者認証機能付きのウェブページを提供している。

6. 個別要求事項

6.1. 機器更新・システム構築にかかる要件

6.1.1.　共通要件

ア　現行の内部メールサーバ（ロードバランサ 2 台を含む）及びメール用ウイルスチェックサーバ（ロードバランサ 2 台を含む）が老朽化していることから、メール送受信の機能は維持したうえで、環境全体の再構築を行うことを想定

する。

イ　また、添付ファイルの分離機能及び添付ファイルの原本保管及び抽出機能を実現するためのサーバを構築すること。

ウ　新たに構築する添付ファイルの分離機能及び添付ファイルの原本保管及び抽出機能を含めたインターネットメールの受信フローイメージは別紙３－１～３－２を参照すること。なお、各サーバのネットワーク上における設置位置は変更可能とする。

エ　外部メールサーバ 2 台及び誤送信対策システムサーバは再構築の対象外とする。

オ　メール用ウイルスチェックサーバのロードバランサは別途構築している誤送信対策システムサーバ及びキャッシュサーバと共用しているため、再構築にあたっては既存システムの動作に影響を与えないよう考慮するとともに、個々のシステムの負荷分散が継続して行えるよう対応を行うこと。

カ　各サーバは、ユーザ数 10,000 ユーザ、クライアント数 10,000 台程度の環境にて問題なく利用が可能であるような性能とすること。

キ　メールクライアントソフトウェアは、Mozilla Thunderbird で問題なく使用できること。

ク　将来的な監査証跡や添付ファイル暗号化等のシステム拡張を行う際に、これを阻害しないような設計を行うこと。

ケ　本システムで導入するサーバ機器等は、NTP または SNTP で時刻同期を行うこと。時刻同期先は現状と同様のサーバを想定しているが、アクセス制限等により、時刻同期が困難な場合は、本県と協議の上で決定すること。

コ　各サーバ機器等のシステムログやメール送受信ログ等を取得・保存し、ログの出力時刻が適切に記録されるようにすること。出力ログの管理において、必要ならば syslog サーバ等を用意してもよい。

サ　通信プロトコルの変更等により、ファイアウォールの通過許可ルール等に変更が必要な場合には、作業指示書等を作成し、運用管理担当者及び FW システム保守事業者へ変更の依頼をすること。なお、これらの変更による実現が困難な場合には運用で回避するなど代替案により実現すること。

シ　構築する機器、サービスの死活監視を行う仕組みを提案すること。

ス　必要なデータについてバックアップを取得する仕組みを提案すること。

セ　運用管理は既存の行政 WAN 内の特定の運用管理端末（以下、「管理端末」という。）から運用管理担当者が操作することを前提とするが、受託事業者によるリモートでの運用管理が必要である場合は、その旨明示すること。

6.1.2.　内部メールサーバ機能

(1) 概要

ア　現行の設定を引き継いだ上で機器更新を行うこと。

イ　必要に応じて、機能追加等の設定変更を行うこと。

ウ　利用者がアクセスするメールボックスは 1 か所とし、送信時には宛先がインターネットであるか LGWAN であるか意識しない運用を前提とする。

(2) 機器更新

ア　内部メールサーバの更新を行うこと。

イ　内部メールサーバは可用性を考慮し、冗長構成とすること。

ウ　構成上、ロードバランサが必要ならば設置してよい。

エ　1 分間に 1,500 通のメール送受信に耐えられる性能とすること。

オ　ウイルスチェックサーバのメンテナンス等に備えて、外部へ送信するメール 1 週間分程度をローカルディスク、または、共有ディスクに保持できること。

カ　各利用端末から内部メールサーバへのメール配送は、認証付きの SMTP が利用できること。

キ　監視システム等からのメールを処理するため、認証なしの SMTP が利用できる内部メールサーバを新設すること。ただし、接続元 IP アドレスにより、接続の制限が行えること。

ク　内部メールサーバに格納されたメールは、各利用端末から POP 及び IMAP により閲覧できるようにすること。なお、各利用端末から Web インターフェースによる閲覧（Web メール）に替えることも可とする。

ケ　内部メールサーバに格納するメールボックスは一人あたり 500MB 以上の容量を確保すること。

コ　各利用端末から POP 及び IMAP で内部メールサーバにアクセスする場合は、ID 及びパスワードがネットワークに平文で流れないようにすること。

(3) 機能

ア　サーバソフトウェアは現行のソフトウェアからの移行が容易で、設定・運用が容易かつ、セキュリティが高いものを使用すること。

イ　内部から受け取ったメールを誤送信対策システムサーバへ転送すること。

ウ　外部から受け取った内部宛てメールを利用者向けに提供すること。

エ　メールボックスを保持すること。

オ　RFC 非準拠のメールに対しても送受信ができるよう設定を行うこと。

カ　メール送受信を行ったユーザや端末を IP アドレス等で識別・特定できるログを取得できること。

キ　メール送受信の成否を追跡できるログを取得できること。
ク　メール送受信サイズは1メールあたりメールヘッダを含め10MB以内に制限すること。
ケ　各ユーザのメールボックス容量を制限なしと設定可能であること。
コ　各ユーザのメールボックス使用量を一括で確認できる仕組みを用意すること。
サ　メール送信時、送信元のユーザ認証ができること。
シ　ユーザ認証において、暗号化パスワードでの認証機能を有すること。
ス　内部から送信されたメールの送信元ドメインが pref.mie.jp や pref.mie.lg.jp と異なる場合にメールを送信できないような設定が可能であること。
セ　ソフトウェアについては、上記仕様を満たし、セキュリティや運用を考慮したものを選定すること。

6.1.3.　ウイルスチェック機能

(1) 概要

ア　現行の設定を引き継いだ上で機器更新を行うこと。
イ　必要に応じて、機能追加等の設定変更を行うこと。

(2) 機器更新

ア　ウイルスチェックサーバの更新を行うこと。
イ　ウイルスチェックサーバは可用性等を考慮し、冗長構成とすること。
ウ　1分間に1,500通のメール送受信に耐えられる性能とすること。
エ　ロードバランサの設置を行うこと。現行のロードバランサは別途構築している誤送信対策システム及びキャッシュサーバと共用になっているため、それぞれのシステムが新ロードバランサに移行できるよう必要な支援を行うこと。

(3) 機能

ア　内部メールサーバ及び外部メールサーバより受信したメールのウイルスチェックを行うこと。
イ　内部から外部宛て、外部から内部宛てのメールをそれぞれ外部メールサーバ、内部メールサーバに転送を行うよう設定すること。
ウ　ウイルスが発見された場合は、駆除・隔離等の処理を行い、ウイルスが発見された旨をメール等で通知できること。
エ　処理したメールの内容を確認するためのログ（メールの処理日時、件名、送信元、あて先、処理結果等の項目を想定）の記録が可能なこと。
オ　ウイルス検知数などの統計情報を確認する機能を有すること。

カ　ウイルスチェック用のパターンファイルの更新を適宜行い、常に最新のパターンファイルでのウイルスチェックができるようにすること。インターネット上のサーバ等から更新情報を取得する際の Web 接続に当たっては、Web プロキシ経由となることに注意すること。なお、別システムで用意しているコントロールマネージャサーバを利用しても良い。

キ　ソフトウェアについては、上記仕様を満たし、現行と同程度のセキュリティレベルや運用性を確保できるものを選定すること。

ク　ソフトウェアについては、現行使用しているものを活用しても新規に調達してもよいが、どちらの場合にも費用は受託事業者の負担となることに留意すること。なお、現行ソフトウェアについて、平成 31 年 8 月末までは本県の所有するライセンスが使用可能である。

6.1.4.　添付ファイルの分離機能

(1) 概要

ア　インターネットから受信するメールに危険な添付ファイルが含まれている場合、当該添付ファイルを内部メールサーバにそのまま配送しないよう必要な対応を行う。

イ　分離された添付ファイルの原本を保存するため、上記処理を行う前のメール（以下、「原本メール」という。）もしくは添付ファイル（以下、「原本添付ファイル」という。）を原本保管サーバに配送する。

ウ　メールの本文中に含まれるリンクや HTML タグ等については処理の対象としない。

(2) 機能

ア　インターネットから受信するメールに危険な添付ファイルが含まれている場合、該当ファイルの分離等を行ったうえで内部メールサーバに配送することを想定している。

イ　原本メールについては添付ファイル分離等の処理の有無にかかわらず原本保管サーバに配送することを想定しているが、分離された原本添付ファイルのみを原本保管サーバに保存する形態としてもよい。

ウ　添付ファイルを分離した際には、内部メールサーバに配送するメールの本文にその旨を示すテキストを追記すること。また、原本添付ファイルのみを原本保管サーバに保存する場合は、原本添付ファイルを取りだすために必要な情報を追記すること。

エ　危険なファイルと判定するファイルの種類は別紙４を基本とするが、適宜追加や修正ができること。

オ　危険なファイルの判定方法は添付ファイルの拡張子によることを基本とする。

カ　実行ファイル等の一部ファイル形式については拡張子が偽装されている場合に対応するため、ファイルの内容を基に判定できること。拡張子とファイル内容が一致しないものを危険なファイルとみなして分離することとしてもよい。

キ　危険なファイルと危険でないファイルの両方を含む場合、危険なファイルのみを分離することを想定しているが、すべてのファイルを分離することとしてもよい。

ク　添付ファイルが ZIP ファイルの場合においては、中に含まれるファイルによって危険なファイルかどうかを判断できること。

ケ　パスワード付きの ZIP ファイルの場合には、含まれるファイルの拡張子によって危険なファイルかどうかを判断できること。なお、ZIP ファイルの中身の分析は 1 階層までとし、ZIP ファイルの中に ZIP ファイルが含まれている場合は危険なファイルとみなし分離することを想定している。

コ　ZIP ファイルの中に危険なファイルがひとつ以上含まれている場合には、危険とみなしてすべて分離することができること。

6.1.5.　添付ファイルの原本保管及び抽出機能

(1) 概要

ア　原本メールもしくは原本添付ファイルを一定期間保管し、原本の確認や抽出が必要となった場合に利用者がダウンロードできる機能を構築する。

イ　添付ファイルを分離する趣旨を踏まえ、そのままの状態で利用端末に取り込むことができない構成とすること。

ウ　原本保管サーバへのアクセスにはインターネット接続環境の仮想端末を利用することを想定しているが、その同時接続数が 1,500 ユーザであることを踏まえて運用が成り立つ方法とすること。

エ　原本保管サーバへのアクセスに別途認証を必要とする場合、インターネットメールアカウント作成時等の運用が簡便になる方法などを検討し提案すること。

(2) 機能

ア　添付ファイルの分離機能によって処理される前の原本メールもしくは分離された原本添付ファイルを保管する機能を有すること。

イ　原本メールの内容を閲覧、あるいは原本添付ファイルを指定し、分離された添付ファイルを保存する機能を有すること。

ウ　インターネット接続環境の仮想端末を利用する場合、仮想端末に特別なソフ

トウェアをインストールする必要がないこと。

エ　原本メールの内容を閲覧する際に、本文に埋め込まれた外部コンテンツ（Web ビーコン）に接続することを抑制できること。

オ　原本メールもしくは原本添付ファイルに簡単にアクセスできる機能を提供すること（添付ファイルを分離されたメールに記載されたリンクやキーワード等によってアクセスできるなど）

カ　原本メール及び原本添付ファイルの保存期間は受信から 60 日以上確保できること。

6.1.6.　メールクライアントのアップデート機能

(1) 概要

ア　利用端末にインストールされているメールクライアント（Mozilla Thunderbird）について、アップデートや一部設定の集中管理を行うためのサーバを構築すること。

イ　現在は三重県共通機能基盤の統合サーバ内で運用されており、その機能を引き継ぐことを想定している。

ウ　Web メールシステムを採用し、メールクライアントが不要となる場合は、この機能の実現は不要である。

(2) 機能

ア　利用端末にインストールされているメールクライアントからのアップデート要求に応え、アップデートモジュールを提供すること。

イ　メールクライアントの一部設定について集中管理を行うこと。

ウ　メールクライアントの新しいバージョンが公開された場合、アップデートモジュールやアップデート用設定ファイルの更新が可能なこと。更新の手順はできる限り自動化すること。

6.1.7.　バックアップ要件

ア　システム障害等に備え、システム及び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　バックアップはシステム及びデータが格納されているハードウェアとは異なるハードウェアに取得すること。

エ　ハードディスク内のローテーションを実施すること。バックアップに必要なソフトウェア及びハードウェアは全て受託事業者の責で用意すること。

オ　取得したバックアップからシステムのフルリストア及びログやメールデータ

の復元ができるようにすること。

カ　システムは 2 世代以上、データは 1 世代以上のバックアップ保存が可能なこと。

6.1.8.　ログ管理要件

ア　各機能の動作状況を把握するため、必要なログを保管すること。

イ　メールの送受信記録を含め、各機能で取得するログは 1 年以上保管することが可能なこと。

ウ　アプライアンス製品等でサーバ内に 1 年以上のログが記録できない場合は、ログ管理サーバ等を用意して syslog 等で転送する構成としてもよい。

エ　障害発生時の切り分けやメール受信状況の調査のため、対象期間やメールの送信元、送信先、件名等の情報から必要なログを取得できる仕組みを設けること。

6.1.9.　運用管理ソフトウェア

運用管理担当者が各機能の管理ができるよう、既存の管理端末に必要なソフトウェア等を導入すること。

ア　運用管理に必要なソフトウェアについては、受託事業者の責でインストールを行うこと。

6.1.10.　その他

仮想化ソリューションの利用により複数のサーバ機能を同一筐体内で稼動させることを想定している。各サーバ機能については冗長性を確保すること。

また、仮想化による実装等に関わらず、運用に支障が出ないようにし、運用に支障が認められた場合には、本業務の範囲内で整備、改善すること。

6.2.　システム・データ移行にかかる要件

6.2.1.　移行の基本方針

ア　インターネットメールシステム移行の際に必要となる移行設計・計画・テストと移行作業及びそれにかかる調査等を行うこと。

6.2.2.　移行計画

ア　業務に支障を来さない移行方法を検討し、受信及び送信メールを消失することがないようリスクの軽減に努めること。

イ　事前にバックアップを取得し、万が一に備えて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。

ウ　移行により現行システムに対する影響が考えられる場合は、休日、平日夜間等での作業を前提とすること。影響がない場合については平日昼間での作業を可能とする。

エ　システム移行時に本県より提供可能なスイッチあるいはパッチパネルのポート数は業務系セグメントで 3 ポート、プロキシセグメントで 3 ポート、インターネット接続セグメントで 2 ポートを想定している。構築・移行にあたり、新システムの収容ポートが不足する場合には、受託事業者の責において、スイッチ等の機器を用意すること。

オ　また、設置予定のラックは新規契約のラックとなるため、当該ラックまでの接続に必要となるラック間配線にかかる費用については受託事業者が負担すること。

6.2.3.　移行対象

ア　内部メールサーバに保管されているメールについてはすべて移行対象とする。ただし、移行にかかる時間を短縮するため、本県において保管されたメールの削減に努めることとする。

イ　内部メールサーバにアクセスするために使用するパスワードについても可能な限り変更不要とすること。ただし、Web メールシステムへ移行する場合はこの限りではない。

ウ　内部メールサーバに設定されている転送設定等についても移行対象とする。

エ　更新対象の各サーバで保留されているメール（メールスプール）については、移行前にすべて配送させてから移行することを想定している。

6.3. 運用引継ぎにかかる要件

本システムの運用業務は運用管理担当者が行うことを前提としている。そのため、システム移行にあたり運用管理担当者に対する運用引継ぎを行うこと。

また、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業務は全て受託事業者にて行うこと。

6.3.1.　各種手順書等の作成

本システムについて、運用業務に必要な以下のマニュアル等を作成すること。

ア　導入機器等の操作説明書

イ　運用手順書

ウ　障害時の対応手順書（切り分け方法やリストア手順書等）

エ　その他、運用業務に必要な資料類

6.3.2. 説明会の実施

本県及び運用管理担当者向けの説明会を実施し、本システム及び運用業務についての説明、各機器の操作説明等を実施すること。実施場所や方法については、本県と協議の上で決定すること。

また、本県の担当者や運用管理担当者が変更となる場合にも、必要に応じて再度説明を行うこと。

6.4. 保守サービスにかかる要件

6.4.1. 受託事業者の業務範囲

保守サービス提供においては、ハードウェア及びソフトウェアの保守を主とするが、定常運用に対する支援も行うこと。

受託事業者とネットワーク運用管理事業者の業務分担を以下のとおりとする。

表 6-1 受託事業者の業務範囲

作業内容	受託事業者	ネットワーク運用管理事業者（運用管理担当者）
日常設定作業		○
バックアップテープ交換・管理（必要な場合）		○
データバックアップ	○	▲
データリストア	○	▲
稼動監視		○
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等	△	○
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	○	
障害一次切り分け		○
障害対応	○	
障害後予防処置・是正措置	○	
運用手順書の改訂	○	

[凡例] ○：責任者、▲：日常業務対応者、△：支援

6.4.2.　保守体制

(1) 障害対応時間

ア　保守対応時間は 24 時間 365 日とする。ただし、個別の障害事象により本県が承認した場合にはこの限りではない。

イ　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。

(2) 障害対応体制

以下の障害対応が行える体制を整えること。

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。ただし、大規模災害発生時においてはこの限りではない。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保守作業員が保守作業場所に到着するまでの時間は、開庁日の 7 時 30 分から 20 時までは 2 時間以内、上記以外の時間帯は 4 時間以内とすること。ただし、大規模災害発生時においてはこの限りではない。

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本県に報告すること。ただし、大規模災害発生時においてはこの限りではない。

エ　障害箇所が冗長化されておりシステム機能が停止していない場合、障害対応は開庁日の 8 時から 18 時以外の時間帯に行うこと。ただし、システム機能を停止させずに障害対応が可能な場合は、本県の承認を受けた上で、開庁日の 8 時から 18 時の間に実施してもよい。

6.4.3.　保守業務

(1) 日常業務に対する支援、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。

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、本県に提案を行うこと。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。

(2) データバックアップとリストア

ア　データバックアップ及びリストアに関しては、前出の「6.1.7 バックアップ要件」に従い実施すること。

イ　運用管理担当者との連携に関しては、本県ならびにネットワーク運用管理事業者等との協議の上で決定すること。

ウ　リストアの手順確認や運用管理担当者の習熟のため、定期的（年に 1 回程度を想定）に運世管理事業者等と連携しリストア訓練を行うこと。

(3) 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、受託事業者は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。

イ　パッチリリースから情報の提供までの期間は開庁日 3 日以内とするが、緊急度の高いものはできる限り速やかに報告すること。また、パッチの適用可否や影響の確認に開庁日 3 日以上必要な場合には、パッチリリース情報を開庁日 3 日以内に報告すること。

ウ　本システムに影響を及ぼす恐れのあるパッチの提供がある場合、運用管理担当者がパッチ適用後の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、パッチ適用後の本システムへの影響の有無を確認すること。

エ　パッチ適用による障害が発生した場合は、受託事業者にて障害対応を行うこと。

(4) バージョンアップによる影響等の情報提供

ア　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かかる情報の提供を行うこと。

(5) バージョンアップ作業

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

イ　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。

ウ　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、脆弱性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。

エ　ファームウェアのバージョンアップ作業も本業務の範囲とする。メーカーより新ファームウェアがリリースされ、より安定した動作等のために、本システムへの適用が必要と判断される場合には、本県と協議の上で、適用を行うこと。

(6) 予防保守交換

ア　本県または運用管理担当者からシステムの異常等の連絡を受けた際には、運用管理担当者と連携し然るべき調査を行い、本県の求めに応じて予防交換を行うこと。

(7) 障害対応

ア　本県または運用管理担当者からの連絡や故障発生等の通知メール等により、本システムの障害を確認した場合、必要な障害対応を行うこと。

イ　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、本県また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。

ウ　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。

エ　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に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。

(8) 障害後是正措置

ア　障害が発生した場合、障害に関する情報を収集した上で、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・予防処置を講じること。また、直ちに障害原因が判明しない場合は、本県の了承を得た上で、継続して調査を行い、障害原因の特定に努めること。

イ　障害情報、是正措置・予防処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。

(9) 運用手順書の改訂

ア　運用作業内容の変更等により、ドキュメント等の修正が発生した場合には履歴管理を行った上で速やかに各種ドキュメントを修正すること。なお、ドキ

ュメントの修正にあたっては本県へ説明を行い、承認を受けた上で本県に提出すること。

(10)　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。

ウ　製造会社のサポートやサービスの終了（EOSL：End of Service Life）等により前項の対応ができなくなった場合は、同等以上の性能を持った代替品等による提供も可とする。その場合、それぞれの機器が EOSL を迎える前に、本県に代替品の承認を受けること。

エ　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、契約期間内において必要な量を見積もり、納入すること。

6.4.4.　リモート保守環境の利用

各サーバは、コンソールまたは行政 WAN 内の許可された管理端末から操作して保守作業することを原則とするが、本県の共通機能基盤として用意しているリモート保守環境を利用して、インターネット回線を介し、遠隔からでもリモート監視やリモート保守が可能である。

ただし、リモート保守環境の利用には、技術面、セキュリティ面の制限事項等により利用できない場合も想定されるので、別紙５を参照した上で、利用可否について判断を行うこと。

なお、リモート保守環境で必要となる回線費用については、受託事業者が負担すること。

また、リモート保守環境を含む共通機能基盤について再構築を予定しており、本システムの運用期間内に接続方法等が変更になる可能性があるため留意すること。

6.4.5.　運用管理担当者の業務

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おり、受託事業者の業務範囲外であるが、そのマニュアル等については受託事業者にて作成し、運用管理担当者に対して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

メールアカウントの登録・削除、LGWAN ドメイン宛て送信用設定ファイルの変更等、運用手順書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

バックアップにテープを利用する必要がある場合、バックアップテープ交換を行う。また、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

システムに変更を加える際にデータあるいはシステムのフルバックアップを取得する。

エ　データリストア

必要に応じてデータあるいはシステムのリストアを行う。

オ　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。

カ　性能・構成管理

各機器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。

キ　ログ管理

各種ログについて異常がないかチェックし、定期的に報告する。

ク　セキュリティ管理

不正アクセスの有無や、ウイルス検出件数等をチェックし、定期的に報告する。

ケ　パッチインストール等

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。また、メールクライアントのアップデート機能を用いてメールクライアントのアップデート用モジュールを提供する。

コ　障害一次切り分け

障害が発生した場合、運用手順書に基づき、障害の一次切り分けを行う。

7. テスト要件

7.1. テスト計画

設計書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、構築した本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　構築した本システムが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、信頼性に関する確認作業を行うこと。

7.2. テスト結果と判定

全ての試験結果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。

8.セキュリティ要件

ア　導入する機器やソフトウェアに関して公開されている脆弱性対策が完了していること。

イ　システムに不要なサービスは停止または削除すること。

ウ　導入する機器やソフトウェアにおいては、導入後の運用期間中も、適切なパッチや脆弱性対策技術情報が適時に提供されること。

9.設備要件

9.1. 設置条件

ア　機器の導入にあたり、各機器の搬入、設置、設定作業は原則としてすべて受託事業者が行うこと。

イ　導入する機器等は、ラックマウント型であること。

ウ　機器は津 DC または伊勢 DC 内の県が別途契約するラック（以下、「指定ラック」という。）に搭載すること。ハウジングラック場所については、本県と協議の上で決定すること。

エ　県が契約するラックについては、1 ラックを想定しており、利用するラックスペースは、25U 以下とすること。また、ラックへの機器マウントについて、必要となるスペースや設置計画を行うこと。なお、ラックの規格は H2,000mm×W700mm×D1,000mm(42U)である。

オ　本業務の契約期間中、指定ラック以上に追加ラックが必要な場合、そのハウジング契約は受託事業者が行うこと。

カ　指定ラックまでのラック間の配線は別途データセンター受託事業者が有償で

行うが、受託事業者はその費用を負担すること。なお、ラック間の配線は、申請から実施まで 2 週間程度を要するため、余裕をもって設置計画を立てること。

キ　サーバのディスプレイ、キーボード、マウスに関しては KVM スイッチを用意し複数サーバ間で共用する等の省スペースに配慮した構成とすること。

ク　指定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。

ケ　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。

コ　機器・電源ケーブル・通信ケーブルにラベル表記すること。

サ　通信ケーブルに負荷のかからないケーブリングを施すこと。

シ　設置場所への納入及び設置作業、配線作業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及び関係者と調整すること。また、搬入時は本県が別途指示する搬入口及びエレベータを使用し、設備、器物破損を防止するための処置を講じること。

ス　機器の納入を円滑に進めるため、本県に事前に説明し、協議の上本県の指示に従い実施すること。

9.2. 電源条件

ア　本システムで導入する機器類は､入力電圧として AC100V に対応していること。

イ　ラックの電源は、2 系統、45A までとする。なお、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。

ウ　データセンターにおいては、停電対策がとられており UPS 等による個別の停電対策は不要である。

10. ハードウェア要件

10.1. ハードウェア要求事項

各機能を実現するサーバについて、機能及び保守運用面等を検討の上で最適なものを提案すること。できる限り仮想化ソリューション等を用いてサーバ台数を削減すること。

また、複数の機能をひとつのサーバ（ソフトウェア）で実現できる場合（例えば、ウイルスチェック機能と添付ファイル分離機能をひとつのサーバで実現する場合など）は個々のサーバを用意しなくてもよい。

ア　機器は全て津 DC もしくは伊勢 DC に設置することを前提とする。そのため、

原則 19 インチラックに搭載可能である機器を選定すること。

イ　必要となる機器のユニット数、重量、電源容量を提示すること。

ウ　アプライアンス製品以外の汎用性をもった機器については、メモリやディスクに 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。

エ　障害等に備えて、適宜機器もしくは部品の多重化を行うこと。また、アプライアンス製品以外の汎用性をもった機器でハードディスクを内蔵しているものについては、RAID 化等により１つのハードディスク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。複数の物理サーバをまとめて一つの仮想ディスクを構成する場合においても、ハードディスク障害に対応する構成とすること。

オ　納入物件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。

カ　納入物件は原則「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。適合外の機器を納入する場合は、事前に本県の承認を得たうえで納入すること。

10.1.1. 内部メールサーバ

「6.1.2.内部メールサーバ機能」の要求仕様を満たす内部メールサーバ機器を選定し、指定ラックに設置すること。

10.1.2. 認証サーバ

認証用として個別にサーバを使用する場合は、必要な要件を満たす認証サーバ機器を選定し、指定ラックに設置すること。

10.1.3. 内部ロードバランサ

「6.1.2(2)ウ」のとおり、構成上必要ならば、必要な要件を満たす内部ロードバランサを選定し、指定ラックに設置すること。

なお、認証サーバでもロードバランサを使用する場合には、必要なプロトコルに対応したものを選定すること。

10.1.4. ウイルスチェックサーバ

「6.1.3.ウイルスチェック機能」の要求仕様を満たすウイルスチェックサーバ機器を選定し、指定ラックに設置すること。

10.1.5. 外部ロードバランサ

「6.1.3(2)エ」のとおり、以下の機器仕様を満たす外部ロードバランサを選定し、指定ラックに設置すること。

外部ロードバランサに求める基本的な仕様ならびに要求事項は以下のとおりとするが、現行のロードバランサは別途構築している誤送信対策システム及びキャッシュサーバと共用しているため、既存システムの動作に影響がないものを選定すること。

表 10-1 外部ロードバランサ機器

No	項目	機能
1	台数	2 台以上
2	筐体形状・サイズ	ラックマウント型 2U 以内
3	メモリ	4GB 以上
4	スループット	1.0Gbps 以上
5	セッション管理方式	Cookie、送信元 IP アドレス、SSL セッション ID
6	対応プロトコル	HTTP、HTTPS、SMTP、SMTPS、POP、POPS、IMAP、IMAPS
7	負荷分散方式	ラウンドロビン、最少接続数
8	LAN I/F	10/100/1000BASE-T × 4 以上

10.1.6. 添付ファイル分離サーバ

「6.1.4.添付ファイルの分離機能」の要求仕様を満たす添付ファイル分離サーバを選定し、指定ラックに設置すること。

ウイルスチェックサーバもしくは原本保管サーバでこの機能を兼ねてもよい。

10.1.7. 原本保管サーバ

「6.1.5.添付ファイルの原本保管機能」の要求仕様を満たす原本保管サーバを選定し、指定ラックに設置すること。

10.1.8. メールクライアントアップデート用サーバ

「6.1.6.メールクライアントのアップデート機能」の要求仕様を満たすサーバを選定し、指定ラックに設置すること。

10.1.9. 共有ディスク

「6.1.2(2)」のとおり、構成上必要ならば、必要な仕様を満たす共有ディスク装置を選定し、三重県内の指定 iDC に設置すること。

10.1.10.その他付帯設備装置

その他、内部メールサーバ機能、ウイルスチェック機能、バックアップ、ログ管理等で必要となる付帯設備機器については、最適な機器を選定の上で納入すること。

11.ソフトウェア要件

ア　納入したソフトウェアは契約期間後も本県にて利用できるものとすること。

イ　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。

ウ　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等の適用を行った上で納入すること。

11.1.　ライセンス

ア　本県では利用者分として、Windows Server 2012 及び Windows Server 2016 のクライアントライセンス（CAL）及び RDS CAL を保有しており、本業務においても利用可能である。ただし、上記以外のライセンスが必要となる場合は、本業務にて準備すること。

イ　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の価格レベル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
サーバ製品群	地域 Select Plus for Government Partners
アプリケーション製品群	地域 Select Plus for Government Partners

ウ　サーバ等に常駐させるウイルス対策ソフトは、本県が保有する以下のライセンスが利用可能である。

OS	ウイルス対策ソフト名
Windows 系	Trend Micro ウイルスバスターコーポレートエディション
Linux 系	Trend Micro Server Protect for Linux

エ　新規で導入するライセンス数については、利用者数 6,600 人、メールアカウント数 7,000 アカウント、接続機器数 8,000 台分の数量を提供すること。

12. 機器の撤去・廃棄の要件

ア　運用期間終了時の本システム用機器の撤去については、本業務の範囲とする。
イ　機器撤去については、平成 36 年 2 月～3 月ごろを予定しており、撤去作業にあたっ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。

13. プロジェクト管理にかかる要件

13.1. プロジェクトの体制

本業務のプロジェクト体制に関する要件は以下のとおり。

ア　受託事業者は、本業務の遂行を確実とする履行体制（支援体制を含む）を確保していること。
イ　作業について十分な知識を有する者が責任ある立場でプロジェクトにあたること。
ウ　本業務に従事する者は、本県職員ならびに関係者と十分な協力が図れる体制とすること。

13.2. プロジェクト管理等

本業務のプロジェクト管理に関する要件は以下のとおり。

ア　受託事業者は、作業前に業務計画書を本県に提示し、承認を得てから作業を行うこと。
イ　原則として、本県と合意した業務計画書に従って作業を実施すること。
ウ　プロジェクトの遂行にあたり、業務計画書の内容に変更が必要となる場合、本県と協議し、承認を得ること。
エ　必要に応じて適宜ミーティング等を実施し、本県に対し報告及び作業内容の説明・協議を行うこと。
オ　全ての作業において、本県が提供した、個人情報を含む業務上の情報は細心の注意をもって管理し、第三者に開示または漏洩しないこと。また、そのために必要な処置を講ずること。

以上