

松阪市
インターネット分離システム
構築仕様書

平成 28 年度

松 阪 市

1. 目次

1.	目次.....	1
1.1.	件名	3
1.2.	作業の目的と概要	3
1.3.	業務委託期間	3
1.4.	支払条件.....	3
1.5.	技術仕様等に関する注意事項.....	4
1.6.	その他注意事項.....	4
2.	各仕様.....	5
2.1.	基本要件.....	5
2.2.	ネットワーク分離要件.....	5
2.3.	アプリケーション仮想化 Web 閲覧要件	6
2.4.	アプリケーション仮想化メール要件.....	7
2.5.	Active Directory.....	10
2.6.	WSUS.....	10
2.7.	シマンテックウイルス対策ソフト管理サーバ	10
2.8.	設計構築機器	11
2.9.	ハウジング環境の利用.....	12
2.9.1.	ハウジング環境調達範囲	12
2.9.2.	ハウジング環境施設要件	13
2.9.3.	接続回線要件	13
2.10.	クラウドサーバの利用.....	14
2.11.	業務内容.....	14
2.12.	業務範囲.....	14
2.13.	ネットワーク・サーバ設計仕様	15
2.14.	構築仕様.....	18
3.	評価試験	20
3.1.	事前検証.....	20
3.2.	現地導入試験	20
4.	職員への教育	21
5.	成果物および納期.....	21
5.1.	納入成果物	21
5.2.	納期	22
6.	検収及び瑕疵担保責任	22
6.1.	検収	22
6.2.	疑義.....	22
6.3.	瑕疵担保責任	22
7.	業務実施体制	23

7.1.	要員の配置	23
7.2.	作業方法	23
8.	特記事項	24
8.1.	基本事項	24
8.2.	機密保持	25
8.3.	遵守事項	25

全体概要

1. 1. 件名

インターネット分離システム構築及び賃貸借保守

1. 2. 作業の目的と概要

社会保障・税番号制度の開始に伴い自治体内で特定個人情報を取り扱うようになり、自治体情報セキュリティの抜本的な対策が求められている。松阪市（以下「本市」という。）では従来インターネット利用を業務用端末から行っていたが、総務省から示されている自治体情報システム強靱性向上モデルに基づき、新たにインターネット利用専用のネットワークを構築し、既存庁内ネットワークからインターネット利用を原則として禁止する計画である。

本業務は既存庁内ネットワーク内の端末および庁内のシステムが直接インターネットと通信しないために、新たにアプリケーション仮想化技術を用いたインターネット利用専用のアプリケーションサーバおよびインターネット接続用の各種サーバを構築するものであり、直接業務で扱っている端末やシステムが直接インターネットと通信できなくなることによる情報セキュリティの向上に加え、将来にわたり安定稼働するネットワーク環境を構築することを目的とする。

1. 3. 業務委託期間

本調達機器の委託期間は下記通りとする。

- (1) 設計・構築業務：契約締結日から平成 29 年 3 月 31 日まで
- (2) 機器賃貸借：平成 29 年 4 月 1 日から平成 34 年 3 月 31 日まで（60 ヶ月）
- (3) 維持運用管理及び保守業務：平成 29 年 4 月 1 日から平成 34 年 3 月 31 日まで（60 ヶ月）

※ システム構築完了日は、平成 29 年 3 月 1 日とする。

※ システム構築完了日から平成 29 年 3 月 17 日までは、システム稼働検証及び職員への研修期間とする。

※ システム切替日は、平成 29 年 3 月 18 日から 20 日までとし、その後平成 29 年 3 月 31 日までは本番環境、動作確認期間とする。なおこれらの日程は、本市と協議を行い調整すること。

1. 4. 支払条件

本業務にかかる費用の支払条件は以下のとおりである。

- (1) インターネット分離システム構築業務委託に要する費用
本市が検収を行った後、契約金額を支払うものとする。（平成 28 年度支払い）
- (2) インターネット分離システム機器賃貸借及び保守料に要する費用
本市が検収を行った後、平成 29 年 4 月 1 日から平成 34 年 3 月 31 日（60 ヶ月）までの間、契約金額（1 円未満の端数は切り捨てた額）を 60 で除した金額を毎翌月に支払う。ただし、計算途中で生じた 1 円未満の端数は切り捨てるものとし、これらの端数は契約開始月分に合算し支払うも

のとする。

1.5. 技術仕様等に関する注意事項

稼働実績のある機器、またソフトウェアでの安定稼働を考慮し、導入機器またはソフトウェアは、原則として入札時点で製品化されていること。

1.6. その他注意事項

- (1) 機器の導入構築、搬入、据付け、配線、電源工事、調整及び現行ネットワーク並びに現行システムとの接続など、本仕様書に記載の要件をすべて満たす積算を行い、入札価格とすること。また、本調達内容を実現するために発生する追加費用は一切認めない。
- (2) 既存ネットワークベンダーとの調整及び設定依頼にかかる費用については、入札金額に含めること。
- (3) 別紙記載の機器以外の製品を使用する場合は、指定日までに事前承諾願書と共に、同等以上の性能を有することを示した機能証明書（カタログ等）と機器選択理由を明記し（任意様式）、本市へ提出し承認を得ること。また、その場合、仮想化システム等については必要に応じて既存システムとの互換性の調査を行い、本稼働後インターネット分離システムの相性等が原因で正常に利用ができないことまたは、異常な遅延等が発生したときは機器の交換または、機器数量の増量などの措置を行い問題の解決をさせること。なお、これらに係る費用は、入札価格に含めること。
- (4) 本構築を実施するに当たり、仕様内容が現行環境と合致しない事項が発生した場合、本市と協議のうえ変更等を行うものとする。
- (5) 設計により機器設置数量が減少する場合は、本市と協議のうえ契約変更または覚書の作成等を行うものとする。
- (6) 本市のセキュリティポリシーを遵守すること。
- (7) 本業務終了時には、本業務にかかる情報資産を一定期間保存後廃棄すること。
- (8) リモート接続による保守を可能とすること。

2. 各仕様

2.1. 基本要件

インターネットセグメント分離を実現する為に、既存庁内ネットワークに接続されている機器について可能な限り設定変更を伴わないように、アプリケーション仮想化技術を実現するための管理サーバ、アプリケーションサーバ、ロードバランサ、ファイル授受器、サーバ収容スイッチ、管理スイッチ、メールサーバ、ファイル無害化システム等の機器の設計構築及び機器導入作業を行う。また、アプリケーション仮想化技術でインターネット上の業務サービスを利用できない場合は、別途本市が用意する物理端末を利用して実現を行う。

構築の際は各システム・庁内ネットワーク停止等の業務への影響を最小限に留めるように作業を行うこと。なお、作業期間については、本市担当者と調整を行うこと。

2.2. ネットワーク分離要件

インターネット分離を実現する為に、情報系からインターネット接続部を分割し、アプリケーション仮想化技術を用いて情報系からインターネットを閲覧する環境（以後、インターネット接続系）を構築する。

また、インターネット分離に伴い、インターネットから送受信されるファイルの授受が継続して実施できることを前提とする。その為、別途インターネット接続中継環境系を構築する。（図 2-1 参照）

インターネット接続中継環境系にはインターネット接続中継環境セグメントを構成すること。ここではファイル無害化を実施するシステムとファイル授受を司る機器を配置し、情報系とインターネット接続系間のデータをセキュアに中継できるネットワークを整備すること。

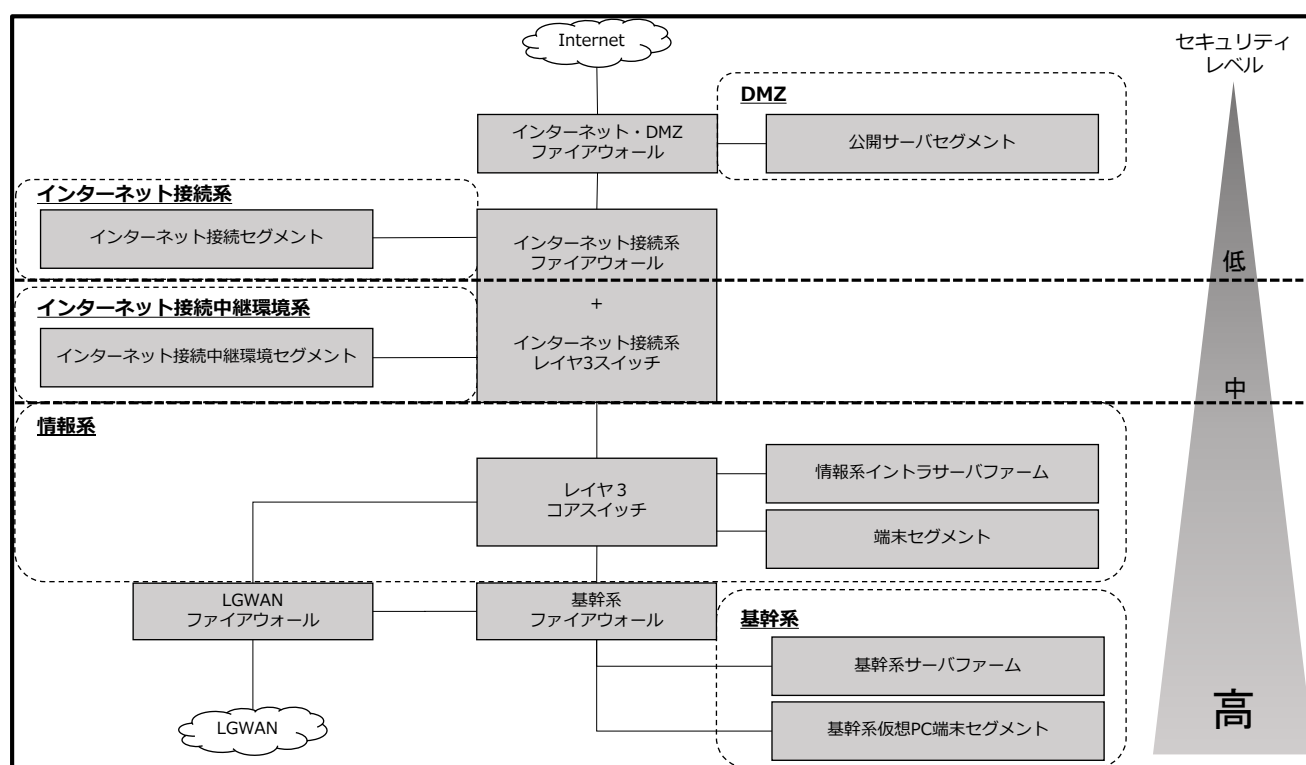


図 2-1 ネットワークセキュリティ概要図

2.3. アプリケーション仮想化 Web 閲覧要件

アプリケーション仮想化技術を用いて情報系の職員端末がインターネットを閲覧するためには、職員端末に配信された Web ブラウザの仮想アプリケーションを実行する。(図 2-2 参照)

この仮想アプリケーションはインターネット接続セグメント上に配置されたアプリケーションサーバ上で稼働するものであり、職員端末にはWebブラウザの画面のみが転送される仕組みである。

その為、Web ブラウザ上でデータファイルのダウンロード等を実施しても職員端末上にデータファイルはダウンロードされず、アプリケーションサーバ上のユーザ個別の領域に一時保存されるものとする。

ダウンロードされたデータは必要に応じ、ユーザがインターネット接続系に配置されたファイルサーバにデータを移動させる。そのファイルは自動的にファイル無害化システムによりファイル無害化処理が実施され、庁内ネットワークのファイルサーバへ移動するものとする。ファイル無害化処理が実施できないファイルに関してはインターネット接続中継環境セグメントに配置されたファイル授受機器を用いて情報系の職員端末にデータファイルを送受信できるようにする。その際、ネットワーク間を跨ぐデータファイルとなるためにウイルスチェックと承認者によってファイルデータの移動確認ができるよう承認フローを実施させることとする。

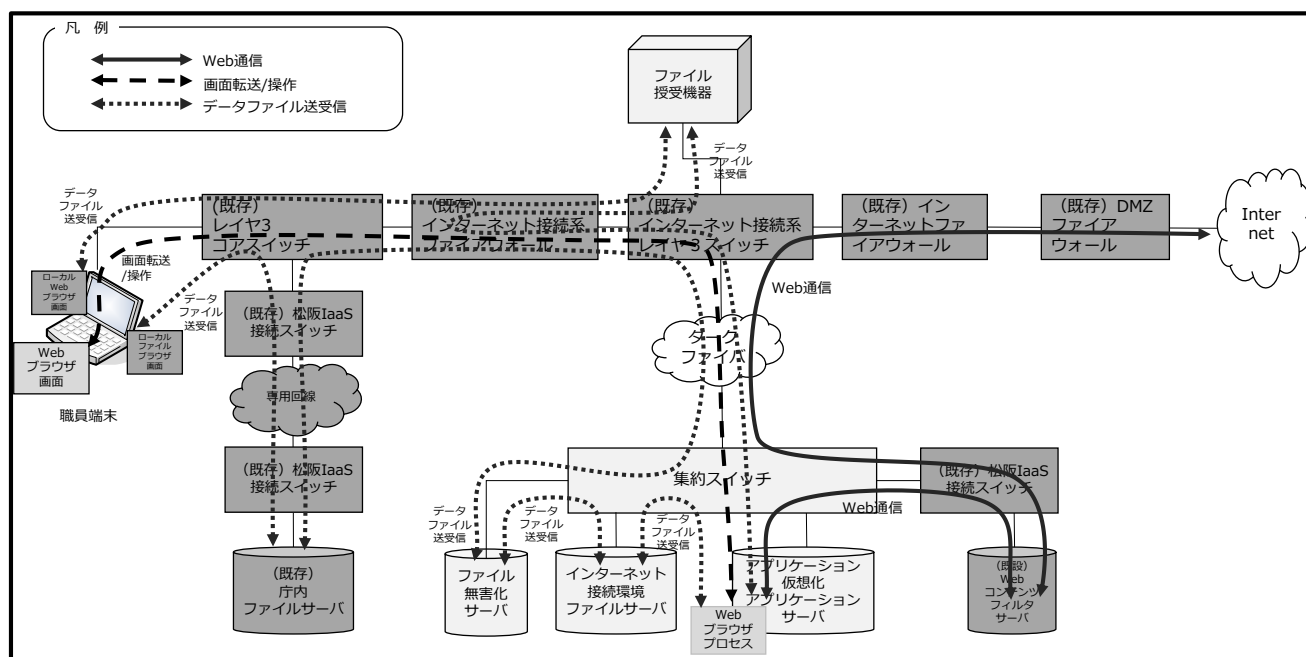


図 2-2 アプリケーション仮想化インターネット通信概要図

利用する Web ブラウザは以下の指定 2 つが利用できること。

- (1) Microsoft Internet Explorer 11
- (2) Google Chrome (最新版)

アプリケーション仮想化技術は外部のデータセンタのハウジング環境に設置すること。

また、本市からハウジング環境までの専用回線について、冗長回線を用意し、サーバ仮想化技術を用いて構築すること。

アプリケーション仮想化技術を利用するユーザは 1550 人を想定し、同時接続 500 人とする。アプリケーション仮想化技術を提供する仮想サーバ 1 台当たり、32 ユーザの利用とする。仮想サーバ 1 台当たり vCPU8 コア以上、vMEM 32GB 以上で構築すること。物理サーバ 1 台当たり 6 仮想サーバ以上搭載すること。

アプリケーション仮想化技術では下記の機能を実装すること。

- (1) アプリケーション仮想化にて表示された Web ブラウザから物理端末の相互間にコピー及び貼り付けを実施する際はテキストデータのみ実行でき、ファイルや画像等は実行できないようにすること。
- (2) 職員からの問い合わせに対応する為にアプリケーション仮想化にて表示された Web ブラウザを管理者からリモートで参照及び操作が実施できる機能を有すること。
- (3) 職員端末からアプリケーション仮想化にて提供される Web ブラウザを利用する際、情報系に配置されている既存の Active Directory と連携し、シングルサインオンを目指すこと。但し、設計上で困難な場合は本市と協議を実施し、方針を決定すること。
- (4) 情報系に配置されている既存プリンターでアプリケーション仮想化にて提供される Web ブラウザから印刷ができること。
- (5) アプリケーション仮想化を提供するアプリケーションサーバはセキュリティの観点より一日単位でリフレッシュさせる機能を有すること。

2.4. アプリケーション仮想化メール要件

現在の構成として、インターネット側でやり取りされるメールと庁内でやり取りされるメール、また LGWAN とやり取りされるメールが同一のメールシステムで構成されている。

インターネット分離を実現する為に、インターネット側でやり取りされるメールと庁内及び LGWAN でやり取りされるメールを分離する。但し、庁内メールと LGWAN メールは同等の取り扱いとする。

各メールの詳細な通信可否を下記の表に示す。

表 2-1 メール送受信可否

宛先 送信元	本市以外の インターネット メールアドレス	本市の インターネット側 市メールアドレス	本市以外の LGWAN メールアドレス	本市の LGWAN/庁内 市メールアドレス
本市以外の インターネット メールアドレス		○		△ ※無害化されたメール転送 のみ可
本市のインターネット側 市メールアドレス (city.matsusaka.mie.jp)	○	○	×	×

本市以外の LGWAN メールアドレス		○		○
本市の LGWAN/庁内 市メールアドレス (city.matsusaka.lg.jp)	×	×	○	○

アプリケーション仮想化技術を用いて情報系の職員端末がインターネット側とやり取りされるメールを送受信する為に、職員端末上に配置された Web ブラウザの仮想アプリケーションを実行し、インターネット接続系に配置する Web メールサーバの Web GUI を利用して実行する。

但し、インターネット側から送られてくるメールはメール無害化サーバにて添付ファイルの削除及びメール本文中のテキストメール化等を実施した上で庁内メールサーバに転送し、情報系既存グループウェアにてメールの閲覧のみ実施できること。情報系既存グループウェアにてインターネット側から無害化されたメールを受信する為に必要な既存庁内側メールサーバー設定及び既存グループウェアシステムのカスタマイズ作業は本市が行う為、詳細は本市と協議を行うこと。

また、インターネット分離側のメールシステムは、個人のメールアドレス及び所属課のメールアドレスの二つのメールアドレスを同じ画面で切替等を行い使用することができ、さらに Active Directory と連携ができる機能を有すること。

Web ブラウザ上から取得したデータファイル(メールに添付されたファイルを含む)次のものを想定し、アプリケーション仮想化技術を用いて情報系の職員端末で確認ができるようにすること。

- (1) PDF ファイル
- (2) 圧縮データファイル(ZIP/LZH/RAR)の解凍と展開
- (3) テキストデータファイル
- (4) JPEG/GIF/ビットマップなどの画像ファイル
- (5) Microsoft Office viewer (Word/Excel/PowerPoint)
- (6) ジャストシステム 一太郎 Viewer

また、これらのデータファイルはファイル無害化システムにて情報系の端末に移動できるようにすること。例外として、ファイル無害化システム非対応のファイルはデータファイル授受機器にて移動できるようにすること。

Web メールサーバのメールボックスの容量は1ユーザあたり100MB以上とし、使用ユーザは2,400人とする。また、所属課用メールボックスの個別容量は300MB以上とし、所属課数は100課とする。

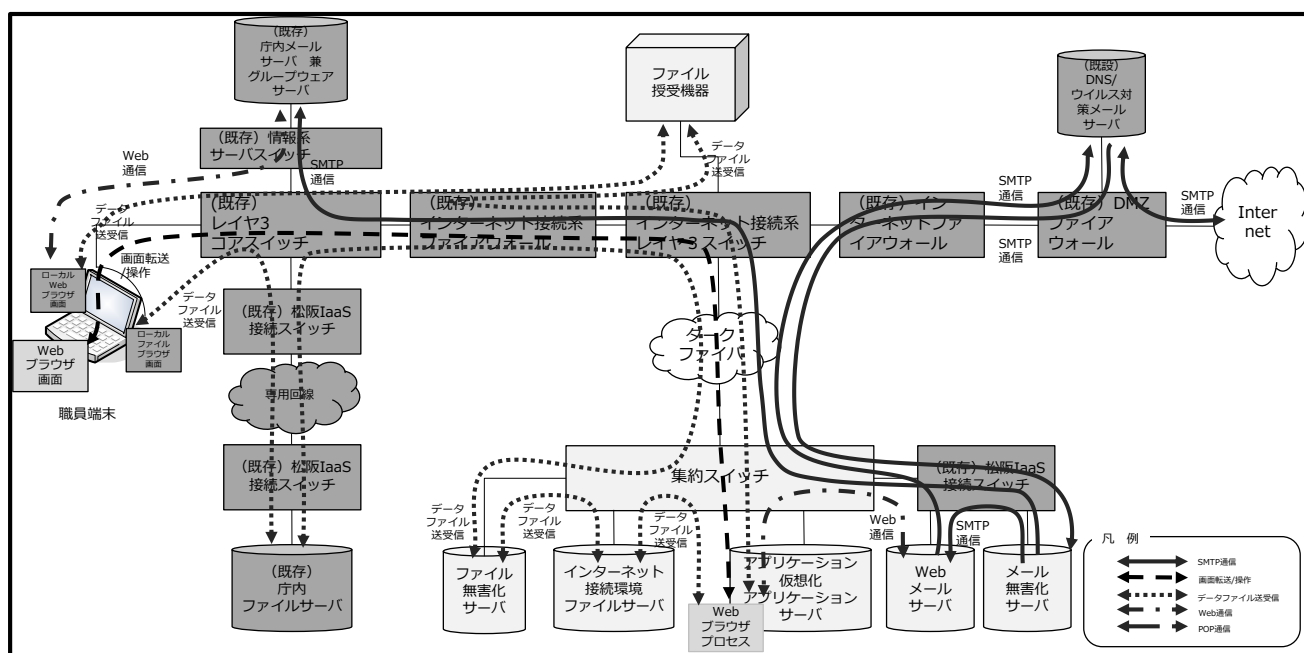


図 2-3 アプリケーション仮想化メール通信概要図

以上の要件を満たすために、インターネット接続系に新たに Web メールサーバを構築すること。

また、メールの無害化（添付ファイルの削除・メールテキスト化等）を実現し、インターネット環境、情報系の両系でメールが閲覧できるようにメール無害化サーバを構築すること。メール無害化サーバはメール転送機能（MTA 機能）にて、庁内メールサーバに無害化されたメールを転送すること。なお、Web メールサーバとメール無害化サーバは原則として本市が別に準備するクラウドサーバ（以下、「松阪市 IaaS」という。）へサーバ仮想化技術を用いて構築すること。またアプリケーション仮想化技術を提供する為に外部データセンタのハウジング環境と松阪市 IaaS サービスは本市マシン室を介さずに直接接続し、ネットワークトラフィックが本市マシン室内を往復することのないように設計構築すること。

各環境で職員が取り扱えるメールの種類について可否を下記の表に示す。

表 2-2 インターネットメール環境別メール可否

メール種別 \ 環境	インターネット接続系	LGWAN 系
メール本文	○	×
無害化処理後 メール本文	○	○
メール添付ファイル	○	×

2.5. Active Directory

新たにインターネット接続系にドメインコントローラーサーバ（Active Directory）を 2 台構築する。このドメインコントローラは情報系セグメントに構築済みのドメインコントローラのデータ利用し、インターネット接続セグメントでも既存と同様相当の認証やセキュリティグループを利用できるよう目指すこと。構築に際して既存ドメインコントローラとの連携が困難な場合は本市と協議し方針を決定すること。

- ・ インターネット接続セグメントにドメインコントローラーサーバ（Active Directory）を 2 台構築すること。
- ・ 情報系セグメントに構築済みのドメインコントローラのデータを利用すること。インターネット接続セグメントにおいて既存と同様相当の認証やセキュリティグループを利用しているよう目指すこと。
- ・ 既存の DC のデータ等の連携のための設定等は既存 DC の運用支援業務の観点から落札業者が既存業者に作業を委託し実施すること。その委託費用は本入札価格に含めること。

2.6. WSUS

情報系及びインターネット接続系に WSUS を構築する。この WSUS サーバは情報系セグメントよりインターネットへ接続ができなくなるため、インターネット接続に整備する WSUS と連携して情報の更新を実施すること。

なお、情報系及びインターネット接続系の WSUS は原則として松阪市 IaaS へサーバ仮想化技術を用いて構築すること。

- ・ インターネット接続セグメントに WSUS サーバを構築すること。
- ・ 情報系セグメントに WSUS を構築すること。
- ・ 情報系セグメントの WSUS とインターネット接続セグメントの WSUS は連携をすること。
- ・ それぞれの WSUS は多様な OS とアプリケーションに対しサービスを提供することが将来にわたり想定されるため、CPU 4 コア以上、メモリ 8GB 以上、DISK 容量 800GB 以上とすること。

2.7. シマンテックウイルス対策ソフト管理サーバ

新たにインターネット接続系にウイルス対策ソフト管理サーバを 1 台構築すること。このウイルス対策ソフト管理サーバは情報系セグメントに構築済みのウイルス対策ソフト管理サーバと連携し、インターネットより最新パッチを取得提供する役割が担えること。

なお、ウイルス対策ソフト管理サーバ原則として松阪市 IaaS へサーバ仮想化技術を用いて構築すること。

- ・ インターネット接続セグメントにウイルス対策ソフト管理サーバを構築すること。
- ・ 情報系セグメントのウイルス対策ソフト管理サーバと連携させ、新たに設置したサーバがインターネットより最新の定義ファイルをダウンロードし、既存のサーバにて最新の定義ファイルを利用可能にすること。
- ・ ウイルス対策ソフト管理サーバは 1 台の構築が必要で、ウイルス対策ソフト（管理ソフトウェア

ア) は以下の通りとする。

- ・ Symantec Endpoint Protection Manager または Symantec LiveUpdate Administrator
- ・ 既存サーバとの連携のための設定等は運用支援業務の観点から落札業者が既存業者に作業を委託し実施すること。その委託費用は本入札価格に含めること。
- ・ 既存のウイルス対策ソフトに関しては本市にて既にライセンスを取得済みのため、今回の調達でライセンスの取得は不要である。

2.8. 設計構築機器

本調達にて設計および構築を行う機器は以下の通りとする。なお、対象機器の詳細仕様については別紙「機器仕様書」を参照し、本書仕様を満たすように設計及び構築を行うこと。

表 2-3 構築機器一覧

項番	名称	状態	数量
①	ブレードサーバ	物理	6 基
②	ブレードシャーシ	物理	1 基
③	共有ストレージ	物理	1 基
④	ファイバチャネルスイッチ（不要な場合は除く）	物理	2 基
⑤	バックアップサーバ	物理	1 基
⑥	集約スイッチ	物理	2 基
⑦	管理スイッチ	物理	2 基
⑧	ロードバランサ	物理	2 基
⑨	ファイル授受機器	物理	1 基
⑩	アプリケーション仮想化管理サーバ※1	仮想	1 式
⑪	アプリケーションサーバ※2	仮想	1 式
⑫	ファイルサーバ	仮想	2 基
⑬	Active Directory サーバ	仮想	2 基
⑭	WSUS (Windows Server Update Services) サーバ	仮想	2 基
⑮	シマンテック ウイルス対策ソフト管理サーバ	仮想	1 基
⑯	Web メールサーバ	仮想	1 基
⑰	メール無害化サーバ	仮想	1 基
⑱	ファイル無害化サーバ	仮想	1 基
⑲	ファイル無害化用アーカイブサーバ	仮想	1 基
⑳	仮想基盤ウイルス対策システム※3	仮想	1 式

※1 アプリケーション仮想化技術に必要な管理系サーバすべてを含む。

※2 アプリケーション仮想化技術をユーザに提供するのに必要なアプリケーションサーバリソース全てを含む。

※3 仮想基盤上で動作するウイルス対策システムであり、このシステムの稼働に必要となるコンポートネットの全てを含む。

2.9. ハウジング環境の利用

各システムの稼働に必要となるサーバ仮想マシンを稼働させるための機器は、外部データセンタのハウジング環境に設置をすること。契約期間中に必要なハウジング費用は入札価格に含むこと。（ネットワーク障害対応を考慮し、松阪市 IaaS 施設へのハウジングを推奨とする。）

また、ハウジング環境及び回線は設計・構築業務にかかる期間において、構築業務や稼働確認及び各種テスト、職員への研修期間やその後の動作確認期間の利用で必要となる初期費用及び利用料についても構築業務の範囲内とし、受注者が支払うものとするため、入札価格に含めること。

2.9.1. ハウジング環境調達範囲

ハウジング環境調達範囲は以下とする。

- (1) ハウジング先ラック及び設置作業、必要な電源、各種配線ならびにネットワークへの接続
- (2) 本市からハウジング環境までの接続回線と回線使用料

2.9.2. ハウジング環境施設要件

ハウジング環境は JDCC（日本データセンター協会）が認定するデータセンターファシリティスタンダードのティア3以上の要件を満たしており、かつ、以下の要件を満たすこと。

- (1) ハウジング施設は日本国内に存在し、国内法を適用とする。また、本市にて緊急対応や技術支援が必要な際に、保守要員及び本市職員が1時間以内に到着可能なこと。
- (2) 海岸より10km以上離れており、標高30m以上の場所であること。
- (3) ISMS 認証取得のサービス提供施設であること。
- (4) LGWAN-ASP ファシリティ登録施設であること。
- (5) サービス提供者はプライバシーマークを取得していること。
- (6) ハウジング環境と松阪市 IaaS サービスが専用回線で接続できること。
- (7) 耐震性に優れた施設及び設備であること。また、建築基準法に基づいた免震・耐震等の安全性を考慮した設計・施工が行われていること。
- (8) マシン室には、外部からの水の浸入を防止する対策がとられている、若しくは浸水の可能性が低い構造であること。
- (9) 自動火災報知設備、消火設備（サーバ室にあってはガス系消火設備）が設置されていること。
- (10) 避雷器等の雷サージ対策、及び、フリーアクセス床への静電気対策塗料の加工等の静電気対策が施されていること。
- (11) 生体認証による個人認証装置又は入退館管理が24時間365日行われること。また、入退館の記録が一定期間保管されていること。
- (12) サーバ室の入室管理は生体認証とICカードによる2要素認証による個人認証を実施していること。
- (13) 無停電電源装置及び非常用自家発電装置を備え、商用停電や電気設備の障害等が発生した場合でも、サービスの提供が継続できること。
- (14) 無停電電源装置はN+1構成となっていること。
- (15) 受電設備は完全二重化されており、それぞれ異なる変電所より受電されていること。
- (16) サーバ室の温度は20℃から26℃前後、湿度は35%から65%前後に適切に保たれていること。
- (17) 重要なセキュリティ境界に監視カメラを設置し、24時間の監視と録画を行うこと。
- (18) ハウジング環境が設置される室内の設置スペースはケージ又はラックごとに施錠管理され、他者がアクセスできない構造であること。

2.9.3. 接続回線要件

- (1) 本市マシン室とハウジング環境を OSI 参照モデルの L1 レイヤで接続すること。また、回線は1Gbps以上の帯域保証型の専用回線で接続すること。回線は他のユーザと共同利

用は認めない。なお、専用回線は異なる経路の回線で冗長化されていること。

- (2) 専用回線は L1 レイヤで明確に分離されていること。
- (3) 本接続回線の利用料及び、初期導入等に必要な費用は、全て本入札価格に含めること。
- (4) データフローの効率的な経路を確保する為、ハウジング環境と松阪市 IaaS サービス間は本市を経由せず、直接松阪市 IaaS サービスが提供されている事業者と接続すること。
- (5) 冗長化されたそれぞれの回線は、障害等が発生した場合に自動的に切り替わる構成となっており、ループが発生しない構成もしくは仕組みを構築すること。

2. 10. クラウドサーバの利用

Web メールサーバ及びメール無害化のサーバ仮想マシンは、松阪市 IaaS に構築を行うこと。また、構築の際には松阪市 IaaS より CPU、メモリ、ハードディスク等のリソースの払出しを行うため、稼動に必要なリソースを割り出し報告すること。

なお、契約期間中の松阪市 IaaS 利用に関する費用は本市が松阪市 IaaS 委託業者へ支払うこととなるが、必要となる松阪市 IaaS の利用料は別途提示する「松阪市 IaaS 単価表」にて算出し本入札額に含めること。また、設計・構築業務及び検証等にかかる期間において、構築業務や稼働確認及び各種テスト等の利用で必要となる松阪市 IaaS の利用料については本業務の範囲内とし、受注者が松阪市 IaaS 委託業者へ支払うものとする。

構築保守業務については、本市が専用端末を準備するため、これを用いて作業を実施すること。松阪市 IaaS 内における責任範囲は、本業務により構築した OS、ミドルウェア、アプリケーション等の範囲とする。なお、障害時の責任分解点について疑義が生じた場合は、松阪市 IaaS 委託事業者と協議するものとする。

2. 11. 業務内容

本業務の業務内容は、本仕様書・添付資料並びに現場説明事項に基づき、次の各号に掲げるとおりとする。

- (1) 納入機器の運搬及び設置調整、構成設定、据付、単体試験
- (2) (1)に係る収容架等部材据付及び配線
- (3) (1)に係るネットワーク伝送路の事前試験・接続・調整
- (4) (1)に係るネットワーク機器の設定・設定変更・確認
- (5) (1)に係るサーバの設定・設定変更・確認
- (6) システムの総合試験（冗長化構成確認等）
- (7) 業務実施にあたって必要となる打合せ及び書類作成
- (8) 本業務の実施に関係する事業者との打合せ及び書類作成
- (9) 完成図書等の必要書類の作成（データ納品含む）
- (10) 納品機器の運用管理方法及び取扱手法の説明

2. 12. 業務範囲

基本要件に基づき、機器の調達・搬入・調整・個別試験、新規構築に伴うネットワーク設計、サーバ設

計、ネットワーク機器設定、サーバ設定、総合動作試験、既存機器との設定調整、本業務の完了に必要な関係部署への諸手続きなど、本業務の目的を達成するために必要なすべてを業務範囲とする。

また、既存ネットワーク機器及び既存ファイアウォール、既存 AD サーバー等との接続及び設定変更に関して、既存機器ベンダーと調整を実施すること。このことによる費用が発生する場合、その費用を入札価格に含めること。ただし、既存 DMZ（NTT ビル内）に設置されているファイアウォール及びメールウイルス対策サーバの設定変更は本市にて実施する為、設定変更内容を本市と協議し作業を支援すること。

構築時及び構築後の検証等の期間において、既存ネットワークやシステムに不具合等の影響を及ぼした際は、受注者の責任において正常な状態に回復させること。

2.13. ネットワーク・サーバ設計仕様

基本要件に基づき、以下の仕様要綱を満たす基本設計、詳細設計を実施し、ネットワーク構築を行うこと。各設計項目については本市に承認を得ること。

(1) ネットワーク構成設計

新規導入のファイアウォールからインターネット接続セグメントを切り出し、既存コア L3 スイッチの配下に本システムを構築する。VLAN や IP アドレスの採番については本市と協議し、決定すること。

(2) 信頼性の向上

故障などによるシステム影響を軽減するため、ネットワーク接続およびネットワーク機器の 2 系統等の冗長化を実施すること。さらに仮想マシンは松阪市 IaaS サービスで提供される仮想技術によるハイアベイラビリティ（高可用性機能）を用いることによって実現すること。

(3) 運用性の向上

本市職員での運用を将来にわたり検討する為、導入機器の配線の簡素化及び、サーバ機器等の設定のテンプレート化を実施するため、ブレードシャーシ型を採用し運用性の向上を図ること。また、サーバ機器には障害箇所を減らすためにハードディスクの搭載を不要とし、共有ストレージよりハイパーバイザを起動させること。

(4) ファシリティ設計

設置される機器およびケーブル類については、既存設置状況やケーブル敷設状況を十分に調査したうえで、現地調査後、協議の上、施工方法及び設置箇所を決定すること。

(5) 機器命名規則

新規導入機器への命名規則を設計し、本市と協議し、決定すること。

(6) セキュリティ設計

本導入業務では、セキュリティ向上のため情報系からインターネットを論理的に分離することを想定している。

① 新たに情報系とは別に以下の環境を用意する。

- ・ インターネット接続系
- ・ インターネット接続中継環境系

- ② 新たなネットワークセグメントとして以下のセグメントを用意する。(参考：図 2-1 ネットワークセキュリティ概要図)
 - ・ インターネット接続系
 - ・ インターネット接続セグメント
 - ・ インターネット接続中継環境系
 - ・ インターネット接続中継環境セグメント
- ③ 情報系への通信は画面転送及び無害化（ウイルスチェックを含む）されたファイルの通信のみ可能とし、それ以外の通信はインターネット接続系と接続不可能な状態とすること。
- ④ インターネットを利用する際は、情報系の端末からインターネットに接続するのではなく、アプリケーション仮想化技術を用いて、インターネットブラウザを画面転送経由でインターネットにアクセスすること。
- ⑤ 情報系の端末にデータファイルが授受できる環境を構築すること。基本的にはファイル無害化システムを利用し、無害化（サニタイズ）を実施し、ファイルサーバ経由でのファイル授受を原則とする。但し、ファイル無害化システムで対応できないファイルについてのみファイル授受機器を用いてファイルの受け渡しを実施すること。その際、データファイルに対してシグネチャベースでのウイルススキャンの実施が完了され、かつ当事者とは別のユーザがデータファイルの確認を実施し、承認を行った上でデータファイルが送受信できること。
- ⑥ データファイルの授受器において操作日時、操作者、ファイル名の証跡管理を行うこと。
- ⑦ 情報系からインターネット接続系へのアクセス制限について、高いセキュリティが確保できるよう設計を実施し、設計内容について本市の承認を得ること。
- ⑧ 導入する Windows Server OS に対するウイルス対策はサーバホストベースのウイルス対策システムを導入し、Windows Server OS 上でウイルス検索エンジンを導入して対応すること。
- ⑨ メールサーバ構築において、既存庁内メールサーバの動作に不具合が発生しないように設計し、また既存メールデータが消失しないように設計すること。
- ⑩ 新規に構築するメールサーバにおいて、メールの無害化（添付ファイル削除/メールのテキスト化等）並びにテキスト化を実装し、メール本文文頭に添付ファイルを削除した旨とテキスト化した旨を記載して庁内メールサーバに配送できるようにすること。
- ⑪ 新規メールサーバにてウイルスメールを駆除できるようにし、危険なメールを庁内環境に配送しない構成で構築すること。
- ⑫ ブレードシャーシとサーバ収容スイッチ間はスイッチごとに 20Gbps 以上の帯域で接続し、回線冗長と十分な帯域を確保すること。
- ⑬ インターネット接続系に配置される機器は管理スイッチで集約し、既存監視ネットワークへ接続すること。

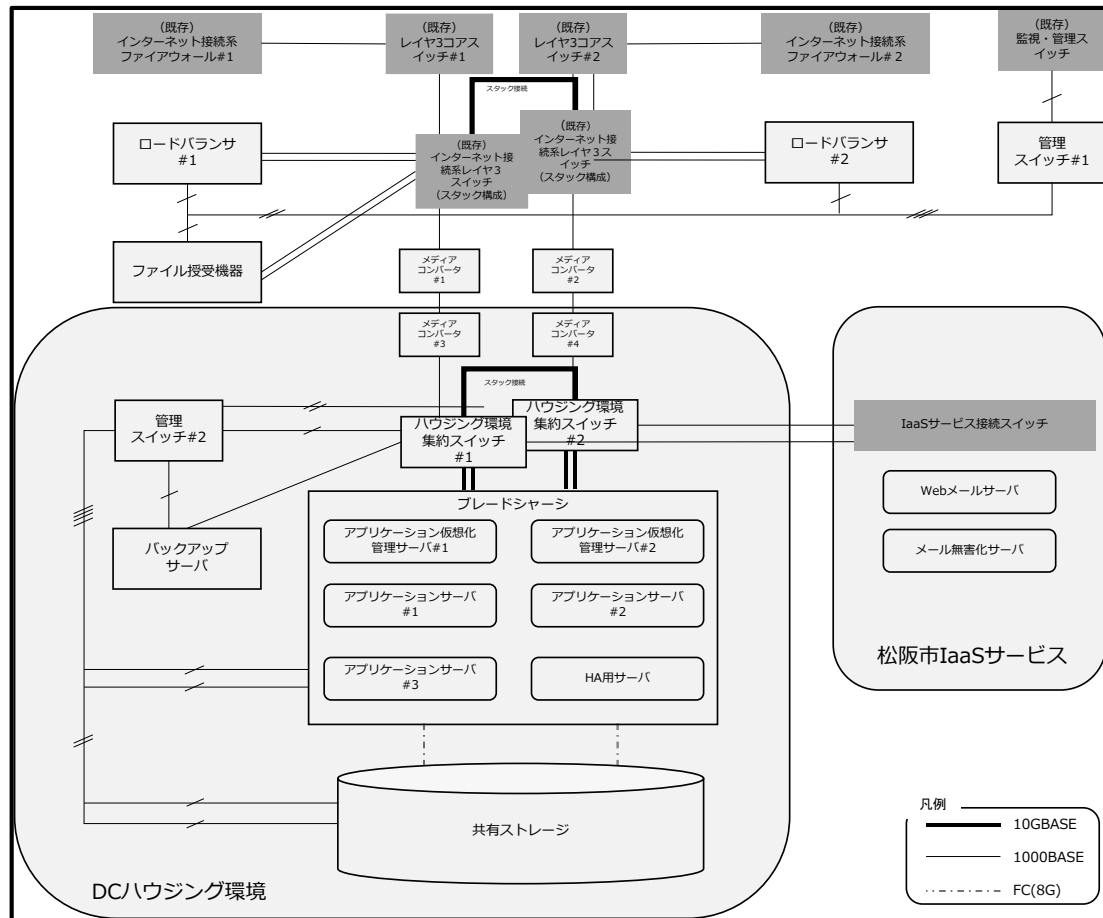


図 2-4 アプリケーション仮想化全体構成概要図

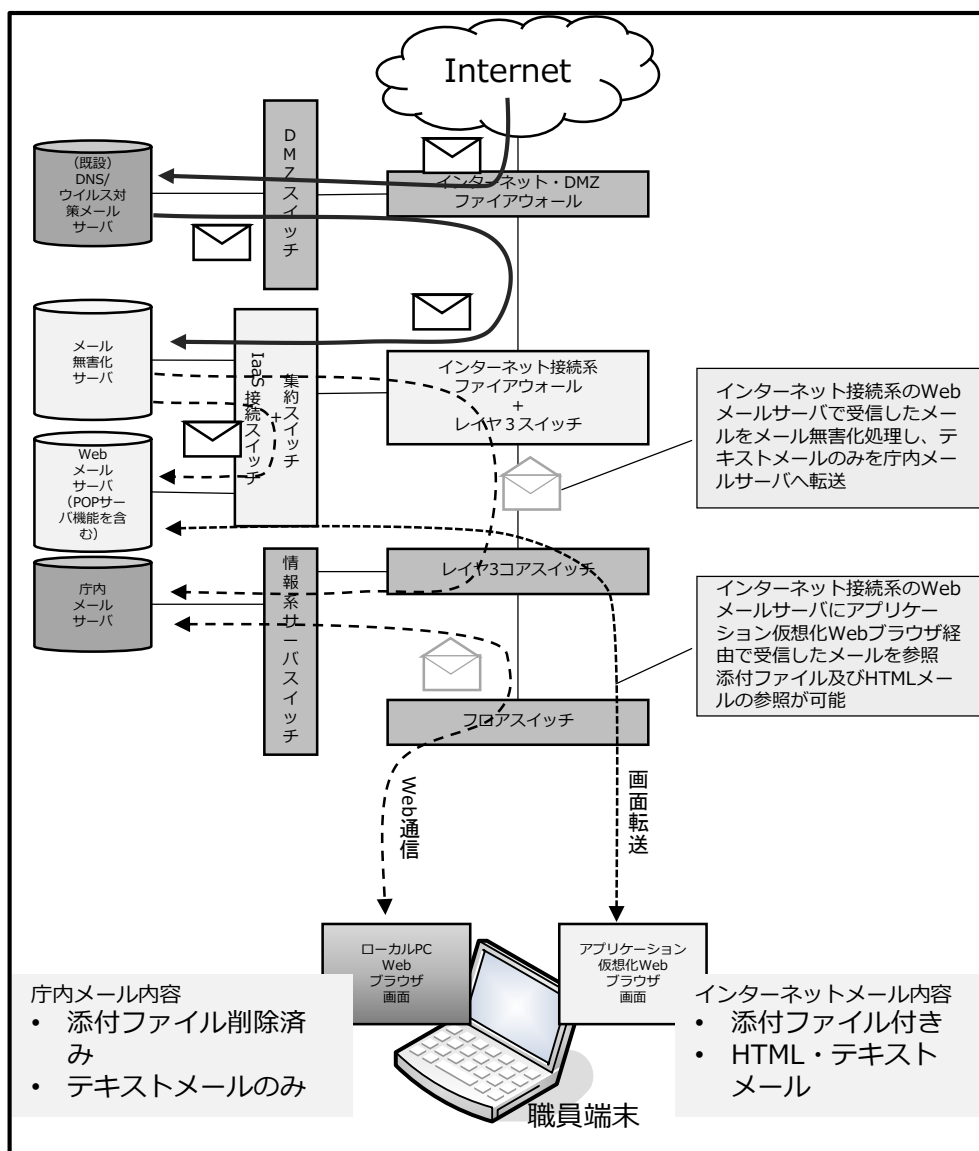


図 2-5 メールフローとメール無害化概要

2. 14. 構築仕様

以下に構築仕様を示す。

実施スケジュールについては、本市の承認を得て決定したスケジュールを遵守すること。

- (1) 本市と機器の設置場所を協議し、導入機器の設置を行うこと。
- (2) 導入機器への接続が必要な場合は新たなケーブルを新設するものとする。機器の導入により光ケーブル等のコネクタ形状が変更になる場合は光パッチケーブル等を変更すること。なお、その費用は本入札価格に含めるものとする。
- (3) ラックに取り付ける際に必要な金具類は本調達に含むものとする。

- (4) 今回の導入機器に接続する全てのケーブルに対し導通試験を実施の上、試験結果を書類にて提出すること。また、導通試験にて通信不良もしくは施行不良が判明した場合、ケーブルの修繕又は再敷設を行うこと。なお、その費用は、本入札価格に含めること。
- (5) 機器動作のため、電源の増設や 200V 電源が必要な場合等は既存環境を調査した上で必要な電源工事を行うこと。
- (6) 使用機材については、あらかじめメーカー名・規格・姿図等を記載した書類を提出すること。
- (7) システム構築にあたっては、必要に応じてバリケード等による安全区画の設定など、十分な安全対策を施し、施工にあたること。また、関係車両の出入りや構築中の騒音等により近隣からの苦情があった場合、誠意をもって対策・対応すること。発生日を含めて、発生から 3 日目以内に苦情内容とその対策を本市へ報告すること。
- (8) 既存システムに付随する形で機器の導入並びにネットワーク環境を構築するため、スケジュールや手順を検討し、システム全体の停止が可能な限り少なくなるよう移行計画を作成すること。
- (9) 業務実施中に、不測の事態が発生した場合は、直ちに業務を中止し、現行の環境に復元させたいうで、早急に本市に報告を行うこと。
- (10) 移行スケジュール（移行準備から正常稼働確認、イベントスケジュール、役割分担、チェックリスト等）、移行時連絡方法、移行検査基準、新システム切替え判定基準、リスク発生時のデッドタイム、本稼働可否の協議及びそのタイミング等、システムを安全かつ円滑に移行するために必要な移行方針を定義した成果物を作成すること。

3. 評価試験

3.1. 事前検証

導入を実施する前に、受託者の用意する本システムで利用する製品と同等環境において、動作確認および導入業務における本システムへの影響確認を実施し、本市の承認を得ること。

調査した結果、使用する機器の変更やソフトウェアの変更が必要な場合は、受託者の責任において再度影響を調査し、本市の承認を得ること。

3.2. 現地導入試験

現在稼働している既存システムに対し、導入時および導入完了後に不具合が発生しないように細心の注意を払って作業すること。また、既存ネットワークや既存システムに不具合等の影響を及ぼした際は、受注者の責任において正常な状態に回復させること。

(1) 検査提出書類

導入業務で行う作業について、機器導入を行う拠点にて動作試験を行い、結果を書類にて提出すること。

(ア) 試験項目一覧表

現場でどのような試験内容を行うのかを一覧表にして提出すること。

(イ) 検査報告書

現場で動作確認を実施後、試験結果（正常動作を確認したもの）を提出すること。

(2) 総合試験

導入したサーバ機器やネットワーク機器については、既存システム等への疎通確認試験を実施すること。

(ア) 導入したサーバ機器・ネットワーク機器より、ネットワーク監視サーバに対して疎通確認を行うこと。

(イ) 既存ネットワーク監視サーバにて導入したネットワーク機器が正常に認識し、障害発生時等にアラーム情報等が送信されることを確認すること。

(3) システム評価試験

サーバ機器・ネットワーク機器を導入した拠点で、各システムの動作確認試験を実施すること。

(ア) 本市と協力しながら、インターネット接続に関連するシステムが正常に動作することを確認すること。

4. 職員への教育

一般利用課職員のシステム利活用や運用管理者のシステム運用を円滑に行うため、以下の研修をそれぞれにおいて実施すること。

(1) 一般利用職員向け研修

本システムの運用に関する一般利用職員向けの研修計画を策定し、研修テキストを作成し、全職員のうち希望者に対して集合研修会方式で3日間（業務時間内）に分けて研修を実施すること。開催日程等は事前に本市と協議して決定すること。

(2) 運用管理者向け研修

本システムの運用に関するシステム管理者向け研修計画を策定し、研修テキストを作成し、1日研修を実施すること。開催日程等は事前に本市と協議して決定すること。

5. 成果物および納期

5.1. 納入成果物

本件における納入成果物は以下に示すとおり。ただし、納入成果物の構成、詳細については、受注後、本市と協議し、その指示に従うこと。

- (1) プロジェクト実施計画書
- (2) 基本設計書
- (3) 機器・ソフトウェア管理台帳
- (4) 各機器・ソフトウェア設定一覧
- (5) テスト計画書／テスト結果確認書
- (6) 全体構成図
- (7) ラック搭載図
- (8) ケーブル配線図（LAN 配線、電源配線）
- (9) 機器操作マニュアル／運用マニュアル
- (10) 運用・保守業務計画書（障害時の対応や報告のフローを記載）

なお、納入成果物については、以下の条件を満たすこと。

- (1) 文書を紙及び磁気媒体等（CD-R 又は CD-RW 等）により提供すること。
- (2) 紙のサイズは、日本工業規格 A 列 4 番を原則とする。図表については、必要に応じて A 列 3 番縦書き、横書きを使用することができる。バージョンアップ時等に差し換えが可能なようにバインダー方式とする。
- (3) 磁気媒体等に保存する形式は、PDF 形式又は Microsoft Office 2016 で扱える形式とする。ただし、本市が別に形式を定めて提出を求めた場合は、この限りではない。

5.2. 納期

プロジェクト実施計画書及び各工程の計画書は、納入決定後に本市の指示に従い提出すること。
その他については、平成29年3月31日までとする。

6. 検収及び瑕疵担保責任

6.1. 検収

納入成果物については、適宜、本市に進捗状況の報告を行うとともに、レビューを受けること。最終的な納入成果物については、『5.1 納入成果物』に記載のすべてが揃っていること及びレビュー後の改訂事項等が反映されていることを、本市が確認し、これらが確認され次第、検収終了とする。なお、以下についても遵守すること。

- (1) 検査の結果、納入成果物の全部又は一部に不合格品を生じた場合には、受注者は直ちに引き取り、必要な修復を行った後、本市の承認を得て指定した日時までに修正が反映されたすべての納入成果物を納入すること。
- (2) 『納入成果物』に規定されたもの以外にも、必要に応じて資料等の提出を求める場合があるため、作成資料等を常に管理し、最新状態に保っておくこと。

6.2. 疑義

本仕様書について疑義が生じた場合は、双方協議の上、仕様内容を変更するものとする。ただし、本仕様書に明示されていない事項で、業務遂行上、各機器が正常に機能するために必要と考えられる事項については、受注者の責任で対応すること。

6.3. 瑕疵担保責任

- (1) 本業務の瑕疵担保期間は、本業務の完了日から起算して1年間とする。なお、瑕疵担保期間中に発生した機器障害等は、すべて受注者の費用負担により適切な対応を行うものとする。
- (2) 本業務の瑕疵に起因して第三者に損害を与えた場合、受注者は、受注者の責任と費用負担により、適切な対応をとらなければならない。なお、損害賠償の請求が第三者より本市にあった場合、本市はその賠償を受注者に請求できるものとする。

7. 業務実施体制

7.1. 要員の配置

本業務を実施するために、以下の体制を整えること。

(1) 統括責任者

(ア) 役割

本業務全体の業務実施状況を管理する者である。

(イ) 要件

情報通信関連の業務経験 5 年以上を有すること。または同等と本市が認める者であること。
本市から要件に適合すると認められない場合、または、本業務遂行に著しい支障をきたす場合は交替を求めることができる。

(ウ) 留意事項

他業務との兼務を認める。

(2) 担当リーダー

(ア) 役割

本業務におけるリーダーであり、関連業務実施者の業務実施状況を把握し、必要に応じて助言等を行う者である。

(イ) 要件

情報通信関連の業務経験 3 年以上を有すること。または同等と本市が認める者であること。
本市から要件に適合すると認められない場合、または、本業務遂行に著しい支障をきたす場合は交替を求めることができる。

(ウ) 留意事項

本業務に含まれる内容ごとに担当リーダーを配置してもよい。ただし、複数の担当リーダーの業務を総括する者を配置すること（統括責任者が兼務してもよい）。他業務との兼務を認める。

7.2. 作業方法

設計及び構築に際しては、以下の事項を順守し実施すること。

- (1) 設計・構築を行うにあたり、想定されるリスクやその対応策等を明示すること。
- (2) 納入決定後、プロジェクト実施計画書を提示すること。また、納入決定以降に変更が発生した場合には、その都度速やかに変更後のプロジェクト実施計画書を提出すること。
- (3) 進捗状況や直近における予定等の報告をすること。報告のタイミングは本市と協議し取り決めを行い、その取り決めに基づき行うこと。それ以外にも、本市又は受注者が必要と判断した場合は、必要に応じて随時追加の報告を行うこと。

8. 特記事項

8.1. 基本事項

受注者は、次に掲げる事項を遵守すること。

- (1) 本件納入にかかる作業の実施にあたり、作業の継続を第一に考え、善良な管理者の注意義務をもって誠実に行うこと。
- (2) 本件納入にかかる作業に従事する要員は、本市と円滑なコミュニケーションを行う能力と意思を有していること。
- (3) 本件納入にかかる作業場所を他の目的の為に使用しないこと。
- (4) 本件納入にかかる作業に従事する要員は、作業場所において所定の名札を着用するなど等、従事に関する所定の規則に従うこと。
- (5) 要員の資質、規律保持、風紀及び衛生・健康に関すること等の人事管理並びに要員の責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。
- (6) 受注者は、本件納入にかかる作業の実施に際し、本市からの質問、検査及び資料の提示等の指示に応じること。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。
- (7) 次回の機器導入等に向けた現状調査、本市が依頼する技術的支援に対する回答、助言を行うこと。
- (8) 本件納入にかかる作業においては、作業完了後の運用等を、受注者によらずこれを行うことが可能となるよう詳細にドキュメント類の整備を行うこと。

8.2. 機密保持

本件納入にかかる作業を実施する上で必要とされる機密保持に係る条件は、以下のとおりとする。

- (1) 受注者は、本件納入にかかる作業を実施する過程で本市が開示した情報（公知の情報を除く。以下同じ。）、本件納入の目的以外に使用又は第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。
- (2) 受注者は、本件納入にかかる作業を実施するにあたり、本市等から入手した資料等については管理台帳等により適切に管理し、かつ、以下の事項に従うこと。
 - ・ 複製しないこと。
 - ・ 業務に必要ななくなり次第、速やかに本市等に返却または消去すること。
 - ・ 本件納入にかかる作業完了後、上記(1)に記載される情報を削除または返却し、受注者において該当情報を保持しないことを誓約する旨の書類を本誌に提出すること。
- (3) 機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

8.3. 遵守事項

本業務を実施するにあたっての遵守事項は、以下のとおり。

- (1) 受注者は、「政府機関の情報セキュリティ対策のための統一基準（第4 版）（平成26年度版）」（2016 年5 月19 日改定、情報セキュリティ政策会議決定）に定めるほか、発注者が定める情報セキュリティの規定を遵守すること。
- (2) 納入業務の実施において、現行システムの設計書等を参照する必要がある場合は、参照方法などについて本市の指示に従い、秘密保持契約を締結するなどした上で、参照すること。
- (3) 本市へ提示する電子ファイルは事前にウイルスチェック等を行い、悪意のあるソフトウェア等が混入していないことを確認すること。
- (4) 民法、刑法、著作権法、不正アクセス禁止法、個人情報保護法等の関連法規を遵守することはもとより、本市が定める規程を遵守すること。
- (5) 受注者は、本業務において取り扱う情報の漏洩、改ざん、滅失等が発生することを防止する観点から、情報の適正な保護・管理対策を実施するとともに、これらの実施状況について、本市が定期又は不定期の検査を行う場合においてこれに応じること。万一、情報の漏洩、改ざん、滅失等が発生した場合に実施すべき事項及び手順等を明確にするとともに、事前に本市に提出すること。また、そのような事態が発生した場合は、本市に報告するとともに、当該手順等に基づき可及的速やかに修復すること。