【 220390 】

松阪市庁内ネットワーク構築及び機器等賃貸借・運用保守業務

【機器等賃貸借・運用保守業務仕様書】

令和５年３月

松阪市 企画振興部

デジタル未来戦略局 情報システム課

【目　次】

1. 業務概要

1.1. はじめに

本仕様書は、松阪市（以下、「本市」という。）が利用している「松阪市庁内ネットワーク機器及びインターネット分離システム」に関する維持管理及び保守、修理等について定めたものである。

1.2. 業務名

松阪市庁内ネットワーク構築及び機器等賃貸借・運用保守【機器等賃貸借・運用保守業務】（以下、「本業務」という。）

1.3. 業務期間

・　令和 6 年 4 月 1 日から令和 11 年 3 月 31 日まで（60 ヵ月）

1.4. 賃貸借対象機器等

「別紙_機器仕様書・別紙_機器設置台数表」記載のとおり

1.5. 機器設置場所

本市が定めた指定場所（「別紙_機器設置台数表」記載のとおり）

1.6. 履行場所

「1.5 機器設置場所」と同じ

1.7. 支払条件

本市が「松阪市庁内ネットワーク構築及び機器賃貸借・運用保守業務（構築分）」の検収を行った後、令和 6 年 4 月 1 日から令和 11 年 3 月 31 日（60 ヶ月）までの間、契約金額を 60 で除した金額を毎月翌月の後払いとする。ただし、月額に 1 円未満の端数が生じた場合は契約開始月に支払うものとする。

2. 保守業務

2.1. 保守対応機器と保守対応時間

保守対応機器とそれぞれの保守対応時間については以下の通りとする。

【ハードウェア製品 保守対応表】

対象機器（ハードウェア）	対応時間
コアスイッチ A コアスイッチ B レイア 3 スイッチ A レイア 3 スイッチ B レイア 2 スイッチ A レイア 2 スイッチ B PoE 対応レイア 2 スイッチ PoE 対応アクセスレイア 2 スイッチ アクセスレイア 2 スイッチ 外局収容ルータ 外局接続用ルータ 基幹ファイアウォール ファイアウォール A ファイアウォール B ネットワーク認証サーバ 無線 LAN コントローラ 無線アクセスポイント A 無線アクセスポイント B 無線 LAN 管理サーバ 無線 LAN ロケーション管理サーバ 仮想基盤用ラックマウントサーバ バックアップサーバ 共有ストレージ SFP	24 時間 365 日　オンサイト保守
ファイアウォール C NAS サーバ	24 時間 365 日 受付 平日（月曜日～金曜日）9:00～17:30 オンサイト保守
管理 PC	24 時間 365 日 受付 翌営業日対応

【ソフトウェア 保守対応表】

対象（ソフトウェア）	対応時間
サーバ仮想化ソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
負荷分散装置（ロードバランサ）	24 時間 365 日 受付 24 時間 365 日 対応 ソフトウェア保守
ウイルス対策システム用ソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
資産管理システム用ソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
Web コンテンツフィルタサーバ用ソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
インターネット分離システムソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
WEB メールシステムソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
メール無害化システムソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
スパムメール対策システムソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
SYSLOG サーバソフト	24 時間 365 日　受付 平日（月～金曜日）9:30～17:30 ソフトウェア保守
ID 連携システムソフト	24 時間 365 日　受付 平日（月～金曜日）8:30～17:30 ソフトウェアサポート
ファイル無害化システムソフト	24 時間 365 日　受付 平日（月～金曜日）9:00～17:30 ソフトウェアサポート
内部ファイル交換システムソフト 外部ファイル交換システムソフト	24 時間 365 日　受付 平日（月～金曜日）10:00～19:00 ソフトウェアサポート

バックアップシステムソフト	24 時間 365 日　受付 平日（月～金曜日）9:00～18:00 ソフトウェアサポート
仮想基盤ウイルス対策システムソフト	24 時間 365 日　受付 平日（月～金曜日）9:00～17:30 ソフトウェアサポート
WindowsOS	24 時間 365 日　受付 平日（月～金曜日）9:00～17:30 ソフトウェアサポート
LinuxOS（Redhat）	24 時間 365 日　受付 平日（月～金曜日）9:00～17:30 ソフトウェアサポート

2.2. 連絡体制

障害連絡窓口については以下の体制を整えること。

(1) 電話とメールにて 24 時間 365 日、障害の受付が可能な体制とすること。
(2) 電話とメール対応については全て日本語にて対応を行うこと。
(3) 連絡窓口の拠点は日本国内であること。
(4) 連絡窓口拠点については、震災・災害時でも異なる拠点で業務が継続できる体制であること。
(5) 障害連絡窓口は全ての製品において一つにまとめる事とし、受託者にて提供を行うこと。
(6) 保守業務の責任者は、受託事業者の正社員であること。
(7) 保守業務の実施者は、受託事業者もしくは保守委託会社の正社員であること。

2.3. 保守業務内容

2.3.1. 保守業務内容

本システムは以下の保守業務が可能な体制を整えること。

(1) 初動対応

- 障害対応を開始してから 30 分以内に、障害内容及び対応策と予想される作業時間について本市に報告すること。
- 障害を検知または本市から連絡を受けた後、下記の時間以内に現地に到着し、作業を開始すること。
- 作業の開始及び復旧見込みが開庁時間外に至ると予測される場合であっても、本市の指示に従い継続して作業を実施すること。

対応時間	拠点	駆け付け時間
開庁時間内 (平日 8:30～ 17:15)	データセンター	60 分以内
	本庁舎	60 分以内
	各地域振興局	90 分以内
	その他	120 分以内
	仮想基盤及び仮想基板上に構築しているシステム	60 分以内
開庁時間外	データセンター	120 分以内
	本庁舎	120 分以内
	各地域振興局	150 分以内
	その他	180 分以内
	仮想基盤及び仮想基板上に構築しているシステム	120 分以内

(2) ログ解析・切り分け

- 障害を検知した場合、対象機器のログ解析を受託者にて行うこと。
- 障害切り分けの支援を行うこと。
- 本市からの依頼があった場合、障害箇所の特定がされていなくても現地に駆け付け切り分けを行うこと。

(3) 障害対応

- 現地障害対応開始から原則 2 時間以内に復旧させること。これを超える場合は本市の了承を得ること。
- 受託者は本市が障害復旧されたことを確認するまでの間、現地に留まること。

(4) 復旧後対応

- 復旧後速やかに本市に報告すること。

(5) 予防交換対応

- 障害箇所の特定ができない場合でも、本市からの依頼があった場合には予防交換対応を行うこと。

2.4. 保守部材

本業務を実施する上で、必要な保守部材を全て受託者が保持していること。
保守部材に関しては、正常性確認の観点から年に 1 回を目安として動作確認を行うこと。また、冗長されていないネットワーク機器に関しては最寄りの拠点に予備機を保管し、障害切り分けが困難な場合、初動駆け付け時に交換が可能なこと。

2.5. 報告業務

作業報告・障害報告を作成し、月次にて本市へ提出すること。
ただし、業務の停止を伴う障害に関しては、3 開庁日以内に障害報告書を提出すること。部品の交換を行った場合には、受託者にて再現試験を行い報告すること。なお、本市から要望があった場合には、メーカー調査を行い根本原因の特定を行うこと。

2.6. 対象外業務

次の各号の保守業務は、本仕様書に定める保守業務の対象外とする。

(1) 事故、または受託者以外の誤操作による障害
(2) 風水害、地震、落雷等の天災、およびテロ、不正アクセス等による破壊。
(3) ウイルス感染・不正アクセスによる改ざん等による障害。
(4) 製品の仕様に適合しない電源容量等の設置機器での利用、もしくは移動。
(5) 製品の取り扱い説明書中で許可されていない取扱い方法による障害。
(6) 受託者以外の第三者により実施された修理ならびに改造による障害。
(7) 機構・機能に影響を及ぼさない外観不良。
(8) 物理的破損・破壊に起因する、ハードウェア機能不良。
(9) メーカー都合による機能変更を伴わない外観を含む形状変更を理由とした交換の要請。
(10) 機器交換対象外となる消耗品やアクセサリの提供。

3. ネットワーク監視・運用業務

3.1. 目的

本ネットワークを正常に稼働・運用、構成機器障害が発生した際に迅速な復旧を行い安定したネットワークを提供することを目的とする。

3.2. サービス概要

導入機器をモニタリングし情報を収集・可視化すること。また、異常を検知した際には機器のログを取得し保守業務への連携を行うこと。

3.3. 対象機器と監視項目

本業務にて導入した製品を範囲し、下記の監視項目を範囲とする。

【 監視項目一覧表】

種別	監視項目		
	死活監視	SNMP-Trap 監視	リモートログ取得
コアスイッチ A	●	●	●
コアスイッチ B	●	●	●
レイヤ 3 スイッチ A	●	●	●
レイヤ 3 スイッチ B	●	●	●
レイヤ 2 スイッチ A	●	●	●
レイヤ 2 スイッチ B	●	●	●
PoE 対応レイヤ 2 スイッチ	●	●	●
外局収容ルータ	●	●	●
外局接続用ルータ	●	●	●
基幹ファイアウォール	●	●	●
ファイアウォール A	●	●	●
ファイアウォール B	●	●	●
ファイアウォール C	●	●	●
認証サーバ	●	●	●
無線 LAN コントローラ	●	●	●
無線 LAN 管理サーバ	●	●	●
無線 LAN ロケーション管理サーバ	●	●	●
負荷分散装置（ロードバランサー）	●	●	●
仮想基盤用ラックマウントサーバ	●	●	●

NAS	●	-	-
バックアップサーバ	●	●	●
共有ストレージ	●	●	●
vCenter	●	●	●
VMware vSphere (ESXi)	●	●	●

●：監視対象　-：監視対象外

3.4. 履行場所

受託会社。

3.5. 対応時間

24 時間 365 日（定期メンテナンスなどの時間帯を除く）

3.6. 連絡体制

以下の連絡体制を整えること。

(1) 電話とメールにて 24 時間 365 日、障害の受付が可能な体制とすること。
(2) 電話とメール対応については全て日本語にて対応を行うこと。
(3) 連絡窓口の拠点は国内にあること。
(4) 連絡窓口拠点については、震災・災害時でも異なる拠点で業務が継続できる体制であること。
(5) 業務責任者は、受託者の正社員であること。
(6) アラートの報告については、監視オペレーターでメール及び電話で連絡すること。

3.7. リモート接続要件

本業務を実施するにあたり、リモートから業務を実施する場合には下記の要件を満たすこと。

(1) 本市とリモート保守拠点間は暗号化した通信を行うこと。
(2) リモート作業端末に関して、利用者の本人確認を行う機能を有すること。
(3) リモート作業に関して、必ず複数人で行うこととし、内一人がその作業を監視することとする。また、全ての作業操作履歴を管理把握し、本市からの依頼があった場合に、報告書（作業者・作業内容・手順）を提出すること
(4) 本市がリモート保守拠点と接続する回線は受託者にて準備すること。なお、その費用は入札金額に含めること

3.8. ネットワーク監視共通事項

モニタリングに関する、対象機器または設定内容の追加・変更・削除等の申請や、本市による計画作業・計画停電等で一時的にアラート検知の連絡を停止する際に対応を行うこと。詳細については次項を参照すること。

(1) 監視変更対応

監視変更対応の内容は以下の通りとする。

【監視変更対応】

項目	内容
対象機器の追加	新たに対象機器の追加を行うこと。
対象機器の監視仕様変更	対象機器のモニタリング項目等が変更される場合、データ変更を実施すること。
対象機器の情報変更	IPアドレス、SNMPコミュニティ名、パスワード、設置場所等が変更される場合、データ変更を実施すること。
対象機器の削除	対象機器の登録を削除すること。
運用内容の変更	本市の運用体制変更等により、アラート連絡先情報と連絡元情報が変わる場合、変更を受け入れること。

(2) 計画停止・停電対応

監視対象機器の計画停止および計画停電における対応を行うこと。

【計画停止・停電対応】

項目	内容
作業日時	申請を受付した時間帯に対応を開始、完了すること。
計画停止	ネットワークの構成変更等により対象機器の停止が計画されている場合、期間と対象機器情報を基にアラートを静観し連絡を行わないこと。
計画停電	法定点検などの計画停電に伴い対象機器の停止が計画されている場合、期間と対象機器情報を基にアラートを静観し連絡を行わないこと。

3.9. ネットワーク監視運用

以下のサービスを提供すること。

(1) 死活監視（Ping）

① サービス内容

モニタリングアプライアンスからの死活（Ping）応答により、対象機器のステータスをモニタリングすること。応答結果から対象機器の稼働状況を判断し、本市との取決めに従い、本市へ連絡すること。

② 仕様

モニタリングアプライアンスから対象機器の登録 IP に対して死活（Ping）応答によるモニタリングを実施すること。なお、死活（Ping）応答の各パラメーターは以下の通りとする。

【死活監視仕様】

項目	内容	ポーリング間隔	タイムアウト値	リトライ回数
Ping Failed	死活（Ping）応答の失敗	5 分	5 秒	3 回
Ping OK	死活（Ping）応答の成功			

(2) SNMP トラップ監視

① サービス内容

監視対象機器から送信される SNMP トラップをモニタリングアプライアンスにて受信し、監視対象トラップについてはアラートとして検知すること。アラートを検知した際は、本市との取決めに従い、本市へ連絡すること。

② 仕様

本サービスで監視対象とするトラップは下記の通りとする。

【SNMP トラップ監視仕様】

NO	内容
1	機器が起動した(電源の OFF/ON、reload コマンド等による再起動を含む)
2	機器または CPU モジュールのソフトウェア的な再起動が発生した
3	インターフェースのダウン（※1）
4	インターフェースのアップ（※1）
5	電圧や温度が危機的な状態になったため、強制シャットダウンする際

6	機器の電圧がしきい値を超過した
7	機器の温度がしきい値を超過した
8	ファン装置に異常が発生した
9	電源装置に異常が発生した
10	モジュールの状態が変化した
11	電源装置の状態が変化した
12	モジュールが挿入された スタックメンバーが追加された
13	モジュールが抜かれた スタックメンバーが削除された
14	ファンの状態が変化した
15	電源の出力が変化した

※1：定期的に linkDown/Up が発生する機器はサービス対象外とする

③ サービス条件

サポートしている SNMP バージョンは、v1、v2c、v3 であること。
個別 MIB、エンタープライズ MIB のトラップ監視に関しても追加が可能なこと。

(3) リモートログ取得

① サービス内容

死活(Ping)及び SNMP トラップの対象機器に対して、アラート検知後に保守部門からリモートで該当機器にログインし、ログ情報の取得を行うこと。
その後、本市との取決めに従い、本市へご連絡すること。
また「2.保守業務」と連係しログ解析及び保守対応準備を行うこと。

② 仕様

リモートログ取得の仕様は以下の通りとする。

【リモートログ取得仕様】

項目	内容
リモート調査開始条件	死活（Ping）または SNMP トラップ にてアラートを検知した際にリモートログ取得開始。
リモートアクセス方法	監視センターからモニタリングアプライアンスを経由して該当機器にリモート接続すること。
ログ情報収集方法	リモート接続後、CLI または GUI で各種ログ参照コマンドを実行。
リモート調査終了条件	ハードウェア障害の疑いがあると判断した場合は、保守部門へ対応を引き継ぐこと。その後、調査結果を電話または本市

	との取決めに従い、本市へ連絡すること。 ハードウェア障害の疑いが無い場合は、本市との取決めに従い、本市へご連絡すること。

(4) サービスポータル

① サービス内容

本市専用の Web ページ上で、モニタリングのアラートやインシデント発生状況、モニタリング対象のパフォーマンス統計情報サマリーを提供すること。また、月次レポートのダウンロードも可能なこと。

② 仕様

- 24 時間 365 日サービス提供さえること。（メンテナンスを除く）
- ユーザ名・パスワードとは別にワンタイムパスワード等の二要素認証されること。
- システム単位で提供され、過去に発生したアラート閲覧やパフォーマンス表示については、90 日前まで可能なこと。
- モニタリング静観依頼などのリクエストが可能なこと。
- モニタリングのアラートやインシデント発生状況、モニタリング対象のパフォーマンス情報などの監視実績のレポートを生成可能なこと。

(5) 監視サーバ要件

- 可用性を高めるため、監視サーバは冗長構成で構成すること。

4. セキュリティ監視・運用業務

4.1. 目的

インターネットに接続するファイアウォール B にて高度なセキュリティ運用を実現することを目的とする。

(1) 通信ログの定期的な分析・レポートにより、潜在する脅威を可視化し、セキュリティ上必要となる対応を実現すること。（緊急度の高い脅威については、即時対応も考慮する。）

(2) 情報漏洩、データ破損等、庁内から庁外への不正な活動を防ぐことを目的とする。

4.2. サービス範囲

セキュリティ監視・運用業務は以下を対象とする。

・　インターネットに接続するファイアウォール B：1 式（2 台分）

4.3. セキュリティ監視概要

以下のセキュリティ監視運用を実施すること。

(1) リアルタイム分析（随時/24 時間 365 日実施可能/リモート作業）
(2) 緊急遮断（随時/24 時間 365 日実施可能/リモート作業）
(3) 月次報告書の提供（毎月 1 回/カスタマーポータルで提供）
(4) 分析レポートの報告会の実施（毎月 1 回/本市役所内）
(5) シグネチャ適用（随時）
(6) バージョンアップ/パッチ適用対応（年 2 回/リモート作業）
(7) カスタマーポータルの提供（24 時間 365 日 ※メンテナンス時間を除く）
(8) 上記業務内容に関する Q&A

4.4. セキュリティ運用内容

(1) リアルタイム分析

・　監視対象機器が発する IPS/IDS ログ、サンドボックスログ、セキュリティアラートの監視・分析を有人で 24 時間 365 日実施すること。

・　緊急度・危険度が高いと判断される場合には、あらかじめ本市と取り決めた連絡先へ通知すること。

・　監視対象機器の持つシグネチャにあらかじめ定義された危険度の分類に依らず、アナリストが関連するログ等の分析により攻撃内容や影響を調査した結果を基に、独自に危険度を判断すること。なお、危険度は以下の例のように複数段階に分類できること。

・

(ア)危険度 3

攻撃が成功しており、緊急事態であると判断したインシデント。

(イ)危険度 2

攻撃が成功した可能性が高いと判断したイシデント。

(ウ)危険度 1

影響を受ける可能性は低いが、経過観察が必要と判断したイシデント。

(エ)危険度 0

問題ない通信ではないが、攻撃ではないと判断したインシデント。

- セキュリティイシデントの危険度を判断する際、分析精度を向上させるため、セキュリティアラートのログの分析に加えて、必要に応じて以下の分析を実施すること。
  (ア)セキュリティデータを用いた分析
  (イ)脅威インテリジェンスを用いた分析
- 危険度の高いセキュリティインシデントを確認した場合は、本市が指定する連絡先に電話及びメールによる緊急連絡を行うこと。

(2) 緊急遮断

- 危険度の高いセキュリティインシデントを確認した場合、攻撃元・コールバック先の IP アドレスや、感染が疑われるシステムの IP アドレス等をファイアウォールにて遮断する設定を行い、以降の不正通信を発生されないように遮断対応を行うこと。
- あらかじめ指定された連絡先と連絡が取れない場合の対応など、遮断対応を行う条件や運用ルールを事前に本市と協議のうえ決定すること。
- 遮断対応の設定手順等を作成し、サービス開始までに本市と合意を得ること。

(3) 月次報告書の提供

- 検知したセキュリティイシデント等について、月次報告書を作成すること。
- 月次報告には、本市個別の情報（本市で検知したセキュリティインシデント件数、緊急度の高いイベントの詳細情報等）を含めること。
- 月次報告書は、翌月第 8 営業日以内に提供すること。
- 本市が要望した場合には、Microsoft Word など編集可能な形式で提供すること。

(4) 分析レポートの報告会

報告会では以下の内容を必ず説明すること。

- 分析レポートの内容報告
- 本市のセキュリティ環境に対してのアドバイス
- インシデント通知時の対応アドバイス
- 最新の国内外のセキュリティトピックスと本市の環境を照らし合わせた観点でのセキュリティ通知時のアドバイス
- 必要に応じてセキュリティに関連する可能性のある国内外のニュートピックの説明

(5) シグネチャ適用

- シグネチャの更新は、原則自動アップデートとする。但し、シグネチャの自動更新に失敗した場合等手動更新が必要な場合は、実施すること。
- 危険性が高い脆弱性に対応するシグネチャの作成と適用をすること。
- 作業実施にあたり本市のネットワーク通信に影響が出る場合には、直ちに設定を解除すること。

(6) バージョンアップ・パッチ適応

- 監視対象機器に対して本市が要望すれば、パッチレベルのバージョンアップを１年に２回まで実施すること。なお、サービス維持を目的とした、メジャーバージョンアップは、後述の「5.3.SE 運用支援」にて実施すること。

(7) カスタマーポータルの提供

- インシデントの対応状況の確認や問合せ、レポートの閲覧を行うことができるポータルサイトを準備すること。
- カスタマーポータルは、ユーザ認証機能によりアクセス制御が行われていること。ユーザ認証機能は多要素認証を実装できること。
- カスタマーポータル閲覧に関する通信は暗号化されること。

(8) 上記業務内容に対する Q&A

- セキュリティインシデント検知やカスタマーポータルで提供している情報等に関する問い合わせに対し、24 時間体制で対応すること。なお、リアルタイム分析サービスにおけるセキュリティインシデントの内容に関する技術的な問い合わせには、アナリストが対応すること。

5. 運用支援業務

5.1. 目的

本業務で調達したシステムを正常に運用させるため、技術相談及び技術支援を行い安定したシステムを提供することを目的とする。

5.2. 運用支援概要

本システムの構成機器に障害が発生した場合、保守統制及び一次切り分け、機器の修理、代替え機への交換などを実施し、正常な状態に復旧させること。また、運用時に必要となる技術情報の提供、解決策の提案、設計提案、それらに伴う設定変更等の運用に関する支援を行う。なお、大幅な構成変更に伴う設定変更は含まない。

5.3. SE 運用支援

5.3.1. 運用支援内容

(1) 月次の運用保守定例会を実施すること。構築完了後 1 年間については、構築を実施した案件担当リーダ以上の担当者が同席すること。

⑵ 年間 60 回程度（週 1 度)、開庁時間から閉庁時間の間で訪問による技術相談及び運用作業を実施すること。また、それ以外に本市から要請があった場合、各種会議及び打ち合わせに参加し、技術的な支援及びアドバイスを実施すること。

5.3.2. SE 運用支援詳細

SE 運用支援に関しては、以下の内容を想定している。保守内容は過去の運用実績に基づいているが、想定を超える場合には本市と協議のうえ対応を行うものとする。

【SE 運用支援詳細】

No	運用項目	作業内容 （想定）	作業回数 （想定）
1	障害対応	障害発生時に原因の切り分けを実施	障害発生時
		障害の暫定対応	障害発生時
		障害の恒久対応	障害発生時
2	運用支援	問い合わせ対応	8 回/月
		作業依頼の実施	8 回/月
		NW 機器の設定作業 ・各スイッチ、ルータ ・各無線アクセスポイント ・各ファイアウォール	8 回/月

		・資産管理システム	
		拠点の NW 機器設定作業 ・拠点機器の機器準備（ルータや無線 AP） ・拠点機器の機器設置	3 回/月
		プロキシサーバのルール追加	3 回/月
		資産管理システムの問い合わせ・設定対応	3 回/月
		ウイルス等のセキュリティインシデント対応	インシデント発生時
		インターネット分離システムの設定変更 ・アプリケーションサーバへの WindowsUpdate ・アプリケーションの更新	2 回/年
		リソース使用状況のレポート作成、報告	1 回/月
		DNS サーバへのレコード情報の更新	3 回/回
		法令停電対応（第一別棟 マシンルーム/本庁舎） ・停電時のシステム停止 ・復電時のシステム復旧・確認 ・翌開庁日の立会い	2 回/年
		三重県情報セキュリティクラウドの更新に伴う切替作業	1 回/年
		定例報告会議の実施 ・報告資料の作成、送付 ・定例報告会議の実施	1 回/月
		仮想基盤バックアップからのリストア	2 回/年
		各 VLAN・IP アドレスの管理及び払い出し	10 回/年
3	人事異動対応	人事異動に伴う各種システムの変更作業 ・LGWAN 系 AD サーバ -新規ユーザのアカウント作成 -退職ユーザの退職者 OU への移動 -退職ユーザの削除 -所属グループの変更 -機構改革対応 ・資産管理システム -申請承認ワークフローの申請者、承認者の異動対応 ・外部 AD サーバ -新規ユーザのアカウント作成	1 回/年

		-退職ユーザの退職者 OU への移動 -退職ユーザの削除 ・WEB メールシステム -新規ユーザのアカウント/エイリアスの作成 -退職ユーザのアカウント無効化及び削除 -課メールのユーザ紐づきの変更 -アドレス帳の更新 ・ファイル無害化システム -フォルダの作成、権限付与 ・内部ファイル交換システム -新規ユーザのアカウント作成 -新規ユーザのフォルダの作成 -部署フォルダへの紐づきの変更 -承認者・代理承認者の承認権限付与 ・外部ファイル交換システム -新規ユーザのアカウント作成 -新規ユーザのフォルダの作成 -部署フォルダへの紐づきの変更 -承認者・代理承認者の承認権限付与 ・翌開庁日の現地立会い	
4	ドキュメント更新	ドキュメント（各設計書）のメンテナンス （主な対象ドキュメント） ・基本設計書 ・詳細設計書（パラメータシート） ・構成図 ・ハードウェア一覧表 ・ソフトウェア一覧表 ・ライセンス一覧表 ・各手順書 保守運用業務の中で、ドキュメントへの変更が必要となった場合	設定変更時
5	システムバージョンアップ	導入システムのバージョンアップ対応 （想定） ・各ファイアウォール（1 回/年） ・Web コンテンツフィルタ ・資産管理システム（1 回/年）	左記に記載

		※端末のエージェント含 ・ウイルス対策システム（1 回/年） ※端末のエージェント含 ・インターネット分離システム（1 回/2 年） ※端末のエージェント含 ・ファイル無害化システム（1 回/年） ・仮想基盤用ラックマウントサーバ（1 回/2 年） ・サーバ仮想化ソフトウェア（1 回/2 年） ・仮想化基盤ウイルス対策システム（1 回/2 年） ・バックアップサーバ（1 回/2 年） ・バックアップシステム（1 回/2 年） ・共有ストレージ（1 回/2 年） その他、関連するコンポーネントなど	
6	システム更改における技術相談	庁内のシステム導入または更改におけるネットワークおよびセキュリティに関する技術支援 ・ネットワーク仕様に関する技術支援 ・ネットワーク変更の計画支援 ・ネットワーク機器の設定変更支援	4 回/年

5.3.3. リモート接続要件

本業務を実施するにあたり、リモートから業務を実施する場合には下記の要件を満たすこと。

(1) 本市とリモート接続端末間は暗号化した通信（SSL-VPN）を行うこと。
(2) 接続元には、セキュリティを十分に担保したうえで接続を行うこと。
(3) 接続元の端末はウイルス対策ソフト、OS のアップデートが行われていること。
(4) 接続認証はユーザ名・パスワードのほかにワンタイムパスワード認証を行うこと。
(5) SSLVPN の接続元のグローバル IP アドレスは制限すること。
(6) 本市がリモート接続する回線は受託者にて準備すること。なお、その費用は入札金額に含めることし、「3.7 章」に記載された回線とは別に用意すること。
(7) 本市から現地での対応を依頼された場合は従うこと。
(8) 本市から接続履歴の提出を求められた場合は提出すること。
(9) 接続構成については、本市から承認を得たうえで構成すること。

6. 疑義

本仕様書について疑義が生じた場合、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。

7. 守秘義務（機密保持）

(1) 本業務の履行に当たって、知り得た秘密を漏らしてはならない。
(2) （1）の規定は、この契約が終了し、又は解除された後においても同様とする。

8. 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通りとする。

(1) 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。
(2) 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、本市が定める規定を順守すること。
(3) 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、情報の適切な保護・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。
(4) 本市のセキュリティポリシーを遵守すること。

【別　紙】

・　別紙_機器仕様書
・　別紙_機器設置台数表