

松阪市広域情報ネットワーク構築及び
運用・保守委託業務
要求仕様書
(概要版)

松 阪 市

目 次

1. 背景と目的	1
1.1. はじめに	1
1.2. 背景	1
1.3. 目的	1
1.4. 再構築方針	1
2. 業務概要	2
2.1. 業務名	2
2.2. 調達の内容	2
2.3. 履行場所、機器設置場所	3
2.4. 業務委託期間	3
2.5. 検収完了条件	3
2.6. 支払条件	4
2.7. 守秘義務（機密保持）	4
2.8. 注意事項	5
3. 全体構成	6
3.1. 広域情報ネットワークの概要	6
3.2. 広域情報ネットワークの課題	6
3.3. 新ネットワークの基本構成	7
3.4. システム構築・移行に関する要件	10
4. ネットワーク拡張機能	11
5. 構築要件	12
5.1. 更新業務	12
5.1.1. 更新業務実施条件	12
5.1.2. 端末移行業務実施条件	13
5.1.3. 移行	14
5.1.3.1. 移行計画書の策定	14
5.1.3.2. 移行手順の作成	14
5.1.3.3. 移行スケジュール	14
5.1.3.4. 移行判定	14
5.1.3.5. 移行・導入作業の実施	15

5.1.3.6. 移行作業の進捗報告.....	15
5.1.4. 試験.....	15
5.2. 既存機器の回収・管理.....	16
5.3. 業務実施体制.....	16
5.3.1. 統括責任者.....	16
5.3.2. 案件担当リーダー.....	16
5.3.3. 案件サブリーダー.....	17
6. 工事要件	17
6.1. 工事基準等.....	17
6.2. 工事詳細.....	17
6.2.1. 光ファイバーケーブル工事.....	17
6.2.2. UTP ケーブル工事	18
6.2.3. 第一別棟マシン室 19 インチラック設置工事.....	18
6.2.4. 保健センター19 インチラック設置工事	18
6.2.5. 第1別棟マシン室 電源コンセント工事.....	19
6.2.6. フロア用機器収納ボックス.....	19
6.2.7. 無線 LAN 機器工事.....	19
6.2.8. 無線 LAN 用 UTP ケーブル工事.....	19
6.3. 仕様部材等仕様.....	19
6.4. 配線施工後の試験	20
7. 構築業務完了報告.....	20
7.1. 提出ドキュメントの作成.....	20
7.2. 現行運用業者からの引き継ぎ業務.....	20
7.2.1. ドキュメントの受領.....	20
8. ネットワーク監視・運用.....	20
8.1. 目的.....	20
8.2. サービス概要.....	21
8.3. ネットワーク監視の範囲.....	21
8.4. 履行場所.....	22
8.5. 保守対応時間.....	22
8.6. 連絡体制.....	22
8.7. リモート接続・運用要件	22
8.8. ネットワーク監視共通事項.....	22
8.9. ネットワーク監視運用内容.....	24

9. セキュリティ運用	29
9.1. 目的	29
9.2. セキュリティ運用範囲	29
9.3. セキュリティ運用概要	29
9.4. セキュリティ運用内容	30
10. 運用支援	33
10.1. 目的	33
10.2. 運用支援概要	33
10.3. 運用支援内容	33
11. 保守	35
11.1. 目的	35
11.2. 保守概要	35
11.3. 保守の範囲	35
11.4. 履行場所	35
11.5. 保守対応時間	35
11.6. 連絡体制	36
11.7. 保守業務内容	36
11.8. 保守部材	37
11.9. 報告業務	37
11.10. 対象外業務	38

1. 背景と目的

1.1. はじめに

本調達仕様書は、松阪市（以下「本市」という。）が利用している、松阪市広域情報ネットワークの再構築業務にかかる設計・機器調達・設置・構築の調達について記載している。また、再構築した情報ネットワークの維持運用業務ならびに保守業務の委託について記載している。

1.2. 背景

現在の松阪市広域情報ネットワーク（以下、「本システム」という。）に関して、平成 20 年度に構築を行い利用開始している。しかし運用から 7 年が経過し、現行システムの老朽化や災害対策などの対応を行う必要が出てきたため、本システムの再構築を行う。また、システムのクラウドサービス利用や外部データセンターの活用に伴いネットワーク構築を実施するものである。

- ・ メーカーサポート切れ
- ・ 災害対策（BCP）

1.3. 目的

現行システムの再構築に伴い、ネットワーク機器の調達、システムの再構築及びそれらに付帯する維持運用業務・保守業務を委託することを目的としている。

1.4. 再構築方針

松阪市広域情報ネットワークの再構築方針は業務利便性のさらなる向上と、セキュリティの担保の観点、そしてシンクライアントシステムの導入やクラウドサーバの導入にあわせ、今後の ICT 環境の変化に柔軟に対応できるようにする。

- ・ ネットワーク統合
- ・ 外部データセンターとの接続
- ・ 無線 LAN 導入
- ・ セキュリティ強化
- ・ 認証システム再整備
- ・ 資産管理システムの再整備
- ・ コスト削減

2. 業務概要

2.1. 業務名

松阪市広域情報ネットワーク構築及び運用・保守委託

2.2. 調達の内容

本調達の内容は、既存広域情報ネットワークを構成している下記構成を更新するものである。詳細は各機器の仕様の通りである。

- (1) 第一別棟マシンルーム内 有線ネットワーク接続機器（スイッチ等）
- (2) インターネット接続用 回線負荷分散装置、IPS・アンチウイルス機能付きファイアウォール、DMZ スイッチ、Web コンテンツフィルタ
- (3) LGWAN 接続用 IPS・アンチウイルス機能付きファイアウォール
- (4) ネットワーク認証 LAN IEEE802.1x 認証システム
- (5) Active Directory 及び DHCP 提供機能
- (6) 本庁舎内 有線ネットワーク接続機器（スイッチ等）
- (7) 本庁舎内 無線ネットワーク接続機器（無線アクセスポイント等）
- (8) 第一分館、第二分館、第三分館、松阪市民病院、第一別棟、第二別棟、第三別棟、第四別棟内 有線ネットワーク接続機器（スイッチ等）
- (9) 第一分館、第二分館、第三分館、第一別棟、第四別棟内 無線ネットワーク接続機器（無線アクセスポイント等）
- (10) 各地域振興局内 有線ネットワーク接続機器（スイッチ、無線コントローラ機能付きスイッチ等）
- (11) 各地域振興局内 無線ネットワーク接続機器（無線アクセスポイント等）
- (12) 第一別棟マシンルーム内 外局接続用ネットワーク接続機器（VPN ルータ、スイッチ）
- (13) 各外局内 ネットワーク接続機器（VPN ルータ、スイッチ等、無線アクセスポイント等）
- (14) 情報系端末資産管理システム（1550 台分）
- (15) ウイルス対策ソフト（1550 台分）
- (16) 上記に伴い必要となる全ての端末設定(1800 台)
- (17) 上記機器の有線ケーブルの付帯工事変更と追加
- (18) 上記に係るシステムおよび機器の運用支援
- (19) 上記に係る機器の保守サポート（リモート監視運用サービスを含む）

2.3. 履行場所、機器設置場所

本調達機器および関連システムなどの納入機器は、下記拠点に納入すること。なお、機器点数や納入方法については、事前に本市と調整を図ることとする。

- (1) 第一別棟マシンルーム内
- (2) 本庁舎各フロア
- (3) 第一分館、第二分館、第三分館、松阪市民病院、第一別棟、第二別棟、第三別棟、第四別棟の各所
- (4) 各地域振興局マシンルーム内（三雲、嬉野、飯南、飯高）
- (5) 各外局、出先拠点（対象拠点は機器数量表に別途記載）

2.4. 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 28 年 12 月 31 日まで
- (2) 機器賃貸借：平成 29 年 1 月 1 日から平成 33 年 12 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 1 月 1 日から平成 33 年 12 月 31 日まで（60 ヶ月）
 - ※ システム移行完了日は、平成 28 年 12 月 1 日とする。
 - ※ システム移行完了日からシステム稼働開始日までは新旧の並行稼働期間とする。
 - ※ システム稼働開始日は、平成 29 年 1 月 1 日とする。

2.5. 検収完了条件

本業務の検収完了条件は以下のとおりである。

1. 構築業務委託に関する検収完了条件
 - 機器の納入、設置及びシステム構築全ての作業が完了した後、本市の立ち会いの下、本仕様書に定められたとおりシステムが正常に動作することを確認する。
 - また、成果物について、本市が実施する検査に合格しなければならない。成果物については別紙を参照すること。
2. 機器賃貸借及び維持運用管理業務委託に関する検収完了条件
 - 各月初日から末日までの期間において、翌月速やかに業務完了届を提出し、本市の確認をもって業務完了とする。

2.6. 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. 庁内ネットワーク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。

2. 庁内ネットワーク機器賃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 1 月 1 日から平成 33 年 12 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。

2.7. 守秘義務（機密保持）

- (1) 本業務における成果物（中間成果物を含む）については、当該業務においてのみ使用することとし、他の目的に使用してはならない。
- (2) 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。
- (3) (1) 及び (2) 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。

2.8. 注意事項

1. 調達、導入に関する注意事項

本業務にかかる注意事項は以下のとおりである。

導入スケジュールは、提出資料に含めるものとする。

導入システムは、平成 29 年 1 月 1 日より本稼働（実運用）を開始する。但し、現行システムとの移行に際して並行稼働もしくは順次切り替えをする場合は本稼働（実運用）期日より前に実施すること。

2. 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、提案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。入札時点で製品化されていない機器またはソフトウェアは、技術的要件を満たしていないものと判断する。

3. 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との接続など、本仕様書に記載の要件をすべて満たす見積もりとすること。本調達における追加費用は一切認めない。
- (2) 入札金額には、各職場の既存機器の撤去とデータ（設定情報）削除の作業費用を含めること。また環境に配慮した処分方法を検討すること。リース会社への搬出は 1 回目の搬出のみ既存納入業者が費用を負担するが、複数回に分割して搬出する場合はその費用を入札金額に含めること。
- (3) 機器撤去の際はデータの流出が起きないように、適切な処分を行うこと。
- (4) 既存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。
- (5) 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認申請書に同等以上の性能を有することを示した機能証明書と変更する理由を明記し、本市へ提出し承認を得ること。また、ネットワーク機器等については現地調査を行い特に無線及び有線ネットワークにおいて、本稼働後ネットワーク機器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解決させること。なお、これらに係る費用は、入札価格に含むこと。
- (6) 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等を行うものとする。
- (7) 本市のセキュリティポリシーを遵守すること。
- (8) 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。

3. 全体構成

3.1. 広域情報ネットワークの概要

本市において現在運用中である広域情報ネットワークの借入期間の満了に伴い、次期広域情報ネットワークの調達及び整備を実施する。

この広域情報ネットワークは本庁舎を含む全出先拠点が接続し、住民サービス提供する基幹系通信、グループウェア・電子メール等の情報系通信に加え、一部拠点においては住民基本台帳データ等を取り扱う戸籍ネットワーク・公的個人認証ネットワーク・住民基本台帳ネットワークの通信がネットワークセキュリティを確保した上で利用されている。

3.2. 広域情報ネットワークの課題

現在の運用中の広域情報ネットワークは下記の課題があり、新広域情報ネットワークで改善する必要がある。

表 3.2-1 広域情報ネットワーク課題

項	課題	概要
1	柔軟性無きネットワーク体型	<ul style="list-style-type: none"> ・ 細分化されたネットワークアドレス体系がネットワークセグメントを跨ぐ移動の弊害となっている。 ・ 組織変更に伴う配置移動や端末移動における運用者のネットワーク機器の設定変更負荷が高い。 ・ 一部分についてシンククライアント端末の導入が進みネットワークアドレスによるロケーション管理の見直しが必要になってきた。 ・ サーバセグメントがシステム毎にサイロ構造になっており、システム毎のネットワーク運用が煩雑になっている。

項	課題	概要
2	無線 LAN 非提供状態	<ul style="list-style-type: none"> ・ ペーパーレス化・柔軟性の高いワークスタイルを実現するために一部導入予定のモバイル端末が無線 LAN 環境が提供されていない為に限られたエリアでしか接続ができない。 ・ 職員配置変更のたびに有線 LAN の配線変更作業が発生し運用負荷が高い。
3	セキュリティ強化	<ul style="list-style-type: none"> ・ インターネット環境で蔓延する未知のマルウェアに対する対策強化が求められている。 ・ 近年に導入される社会保障・税番号制度（マイナンバー制度）に対応する為、広域情報ネットワークのセキュリティレベルの強化が求められている。 ・ 外部ネットワークからのゼロデイアタックが流行しており、対策が求められている。
4	ネットワーク運用負荷	<ul style="list-style-type: none"> ・ ネットワーク機器点数の増加に伴う職員による運用負荷が増してきている。 ・ 専門的知識（ネットワーク・セキュリティ共）の習得が必要となってきた。
5	機器老朽化	<ul style="list-style-type: none"> ・ 現広域情報ネットワークの構成機器が導入され 5 年以上が経過することで経年劣化による故障頻度が増してきている。

3.3. 新ネットワークの基本構成

新ネットワークでは業務の利便性とさらなる向上とセキュリティの担保そして現運用中のネットワークで抱える課題を改善するために新ネットワークでは以下の基本構成を新たに設計に含め構築すること。

(1) シームレスな職場ネットワーク構成

本庁舎、各別館、各分館において利便性と柔軟性を確保し、シームレスなネットワーク環境を提供する為にネットワークセグメントの統合を検討する。

具体的には対象建屋において基幹系・情報系の端末が接続するネットワークセグメントを1セグメント化し、対象建屋内の端末移動が発生してもネットワーク機器や端末の設定変更せずにネットワーク利用ができるように検討する。

但し、セキュリティ上の理由で統合できないシステムに関しては本市の承認を得た上で分離すること。

(2) サーバセグメントの統合

第一別棟と本市が利用しているクラウドサーバ（以下、「松阪市 IaaS」という。）に配置されるサーバセグメントを新ネットワーク構築後に更改するタイミングで順次ネットワークセグメントの統合を実施する。

具体的には現在システム毎に分離されたネットワークセグメントを大きく情報系と基幹系に分離し、端末接続ネットワークと情報系と基幹系のネットワーク間の通信制御が実現できるように設計する。本仕様に含まれるシステムはこの基本構成に従って設計し構成すること。但し、戸籍ネットワーク、公的個人認証系、住民基本台帳ネットワークはセキュリティの観点から各々を分離した構成とすること。

(3) 無線 LAN の導入

本庁舎、各別館、各分館、各地域振興局において定期的な組織変更への柔軟な対応とフレキシブルな業務環境を構築する為に無線 LAN の導入をする。

具体的には対象建屋の執務環境と会議室にて無線 LAN 対応端末やモバイル端末がネットワークに接続できるように無線 LAN 環境を構成し、場所に依存しない職場環境の提供をする。

(4) ネットワーク認証の強化

現在稼働中のネットワークではネットワークに接続する端末の MAC アドレスを元にネットワーク認証を実施しているが、新ネットワークではネットワーク接続の柔軟性と利便性が向上するために、有線 LAN、無線 LAN 共に接続する端末の利用制限をより強化する。

具体的には本庁舎、各別館、各分館、各地域振興局、市民病院は利用する端末はすべて Active Directory のドメイングループに参加する。ワークグループでの利用は禁止とする。さらに有線 LAN、無線 LAN（市民病院は除く）に接続する為に電子証明書を配布し、ネットワークスイッチや無線システムと IEEE802.1x 認証による強固なネットワーク認証を実施する。IEEE802.1x 認証が実施できない機器は MAC アドレスによる認証を実施する。各外局はネットワークスイッチポートに接続する端末の MAC アドレスを登録し、例外の端末が接続できないように制限を実施する。

(5) 次世代セキュリティ対応

近年悪質で巧妙化しているマルウェアへの対応を実施する。

具体的にはインターネット接続用ファイアウォールと LGWAN 接続用ファイアウォールでアプリケーションレベルでの通信制御を実施する。さらにゼロデイ攻撃に迅速に対応できるよう IPS 機能を備えた防御機器を構成し、外部攻撃から守ると共に内部から情報が流出することへも対策を実施する。

インターネット接続ファイアウォール等にサンドボックス機能を有し、通信ログや脅威ログをリモートによるモニタリングを実施し、有事に対策を実施できるようにする。また定期的にセキュリティ専門家によるログの分析を実施し、問題点に対してセキュリティ対策の改善を実施する。

(6) リモート保守・監視運用の導入

現運用中のネットワーク機器点数に加え、今後無線 LAN システムの導入に伴い監視する機器点数が大幅に増加する。ネットワークの重要性の向上に伴い、更なる安定稼働を目的にリモート運用監視を導入する。

監視運用を 24 時間 365 日リモートより実施し、職員の運用負荷の軽減を図る。

(7) 次期ネットワークへの段階移行

本市は松阪市 IaaS をはじめとするサーバ仮想化基盤の採用を積極的に実施し、システム全体の効率化を強く推進している。本調達において、ネットワークシステムについても仮想化技術を採用し、さらなる効率化を推進する。

具体的にはネットワーク機器のリソースを最大限に活用できるよう、コアスイッチや L3 スwitch を仮想化技術やスタック技術を積極的に用い、冗長化要件を確保しながら最大限リソース利用ができるように構成する。

3.4. システム構築・移行に関する要件

本システムの構築及び移行については以下の要件を満たすようにすること。

(1) システム設計

ネットワークシステムの設計、構築および稼働確認を行う。付帯する作業についても本調達範囲に含めること。また、システム構成・設定に関する情報を取りまとめた文章を作成し、さらにシステム構成などについて本市担当者へ説明を行うこと。

(2) システム詳細設計

本仕様書に定義する各要件を満たすことを前提とし、より信頼性や柔軟性の高い設計案があれば受注者から提案し、本市の了承を得たうえで積極的に詳細設計を行うこと。

(3) システム構築

ネットワーク機器等を更新するにあたって、更新や移行に関する設計作業、および機器設置作業を行う。

(4) ネットワーク回線敷設作業

本庁舎の各フロア、各分館、各別棟、松阪市民病院、各地域振興局、各出先機関の無線 LAN システムに必要な UTP ケーブルの新規敷設と既存有線 LAN の変更に伴う UTP ケーブルの敷設と機器ラック等の設置を行う。また、既存有線ケーブルの撤去処分を行う。

(5) 現行機器運用と並行した移行作業

機器の設置場所が複数拠点に及ぶことから、旧機器から新機器への入れ替えを順次行うこと。ネットワーク構成の変更及び移行に伴い、各拠点で利用している業務

システムの利用に影響の出ないこと。特に住民サービスに直結する窓口系システムにおいては、移行後の正常動作を確認すること。また、既存システムに影響を与えた場合は受注者において解決すること。

(6) クラウドサーバの利用

各システムの稼働に必要なとなるサーバ仮想マシンは、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。）に構築を行うこと。現在本市と松阪市 IaaS は 100Mbps の帯域で利用しているが、1Gbps まで拡張を予定している。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、稼働に必要なリソースを割り出し報告すること。リソース不足によってシステムが不安定な状態となった場合は、受託者の負担でシステムが安定して稼働する状態までリソースを増強させること。

なお、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、契約期間中に必要となる松阪市 IaaS の利用料は別途提示する「松阪市 IaaS 単価表」にて算出し本見積に含めること。また、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の利用で必要となる松阪市 IaaS の利用料については更新業務の範囲内とし、受託者が松阪市 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、本市情報企画課に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、更新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、障害時の責任分界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。

4. ネットワーク拡張機能

本調達により導入するシステムは、将来、利用を想定している機能が必要になった場合でも対応できるようにそれぞれ機能を有すること。

5. 構築要件

5.1. 更新業務

更新業務実施については、本市が了承したスケジュールを遵守すること。

5.1.1. 更新業務実施条件

- ・ 現行ネットワークから次期ネットワークへの移行にあたっては、現行ネットワークの安定稼働に類し、業務の継続に影響を与えることなく実施すること。
- ・ ネットワークの安定した稼働及び業務の継続に影響を与えることがないように安全で確実な作業を優先すること。
- ・ 担当職員が承認した時間を除き、現在稼働中のネットワークの全サービスを停止することなく、移行・導入すること。
- ・ ネットワークの停止に伴う作業が発生する場合には利用者の業務への影響を最小限にするため、土日及び休日を作業実施日の基本とし、その他平日においては勤務時間外で検討すること。また、停止日時及び停止による影響範囲について本市の承認を得ること。
- ・ 機器の搬入及び設定作業について利用者の業務に支障を与えないように対応すること。また、搬入の際に発生する廃材の処理に必要な全ての経費は本作業の費用に含めること。導入する機器は事前に機器へ設定作業を実施しておくこと。

- ・ 既存システムから段階的に移行することとなるため、移行の手順については、事前に検証を実施した上で、原則業務に影響がないような手順を確立すること。また、その移行計画を作成し、事前に本市の了承を得ること。
- ・ 機器導入作業時、設置個所の作業前、作業後の写真記録を取得し、後に本市へ提出すること。
- ・ 本委託業務における要員の配置や連絡先等を記した体制図を作成すること。
- ・ 移行・導入の際にネットワークに影響を与える事態が発生する場合には、事前に本市に連絡をすること。
- ・ 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うえで、早急に本市に報告を行うこと。
- ・ 移行・導入作業で不足の事象により作業が中断した場合は、次の工程に影響が出ないように迅速にその原因を明らかにしたうえで作業を再開できるようにすること。

5.1.2. 端末移行業務実施条件

ネットワーク再構築に伴い必要となる以下の端末設定と動作確認を実施すること。

(1) 端末設定

- ・ IP アドレス等のネットワーク設定
- ・ 無線 LAN 接続設定
- ・ 資産管理ソフトの設定
- ・ Web コンテンツフィルタ設定
- ・ ウイルス対策ソフトの設定

(2) 対象端末

本庁、各分館、各別棟、松阪市民病院、各地域振興局、各外局の全ての端末（シンクライアント端末含む）1800 台を対象とする。

(3) その他

- ・ シンクライアント端末の設定については、シンクライアントシステム保守委託事業者と十分に協議を行い、移行設計を行うこと。
- ・ 各端末において利用が必要な業務システムの動作確認を行うこと。
- ・ その他動作確認が必要なシステム等については、本市と十分に協議したうえで、動作確認を行うこと。

5.1.3. 移行

5.1.3.1. 移行計画書の策定

移行について移行計画書として提示し、移行前までに本市職員と協議を行い、了承を得ること。また、了承された移行計画書に基づき、進捗管理を確実に実施すること。

(1) 移行計画書を策定するうえでの留意点

- ・ 移行計画は現行ネットワークの安定稼働及び業務の継続に影響がないこと。
- ・ 稼働システムのスケジュールを考慮し、可能な限り影響を少なくした移行計画をすること。

(2) 移行計画書に記載が必要となる項目は以下のとおりである。

- ・ 移行概要
- ・ 作業項目
- ・ 移行対象
- ・ 移行スケジュール
- ・ 移行体制
- ・ 移行判定

5.1.3.2. 移行手順の作成

- (1) 準備作業、移行・導入作業及び検証等を対象とした移行手順を作成すること。移行・導入作業の手順に記載した作業が正しく行われていることの確認を含めること。
- (2) 準備作業、移行・導入作業及び事後作業等を対象としてタイムチャートを作成すること。
- (3) 関係者を含む作業体制図、連絡先一覧を作成すること。
- (4) トラブルが発生した場合に切戻しを行う必要があるか検討の上、必要に応じて切戻し手順を作成すること。

5.1.3.3. 移行スケジュール

受注者が移行スケジュールを提示すること。移行スケジュールの作成にあたっては以下を考慮すること。

- (1) 稼働システムの繁忙期、その他イベントなど
- (2) 本市が実施する現行 PC の変更作業項目を洗い出し、実施期間を見積もったうえ、本市と協議し調整すること。

5.1.3.4. 移行判定

移行時の各チェックポイントにおいて、移行判定基準を設けること。また、各移行判定

基準について、実績値を報告し、移行作業の実施について本市の承認を得ること。

5.1.3.5. 移行・導入作業の実施

- (1) 本番稼働への影響がないように移行・導入作業を実施すること。
- (2) 移行・導入作業において、トラブル等が発生した場合、移行手順書に従って関係者に連絡を行うこと。
- (3) 移行導入作業の結果について、速やかに報告し、本市の承認を得ること。
- (4) 移行導入作業は原則として受注者において実施すること。ただし、担当職員の立会いについてはこの限りではない。
- (5) 平行稼働期間中の既存を含む本ネットワーク構成製品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、代替機への交換などを実施し、迅速に正常な状態に復旧させること。

5.1.3.6. 移行作業の進捗報告

移行計画書に記載されたスケジュールに基づき作業を実施し、定期的または本市の求めに応じて進捗状況の報告を行うこと。

5.1.4. 試験

各試験項目については、スループット、冗長性、遅延などの試験項目の検討を行い、単体試験・区間試験・総合試験などの試験計画書を作成すること。

ネットワーク機器の導入後は各拠点で試験を実施し、その結果の評価を行い本市の了承を得ること。

また、更新機器の調達にあたっては、事前に設計内容について本市の了承を得ること。

対象は各外局を含む全拠点とする。必要に応じて再試験等を実施すること。ただし、各試験の計画・実施にあたっては、本市の了承を得てから行うこと。

また、第一別棟設置のコアスイッチ及び下記システムに関連するネットワーク機器を更新した際は、関連する全ての端末で下記記載のシステムの正常動作確認を実施すること。

- ・税務総合システム
- ・住民情報システム
- ・介護保険システム
- ・後期高齢者医療システム
- ・戸籍システム
- ・自動交付システム

- ・住民基本台帳ネットワークシステム
- ・総務管理システム（職員ポータル）
- ・その他、本市が指定するシステム

5.2. 既存機器の回収・管理

既存機器は現地から回収し、初期化及び完全にデータを削除すること。リース会社への搬出は 1 回目の搬出のみ既存納入業者が費用を負担するが、複数回に分割して搬出する場合は本作業の費用として含めること。

5.3. 業務実施体制

構築業務を実施する体制については、統括責任者・リーダー・サブリーダーで構成された構築体制であること。また、業務体制の中には、Cisco 技術認定資格 CCIE を所持した者を参画させること。

5.3.1. 統括責任者

(1) 役割

構築業務および運用保守業務全体の業務実施状況を管理する者である。

(2) 要件

過去 10 年以内に、全庁ネットワークの設計、構築又は運用実績があり、ネットワーク設計、構築業務経験 10 年以上を有する、受託者の社員であること。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、本委託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。

(3) 留意事項

他業務との兼務を認める。

契約時に職務経歴書を提出すること。

5.3.2. 案件担当リーダー

(1) 役割

本委託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。

(2) 要件

過去 10 年以内に、全庁ネットワークの設計、構築又は運用実績があり、ネットワーク設計、構築業務経験 3 年以上を有する受託者の社員であること。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、本委託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。

(3) 留意事項

本委託業務に含まれる内容ごとに担当リーダを配置しても良い。ただし、複数の担当リーダ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良い）。
他業務との兼務を認める。

5.3.3. 案件サブリーダ

(1) 役割

統括責任者及び担当リーダの指示の下、業務に従事する者である。

(2) 要件

過去 10 年以内に、全庁ネットワークの設計、構築又は運用実績があり、業務経験 2 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、本委託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。

(3) 留意事項

必要に応じて配置すること。

6. 工事要件

6.1. 工事基準等

- (1) 本工事の着工前には本市と十分な打ち合わせを行い、協議の上、施工計画書、施工図、工事工程表を作成し、承認を得た後に施工すること。
- (2) 本工事の受託者は、安全管理体制表及び作業者一覧表を本市に提出すること。
- (3) 請負者は、施工に際し施工現場周辺並びに他の構造物及び施設などへ影響を及ぼさないように施工すること。また、影響が生じた場合にはただちに本市に通知しその対応方法等に関して協議すること。また、損傷が請負者の過失によるものと認められた場合、請負者自らの負担で現状復帰すること。
- (4) 本工事の施工前後の写真を撮影し、提出すること。

6.2. 工事詳細

6.2.1. 光ファイバーケーブル工事

- (1) 第 1 別棟 2 階マシン室から各建屋間光ファイバーケーブルは、既設を用いても良いが通信不良があった場合は修繕または再敷設を行い、その費用は本調達に含めること。基幹の光ファイバーケーブル、特に 6 階の部分について、ケーブル切断防止のための保護を行うこと。
- (2) 機器更新に伴い、光パッチコードの交換を行うこと。

- (3) 第1別棟2階機械室内の新規19インチラックから既設光スプライスユニットへコード集合型光ケーブルを配線、接続を行うこと。
- (4) 光パッチコードには、両端の接続先がわかるようにラベリングを行い、導入後のメンテナンス性を高めること。
- (5) 新規配線には、環境配慮型ケーブルを使用すること。

6.2.2. UTP ケーブル工事

- (1) 本市が指定する機器収納ボックスより UTP ケーブルを配線すること。特に記載なき場合はエンハンスドカテゴリ5規格相当の部材を使用すること。
- (2) 第1別棟2階マシン室のサーバスイッチから各サーバに対して UTP ケーブルを配線すること。
- (3) 各フロアスイッチの集約に伴い、プリンタ向けの UTP ケーブルを配線すること。
- (4) 庁舎の既存 LAN 配線を把握し、既存配線を有効利用しながら新規配線を追加すること。
- (5) 新規配線には、環境配慮型ケーブルを使用すること。
- (6) 情報コンセントは、Cat5e 1口 シャッター付を使用すること。
- (7) 全ての RJ45 プラグは、爪折れ防止対策が施されていること。(ブーツ取り付けによる爪折れ防止は不可)
- (8) UTP パッチコードには、両端の接続先がわかるようにラベリングを行い、メンテナンス性を高めること。
- (9) 階渡り配線に必要な貫通穴は施工後耐火処理を必ず施すこと。
- (10) UTP ケーブルの敷設に際し、露出配線を行う場合はケーブル保護を行うこと。
- (11) 不要な UTP ケーブル、特に撤去した既存ケーブルは、本市と協議のうえ撤去を行うこと。

6.2.3. 第一別棟マシン室19インチラック設置工事

- (1) 第1別棟2階マシン室内に19インチラックを3架新設すること。
- (2) 転倒防止策として、架台による耐震固定を行うこと。

6.2.4. 保健センター19インチラック設置工事

- (1) 保健センター2階に19インチラックを1架新設すること。
- (2) 転倒防止策として、耐震固定を行うこと。
- (3) 健康センターは平成28年度竣工予定であり、施工業者と協議を行いながら工事をすすめること。

6.2.5. 第1別棟マシン室 電源コンセント工事

- (1) 第1別棟2階マシン室内分電盤より更新機器に対し、必要に応じて電源ケーブルを配線し、コンセントを取り付けること。
- (2) 更新機器に必要な回路が不足する場合、分電盤回路の増設を行うこと。
- (3) 分電盤改造に必要な費用は、本調達に含めること。
- (4) 分電盤及びコンセントにラベリングを行い、メンテナンス性を高めること。

6.2.6. フロア用機器収納ボックス

- (1) 既設フロア用機器収納ボックスを用いてもよいが、更新機器設置に必要な場合は機器収納ボックスを新設又は交換をすること。
- (2) 機器収納ボックス新設に伴い電源工事が必要な場合は、その費用を含めること。
- (3) 更新機器の設置に必要な取り付け金具は、調達に含めること。

6.2.7. 無線 LAN 機器工事

- (1) 機器収納ボックス内に給電スイッチを設置し、無線アクセスポイントへ給電を行うこと。
- (2) 無線アクセスポイントの設置場所については、十分協議の上設置を行うこと。
- (3) アクセスポイントの設置は天井面または壁面として設置すること。
- (4) 無線 LAN 機器設置場所の無線事後サーベイを実施すること。

6.2.8. 無線 LAN 用 UTP ケーブル工事

- (1) エンハンスドカテゴリ 5 規格相当の部材を使用することとし、エンハンスドカテゴリ 5 規格については、TIA/EIA-568B を適用すること。
- (2) 新規配線には、環境配慮型ケーブルを使用すること。
- (3) 無線アクセスポイントへの端末処理は、RJ45 プラグにて成端を行うこと。
- (4) RJ45 プラグは、爪折れ防止対策が施されていること。(ブーツ取り付けによる爪折れ防止は不可)
- (5) UTP ケーブルには、両端の接続先がわかるようにラベリングを行い、メンテナンス性を高めること。
- (6) 無線 LAN 不具合時のバックアップ用に、無線アクセスポイント設置場所付近に情報コンセント (1 口) を設置すること。但し、既設の情報コンセントがある場合はその限りではない。

6.3. 仕様部材等仕様

機器仕様詳細は別紙を参照すること。

6.4. 配線施工後の試験

- (1) 配線施工後の検査は、ケーブルテスター等で以下の内容を測定すること。
- (2) UTP ケーブルの性能試験は専用のケーブルテスター（参考：FLUKE 社 DTX1800 同等品以上）で測定し、測定データを試験結果として提出すること。
- (3) 光ケーブルの性能試験は専用のケーブルテスター（参考：FLUKE 社 DTX1800 同等品以上）で測定すること。試験種類は挿入損失法（パワーメータ試験）とし、測定器から抽出した測定データを試験結果として提出すること。
- (4) 電源ケーブルの性能試験は、絶縁抵抗試験、電圧試験を行い、試験結果を作成すること。

7. 構築業務完了報告

7.1. 提出ドキュメントの作成

- (1) 本委託業務を実施した結果、別紙の一覧によるドキュメントを提出すること。また、使用する機器名及びシリアルナンバー等の管理情報が変更となった場合、本市の承認を得たうえで必要なドキュメントを更新し提出すること。ドキュメントは、紙データ及び電子データとする。

7.2. 現行運用業者からの引き継ぎ業務

本委託業務開始後、速やかに引継ぎ計画を本市に提示すること。

7.2.1. ドキュメントの受領

- (1) 業務内容
現行運用業者が本市に納品したドキュメントを受領する業務である。
- (2) 業務実施条件
ドキュメントの受領については、本市の指定する場所及び日時にて実施すること。
- (3) 留意事項
内容についての質問は、本市もしくは現行運用業者に対して行うこと。
各ドキュメントの情報については、必要に応じて現行運用業者にて最新化を実施する。

8. ネットワーク監視・運用

8.1. 目的

本ネットワークを正常に稼動・運用させ、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。

8.2. サービス概要

本庁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対応への連携を行うこと

8.3. ネットワーク監視の範囲

本調達にて導入した製品を範囲とし、下記の監視項目を範囲とする。

種別	監視項目			
	死活監視	SNMP-Trap 監視	リモート ログ取得	性能監視
コアスイッチ	●	●	●	●
レイヤ3スイッチA	●	●	●	●
レイヤ3スイッチB	●	●	●	－
レイヤ3スイッチC	●	●	●	－
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	●	－	●	－
インターネット接続用ルータ	●	●	●	●
WAN 回線負荷分散装置	●	●	●	●
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	●	●	●	●
無線 LAN 管理サーバ	●	●	●	●
無線 LAN ロケーション管理サーバ	●	●	●	●
種別	監視項目			
	死活監視	SNMP-Trap 監視	リモート ログ取得	性能監視
ネットワーク認証サーバ	●	●	●	●
無線コントローラ	●	●	●	●

●：監視対象 －：監視対象外

8.4. 履行場所

受託会社。

8.5. 保守対応時間

24 時間 365 日。

(※定期メンテナンスなどの時間帯は除く)

8.6. 連絡体制

以下の連絡体制を整えること。

- 障害連絡窓口

- (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。

8.7. リモート接続・運用要件

本業務を実施に当たり、リモートから業務を実施する場合には、下記要件を満たすこと。

- (1) 本市とリモート保守拠点間を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は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) 本市とリモート保守拠点を接続するために受託者は市の保有する回線とは別に回線を準備すること。また、その回線は、今回整備するインターネット用接続機器を経由すること。その回線費用等は入札金額に含めること。

8.8. 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。

表 8.8-1 監視変更対応

項目	内容
対象機器の追加	新たに対象機器を追加します。
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。

表 8.8-2 計画停止・停電対応

項目	内容
作業日時	申請いただい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。

8.9. ネットワーク監視運用内容

以下のサービスを提供すること

(1) 死活 (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は以下の通りとする。

表 8.9-1 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	3 秒	3 回
Ping OK	死活 (Ping) 応答の成功			

(2) ポータル提供

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

ポータルへ表示される内容は、システム単位で提供し、過去に発生したアラート閲覧、パフォーマンスの表示については 90 日以上前まで可能なこと。

収集したパフォーマンスデータは下表に示す 4 種類の表示形式にて提供でき、これらのグラフはポータルにアクセスすることで参照することができること。

また、モニタリング静観依頼などのリクエストの閲覧・登録・検索などもポータルから可能なこと。

表 8.9-2 ポータル提供仕様

種別※1	説明	データ保存期間
1 時間グラフ	過去 1 時間のサマリグラフを表示	90 日以上
1 日グラフ	過去 1 日のサマリグラフを表示	
1 週間グラフ	過去 7 日のサマリグラフを表示	
1 カ月グラフ	過去 30 日のサマリグラフを表示	

※1：期間指定も可能なこと

(3) 月次レポート

① サービス内容

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サマリー等を月次のレポートにまとめ、ポータルより提供すること。

② 仕様

月次レポートの項目については、下記の通りです。

- ・月次サマリー
- ・モニタリングのアラート発生状況
- ・インシデント対応状況一覧

③ サービス条件

月次レポートのダウンロード可能期間は、発行より 12 ヶ月間可能なこと。

毎月第 10 開庁日日までに前月分についての月次レポートがダウンロード可能なこと。

(4) 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います。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、後述の「保守」と自動連携しログ解析、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です。

表 8.9-3 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、保守部門へ対応を自動的に引き継ぐこと。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。

(5) SNMP トラップ

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。

表 8.9-4 SNMP トラップ仕様

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：アクセス層スイッチや定期的に 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。

(6) パフォーマンス

① サービス内容

対象機器の管理 IP アドレスに対して、モニタリングアプリケーションから定期的に特定プロトコルを用いてパフォーマンス情報を収集すること。

収集した情報はブラウザ経由でポータルにアクセスし、ユーザ画面からサマリー情報を参照することが出来ること。また、モニタリング対象項目に閾値を設定した場合はアラートとして検知し、異常状態および正常状態へ復旧した際に本市との取決めに従い、本市へ連絡すること。

② 仕様

異常状態と正常状態については、以下のように定義する。

表 8.9-5 パフォーマンス仕様

カテゴリ	パフォーマンス取得項目	備考
ネットワーク機器	CPU 使用率、メモリ使用率、インターフェーストラフィック	インターフェーストラフィックはポート単位で取得
セキュリティ機器	CPU 使用率、インターフェーストラフィック、セッション数、バージョン情報	

③ サービス条件

ネットワーク環境やアラートが頻発する場合や継続的にパフォーマンス情報が閾値を超過する場合など、状況に応じてパラメーターをチューニングすること。

9. セキュリティ運用

9.1. 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) 既存のセキュリティ対策システムでは検知できない攻撃によって引き起こされる情報漏洩、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。

9.2. セキュリティ運用範囲

セキュリティ運用の範囲は以下の物とする。

- ・ インターネットに接続するファイアウォール B： 1 セット

9.3. セキュリティ運用概要

以下のセキュリティ運用を実施すること。

- (1) 通信ログの分析レポートの提出（毎月 1 回/メール等電子データによる提出）
- (2) 分析レポートの報告会の実施（毎月 1 回/本市役所内）
- (3) セキュリティ監視（随時/24 時間 365 日実施可能/リモート作業）
- (4) リモート緊急対応（随時/24 時間 365 日実施可能/リモート作業）
- (5) シグネチャ・設定管理（随時）
- (6) バージョンアップ/パッチ適用対応（適用必要時/リモート作業）
- (7) 対象機器の稼働監視（随時/24 時間 365 日）
- (8) 上記業務内容に対する Q&A（営業時間内/メール・電話等）

9.4. セキュリティ運用内容

(1) 通信ログの分析レポートの提出

- ・ 監視対象機器の稼働状況およびアプリケーション分析状況を、月次レポートにて報告すること。
- ・ レポート作成の過程において通信ログ・その当時のセキュリティトレンドを踏まえ全体の傾向分析もおこなうこと。なお、取得した通信ログは、第三者に開示してはならない。

(2) 分析レポートの報告会の実施

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
- ・ 最新の国内外セキュリティトピックと本市の環境を照らし合わせた観点でのセキュリティに対するアドバイス
- ・ 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ストピックの説明

(3) セキュリティ監視

緊急のセキュリティインシデントの兆候、発生を検知するため以下の 24 時間 365 日セキュリティ監視を行うこと。

- ファイアウォールログ分析監視
 - ・ 運用者で独自に管理されたブラックリスト IP アドレスと、監視対象機器のログで相関監視を実施し、庁内からの不正通信を検知すること。
 - ・ 定常的な通信と異常な通信を分析し、ワームなどによる攻撃の兆候を監視すること。
- アンチウイルス監視
 - ・ ネットワーク上を流れるウイルス感染ファイルや、ウイルスが検知され監視対象となるネットワーク上においてウイルスが拡散されているかを監視すること。
- IPS (IDS) /Anti Spyware 監視
 - ・ マルウェア感染監視。運用者のナレッジをもとにマルウェア配布サイトや悪意のある第三者の管理するサーバとの接続を監視すること。
 - ・ ゼロデイ脆弱性の攻撃監視。最新の脅威情報を元に攻撃通信や攻撃成功を監視すること。
 - ・ 運用者のナレッジをもとにブラックリスト IP アドレスと IPS(IDS)のログから相関監視を実施すること。

(4) リモート緊急対応

セキュリティインシデントにおいて外部からの攻撃及び、庁内から庁外への意図しない通信が確認された場合、あらかじめ決められた内容、もしくは本市と協議を行い監視対象機器に対してリモートより対処可能な設定を速やかに対処すること。

主な対処方法として ACL の設定変更や URL フィルタリングでの遮断設定、IPS での遮断設定などを想定している。

セキュリティインシデント監視に基づき検知された以下の内容が含まれたインシデント内容を連絡すること。

表 9.4-1 インシデント通知内容

NO	通知項目	説明
1	イベント発生日時	イベントの発生日時
2	イベント概要	イベントの発生原因
3	送信元情報詳細	送信元 IP アドレス情報、国、ポート 等
4	送信先情報詳細	送信先 IP アドレス情報、ターゲットポート 等
5	補足事項	必要に応じ補足事項を連絡すること。

あらかじめ本市の環境において脅威のあるイベントについてはリアルタイムに検知し以下の内容を都度通知すること。

表 9.4-2 リアルタイム検知通知内容

NO	通知項目	説明
1	イベント発生日時	イベントの発生日時
2	送信元アドレス情報	送信元 IP アドレス 等
3	送信先アドレス情報	送信先 IP アドレス 等
4	イベント ID	イベント ID
5	発生イベント名	検知イベント名
6	発生イベント詳細	検知イベントの詳細情報

(5) シグネチャ・設定管理

- 最新の攻撃に対応できるようメーカから提供される最新のシグネチャ情報を日々収集して更新作業を迅速に対応すること。
- 最新のシグネチャ情報の分析を行い、本市の環境に適したシグネチャ設計を実施し、その内容に問題が生じないことを確認したうえで適用作業を実施すること。
- 緊急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。
- セキュリティインシデント発生時に本市にインシデントを通知した結果、該当するインシデントが明らかに無効である場合、誤検知と判断し、速やかに本市の環境にシグネチャ設計と適用作業を実施すること。
- 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、以下の内容

を通知すること。

表 9.4-3 作業事前連絡内容

NO	通知項目	説明
1	作業概要	作業の概要を明記すること。
2	作業理由	ネットワーク通信に影響がでる場合のその根拠となる情報。と作業を行うことでどのようなセキュリティインシデントに対応出来るかを明記すること。
3	作業希望日時	作業可能な希望日時を提示すること。
4	作業予定時間	おおよその所要時間を明記すること。

- ・ 作業実施後に以下の内容を通知すること。

表 9.4-4 作業事後連絡内容

NO	通知項目	説明
1	作業概要	作業の概要を明記すること。
2	作業理由	ネットワーク通信に影響がでる場合のその根拠となる情報と作業を行うことでどのようなセキュリティインシデントに対応出来るかを明記すること。
3	作業終了日次	作業完了日時を明記すること。

(6) バージョンアップ/パッチ適用対応

- ・ 監視対象の新バージョン及びパッチリリース情報を収集し、本市の環境への影響内容を精査して適用が必要と判断した場合、適用作業を随時リモートで実施すること。

(7) 対象機器の稼働監視

- ・ 監視対象機器に対して稼働確認を行い、障害発生にアラート内容の確認と一次切り分けを実施すること。

(8) 上記業務内容に対する Q&A

- ・ 専門の窓口を開設し、電話並びに電子メールによる問合せ対応を実施すること。
- ・ 本運用範囲に対する Q&A を平日 9:00～17:00 で実施すること。

10. 運用支援

10.1. 目的

本ネットワーク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ネットワークを提供することを目的とする。

10.2. 運用支援概要

本ネットワーク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。なお、本仕様書における支援業務とは、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、等の運用に関する支援を指し、大幅な構成変更等に伴う設定変更は含まない。

10.3. 運用支援内容

- (1) 月次の運用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、案件担当リーダー以上の担当者が同席すること。
- (2) 年間 60 回程度、開庁時間から閉庁時間の間で訪問による技術相談および技術支援を実施すること。但し、時間内であっても本市が与えた技術相談および技術支援が完了した場合は終了しても良い。また、それ以外に本市が要請した場合、各種会議及び打合せに参加し、技術的な支援及びアドバイスを実施すること。
 - ① ネットワーク機器及びセキュリティ機器の設定、追加に対する技術支援
 - ② 障害に対する相談、技術支援
 - ③ ネットワーク稼動状況の確認（トラフィック分析、ログ検査、問題時の対応）
 - ④ 年 2 回の法定点検によるネットワーク停止、起動支援
 - ⑤ 年 2 回程度の資産管理システム及び Web コンテンツフィルタサーバのソフトウェアパッチ適用作業
- (3) メールおよび電話による Q & A 対応
- (4) ネットワークセキュリティの課題に対する対策検討および改善策検証の支援
- (5) 年に一回程度の組織変更に伴う、ネットワーク構成変更支援（AD のユーザー情報及び OU の変更作業を含む。）
- (6) 月次定例会での作業報告実施

(7) 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

- ① ネットワーク仕様の検討支援
- ② ネットワーク変更の計画支援
- ③ ネットワーク機器の設定変更支援

11. 保守

11.1. 目的

本ネットワークを正常に稼動・運用させるため、構成製品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。

11.2. 保守概要

本ネットワーク構成製品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、全ての機器について現地機器交換作業を含むこと。

11.3. 保守の範囲

本調達にて導入したネットワーク構成製品。(ネットワーク機器・アプライアンス製品・ソフトウェアほか)

11.4. 履行場所

本ネットワーク導入に関する全施設。

11.5. 保守対応時間

以下の対応を行うこと。

24 時間 365 日オンサイト保守とする。

11.6. 連絡体制

以下の連絡体制を整えること。

- ・ 障害連絡窓口
- (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) 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。

11.7. 保守業務内容

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、障害の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。

表 11.7-1 初動駆け付け時間

対応時間	拠点	駆け付け時間
開庁時間内 (平日 8:30～17:15)	本庁	60 分以内
	各地域振興局	90 分以内
	その他	120 分以内
開庁時間外	本庁	120 分以内
	各地域振興局	150 分以内
	その他	180 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に了承を得ること。
- ・ 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

- ・ 障害箇所の特定が出来ていない場合でも、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。

11.8. 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、冗長化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。

11.9. 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。

部品の交換を行なった場合には、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。

11.10. 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) 以下に起因する受託者以外の利用による業務対象機器の不良の場合
 - ・ 故意、過失による場合
 - ・ 業務対象機器の取扱いに関する説明書に基づかない業務対象機器の使用又は取扱いによる場合
 - ・ 設置条件、使用電源条件等、業務対象機器の仕様又は条件に反した使用による場合
 - ・ 修理若しくは改善又は請負者が指定する方法以外の方法による業務対象機器の移動に伴う不良の場合
 - ・ 自然災害による機器不良の場合
- (2) 受託者以外による業務対象機器の仕様変更(改造など)に伴う作業
- (3) 受託者以外による将来の障害発生を予防するために行われるオンサイトでの作業
(障害の修復作業に付随してなされる場合を除く)

以上