令和５年度

山元町庁内業務インフラDX推進事業業務委託

提案要求書

令和5年12月

山元町

目次

1. はじめに

山元町（以下「本町」という）では平成 28 年に自治体情報強靭化対応として、インターネット接続系ネットワークと LGWAN 接続系ネットワークを分離した環境を購入した。その環境の機器保守期限を迎えることから、システムの更新が必要である。

庁内情報システムの3層分離環境を維持し、インターネット接続系システム及び LGWAN 接続系システムの更改及び庁内無線ネットワーク環境構築を構築対象範囲とする。

なお、基幹系システムの更改については本調達の範囲外とする。

2. 目的

本町は、平成 28 年に国の示す「三層の対策」の考え方のもと、セキュリティ強靭化対応として、インターネット接続系と LGWAN 接続系のネットワークを分離した環境を整備した。 現在、当時整備したネットワーク機器等について更新時期を迎えているが、単なる機器更改とはせず、現環境で抱える課題の解消と、時代の求める DX の取り組みの一つとして、職員の働き方改革を実現すべく、今回、電子決裁・コミュニケーションツールの導入、テレワーク環境・庁内無線環境の整備等、庁内業務インフラを刷新するため本事業を実施する。

3. 本町の抱える課題

3.1. 課題

本町の抱える課題に対して、具体的かつ実現可能な解決策を提示すること。

なお、1、4、5、6は次項で掲げる必須要件を満たすこと。

項番	項目	課題	解決策（例）
1	業務環境	業務に応じて複数端末を往復しなければならない。	一端末で複数業務が可能：インターネット接続系・LGWAN 接続系
2	パソコン処理速度	パソコンの劣化等により処理速度が遅い。	高スペックなパソコン導入で軽快に。
3	電子決裁	紙による決裁事務が主。	グループウェア(Garoon 利用)によるワークフロー化。
4	メール運用	国・県からの新着メール（LGWAN）は座席を移動しないと確認できず、すぐに気づけない。	自席の端末で LGWAN メールも確認可能。
5	コミュニケーション	対面、電話が基本。打合せ場所確保が必要でコミュニケーションがとりづらい。	職員間の Web ミーティング・チャット機能により職員間のコミュニケーションの活性化。

6	スケジュール管理	職員私用の手帳とグループウェアによる 2重管理。	グループウェアと Microsoft 365 間 でスケジュール連携により、私用スマートフォンでもスケジュールの確認が可能。
7	登庁必須	職場に来ないと仕事ができない。	テレワーク環境の実現により自宅でも職場と同じ業務環境を実現。
8	機器（パソコン）	ノートPC の画面が小さく、作業効率が悪い。	主要機器のタブレット化、大型ディスプレイへの出力により可視範囲拡大。
9	有線ネットワーク	業務場所が固定されている。	庁内の場所によらず、どこでも仕事ができる無線環境。
10	紙を主体とした事務	印刷、製本時間のロスが大きい、用紙代が膨大。	電子化により印刷製本時間、紙使用量の削減。

3.2. 必須要件

課題に対する必須要件は以下とする。

項番	項目	必須要件
1	業務環境	・インターネット接続系を主業務環境とすること ・インターネット接続系と LGWAN 接続系が1つの端末でセキュアに接続可能な環境であること ・インターネット接続系については、個人ごとにソフトウェアをインストールできること ・インターネット接続系、LGWAN 接続系ともに各接続系のネットワークプリンタから印刷処理が可能なこと
4	メール運用	・LGWAN 接続系で受信したメールをインターネット接続系に転送すること ・インターネット接続系及びLGWAN 接続系で、組織（班）及び個人メールの送受信が可能なこと ・インターネット接続系から、LGWAN 接続系へのメールも送信が可能なこと ・メール受信時、ポップアップによる受信確認が可能なこと ・組織（班）メールアドレスはインターネット接続系及び LGWAN 接続系において同一のものを用意すること ・個人メールアドレスはインターネット接続系及び LGWAN 接続系において同一のものを用意すること

5	コミュニケーション	・職員と議員間のチャットなど直接のコミュニケーションは不可とする
6	スケジュール管理	・許可された私用スマートフォンからスケジュールの確認が可能なこと

4. 調達要件

4.1. 調達要件及び構成内訳

(1) 案件名

令和5年度山元町庁内業務インフラDX推進事業業務委託

(2) 構成内訳

以下の物品を調達するものとし内訳については、構成内訳詳細にて示すものとする。

1. インターネット接続系・LGWAN 接続系各々のサーバー仮想化基盤 一式
2. バックアップシステム 一式
3. インターネット接続系で必要となる機能を提供するサーバー群 一式
4. LGWAN 接続系で必要となる機能を提供するサーバー群 一式
5. 3 層分離環境間ファイル受け渡しシステム 一式
6. 3 層分離を考慮した有線ネットワーク機器 一式
7. LGWAN 接続系・インターネット接続系の無線ネットワーク機器 一式
8. その他の必要物品 一式
9. 私用スマートフォン管理 一式
10. 職員端末 一式
11. 議員端末 一式
12. 保守・監視・運用 一式

(3) 履行期間

構築期間は契約締結の日から令和 6 年 3 月 31 日 までを目途とする。

ただし、議会承認が得られた場合に協議のうえ、契約を変更することができるものとする。

運用引継ぎ期間として引き渡しの日までに職員、議員の運用習熟期間 2 か月程度を設ける

こと。

システム運用開始は令和 6 年 4 月 1 日を目標年、利用想定期間は運用開始から 5 年間とする。

(4) 業者選定方法

公募型プロポーザルにより優先交渉権者及び次点候補者を決定する。詳細は別紙「令和5年度山元町庁内業務インフラDX推進事業業務委託　公募型プロポーザル実施要領」を参照のこと。

(5) 調達方法

初年度保守運用費用を含んだ買い取りとする。

(6) 導入場所

導入場所は本町が指定する下記の通りとする。

a. 山元町役場

b. 町内出先拠点 9 か所

4.2. 技術的要件の概要

(1) 本調達に関わる性能、機能及び技術など（以下「性能など」という）の要求要件（以下「技術的要件」という。）は「5. 調達物品に備えるべき技術的要件」に示すとおりである。

(2) 技術的要件は全て必須の要求要件であるが、代替案を示す場合は本町が判断可能な根拠資料を提出し、本町が認めた場合のみ採用する。

4.3. システム構成イメージ

システム全体の構成イメージは別紙 1 の通りとする。

4.4. 環境情報

(1) 既存のメールリレーについては別紙 2 の通り。

(2) 庁舎内の概略図については別紙 3 の通り

(3) 職員数は 220 名とし、今後 5 年間不変と仮定する。

4.5. 構成内訳詳細

いずれの構成機器も技術的要件を満たすものとする。

構成機器		要求要件	数量
1	インターネット接続系・LGWAN 接続系各々のサーバー仮想化基盤		
仮想化基盤サーバー		インターネット接続系・LGWAN 接続系各々の仮想化されたサーバー群が稼働可能な機能を有すること	1 式
仮想化基盤共有ストレージ及びファイルサーバー		仮想化基盤サーバーの共有ストレージ及びファイルサーバー機能を有すること	1 式
2	バックアップシステム		
バックアップサーバー		仮想化基盤サーバーで稼働するサーバー群及びファイルサーバー、NW機器をバックアップする機能を有すること	1 式
3	インターネット接続系で必要となる機能を提供するサーバー群		
メールサーバー		「@town.miyagi-yamamoto.lg.jp」ドメインを使用し、メールを送受信できる機能を有すること	1 式
メール無害化		インターネット接続系・LGWAN 接続系のそれぞれで冗長化され、メール無害化機能を有すること	1 式
グループウェア		Garoon を導入すること	1 式

セキュリティ・ウイルス対策	職員端末、庁外持ち出し端末、インターネット接続系のサーバーのセキュリティ対策として、EPP、EDR 機能を有した製品を導入し、MDR サービス含めて提供すること	1 式
資産管理	職員端末及び庁外持ち出し端末の情報収集や、リモート操作可能な機能を有すること	1 式
MDM	庁外持ち出し端末のアプリケーション管理や、遠隔ロックする機能を有すること	1 式
ユーザー認証サーバー	インターネット接続系のユーザー管理を可能とする、Microsoft Entra ID と、Active Directory を導入すること	1 式
Microsoft 365 連携サーバー	Microsoft Entra Connect を導入すること	1 式
スケジュール連携	Garoon と Microsoft 365 のスケジュールを連携	1 式
コラボレーションツール	Microsoft Teams を導入すること	1 式
DNS	インターネット接続系の管理システム及び業務システムの名前解決を可能とする内部 DNS を提供すること	1 式
NTP	NTP サーバーとして本調達に係る機器に対し、正しい時刻情報を取得・配信する機能を有すること	1 式
WSUS	職員端末、庁外持ち出し端末及び Windows Server に対し、Windows OS 及び Windows Server OS 、Office のパッチを配信する機能を有すること	1 式
KMS	職員端末、及び WindowsServer の OS のライセンス認証機能を有すること	1 式
4	LGWAN 接続系で必要となる機能を提供するサーバー群	
メールリレーサーバー	インターネット接続系から LGWAN 接続系ドメイン宛のメールを転送する機能及び LGWAN 接続系ドメインに受信したメールをインターネット接続系に転送する機能を有すること	1 式
セキュリティ・ウイルス対策	LGWAN 業務環境及び LGWAN 接続系サーバーのセキュリティ対策として、EPP 機能を有した製品を導入すること	1 式
ユーザー認証サーバー	LGWAN 接続系のユーザー管理を可能とする Active Directory を導入すること	1 式
DNS	LG-WAN 接続系の管理システム及び業務システムの名前解決を可能とする内部 DNS を提供すること	1 式
NTP	NTP サーバーとして本調達に係る機器に対し、正しい時刻情報を取得・配信する機能を有すること	1 式

WSUS	LGWAN 業務環境及び、Windows Server に対し、Windows OS 及び Windows Server OS 、Office のパッチを配信する機能を有すること	1 式
KMS	LGWAN 業務環境及び WindowsServer の OS のライセンス認証機能を有すること	1 式
LGWAN 業務環境	インターネット接続系 の職員端末から接続可能な、財務会計システム等の LGWAN 業務環境を提供すること	1 式
5	3 層分離環境間ファイル受け渡しシステム	
ファイル授受・無害化システム（インターネット接続系-LGWAN 接続系間）	インターネット接続系・LGWAN 接続系の相互でファイルを授受する機能及びファイル無害化機能を有すること	1 式
ファイル授受システム（LGWAN 接続系-基幹系間）	LGWAN 接続系基幹系間での相互でファイル授受機能を有すること	1 式
6	3 層分離を考慮した有線ネットワーク機器	
コアスイッチ	本調達に関わる機器類の相互接続する機能を有すること	2 台
フロアスイッチ	主にコアスイッチと無線 AP 及び一部の有線接続機器との接続機能を有すること	6 台
拠点収容装置	本庁と出先拠点間の接続において本庁側の接続機能を有すること	1 台
拠点接続装置	本庁と出先拠点間の接続において出先拠点側の接続機能を有すること	9 台
ファイアウォール	3 層分離 NW 間の相互接続機能を有すること	1 台
7	LGWAN 接続系・インターネット接続系の無線ネットワーク機器	
無線 LAN コントローラー	無線 AP の集中管理を行う機能を有すること	1 式
無線 LAN アクセスポイント	無線 LAN クライアントが接続できる機能を有すること	34 台
無線 LAN 認証サーバー	無線 LAN クライアントの接続認証機能を有すること	1 式
8	その他の必要物品	
Microsoft 365 ライセンス	Microsoft 365 Business Premium 相当機能を有すること	240 ユーザー
9	庁舎外でのデバイス管理	
Azure AD ライセンス	Azure AD Premium P1 相当機能を有すること	240 ユーザー
10	職員端末	
職員端末	利用想定期間内は職員が快適に利用できるスペックを有すること	220 台

11	議員端末		
議員端末		利用想定期間内は議員が快適に利用できるスペックを有すること	20 台
12	議員端末に関する要件		
通信要件		庁内ネットワークへのアクセスを原則不可とすること	1 式
認証要件		ローカル認証ではなく、Microsoft Entra ID や Active Directory などと連携しユーザー認証を行うこと。	1 式
セキュリティ・ウイルス対策		セキュリティ対策・ウイルス対策として EPP 機能を有すること	1 式
資産管理		端末の情報収集や、リモート操作可能な機能を有すること	1 式
MDM		端末のアプリケーション管理や、遠隔ロックする機能を有すること	1 式
コラボレーションツール		Microsoft Teams を導入すること	1 式
メールシステム		メールシステムとして Exchange Online を利用すること	1 式
13	監視・運用・保守		
保守		導入システムの保守を提供すること	1 式
運用		導入システムの運用を提供すること	1 式

4.6. その他

(1) 技術仕様などに関する留意事項

1 導入予定製品一覧を提出すること。

2 機器又はソフトウェアは、原則として提案時点で製品化されていること。提案時点で製品化されていない機器又はソフトウェアによって提案する場合には、技術的要件を満たすこと及び納入期限までに製品化され納入できることを証明できる書類を添付すること。

(2) 導入に関する留意事項

1 導入までのスケジュールについては、本町と協議の上、その指示に従うこと。

2 導入システムは令和6年 4 月 1 日より運用開始を目標とする。

ただし、履行期間が変更になった場合は、別途協議するものとする。

職員端末の導入は契約日から 4 か月以内に実施することを目標とする。

(3) その他の留意事項

1 本調達システムの費用には、ハードウェア、ソフトウェア、設計、構築、導入及びテスト等の費用を含むこと。

2 搬入、据付、配線、調整、既設設備との接続に要する全ての費用は本調達に含むこと。

3　記載はないが導入業者が必要と想定される作業については、費用も含め本町と協議のうえ実施すること。

5. 調達物品に備えるべき要件（機能要件及び非機能要件）

本調達では「3. 本町の抱える課題」、及び「4. 調達要件」を勘案し、以下に掲げる要件を満たす提案とすること。

5.1. インターネット接続系・LGWAN 接続系各々のサーバー仮想化基盤

仮想化基盤のモデルとして HCI、3Tier は問わないが以下の要件を満たすこと。

i. 仮想化基盤基本要件

(1) サーバーは本町サーバー室に設置するオンプレミス構成とし、SaaS サービスを組み合わせた環境を提供し、効率的なネットワーク構成とすること。

(2) 3Tier 構成の場合、仮想化基盤サーバーが 1 台故障した際でも業務影響なく稼働できるスペックであること。

(3) HCI 構成の場合、ホストが 1 台使用不可となった際に業務影響なく稼働できるスペックであること。

(4) クラスタ管理された仮想化基盤サーバーにおいて、機器停止を伴う障害が発生した場合、正常稼働中の異なる仮想化基盤サーバー上で仮想マシンを再起動させることにより、仮想マシンの可用性を確保するための機能を有すること。

(5) 電源装置が冗長性を備えていること。

(6) 電源装置がホットプラグに対応していること。

(7) コアスイッチとの接続は、10Gbps 以上の通信速度に対応したケーブルで接続し、ケーブル冗長とすること。

(8) 筐体のフロントベゼルに施錠可能なカバーを装着可能なこと。なお、サービス状態やホスト名を文字で表示可能な LCD パネルを有することが望ましい。

(9) データ保護の観点から故障時等で機器交換（パーツ交換）の際、HDD はデータ消去のうえ、廃棄証明書を発行すること。

(10) ハイパーバイザーにより、CPU、メモリ、ストレージ、その他デバイスなどのハードウェアリソースを仮想マシンに割り当て管理する機能を有すること。

(11) クラスタ管理された仮想化基盤サーバー間において、仮想マシンにハードウェアリソースを割り当てる仮想化基盤サーバーの変更(移動)を行う機能を有すること。

(12) セキュリティと安定性の観点から仮想化基盤は汎用 OS を利用せずに仮想化ハイパーバイザーのみで構成すること。

(13) 仮想マシンの構成変更が発生した際に、Windows 仮想マシンに関しては、仮想マシンを停止することなく、仮想 CPU・メモリ・ディスク・NIC の割当量等を動的に拡張できること。

(14) 他の仮想マシンのリソース消費によるサービス影響をうけないよう、仮想マシンに割り当てる CPU 及びメモリのリソースは、物理リソースの予約、上限値設定(制限)、複数仮想マシン間での相対値（シェア値)による設定が可能なこと。

(15) 仮想マシンを稼働させるのに必要十分なリソースを確保すること。また、サイジング根拠を提示すること。

ii. 仮想化基盤管理要件

(1) 仮想環境管理ソフトウェアは、仮想化基盤を構成するハイパーバイザーと同一メーカーが提供する商用製品を利用すること。

(2) ハイパーバイザーを Web ベースの管理画面で一元的に管理する仮想環境管理サーバーを構築すること。

(3) 仮想環境管理サーバーは 2 台以上のハイアベイラビリティ構成とし、ホスト及びハードウェアの障害から保護する機能を有すること。

iii. 仮想化基盤共有ストレージ及びファイルサーバー

HCI 構成の場合、共有ストレージとしての別筐体の調達は不要とするが、以下ストレージ機能要件を満たすこと。

(1) メールスプールは 2TB 以上のストレージ容量を用意すること。

(2) 部署及び個人単位に利用するファイルサーバーは 18TB 以上のストレージ容量を用意すること。

(3) グループウェア（Garoon）のデータ保管領域として 4TB 以上のストレージ容量を用意すること。

(4) 仮想マシンを稼働させるのに必要十分なストレージ容量を確保すること。また、サイジング根拠を提示すること。

(5) 3Tier 構成の場合、コアスイッチとの接続は、10Gbps 以上の通信速度に対応したケーブルで接続し、ケーブル冗長とする。

(6) 仮想サーバー及び仮想マシンのデータストアやログ等の一次領域のストレージ容量は必要分用意すること。

(7) フラッシュのみを搭載したオールフラッシュストレージであること。

(8) HCI 構成の場合は、ノードに搭載された仮想化ソフトウェアのストレージ機能の障害が、仮想マシンのストレージアクセスに影響を与えない構成とすること。

5.2. バックアップシステム

バックアップシステムとして、以下の要件を満たすこと。

(1) バックアップ対象は本調達に含まれる仮想マシン及びサーバーとする。

(2) グループウェアについては、週に1度以上のフルバックアップを取得すること。また、1日1回以上の差分又は増分バックアップを取得し、7 世代以上のデータを保管すること。

(3) BCP として別筐体とすること。

(4) コアスイッチとの接続は、10Gbps 以上の通信速度に対応したケーブルで接続し、ケーブル冗長とする。

(5) ファイルサーバーについては、週に1度以上のフルバックアップを取得し、且つ、1日1回以上の差分又は増分バックアップの取得及び 7 世代以上のデータの保管が望ましいが、ミラーリング構成も可とする。

(6) グループウェアとファイルサーバー以外のバックアップについては月に1度以上とし、3世代以上のデータを自動で保管することが望ましいが、各サーバーの性質に応じて提案すること。

(7) 稼働中の仮想マシンを無停止でバックアップを取得できること。

5.3.インターネット接続系で必要となる機能を提供するサーバー群

インターネット接続系における必要機器について以下の要件を満たすこと。

【メールサーバー】

(1) 「@town.miyagi-yamamoto.lg.jp」のドメインで提供すること。

(2) IMAP4 プロトコルによる Outlook などの一般的な MUA での利用が可能なこと。

(3) OAuth 認証を実装すること

(4) メーリングリストを作成でき、リストのユーザーはメーリングリスト宛のメールを受信できること。

(5) メーリングリストのアドレスを送信元としてリストのユーザーがメール送信できること。

(6) SMTP プロトコルに対応した送信メールサーバーを提供すること。

(7) 送信メールサーバーでメール送信する際に LGWAN 側のメールは LGWAN 接続系へ、その他のメールはセキュリティクラウド側へ振り分けて送信すること。

【メール無害化】

(1) LGWAN 側に送信(リレー)するメールに対して無害化処理を実施するよう設定すること。

(2) 無害化処理についてはメール本文及び添付ファイルを対象とすること。

【グループウェア】

(1) 現在使用しているグループウェア(Garoon)の最新バージョンを導入すること。

(2) スケジュールをコラボレーションツールと同期すること。

(3) 職員(220 名)以上のライセンスを提供すること。

(4) インターネット接続系の職員端末からアクセスが可能なこと。

(5) グループウェアで少なくとも以下機能を実装すること。

a. スケジュール・施設予約

b. 掲示板

c. メッセージ

d. スペース

e. メール

f. アドレス帳

g. メモ

h. ファイル管理

i. ワークフロー

(6) グループウェアを稼働させる仮想マシンのディスク容量は 4TB 以上とすること。

(7) 現行の Garoon(ver3.7)からデータを移行すること。また、移行対象は本町と協議の上決定すること。

【セキュリティ対策・ウイルス対策】

(1) インターネット接続系のサーバー及び職員端末に対するセキュリティ対策・ウイルス対策として、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン(令和 5 年 3 月版)」に沿って EPP 及び EDR・MDR 機能を有すること。

(2) EPP 及び EDR・MDR の対象は以下とする。

	EPP	EDR	MDR (SOC)
インターネット系端末	○	○	○
庁外持ち出し端末	○	○	○
インターネット系サーバー	○	○	○

(3) EPP、EDR の対象 OS として、Windows Server OS 及び Linux Server OS に対応していること。

(4) サイバー攻撃によるマルウェア及びランサムウェア等の脅威のエンドポイントへの侵入を防ぐ EPP の機能を有すること。

(5) EPP はエンドポイントがネットワークに接続していない時にも、エンドポイントの保護が可能なこと。

(6) EPP はシグネチャの更新が不要なこと。

(7) エンドポイントからデータを継続的に収集し、リアルタイムで分析をすることにより、既知又は未知のサイバー脅威を検知し、自動的に対応が可能な EDR の機能を有すること。

(8) EDR により脅威を検知した際に SOC により適切な対処を行う MDR の仕組みを有すること。

(9) 24 時間 365 日体制で MDR プラットフォームの管理及び EDR ログのモニタリングを実施すること。

【資産管理】

(1) 対象端末のログ収集が可能であること。

(2) ハードウェア及びソフトウェア情報を自動収集し、台帳管理できること。

(3) ネットワーク上に存在する各種機器情報を収集・登録し、一元管理できること。

(4) メンテナンスのため端末のリモート操作が可能であること。

【MDM】

(1) 庁外持ち出し端末を MDM で管理すること。

(2) 庁外持ち出し端末の紛失時に遠隔からロックなどのセキュリティ対策を実施できること。

(3) 庁外持ち出し端末の不要アプリケーション管理などデバイス制御や管理機能を有すること。

【ユーザー認証サーバー】

(1) Microsoft 365 を利用するためのユーザー認証サーバーとして Microsoft Entra ID を導入すること。

(2) インターネット接続系のユーザー管理を可能とするために Active Directory を導入すること。

(3) 既存 Active Directory から、本町が指定するオブジェクトデータを引き継ぐこと。

(4) Active Directory 及び Microsoft Entra ID は 1 フォレスト 1 ドメインで構成すること。

(5) Active Directory は 2 台以上の冗長構成とすること。

(6) ActiveDirectory はドメイン/フォレスト機能レベル Windows Server 2016 以上に移行すること。

【Microsoft 365 連携サーバー】

(1) ユーザー認証サーバーと Microsoft 365 のユーザアカウントを同期し、インターネット 接続系ドメインユーザアカウントで Microsoft 365 の 使用を可能にすること。

【スケジュール連携】

(1) Garoon と Microsoft 365 の双方向からのスケジュール連携が可能なこと。
(2) 管理者以外の職員がスケジュール連携のための設定をする場合には簡易かつ直感的な操作で実施が可能なこと。
(3) 許可された私用スマートフォンからのスケジュール閲覧を可能とすること。

【コラボレーションツール】

(1) Microsoft Teams を導入すること。
(2) 職員が利用するインターネット接続系システムにおいて、映像会議、チャット、タスク管理機能を提供すること。
(3) Microsoft Teams で以下機能を実装すること。
   a. チームの作成
   b. Teams の組織全体のポリシー設定
   c. Teams 作成制限設定
   d. Teams 容量制限設定
   e. 外部共有設定

【DNS】

(1) 内部 DNS を提供するものとし、現行の DNS サーバー構成を参考に適切な設定とすること。
(2) インターネット接続系の外部 DNS については、既存で利用しているシステムを利用する構成とすること。
(3) インターネット接続系の管理システム及び業務システムの名前解決を可能とすること。
(4) 内部 DNS は 2 台以上の冗長構成とすること。

【NTP】

(1) NTP サーバーとして本調達に係る機器に正しい時刻情報を取得・配信を行うこと。
(2) 外部 NTP サーバーを参照する場合は本町が指定する参照先を設定すること。

【WSUS】

(1) 出先拠点を含むインターネット接続系の職員端末及び、Windows Server に対し、Windows OS 及び Windows Server OS 、Office のパッチを配信可能な環境を提供すること。
(2) 配信先の端末に対する WSUS の設定についても、Active Directory を用いて実施すること。

【KMS】

(1) 本調達に含まれるインターネット接続系の職員端末及び Windows Server の、OS のライセンス認証を提供すること。

5.4. LGWAN 接続系で必要となる機能を提供するサーバー群

LGWAN 接続系における必要機器について以下の要件を満たすこと。

【メールリレーサーバー】

(1) 「地方公共団体における情報セキュリティポリシーに関するガイドライン」に準ずるように SMTP プロトコルに対応したメールリレーサーバーを用意すること。

(2) メールリレーサーバーではインターネット接続系から送信された LGWAN ドメイン宛のメールの転送を行うこと。

(3) メールリレーサーバーでは LGWAN ドメインから受信するメールをインターネット接続系に転送すること。

【セキュリティ・ウイルス対策】

(1) LGWAN 接続系の業務環境及びサーバーに対するセキュリティ対策・ウイルス対策として、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 5 年 3 月版）」に沿って EPP 機能を有すること。

(2) EPP の対象は以下とする。

	EPP
LGWAN 業務環境	○
LGWAN 系サーバー	○

(3) EDR については自由提案とする。

(4) EPP の対象 OS として、Windows Server OS 及び Linux Server OS に対応していること。

(5) サイバー攻撃によるマルウェア及びランサムウェア等の脅威のエンドポイントへの侵入を防ぐ EPP の機能を有すること。

(6) EPP はエンドポイントがネットワークに接続していない時にも、エンドポイントの保護が可能なこと。

(7) EPP はシグネチャの更新が不要なこと。

【ユーザー認証サーバー】

(1) LGWAN 接続系のユーザー管理を可能とするために Active Directory を導入すること

(2) 既存 Active Directory から、本町が指定するオブジェクトデータを引き継ぐこと。

(3) Active Directory は 1 フォレスト 1 ドメインで構成すること。

(4) Active Directory は 2 台以上の冗長構成とすること。

(5) ActiveDirectory はドメイン/フォレスト機能レベル Windows Server 2016 以上に移行すること。

【DNS】

(1) 内部 DNS を提供するものとし、現行の DNS サーバー構成を参考に適切な設定とすること。

(2) LGWAN 接続系の外部 DNS については、既存で構築されているシステムを利用する構成とすること。

(3) LGWAN 接続系の管理システム及び業務システムの名前解決を可能とすること。

(4) 内部 DNS は 2 台以上の冗長構成とすること。

【NTP】

(1) NTP サーバーとして本調達に係る機器に正しい時刻情報を取得・配信を行うこと。

(2) 外部 NTP サーバーを参照する場合は適切な参照先を選定すること。

【WSUS】

(1) LGWAN 接続系の職員端末及び、Windows Server に対し、Windows OS 及び Windows Server OS 、Office のパッチを配信可能な環境を提供すること。

(2) 配信先の端末に対する WSUS の設定についても実施すること。

【KMS】

(1) 本調達に含まれる LGWAN 業務環境及び LGWAN 接続系 Windows Server の、OS のライセンス認証を提供すること。

【LGWAN 業務環境】

(1) すべての職員に LGWAN 業務環境を提供すること。

(2) インターネット接続系に置かれている職員端末から仮想化された環境に接続し、利用することが可能なこと。

(3) 行政情報の漏洩を防ぐための高度なセキュリティも必要であるため、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」に即した環境、接続方法を提供すること。

(4) 仮想ブラウザ及びローカルコンテナ等で起動できないソフトウェアのインストールにも対応できるような環境も用意すること。

(5) 仮想環境を（VDI、RDS などの）仮想デスクトップで提供する場合には、1台当たり次の要件を満たすものとする。

a. CPU :2 コア以上

b. メモリ: 8.0 GB 以上

c. ディスク: 100 GB 以上

(6) (5)に記載された LGWAN 業務環境の OS は Windows11 Pro 64bit 版 相当以上とすること。

(7) LGWAN 業務環境について、ソフトウェア等の更新や、問題発生時の変更、修正が煩雑な手順とならず対応可能な管理とすること。

5.5. 3 層分離環境間ファイル受け渡しシステム

3 層分離環境間のファイル受け渡しとして、以下の要件を満たすこと。

(1) LGWAN 系、インターネット系の 2 つのネットワークをまたいだ双方向のファイル授受が行えること。

(2) 基幹系、LGWAN 系の 2 つのネットワークをまたいだ双方向のファイル授受が行えること。

(3) インターネット系から LGWAN 系へのネットワークをまたいだファイル授受の際に無害化システムと連携しファイルの無害化処理を行えること。

(4) インターネット系から LGWAN 系へのネットワークをまたいだファイル授受の際にアンチウイルス機能を有すること。

(5) 連携するファイル無害化サーバーは、ファイルを分析し、スクリプトやマクロや OLE オブジェクトなどリスクの高い因子について総務省ガイドラインの無害化処理要件を満たす無害化処理機能を有すること。

5.6. 3 層分離を考慮した有線ネットワーク機器

【コアスイッチ】

(1) 本町の NW を集約し、L3 スイッチとして適切にルーティングを行うこと。

(2) 論理的に 3 層（インターネット接続系、LGWAN 接続系、基幹系）分離を行うこと。

(3) 2 台以上の冗長構成とすること。

(4) 本調達における機器類を収容可能であること。

(5) 既存のサーバースイッチを収容すること。そのためのコアスイッチ一台当たり 5 ポート以上 1000Base-T にて接続可能なポートを用意すること。

(6) 以下の機器との接続は 1Gbps 以上の通信速度に対応したケーブルを使用し、ケーブル冗長とすること。

a. 無線 LAN コントローラー（物理アプライアンスで構築する場合）
b. ファイアウォール
c. 出先収容装置
d. 管理スイッチ

(7) 以下の機器との接続は 10Gbps 以上の通信速度に対応したケーブルを使用し、ケーブル冗長とすること。

a. バックアップサーバー
b. 仮想化基盤サーバー
c. 共有ストレージ兼ファイルサーバー（3Tier 構成の場合）
d. フロアスイッチ

【フロアスイッチ】

(1) 本調達の庁舎内に設置する無線 LAN アクセスポイントを収容すること。

(2) 既存フロアスイッチから本フロアスイッチにダウンリンクを移設すること。既存フロアスイッチは アライドテレシス AT-GS924MX の 2 台スタック構成で、6 セットで稼働している。

(3) コアスイッチとは、10Gbps 以上の通信速度に対応したケーブルで接続し、ケーブル冗長とすること。

(4) 無線 LAN アクセスポイントとは、1Gbps 以上の通信速度に対応したケーブルで接続すること。

(5) IEEE 802.3at に準拠し、12 ポート利用時に最大 30W の電源供給が可能であること。
(6) 本調達の無線 LAN アクセスポイントを収容可能な総 PoE 電力容量を有していること。

【拠点収容装置】

(1) 本庁と出先拠点間の接続において本庁側の接続機能を有すること。
(2) コアスイッチとは、1Gbps 以上の通信速度に対応したケーブルで接続し、ケーブル冗長とすること。
(3) Active Directory と連携し、認証機能を有すること。
(4) GUI は一般的な Web ブラウザを利用したものであること。
(5) WebUI は日本語対応していること。

【拠点接続装置】

(1) 本庁と出先拠点間の接続において拠点側の接続機能を有すること。
(2) 既存の出先拠点の機器類を収容可能であること。

【ファイアウォール】

(1) 3 層分離 NW 間の相互接続機能を有すること。
(2) コアスイッチとは、1Gbps 以上の通信速度に対応したケーブルで接続し、ケーブル冗長とすること。
(3) 電源部・ファン部が冗長化可能であること。
(4) ホットスワップ機能を有すること。
(5) Active Directory と連携し、認証機能を有すること。
(6) ファイアウォール機能、次世代ファイアウォール機能(アプリケーション制御) を有すること。
(7) Web フィルタリング機能を有すること。
(8) GUI は一般的な Web ブラウザを利用したものであること。
(9) WebUI は日本語対応していること。

【庁外リモートアクセス】

(1) 庁外リモートアクセスに必要な回線及びグローバル IP アドレスによる ISP の利用料金を本調達に含めること。
(2) 庁外持ち出し端末について庁内インターネット接続系にアクセスできるようにすること。
その際、SSL VPN や IPSec VPN 等を用いセキュアにアクセスさせること。
(3) 庁外持ち出し端末は庁外から、庁内と宮城県自治体情報セキュリティクラウド（第2期）を経由しインターネットへアクセスすること。
(4) 庁外持ち出し端末の接続先を制御できること。
議員端末の通信に関しては 5.11.1【議員端末に関する要件】を参照すること。

5.7. LGWAN 接続系・インターネット接続系の無線ネットワーク機器

【無線 LAN コントローラー】

(1) 無線 AP の集中管理を行う機能を有すること。
(2) 物理アプライアンス又はクラウド上で構成すること。

(3) 物理アプライアンスで構築する場合、コアスイッチとは 1Gbps 以上の通信速度に対応したケーブルで接続し、ケーブル冗長とすること。
(4) 無線 LAN アクセスポイントについて、本調達の 34 台以上を管理する性能を有すること。
(5) 無線 LAN を利用する端末について、220 台以上を管理する性能を有すること。
(6) 認証サーバーと通信を行い認証結果により端末の接続を制御できる機能を有すること。
(7) IEEE 802.1X 認証に対応していること。
(8) MAC アドレスによる認証機能を有すること。
(9) EAP-TLS に対応した認証を行う機能を有すること。

【無線 LAN アクセスポイント】

(1) 無線 LAN クライアントが接続できる機能を有すること。
(2) フロアスイッチとは、1Gbps 以上の通信速度に対応したケーブルで接続すること。
(3) 無線 LAN コントローラーにより統合的に管理・連動する機能を有すること。
(4) チャネル帯域幅を自動調整する機能を有すること。
(5) 無線 LAN アクセスポイントについて フロアスイッチ(PoE 対応)を用いて給電すること。
(6) IEEE 802.11i に準拠、及び WPA/WPA2/WPA3 に対応していること。
(7) 無線 LAN を利用する端末について、30 台以上を同時接続が可能であること。
(8) IEEE 802.3af 又は 802.3at 規格の PoE に対応していること。
(9) 5GHz 帯の IEEE 802.11a/n/ac/ax に対応していること。
(10) 2.4GHz 帯の IEEE 802.11b/g/n/ax に対応していること。
(11) 無線接続端末に対して DHCP サーバーにて IP アドレスの払い出しをすること。

【無線 LAN 認証サーバー】

(1) 無線 LAN クライアントの接続認証機能を有すること。
(2) RADIUS 機能を有し、認証サーバーとして利用できること。
(3) 無線 LAN 認証方式を EAP-TLS とすること。
(4) 認証に用いるアカウントは 5,000 以上登録できること。
(5) ネットワーク機器と連携し、MAC アドレス認証を行う機能を有すること。
(6) 認証局機能を有し、ユーザー証明書、及びサーバー証明書を発行できること。
(7) 発行するデジタル証明書の有効期限は有効日数もしくは日付から選択できること。
(8) 登録アカウントの管理は個別のほか、CSV ファイルからの一括登録・変更・削除ができること。
(9) ネットワーク認証サーバーへの通信に対し、機器インターフェイス、プロトコル、送信先・送信元ネットワーク情報(IP アドレス、サブネットマスク、ポート番号)の組合せにより、許可・拒否などの制御ができること。

5.8. その他の必要物品

本調達では以下の物品も含めることとする。

(1) Microsoft 365 Business Premium 相当以上のライセンスを 240 ユーザー利用できるようにすること。ただし、後年ライセンスの値上がりがあった場合には別途協議するものとする。

5.9. 私用スマートフォン管理

本調達における私用スマートフォン管理では以下の要件を満たすこととする。

(1) Azure AD Premium P1 相当のライセンスをユーザー数分導入すること。

(2) Microsoft 365 テナントが開設されており、Microsoft Intune が利用できること。

(3) Intune ではアプリケーション保護ポリシーの対象は以下とすること。

a. iOS

b. Android

(4) 私用スマートフォンからはスケジュールの確認のみを可能とし、庁内データを私用スマートフォンへダウンロード及びテキストのコピー＆ペーストをできないよう制限すること。

(5) Intune では以下の機能実装を用いてセキュリティ及びアクセス制御を検討すること。

a. 動的セキュリティグループ作成

b. 条件付きアクセス制御作成

(6) IP アドレスの制限や、端末制限などを用いて不特定多数の Microsoft 365 へのアクセス制限を実装すること。

5.10. 職員端末

職員に貸与する端末として以下の要件を満たすものを 220 台とする。

(1) 2in1 タイプのノート型パソコンとする。

(2) 端末の形状についてはタブレット型、コンバーチブル型、セパレート型を問わない。

(3) 外付けキーボードを添付すること。

(4) 画面サイズが 13 型以上の端末とすること。

(5) タッチスクリーンを搭載した端末とすること。

(6) OS は Windows11 Pro 64bit であること。

(7) CPU は Intel 製であれば Core i5 の第 13 世代以上、AMD 製であれば Ryzen 5 第 5 世代以上とすること。

(8) メモリの容量は 16GB 以上搭載すること。

(9) ストレージは SSD で容量は 256GB 以上搭載すること。

(10) ネットワークインターフェースとして、有線(1000BASE-T)、無線(IEEE 802.11ax)、WWAN(LTE/5G)に対応していること。

(11) スタイラスペンを添付すること。

(12) 27 インチワイド液晶ディスプレイを添付すること。なお、ディスプレイは机上台もしくはクランプアームなどにより設置すること。また、クランプアームの場合には縦置きにも切り替えられることが望ましい。

(13) ドッキングステーション（ディスプレイ、外付けキーボードなどの周辺機器接続）を添付すること。なお、ドッキングステーションはディスプレイ背面に固定できることが望ましい。

(14) ノートパソコンスタンド、ヘッドセット等を添付すること。

(15) Windows Hello(顔認証)に対応したカメラを備えること。

(16) TPM (Ver2.0 以上)を搭載していること。

5.11. 議員端末

町議会議員に貸与する端末として以下の要件を満たすものを 20 台とする。

(1) 2in1 タイプのノート型パソコンとする。
(2) 端末の形状についてはタブレット型、コンバーチブル型、セパレート型を問わない。
(3) タブレット型、セパレート型の場合は外付けキーボードを含めること。
(4) 画面サイズが 13 型以上の端末とすること。
(5) タッチスクリーンを搭載した端末とすること。
(6) OS は Windows11 Pro 64bit であること。
(7) CPU は Intel 製であれば Core i5 第 13 世代以上、AMD 製であれば Ryzen 5 第 5 世代以上とすること。
(8) メモリの容量は 16GB 以上搭載すること。
(9) ストレージは SSD で容量は 256GB 以上搭載すること。
(10) ネットワークインターフェースとして、有線(1000BASE-T)、無線(IEEE 802.11ax)、WWAN(LTE)に対応していること。
(11) スタイラスペンを添付すること。
(12) Windows Hello(顔認証)に対応したカメラを備えること。
(13) TPM (Ver2.0 以上)を搭載していること。
(14) インターネット接続可能な SIM は本町にて調達する。

5.12. 議員端末に関する要件

議員端末は 20 台調達すること。

【通信要件】

(1) LTE 通信及び WiFi 通信を可能とすること。(SIM は別調達)
(2) 議員端末は庁内ネットワークへのアクセスを原則不可とすること。
ただし、資産管理等の管理通信のみ必要に応じて実施すること。
その際、SSL VPN や IPSec VPN 等を用いセキュアにアクセスさせること。
(3) 不要なサイトへのアクセスを制限するため、Web フィルタリングを行うこと。

【認証要件】

(1) ユーザー認証については、ローカル認証ではなく、 Microsoft Entra ID や ActiveDirectory 等と連携しユーザー認証を行う。認証の際、生体認証を行えるようにすること。

【セキュリティ・ウイルス対策】

(1) セキュリティ対策・ウィルス対策として、EPP 機能を有すること。

【資産管理】

(1) 議員端末を対象とすること
(2) インターネット系端末と同様の機能・管理方法を構成すること。
5.3 インターネット接続系で必要となる機能を提供するサーバー群【資産管理】を参照。

【MDM】

(1) 議員端末を対象とすること。

(2) 庁外持ち出し端末と同様の機能・管理方法を構成すること。

5.3 インターネット接続系で必要となる機能を提供するサーバー群【MDM】事項とを参照。

【コラボレーションツール】

(1) 映像会議、チャット、タスク管理を提供すること。

(2) 議員用のテナントは職員用と分ける構成とすること。

(3) 職員と議員間のチャットなど直接のコミュニケーションは不可とすること。

(4) 議員用メールアドレス(アカウント)は、職員とは別ドメインにて作成すること。

【メールシステム】

(1) 議員端末におけるメールシステムとして Exchange Online を利用すること。

(2) 議員用メールアドレス(アカウント)は本メールシステムで管理すること。

(3) Exchange Online では以下の設定を実装すること。

a. メールボックスやスケジュールの初期設定

b. アーカイブの設定

c. 訴訟ホールドの設定

d. メール配信経路設定(組織外に対するメール送信制御のためのトランスポートルールの設定)

5.13. 保守・監視・運用

【保守】

本調達により導入した機器類はシステム稼働後 5 年間以下の条件で保守対応を行うこと。

(1) ハードウェア類は平日 9 時から 17 時のオンサイト保守。

(2) 故障受付窓口を準備し、平日8時30分から17時30分で対応すること。

(3) 故障受付窓口は Web サイト、又はメール、電話のいずれかの方法に対応すること。

(4) ソフトウェア類はシステム稼働後 5 年間の製品サポートを提供すること。

(5) 職員端末・議員端末については標準保証を必須とし、その他追加保守については任意とする。

(6) 本町に部品を送付し、本町職員が部品交換作業を行う保守形態は不可とする。(本件受注者が機器手配・交換作業実施)

【監視】

本調達で導入した機器類の監視については自由提案とする。

【運用】

システム稼働後の運用として以下の対応を行うこと。

(1) 導入時に本町が行うシステムの管理者向け操作説明会に技術担当者が立ち合い支援すること。

(2) 3 年に 1 回の頻度で予定されている計画停電時に、システム停止・システム起動の作業に技術担当者が立ち合い支援すること。

(3) 導入初年度のみ3か月に1度の頻度で Feature Update を、職員端末及び議員端末、仮想化基盤、仮想マシンに対して適用すること。
また、それ以降の年度については別途導入初年度に本町の職員が対応できるように運用手順をレクチャするか、運用サービスを提供するかを本町と協議のうえ決定し対応すること。

6. 納入成果物

本調達では以下に示す成果物を紙媒体及び電子媒体で納入すること。

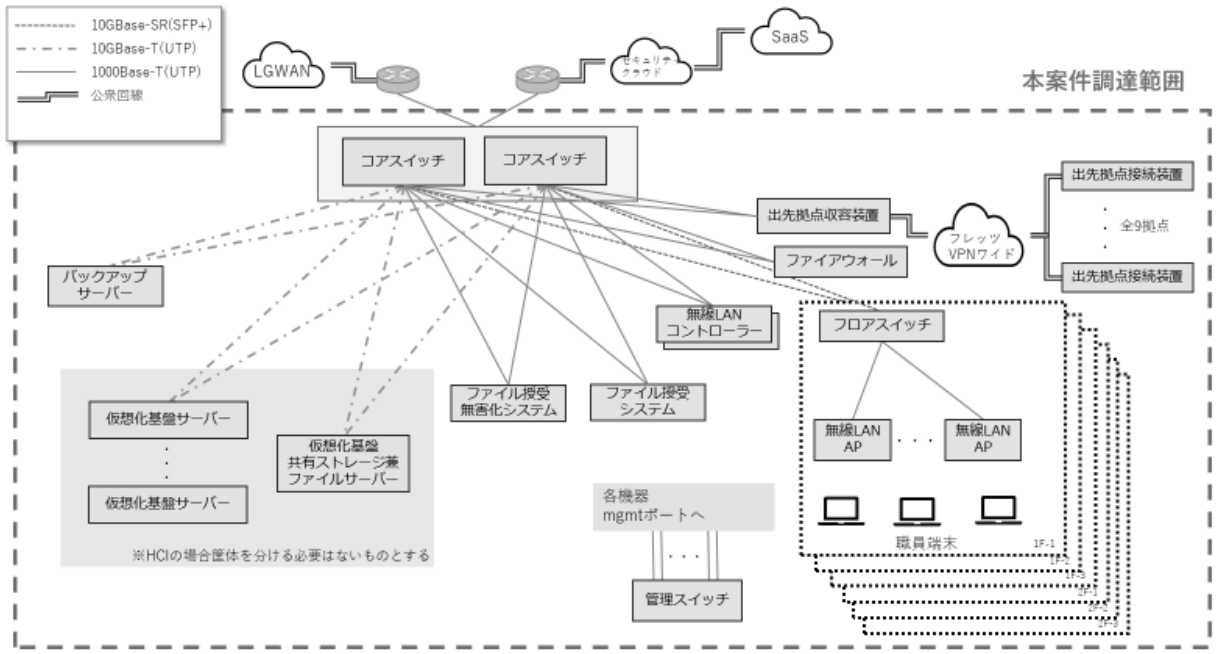
a. 業務実施計画書 ： 全体スケジュール、体制表、役割分担など
b. 導入予定製品一覧表(製造番号を記載) ： 全納品物の一覧表
c. 基本設計書 ： 仮想基盤システム等の基本設計書
d. 詳細設計書 ： 仮想基盤システム等のパラメータシート
e. システム構成図 ： システム全体の物理/論理構成図、電源系統図など
f. ネットワーク構成図 ： 個別システムのネットワークを含めたネットワーク構成図
g. ラック搭載図 ： サーバーラック内の機器の搭載図
h. 保守・連絡系統図 ： 初年度の保守体制、故障時の連絡系統図
i. システム運用マニュアル ： システム管理者の運用や障害時の対応手順などを記したマニュアル
j. テスト計画書兼結果報告書 ： 単体試験、結合試験、運用試験等の計画書とその実施報告書など
k. プロジェクト管理資料 ： スケジュール表、作業タスク管理表(WBS)、打合せ議事録、問題・課題管理表など
l. 初年度以降の保守体制図:保守の内容とそれに対する障害時の連絡及び連携体制など

7. 準拠する法令等

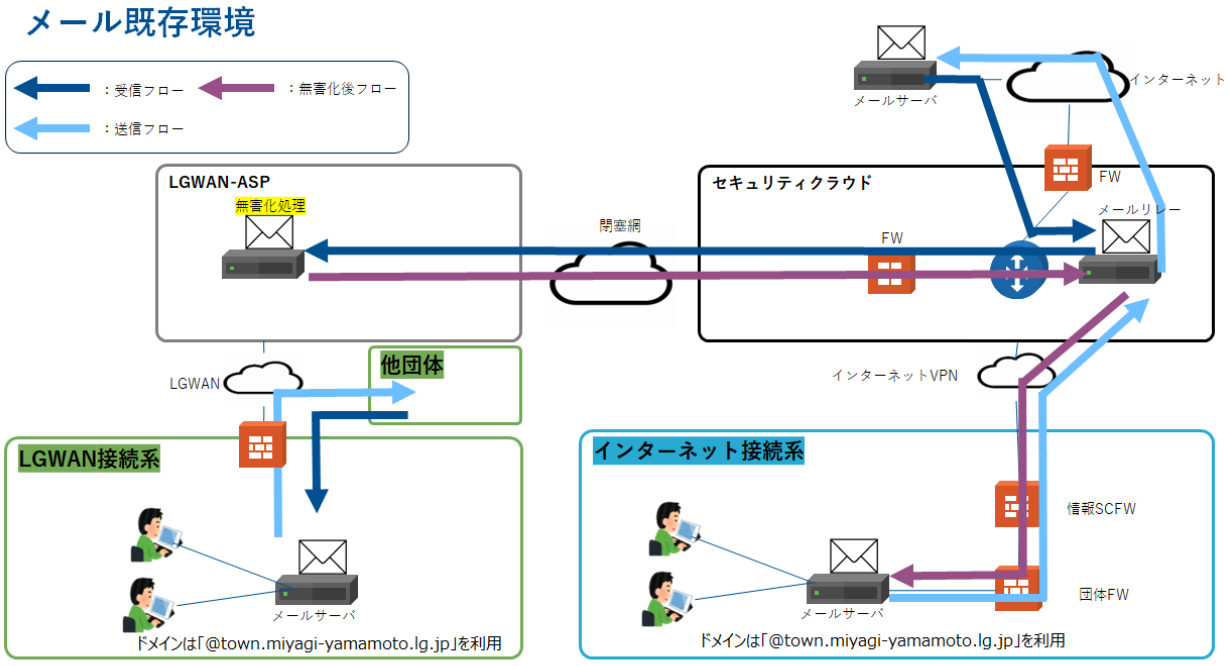
本業務履行に当たっては、本提案要求書による他、次に掲げる関係法規等の最新版に準拠し、実施するものとする。

(1) 総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン
(令和 5 年 3 月版)」
(2) 総務省の「テレワークセキュリティガイドライン(第 5 版)(令和 3 年5月)」

システム全体構成イメージ



既存メール環境



インターネット側もLG側も同一ドメインにより、アドレスは全く同じものを利用している。

別紙 3

庁舎内概略図(1F)

庁舎内概略図(2F)