

別紙 1 業務要件

本業務にあたり、次の要件を満たす機器等の用意をすること

大分類	中分類	小分類	機能要件
ネットワーク	ルーター	機器要件	インターネットにPPPoE又はIPoEで接続するためのルーターを1台設置すること。 (回線は本市で用意し、シングル構成、回線速度は1Gbpsのベストエフォート、固定IPアドレス取得の予定。)
			2,000台程度の端末からMicrosoft 365への認証が行うのに十分な性能があること
			SFPポートを1つ以上有し、1000BASE-T 対応であること
			1GbE WAN ポートを2ポート以上搭載していること
			1GbE LAN ポートを8ポート以上内蔵していること(外付けスイッチでの代替不可)
			スタティックルーティング対応であること
			IPv6/IPv4のデュアルスタック対応であること
			インターネット向けトラフィックのNAPT変換対応しており、複数セッションの同時処理が可能なこと
			IPフィルタリング、URLフィルタリング、ステートフルパケットインスペクションに対応していること
			アクセスロギング(syslog)に対応していること
			SSHアクセス等のリモートメンテナンスに対応していること
			SNMP(v2c以上) クライアント対応であること
			CLI / Web GUI による設定・管理に対応していること
システム要件	ローカルブレイクアウト	機器要件	19インチラックに収容でき、ユニットの高さは1Uであること
			冗長構成(2台構成)とすること
			1GbE銅ポートを7、10GbEファイバー(SFP+)ポートを4、25GbEファイバーポート(SFP28)ポートを2以上有すること
			L4CPS(connections per second)が300,000以上であること
			同時セッション数が3,200万以上であること
			L4、L7でそれぞれ10Gbps / 10Gbps以上のアプリケーションスループットを有すること
			鍵長2,048bit時のSSL終端時のスループットが10Gbps以上であること
			SSL終端時のCPS(connections per second)がRSA:15,000、ECDSA:5,000以上であること
			鍵長2,048bit時のSSLインサイト使用時のスループットが1Gbps以上であること
			SSLインサイト使用時のCPS(connections per second)がRSA:2,000 / ECDHE:1,200以上であること
			2,000台程度の端末からMicrosoft 365への認証が行うのに十分な性能があること
	ネットワーク要件	ネットワーク要件	インターネット回線向けの通信とそれ以外の通信を識別し、振り分けられること
			クラウドサービスの宛先をURL等で特定し、URLの違いに応じて転送可否を設定できること
			クライアントがブラウザにIP、ポートを指定してプロキシ機能を利用する明示プロキシに対応していること
			以下の機能を接続先Hostヘッダ、URL、IPアドレスのいずれかをを用いて制御が可能であること
			1) 特定の接続先への通信を遮断する
			2) 特定の接続先への通信は上位Proxyサーバへ多段接続する
			3) 接続先に応じて転送するNext-hopの機器を選択する
			プロキシ接続を行う端末(送信元アドレスや認証情報)に応じて1)~3)を優先順位付けした上、組み合わせて設定が可能であること
			RADIUS、LDAP、Windows ADなどの認証サーバと連携し、認証プロキシの機能を提供可能であること
			プロキシサーバが代理でWebコンテンツを取得する際、任意のソースIPアドレスに変換する、もしくは接続元のクライアントのIPアドレスのまま接続するかを選択可能であること(ソースNATのルールを柔軟に設定可能であること)
			X-Forwarded-Forなどの任意のHTTPヘッダを挿入可能であること
			SSL/TLS可視化の設定が可能であること
			SSL/TLS可視化時に以下の機能が設定可能であること
			・SSL/TLS通信であればTCPポート番号・上位プロトコルにかかわらず動的に復号化する機能
			・接続先WebサイトとのSSLハンドシェイクが失敗した場合、自動的に可視化をバイパスする機能
			・接続先のWebサイトがクライアント証明書を要求した場合、自動的に可視化をバイパスする機能
			・バイパスするWebサイトを明示的に指定できる機能
			Webブラウザで利用可能なGUIを有しており、日本語に対応していること
			本市既存ネットワーク機器との接続に必要な設定を行うこと

大分類	中分類	小分類	機能要件
		Microsoft 365 認証の要件	Microsoft 365への通信の際に、既存の庁内プロキシサーバへの負荷の増加を回避するための仕組みを導入すること Microsoft 365アカウントの利用を制限するため、本市からMicrosoft 365へのアクセスは、本市のテナントのみに接続し、他のテナントへの接続を制限する仕組みを導入すること(そのためのHTTPS通信の可視化を追加ライセンスなく利用できること) Microsoft 365のクラウドサービスのURL情報のリストを動的に更新できること 振り分けに必要なMicrosoftクラウドサービスのFQDNは自動取得ができる仕組みとすること（別途事業者が提供するサービスとの組み合わせも可とする）
		その他	Adobeの認証ができるようにすること
機器全般	非機能要件	パッチ	緊急性の高いパッチは即時に適用し、それ以外は定期保守時に適用を行うこと。
		アクセス制限	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみ許可するよう、アクセス制限を行うこと。
		ログ	不正やインシデントを検知するために、必要な内容及び期間のログを適切に保存すること。取得するログの内容及び期間、責任範囲について整理し示すこと。ログは、別途本市が用意するログサーバーに保存すること。
		監視	稼働状況を監視し、必要に応じて警告等を発する機能を設けること。監視情報について責任範囲を整理し、示すこと。
		RPO	RPO（目標復旧地点）は1営業日前の時点を目標とする。
		RTO	RTO（目標復旧時間）は6時間以内を目標とする。
		稼働率	原則 24 時間 365 日無停止の運用となるが、年間稼働率は99.9%以上を目標とする（計画停止を除く）目標未達の場合、受注者は原因分析及び再発防止策について報告すること。
導入要件	プロジェクト管理	全般	本業務の開始に先立って、スケジュール、体制、プロジェクト管理方針等を記載したプロジェクト計画書を策定すること。 調達仕様及び提案内容に基づき、システム構成、機能要件、非機能要件等における対応方針を記載した要件定義書を策定すること。 要件定義書に基づき、基本設計及び詳細設計を行い、機器一覧、物理及び論理構成図、環境設定パラメータ、バックアップ設定等について資料として取りまとめて提出すること。 基幹LANとのネットワーク接続においては、本市が委託するネットワーク運用保守業者を含め、発注者と十分に論理、物理設計を行うこと。（設計資料等の必要資料は受注者にて作成、提示すること。） システムテストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、本市と実施内容の調整を行うこと。その後のテスト結果報告書についても提出すること。
			ラック内及び基幹LANとの各ケーブル配線を行うこと。 ※各ケーブル・サーバ・UPSへは、ケーブルタグ及び管理シールをつけること。
			導入する機器の稼働環境構築及びその他必要な設定を行うこと。 本市ネットワークへの接続設定を行うこと。
			移行作業
			本事業の全体観点から移行スケジュールおよび移行手順、切り戻し手順、確認観点、役割分担等を記述した移行計画書を作成すること。
運用保守要件	運用保守	全般	稼働までに運用保守における年間・月間想定スケジュール及び作業内容、サポートを担当する部署、連絡先、責任者等、各種実施手順を取りまとめた運用保守計画書を策定し、本市に提出すること。また、変更時には随時更新を行うこと。 操作手順書として、機器の起動及び停止方法、管理コンソールのログイン及び利用方法、停電・復電時の操作フロー、システムバックアップ及びリストア、管理者パスワードの変更（管理ユーザの追加手順含む）、修正パッチの適用方法、ローカルブレイクアウトさせるサービスの追加方法、障害発生時の切り替え・切り戻し手順等について整備すること。 ローカルブレイクアウト環境の稼働1週間前までに研修を実施すること。 対象者 システム管理者5名程度 ・ 機器の概要（基本機能の説明） ・ 起動、停止方法 ・ 管理コンソールのログイン及び利用方法（確認方法など） ・ 停電・復電時の対応 ・ 障害が発生したときの対応 ハードウェア・ソフトウェア含めた一括サポート窓口を提供すること。 サポート窓口は24時間365日受付であり、契約期間中サービス提供されること。 連絡手段として電話およびメールでの対応が可能であること。 運用保守におけるサポートは日本語によるものとすること。 保守作業後に作業内容、作業者、作業日時等を記載した報告書を提出すること。
			稼働時
			稼働当日は不測の事態に即時対応できる、本事業に関する知見の深いメンバーを立ち会いさせること。また、稼働日から2週間は、構築に携わったメンバーが即応できる体制を整えること。

大分類	中分類	小分類	機能要件
		ハードウェア 保守	ハードウェア保守は 24 時間 365 日オンサイト方式とする。
			ハードウェア保守用部品は本システム稼働後、最低 5 年間は提供が保証されていること。
			保守作業時の交換前ディスク（SSD/HDD）は回収しないオプションを有すること。または、本庁舎内で物理破壊の上、データ消去報告書を提出する方式とすること。
		ソフトウェア 保守	ソフトウェアのバージョンアップ更新や脆弱性情報が発見された場合、速やかに本市に報告し、今後の対応方法・スケジュールについて協議を行い、是正を図ること。
			ソフトウェアの更新又はバージョンアップを行う場合は、事前の動作確認を行い、変更点について、操作マニュアル等への反映を適宜行うこと。
		障害対応	本システムの関与が疑われる障害が発生した場合は、原因の切り分け作業について協力すること。
			システム継続が不可能など重大障害における連絡受付については、24時間365日対応できる体制を整えること。ただし、定常時対応時間帯とは異なる体制でも構わない。
			障害発生連絡を受けた場合、2時間以内に現着できる範囲に拠点があること。
			障害発生時には、影響範囲の調査、原因究明を行い、復旧作業を行うこと。また、障害内容について再発防止策を検討の上、報告すること。