ファイアウォール機器等一式の再構築業務及び運用保守業務仕様書

1. 概要

本市において導入済みである各ゲートウェイシステムについて、機器の老朽化、ソフトウェア、ハードウェアのサポート終了に伴いリプレイスを行う。

リプレイスを行うにあたり、今後、更なるインターネットを活用する業務が増えることが予想されるため、ゲートウェイシステムは将来に耐えうるシステムとして導入します。

2. 調達の範囲

2.1 調達の概要

本調達の範囲については、以下のとおりとする。

(1) ファイアウォール機器等一式の再構築業務

下記 2.3 調達機器に指定する各機器について、3.基本要件を満たす機器を導入し、4. 設定に関する要件に定める各種設定等作業を実施すること。

契約期間：契約締結日から令和8年9月30日まで

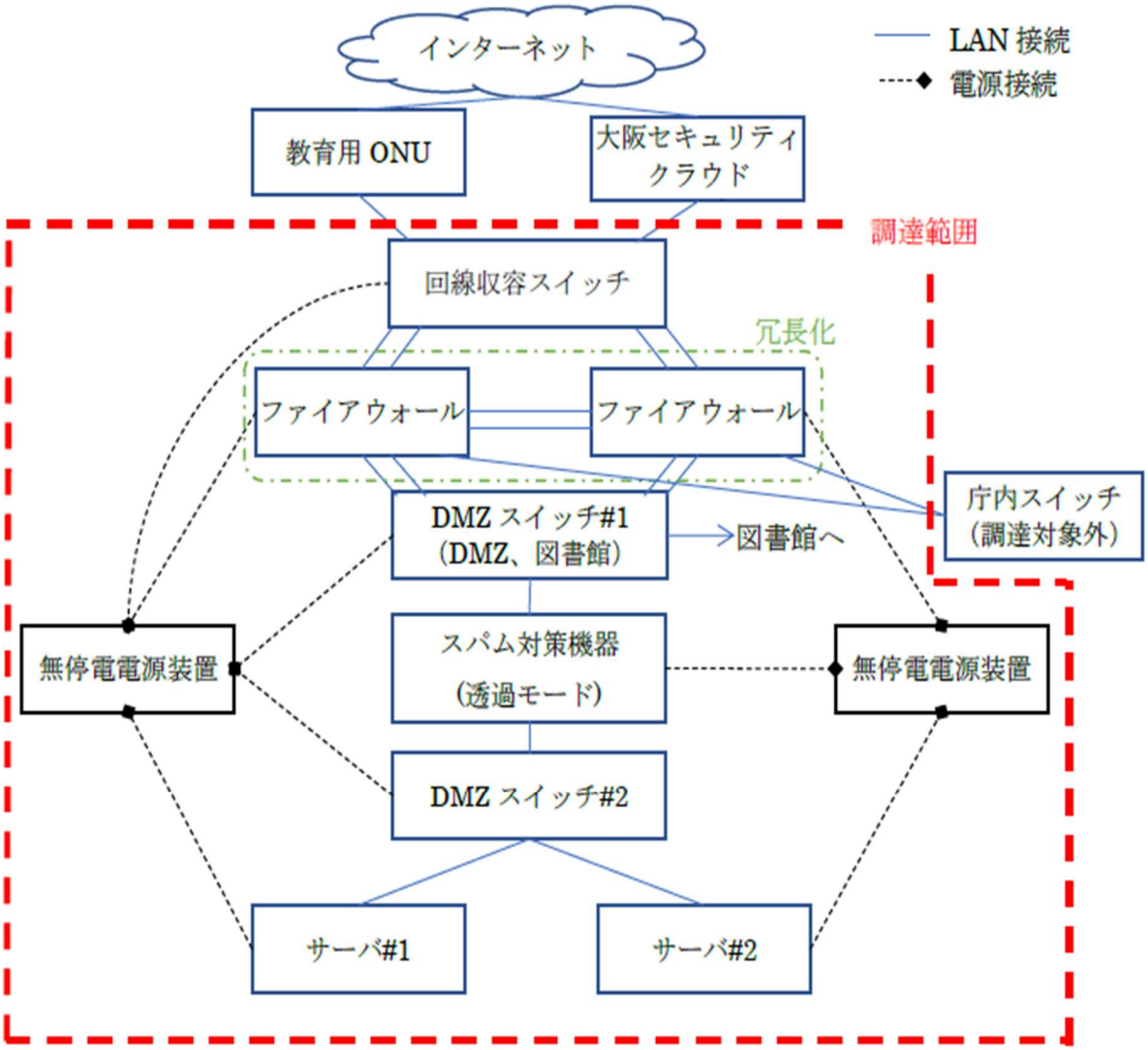
(2) ファイアウォール機器等一式の運用保守業務

上記(1)において導入した機器等一式について、5.保守・運用に関する要件に定める運用保守業務を実施すること。なお、ファイアウォール機器等一式の運用保守業務は地方自治法（昭和 22 年法律第 67 号）第 234 条の3に規定する長期継続契約を予定している。

契約期間：令和8年10月1日から令和13年9月30日まで（60 か月間）

2.2 機器構成

本市におけるゲートウェイシステムは以下の通りである。



2.3 調達機器

(1) ファイアウォール…2台

教育 FW、教育・行政振り分けルータ、FW 機能を有すること、停止すると業務影響が大きいため、2台で冗長化構成とする。

(2) L2 スイッチ…3台

回線収容スイッチ用に1台、DMZ スイッチ＃1 と図書館用スイッチをまとめ 1 台、DMZ スイッチ＃2 を 1 台とする。

(3) スパム対策機器…1台

スパム対策製品は庁外から送信される大量のスパムメールに対応するため、スパム専用のフィルタリ

ングサーバを導入する。

（4） サーバ（バックアップ装置含む）…2台
　庁外から送信されるメールおよび本市から送信するメールのリレーサーバーおよび、一部庁内からのHTTP プロキシサーバとして利用している。負荷軽減および業務上停止時間を極力なくす必要があることから2台の冗長化構成とする。

（5） KVM スイッチ…1式

（6） 無停電電源装置…2台以上

（7） 機器導入および設定作業（詳細は後述する）

3. 基本要件

（1） 令和８年９月末日までに、下記に定める設計・設定・移行・設置作業を実施の上、本市の指定する場所に納入すること。

（2） 納入する機器は、必要な要件を満たし、全ての機能が正常に動作することを確認したうえで納入すること。

（3） 機器は本市が指定する既設 19 インチラックに収容すること。

（4） ファイアウォール並びにスイッチは既設 19 インチラックにラックマウントすること。

（5） 構築作業完了後、5年間の運用保守が可能な機器を導入すること。

（6） 5年間内にメーカサポートが終了するなど運用保守ができなくなった場合は、落札者の責任においてサポート可能な機材へ無償で入れ替えること。

（7） 既設ネットワーク機器との接続に使用するために、必要なケーブルや変換コネクタ等、落札者にて準備すること。

3.1 機器詳細仕様
機器仕様は機器１台当たりの要件とする。

3.2 ファイアウォール
（1） 基本要件
① 冗長構成とするため各要件については、機器1台当たりの要件とする。
② 冗長構成の機器同士は、設定情報及びセッション情報の同期が可能であること。
③ ハードウェアアプライアンスであること。
④ ネットワークインターフェイスは、10Base-T/100Base-T/1000Base-T 対応のコネクタ形状 RJ-45 で、任意のネットワーク割り当てられるポートを８ポート上備えていること。

（2） 機能要件

① ステートフルインスペクション技術を採用したファイアウォール機能を有すること。
② 仮想的に 3 個以上のファイアウォールを稼働させることが可能であること。
③ アドレス変換(NAT)機能、ポート番号変換(PAT)機能、アドレス変換とポート番号変換(NAPT)機能を有し、ポリシー単位での制御が可能であること。
④ グローバルIPアドレスと内部プライベートIPアドレスの変換が可能であること。
⑤ 1つの仮想IPアドレスに対し、複数のサーバのポートをマッピング可能であること。
⑥ 通信ポリシーごとに帯域制限および帯域保証を設ける機能を有すること。
⑦ トラフィック管理として diffserv に対応可能であること。
⑧ スタティックルーティング、ダイナミックルーティング(RIPv1/v2 、OSPF 、BGP)及びポリシーベースルーティングに対応可能であること。
⑨ マルチキャストルーティングに対応可能であること。IGMP(v1/v2) や PIM シングルモード等の一部機能実装での対応でも可能とする。
⑩ IEEE802.1q に準拠した VLAN タギングに対応可能であること。
⑪ PPPoE/DHCP で IP アドレスが割り当て可能であること。
⑫ DHCP リレー機能を有すること。
⑬ PortScan 、SYN flood 、UDP flood 及び ICMP flood 等の攻撃の検知及び防御が可能であり、攻撃とみなす閾値の設定変更が可能であること。
⑭ IPsec について、暗号アルゴリズムは DES 、3DES 及び AES256 、認証アルゴリズムは MD5 及び SHA256 、鍵交換は DH1,DH2 及び DH5,DH19,DH20 に、それぞれ対応可能であること。

(3) 性能要件
① ファイアウォールスループットは、1518 バイト UDP パケットにおいて 39Gbps 以上であること
② 処理可能なパケットは、1 秒あたり 39.7Mpps 以上であること。
③ 最大同時セッション数は、11M 以上であること。
④ 1 秒間に接続できる新規セッション数は、400,000 以上であること。
⑤ 登録可能なポリシー数は、10,000 以上であること。
⑥ VPN(IPsec)の暗号化パフォーマンスは、7Gbps 以上であること。

(4) 管理要件
① SNMPv1/v2 機能を有し、SNMP マネージャより管理が行えること。
② Syslog サーバへのログ転送が可能であること。
③ HTTP 又は HTTPS を用いた Web ブラウザによる設定が可能であること。
④ シリアルコンソール、Telnet および SSH による管理及び設定が可能であること。
⑤ Web ブラウザ又は TFTP を用いた設定情報のダウンロード／アップロードおよびファームウェアのアップグレードが可能であること。
⑥ 特定IPアドレスのみ設定画面へ接続可能とする制限機能を有すること。

3.3 L2 スイッチ
(1) 基本要件
① 10Base-T/100Base-T/1000Base-T に対応可能なこと。
② 24ポート以上を備えていること。
③ Auto-MDI/MDIX 対応であること。
④ 10/100/1000Mbps 自動認識機能を有すること。

（2） 機能要件
① マネージドIPアドレスが割り当てられること。
② 監視装置によりマネージドIPアドレスに対し ping による死活監視が行えること。
③ 802.1QVLANtagging に対応していること。
④ 802.3ad の LACP に対応していること。
⑤ VLANID は 4093 まで対応していること。
⑥ リンクアグリゲーション数は 4 以上対応していること。

（3） 性能要件
① MAC アドレステーブル数は、32,000 以上であること。
② スイッチ容量は、126Gbps 以上であること。
③ パケット処理能力は、190Mpps 以上であること

3.4 サーバ
（1） 基本要件
① アナログ RGB ミニ D-sbu15 ピンを 1 個以上実装すること。
② USB2.0 準拠以上を 3 個実装すること。
③ LAN インターフェイス（RJ45）は、2 個以上実装すること。
④ OS は Linux であること。
⑤ サーバ筐体は既設の 19 インチラックに取り付けることとし、1U または 2U サイズであること。

（2） 機能要件
① 商用電源が断たれた場合、無停電電源装置と連動し安全にシャットダウンが可能であること。
② サーバのバックアップを取ることのできるものとし、外付け、内蔵を問わない。
また、バックアップを自動的に取ることができ、それぞれ復元が可能な状態で保存可能であれば、形式、台数は問わない。
③ バックアップ装置が外付けの場合はサーバ機器と同様ラックマウントに取り付けること。

（3） 性能要件
① CPU は Intel Xeon プロセッサ 4 コア/3Ghz 以上/キャッシュ 8M 以上を 2 個相当以上
② メモリは 32GB 以上
③ HDD は SAS 接続で 320GB×2 個以上（RAID1 構成をとること）

3.5 スパム対策
（1） 基本要件
① ハードウェアアプライアンス機器とし、VMware や Hyper-V などの仮想アプライアンスは不可とする。
② メールユーザ数は約 4,000 ユーザ
③ メール送受信数は、約 50 万件/月（外部からのスパムメール・宛先不明等のメール受信数を含む。）

（2） 機能要件
① IP アドレス、ドメイン、ブラックリスト、本文解析等複数の条件によるフィルタリングが可能であること。
② メールアドレスによる除外指定が可能であること。

③ スパム検知後のアクションを遮断・統計・配送（タグ付き）等複数から選択し指定可能であると。
④ 遮断後のメールについて、個別に配送が可能であること。
⑤ メール受信のログを取得でき、一覧表示が可能であること。
⑥ 送信者・受信者のメールアドレス（全部／一部一致）キーワード等による検索・抽出が可能なこと。
⑦ ログ画面等から、スパムと検知し遮断したメールの送受信者、メール本文等が確認でき、また、確認画面から配送もしくは除外リストへの登録が簡易な方法で可能なこと。
⑧ 複数の管理者設定が可能なこと/管理者別に権限設定可能なこと。
⑨ 機器障害時にはバイパス機能（透過モード）を使い、機器故障時もメールの送受信を停止させない機能を有すること。
⑩ 送信国による遮断設定が条件付きで対応可能なこと。
⑪ 商用電源が断たれた場合、無停電電源装置と連動し安全にシャットダウンが可能であること。
⑫ メールを送受信する際、ウィルスメールを検出するフィルタ機能が利用可能であること。
⑬ 添付ファイル拡張子を検査し、有害ファイルを隔離可能なこと。

3.6 メールセキュリティ

（1） 基本要件
① 上記 3.4 サーバに搭載出来るソフトウェアを選定すること

（2） 機能要件
① メールヘッダ解析、メッセージ本文のフルテキスト解析、メールシグニチャ、データベース、DNSルックアップ、URLデータベース解析、ユーザ定義による複合解析が可能なこと。
② Web 管理インターフェースを有すること。
③ 高検出率、低誤検知として信頼性の高いアンチウィルスエンジンを搭載していること。
④ 1 時間ごとのウイルス定義ファイル自動更新機能を有すること。
⑤ 検出エンジン、解析モジュールの自動アップデート機能を有すること。
⑥ ウイルス検知時のメール通知機能を有すること。
⑦ 月次レポート、ログ管理機能を有すること。

3.7 KVM

① ポートは 8 ポート以上であること。
② KVM およびサーバに接続するためのケーブルを機器ごとに 8 本用意すること。
ケーブル長は 2m 以上とし、サーバ側マウス・キーボードコネクタは USB であること。
③ サーバを切り替えて表示および操作可能な切り替え装置であること。
④ KVM は 19 インチラックマウントが可能であること。
⑤ KVM は KVM 本体とサーバに接続するための機器間は Ethernet ケーブルで接続するタイプが望ましい。

3.8 無停電電源装置

① 本仕様で調達するサーバ 2 台に対しそれぞれ 1 台ずつ無停電電源装置を接続する。
② サーバと無停電電源装置を接続するためのケーブル、ソフト類等は全て落札者にて用意すること。
③ サーバが正常にシャットダウン可能な時間、無停電電源装置から電源供給可能な機器を選定すること。
④ 本無停電電源装置にファイアウォール、スパム対策製品も接続することから考慮に入れること。

ファイアウォール、スパム対策製品は無停電電源装置と連動しシャットダウンできなくとも可とする。

4. 設定に関する要件

4.1 共通

（1）導入機器全てのインストール、構築、設定作業を実施の上、本市の指定する日時、場所に設置し、動作試験を行い、使用環境を整えること。
（2）構築作業については、動作試験及び本稼働を含め令和８年９月末までに完了すること。
（3）構築、設定にあたっては、基本設計案、構築スケジュールを事前に提示し、本市と協議を行うこと。

4.2 ファイアウォール

（1）ファイアウォールは既存の設定を引き継ぐこと。
（2）既存ファイアウォールのポリシー数は 250 以上、制定ルーティング数は 70 以上、ポリシールーティングも利用している。
（3）行政・教育振り分けルータでは、行政と教育のトラフィックを個別に振り分けており既存設定を引き継ぐこと。
（4）ファイアウォールの冗長構成及び複数回線によるインターネット接続に対応させるなど必要に応じ本市と協議の上設定を行うこと。

4.3 L2スイッチ

（1）この度、DMZ スイッチ#1 と図書館用スイッチを一つにまとめるため、VLAN 設定を行い論理的に分離すること。
（2）回線収容スイッチは、大阪 SC ルータと教育用 ONU 接続を収容するため VLAN 設定を行い論理的に分離すること。
（3）本市の指示に従い、機器 IP アドレス等の設定を行うこと。

4.4 サーバ構築

（1）上記仕様の 3.6 メールセキュリティソフトを本サーバに導入すること。
（2）リモート管理は SSH V2 を導入すること
（3）不要なポートを止め、ホストベースファイアウォールを導入すること。
（4）庁内向け NTP サーバを導入すること
（5）DNS は各々master/slave サーバとして設定し、既存 DNS の設定内容の移行および、今回導入するサーバ情報を設定すること。
（6）利用している庁外から送信されるメールおよび本市から送信するメールのリレーサーバーおよび、一部庁内からの HTTP プロキシサーバの既存設定を引き継ぐこと。
（7）本仕様で導入するサーバを MX サーバとして登録すること。
（8）教育系ドメインに関しては、メールのウイルスチェック設定を行うこと。行政系ドメインに関してはサーバでウイルスチェックを実施してはならない。
（9）ホストベースのファイアウォールを導入し、サービス提供に必要のない接続ポートを遮断しておくこと。
（10）保守管理用に SSH v2 を導入すること。
（11）SSH v2 は固定の IP アドレスからの接続に限定するものとし、また root 接続は禁止しておくこと。
（12）NTP サーバ（master サーバ）として設定すること。

（13）バックアップについては、指定した時間に自動的にバックアップができるよう設定を行うこと。
（14）大阪 SC に申請が必要となる場合は、本市から申請を行うが、落札社が責任をもって本市に必要情報の提供を行うこと。
（15）現行の IP アドレスを引き継ぐこと。

4.5 スパム対策

（1）スパムフィルタリング機能について、現行保持している設定情報等を移行して、現用運用に支障無いように構築すること。
（2）協議の上決定した設定内容について、全て設定作業を行い、本市指定のサーバラックに設置すること。
（3）透過モードでスパム対策を実施できるように設定すること。

5. 保守・運用に関する要件

（1）機器のハードウェア及びソフトウェアは、導入後 5 年間の保守を行うこと。
（2）無停電電源装置のバッテリーも保守対象とし、劣化した場合には交換対応を行うこと。
（3）本市からの各種問い合わせに対する対応時間は、平日 9 時から 17 時とし、ハードウェアの障害に関しては、当日訪問修理以上の内容とする。但し、冗長構成等により通常運用に支障が出ない場合は翌日訪問修理以上の内容で可とする。
（4）サーバのハードウェア保守は平日 9 時から 17 時の当日訪問修理以上の内容とする。
（5）ソフトウェア（ファームウェア含む）は、最低週 1 回パッチの有無を確認し、パッチ配布後 1 週間以内にアップデート作業を実施すること。
（6）アップデート作業はリモートでの作業で構わないが、作業時に本市に対しメールでアップデート内容の通知を行うこと。
（7）システムの再起動を伴うアップデート作業については、事前に本市とスケジュール調整の上、オンサイトで作業を実施すること。
（8）システム再起動を伴うオンサイトの作業は、月 1 回までを上限とし、月 1 回を超える回数のシステム再起動を必要とするパッチが配布された場合の取り扱いについては、別途本市と協議の上、対応方法を決定する。
（9）本市から電話・E-Mail 等を用いた障害・運用保守に係る問い合わせについて、電話対応及び現地対応により一時切り分けを含む障害切り分け並びに保守対応を実施すること。
（10）本入札における落札業者においては、入札金額内訳書に記載の月額保守費用を契約金額とする運用保守業務契約を本市と別途締結するものとする。本運用保守契約は令和 8 年 10 月 1 日から 5 年間の長期継続契約※を行う。

※ 長期継続契約においては、八尾市は翌年度以降において八尾市の歳出予算におけるこの契約の契約金額について減額又は削減された場合には、この契約を解除することがあります。また、契約締結業者はこの契約を解除された場合において、損害が生じたときは、八尾市に対してその損害の賠償を請求することができます。

6. 完成図書

ファイアウォール等機器の設定内容、ソフトウェア導入・設定内容を詳細に記し、再導入が可能な内容のものを令和 8 年 9 月末日までに納品すること。

7. その他留意事項

（1）納入した機器製品に添付される付属品、取扱説明書、保証書など一式を含めて納品すること。
（2）機器の空箱、梱包材は機器設置作業終了後持ち帰ること。
（3）機器は、本市が指定する場所に納入すること。なお、指定場所は契約後指示することとする。
（4）納入した機器に起因する障害については、設定作業後も無償にて速やかに対応し障害を除去すること。