**α’モデル新規構築事業**

**仕様書**

**2024年（令和6年）年10月**

**釧路市**

１．契約名

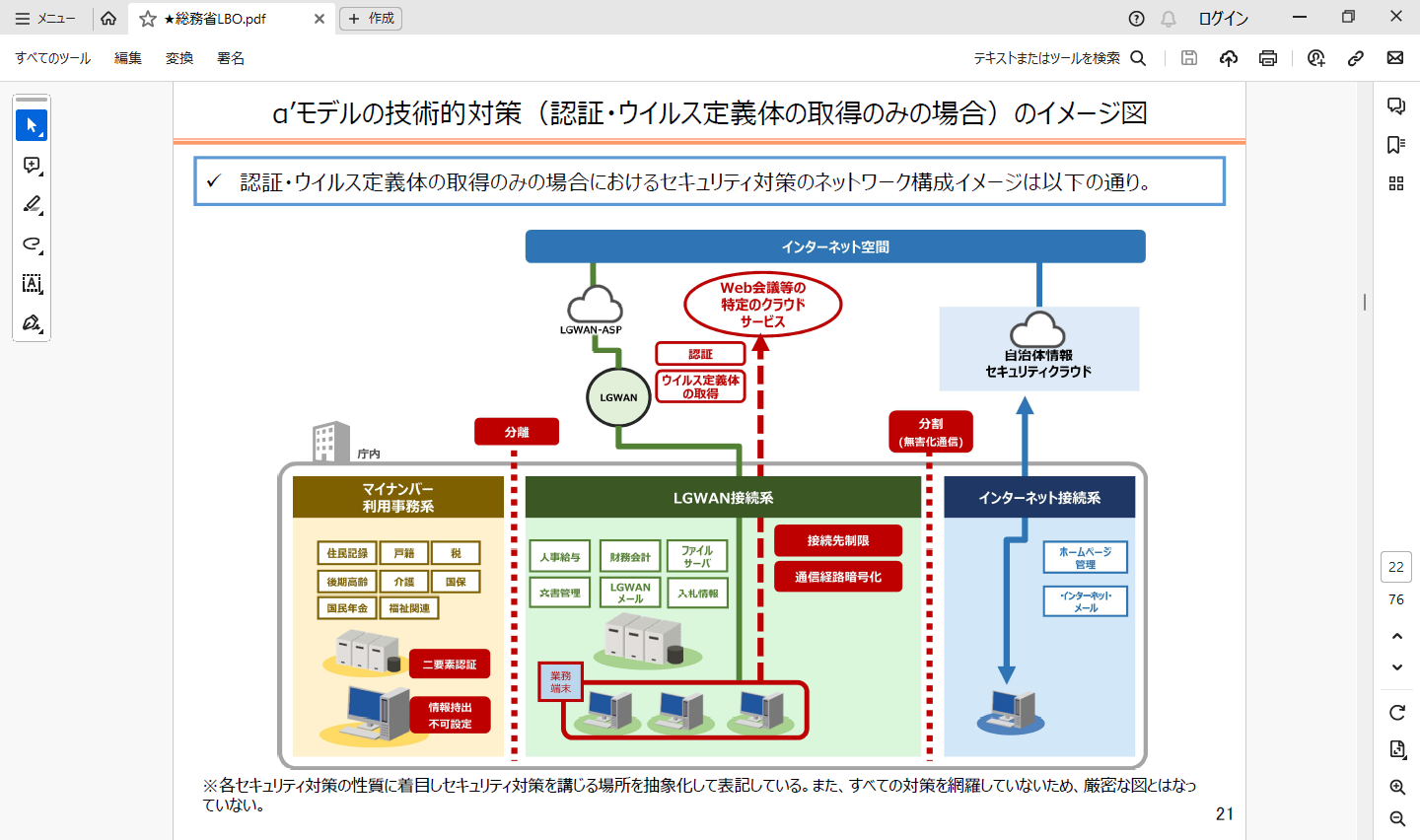
α’モデル新規構築事業

２．目的

　　釧路市（以下、「当市」という。）では、現行のインターネットが分離された環境であるαモデルにおいて、αモデルを維持しつつ、Microsoft365に代表されるクラウドサービスや特定のインターネットサービス利用に際して、安全で効率的な運用及び情報管理を図るため、ローカルブレイクアウトを可能とするα’モデルを構築し、特定の通信を安全に接続するプロキシ装置を導入するもの。

３．業務概要

図１構成イメージの調達対象機器の導入構築及び庁舎内各端末への設定



Entra ID conect

サーバーの構築

調達範囲

**光回線**

プロキシ装置

図1構成イメージ

(1) LGWAN接続系から特定のクラウドサービスへ接続する通信環境を構築すること。

(2) ローカルブレイクアウトする回線は、北海道セキュリティクラウドへの回線とは別のインターネット回線を利用すること。なお、当該インターネット回線については本調達に含まれるものとする。

(3) 利用想定は、サブスクリプション版Office（Microsoft365 Apps for enterprise）利用のみである。

(4) 総務省が発出している「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の内容を熟知し、ブレイクアウトとセキュリティの双方の要件を満足するシステムを選定すること。

４．賃貸借期間

2025年(令和7年)3月3日から2030年(令和12年)2月28日まで

５．賃貸借物件

(1) ハードウエア

|  |  |
| --- | --- |
| 台数 | 2台 |
| 形状 | 19インチラックに収容でき、1Uに収まること。 |
| インターフェース | ・1GbE RJ-45インターフェースを16ポート以上有すること。  ・1GbE SFPインターフェースを8ポート以上有すること。  ・10GbE SFP+インターフェースを4ポート以上有すること。  ・25GbE SFP28 / 10GbE SFP+インターフェースを4ポート以上有すること。  ・1GbE RJ-45MGMT/HAインターフェースを2ポート以上有すること。 |
| 記憶装置 | 240GB以上のSSD（ソリッドステートドライブ）を2つ以上搭載していること。ただし、外部にログを保存する場合は別途専用装置の利用または当市が準備する仮想基盤上に構築する。その場合、本体内部にログを保存する記憶領域の保存方式に準じること。 |
| 電源 | ・冗長化可能なこと。  ・平均消費電力、最大消費電力を提示できること。  ・熱量（BTU/h）を提示できること。  ・MTBF(hrs)の値を提示できること。 |

1. パフォーマンス

|  |  |
| --- | --- |
| アプリケーションスループット | ・NGFWスループットはエンタープライズ混合テストかつログを有効にした状態で11.5Gbps以上であること。  ・脅威保護スループットはエンタープライズ混合テストかつログを有効にした状態で10.5Gbps以上であること。  ・IPv4ファイアウォールスループットは1518 / 512 / 64byte UDPで139 / 137.5 / 70Gbps以上であること。  ・ファイアウォールのレイテンシは64byte UDPで4.12μsであること。  ・IPsec VPNスループットはAES 256,SHA-256を用い、512byteで55Gbps以上であること。  ・SSLインスペクションのスループットはHTTPSを利用し、IPSを実施した際の平均値が9Gbps以上であること。 |

1. 機能要件

|  |  |
| --- | --- |
| 通信可視化 | HTTPS通信の可視化とヘッダの挿入を追加ライセンスなく実施できること。 |
| 振り分け | 宛先ドメイン名に応じて通信を振り分けること。 |
| URLの更新機能 | 不定期で変更となるMicrosoft 365のクラウドサービスのURL情報のリストを自動的に更新できること。 |
| テナント制御 | 指定した法人アカウントのみクラウドサービスへのログインを許可し、個人アカウントや他の法人アカウントでのログインを制限可能なこと。 |
| 冗長化 | 冗長構成を実現できる製品を選定し、トラフィックの負荷分散や故障時の自動での切換えなどに対応すること |
| 負荷分散 | ラウンドロビン、重み付き最速応答時間に対応していること。 |
| 認証機能 | RADIUS、LDAP、Active Directoryと連携し認証プロキシの機能を提供できること。 |
| UTM機能 | UTM機能を有すること。 |

1. ソフトウェア

|  |  |
| --- | --- |
| ライセンス | 現在利用中のライセンスはMicrosoft 365 Apps for enterpriseであり、本調達には含まない。 |

1. 設置場所

　　当市総務部情報システム課サーバー室内の当市が指定するラック内に搭載すること。

1. 契約期間満了後、機器を無償譲渡すること。

６．稼働予定日

　　受託者と釧路市の協議により決定する。

　　賃貸借料には導入準備期間における作業費を含めること。

７．賃貸借に関わる付帯作業の内容

(1) 作業スケジュールの管理等

① 機器更新に向けた具体的な作業項目、その役割分担を検討、整理し明確にすること。

② 移行試験、運用試験について明確にスケジュール化し、当市との合意をとること。

③ 上記作業についてスケジュールを作成し、進捗管理及びスケジュール調整すること。

(2) 構築範囲

① 概要

(ア)　LGWAN系端末からOffice365のライセンス認証ができるよう、本調達のクラウドサービス用α’モデル対応機器（セキュリティ機器、ローカルブレイクアウト装置）プロキシ装置を構築すること。

(イ)　Entra ID Connect Serverを当市が準備する仮想基盤上に構築し、既存認証サーバー（Active Directory）（以下、「既存AD」という。）とEntra IDの情報を同期すること。なお、認証方法はパスワードハッシュ同期とすること。

(ウ) Entra ID Connect Serverで利用するWindows Server OSは当市が提供するものとする。

(エ)　Office展開ツール（ODT）を利用したインストーラーの作成し提供すること。

(オ)　既存ADに関する作業については、既存AD保守業者と調整すること。

(カ)　既存ネットワークに関する作業については、既存ネットワーク保守業者と調整すること。

② 詳細

1. LGWAN接続系からMicrosoft 365や当市が指定する特定のクラウドサービスへ接続する通信環境を構築すること。
2. Microsoft、Google、Adobe、Salesforce、Box等の大手SaaSに関するIPアドレス、ポート番号等の情報をデータベースとして保有し、ルーティングによるローカルブレイクアウトが可能であること。また、データベース情報は随時自動更新されること。
3. SaaSベンダーが公開する接続先情報に基づき、FQDNベースでのローカルブレイクアウトが可能であることまた、その接続先情報を自動更新する仕組みを有すること。
4. SaaS接続先情報を自動更新する仕組みは、メーカー代理店のサービスを活用してもよいものとする。ただし、以下の３点を条件とする。

・当該サービスを無償で利用できること

・当該サービスに関する問合せ専用のメールアドレスを有するなど、保守サポート体制があるサービスであること

・認可された機器にのみ当該サービスの提供を行う、認証の仕組みを有すること

（オ） 管理者が手動で設定したFQDNを元にしたローカルブレイクアウトの設定が可能であること。

（カ）ローカルブレイクアウトしたいSaaS毎にFQDNベースとIPアドレスベースを使い分けでき

ること。

（キ）機器として多段プロキシ構成が可能なExplicit Proxy機能を有すること。

（ク）Microsoft365、GoogleWorkspace等のテナント制御を実施するために、SSL通信の復号化及びHTTPヘッダー情報を埋め込む機能を有すること。

（ケ）IDS／IPS機能、アンチウイルス機能、CDR機能、Webフィルタリング機能等の総合的なセキ

ュリティ機能を有する統合型脅威管理（UTM）装置としても使用できること。

（コ）次世代型FWとしてアプリケーション毎に通信を識別してアプリケーションコントロールが可

能であること。また、SSLインスペクション機能と組み合わせて、https通信のアプリケーシ

ョンであっても、アプリケーションの識別及びコントロールが可能であること。（例：Microsoft OneDriveのダウンロードのみ止める、など）

（サ）ただし、上記機能については機器として機能を有していればよい。実際にどの機能を使用するかは、導入打合せ等により当市担当者と協議の上、決定するものとする。

(シ) ユーザ管理にかかる初期設定をすべて完了したうえで納品とすること。なおユーザ管理にはEntra IDを利用すること。

(ス) 現在使用しているメールドメインである、@city.kushiro.lg.jpをMicrosoft365アプリケーション内で継続して使用できるよう調整すること。

(セ) Microsoft365のOneDriveの利用を制限すること。

(ソ) 既存ADがもつユーザとEntra IDを同期連携できるように設定すること。

(タ) 既存ADにOffice認証用のOU（組織）を作成し、そのOUのみ同期をとる設定とすること。

(チ) Office展開ツール（ODT）を利用したインストーラー~~の作成し~~を提供すること。ただし、端末へのインストールは含まないこととする。

(ツ) 既存ADを調整し、端末がMicrosoft365向け通信のプロキシサーバーとして、本調達のクラウドサービス用プロキシ装置を設定するよう調整すること。

(テ) 既存環境に影響がないことを確認すること。

(3) 当市への報告事項

①　策定したスケジュールの進捗状況を随時報告すること。

②　次工程に進む前に必ず当市の承認を得ること。

③　本稼動の判定については、当市と協議の上判断を行う。

８．インターネット回線要件

(1) 本事業で新たに本プロキシ装置を経由するクラウドサービスなどへの通信専用の光回線を１回線敷設すること。

(2) 回線の敷設にかかる費用は本調達に含めること。

(3) 回線故障時の受付は専用のコールセンタを有し、受付対応は24時間365日とする。

(4) 回線の故障修理対応も同様に24時間365日とする。

(5) 技術規格上の最大通信速度はデータ受信・送信について概ね1Gbpsとする。

(6) インターネット回線を収容するルーターを本調達に含めること。但し、ルーター機能をプロキシ装置で具備できる場合は、この限りではない。

９．保守要件

(1) システム保守

導入年度内については、SEサポートを行い、設定内容についての問合せ対応、不具合時の調査支援を行うこと。また、重大な障害等で仮想マシンの再構築が必要と判断した場合においては、既存仮想基盤側でのバックアップ復旧を現行保守業者が行うが、動作確認等は行うこと。２年目以降のシステム保守については、別途契約を予定しているため本調達に含めない。

(2) ハードウェア保守

　契約期間中のハードウェア保守については、24時間365日対応とし、本調達に含めること。交換作業等のハードウェア保守に含まない作業がある場合については別途調達として構わない。

１０．法令・条例等の適用

賃貸人は、業務の実施にあたり、関係する法令・条例等を遵守しなければならない。

１１．損傷部保証

賃貸人は当市の建造物、機器等を損傷しないように十分注意すること。万一損傷した場合には、当市職員の指示に従い、同等以上の資材を持って、速やかに現状復旧をはかること。

なお、復旧に要する費用はすべて賃貸人の負担とする。

１２．秘密の保持等

(1) 釧路市個人情報保護条例及び関係規定を遵守しなければならない。

(2) 賃貸人は、業務に関して知り得た一切の事実を、第三者に漏洩してはならない。

(3) 資料作成等で持ち帰り作業が必要な場合については、賃貸人の事業所を作業場所とする。ただし、個人データの持ち出しに関しては、これを一切禁止する。

(4) 賃貸人は、当市が特に認めた場合を除き、業務の処理に必要なデータ及び資料を複写し、若しくは複製してはならない。

(5) 賃貸人は、当市が特に認めた場合を除き、業務の処理に必要なデータ及び資料を他の目的に使用してはならない。

(6) 賃貸人は、作業を行うにあたり常に事故又は災害の防止に努め、事故、若しくは災害、又はセキュリティに関する事案が発生したときは、直ちに当市に対し通報して適切な措置をとるとともに、遅滞なく書面をもって報告しなければならない。

(7) 賃貸人は、業務の処理にかかる磁気記録媒体に記録されているデータの内容を侵す一切の行為をしてはならない。

(8) 賃貸人は、業務の処理に使用した全ての記録、資料等について、業務終了後すみやかに当市に返還しなければならない。

１３．提出物等

業務完了後、以下の資料等を提出すること。併せて電子媒体による提出も行うこと。

|  |  |
| --- | --- |
| 設定書 | Entra ID Connect Server設定書  クラウドプロキシ装置設定書  （データおよび紙媒体各1部） |
| 工程写真、材料写真 | 一式（データおよび紙媒体各1部。特に、材料がもれなく納品されたことが確認できるよう全て撮影すること） |

１４．その他

(1) 作業開始にあたっては、速やかに当市と作業方法、作業スケジュール、作業体制及び作業分担等に関し、打ち合わせを行うこと。

(2) 作業担当者が交替する場合等は、事前に当市の同意を得ることとし、以後支障のないよう十分引き継ぎを行うこと。

(3) 作業上作成した資料については、適宜当市の確認を受けること。

(4) 作業上必要な打ち合わせは、適宜行うこと。各作業の打ち合わせ結果は、速やかに議事録を作成し、当市にその都度提出すること。

(5) 現場での作業にあたっては、通常業務への影響が最小限となるように調整し、効率的に進めること。また、それぞれの作業場所の管理を行う職員の指示に従うとともに、それぞれの運用ルールに従うこと。

(6) 納入時に排出される梱包材等については、受託者が回収し適切に処理すること。

(7) この仕様書に定めのない事項については、必要に応じ、当市及び賃貸人で協議の上、定めるものとする。