共用LANシステム
リモートワーク向けインフラ基盤の更新及び運用保守
調達仕様書

令和8年2月

独立行政法人　医薬品医療機器総合機構

目次

１　調達案件の概要に関する事項.....1
（１）　調達件名 1
（２）　用語の定義..... 1
（３）　調達の背景と目的..... 1
（４）　作業スケジュール..... 1
２　調達案件及び関連調達案件の調達単位、調達の方式等に関する事項.....1
（１）　調達案件及び関連する調達案件の調達単位、調達の方式、実施時期 1
（２）　調達案件間の作業区分 3
３　作業の実施内容に関する事項.....3
（１）　作業の内容..... 3
（２）　成果物の期日等 4
４　作業の実施体制・方法に関する事項.....4
（１）　作業実施体制..... 4
（２）　作業場所 5
５　作業の実施に当たっての遵守事項.....5
（１）　基本事項 5
（２）　機密保持、資料の取扱い..... 5
（３）　遵守する法令等 6
６　成果物の取扱いに関する事項.....7
（１）　知的財産権の帰属..... 7
（２）　契約不適合責任 7
（３）　検収..... 8
７　入札参加資格に関する事項.....8
（１）　**入札参加要件** 8
（２）　**入札制限** 9
８　情報セキュリティの履行状況の確認に関する事項 9
９　再委託に関する事項 10
１０ その他特記事項.....11
（１）　環境への配慮..... 11
（２）　その他..... 11
１１ 附属文書.....11
（１）　要件定義書..... 11
１２ 窓口連絡先 11

１　調達案件の概要に関する事項

（１）　調達件名

共用 LAN システム リモートワーク向けインフラ基盤の更新及び運用保守

（２）　用語の定義

表 １.１ 用語の定義

用語	概要
共用 LAN システム	PMDA の共通的基盤システム。メールサーバやグループウェアサーバ、クライアント端末、ネットワーク機器等で構成されている。
共用 LAN 運用支援業者	共用 LAN システムを運用するにあたり、PMDA から運用業務の一部を委託されている業者。
業務用 PC	PMDA で業務を行うにあたり職員が使用している端末。

（３）　調達の背景と目的

独立行政法人医薬品医療機器総合機構（以下「PMDA」という。）では、役職員が利用するメール、電子掲示板、電子書庫等の機能や、PMDA 内の各業務システムの基盤として、PMDA の基幹業務システムである共用 LAN システムを整備し、運用を行っている。

共用 LAN システムではリモートワークを行うための情報システム（以下リモートワーク基盤）を運用しており、ある程度の業務をリモートワークでも実施できる体制を取っている。現行のリモートワーク基盤は導入から 3 年以上経過しハードウェア等の保守期限が迫ってきたことからシステム更新を行う(以下「本調達」という。)。本システムは PMDA の職員が業務を行うための基盤となるため、高い信頼性と運用柔軟性を確保できるように構成する。

（４）　契約期間

構築：契約開始日から令和 9 年 5 月 31 日まで

運用・保守：令和 9 年 6 月 1 日から令和 14 年 5 月 31 日まで

（５）　作業スケジュール

本業務に係る想定スケジュールの概要を「別紙 1 概略スケジュール」に示す。

２　調達案件及び関連調達案件の調達単位、調達の方式等に関する事項

（１）　調達案件及び関連する調達案件の調達単位、調達の方式、実施時期

関連する調達案件の調達単位、調達の方式、実施時期は次の表の通り。

表 2.1　関連する調達案件の調達単位、調達の方式、実施時期等

項番	調達案件名	補足
1	共用 LAN システム 業務用 PC の更新	本調達で使用する業務用 PC を購入する。
2	共用 LAN システムに係る運用支援業務	-

（2）　調達案件間の作業区分

表 2.1　関連する調達案件の調達単位、調達の方式、実施時期等に示した案件との作業区分は以下の通り。

① 共用 LAN システム 業務用 PC の購入

本件で購入した業務用 PC を使用して本調達はシステム設計を行う。システム設計時、構築時に業務用 PC のハードウェア仕様に起因される課題が発生した場合、本調達の受注者は本件のハードウェア保守手順に基づいてハードウェアのサポートに問い合わせを行い課題の解決を行うこと。

また PC は本件受注者宛に納品するため、本件受注者は保管に必要な場合は倉庫等を準備すること。

② 共用 LAN システムに係る運用支援業務

本調達の受注者は本調達で導入したシステムの定常的な運用管理、保守体制、業務用 PC の運用サイクル手順を作成し、PMDA 及び本件受注者に引継ぎを行うこと。

3　作業の実施内容に関する事項

（1）　作業の内容

本調達の業務内容を以下に示す。これらの業務に伴う PMDA との協議、打ち合わせ等の出席、資料作成を含む。詳細な要件は本調達仕様書の各別紙に記している。

① リモートワーク向け情報システムインフラの設計・構築・移行

受注者は本紙及び別紙に記載のシステム要件を満たす情報システムの設計及び構築、システム移行作業を行うこと。

② 業務用 PC のキッティング

受注者はPMDAが支給する業務用PCハードウェアのキッティングを行うこと。またPCキッティング運用を行うための環境の整備も行うこと。

③　ドキュメントの作成

受注者は「別紙3 システム詳細要件」に示すドキュメントを作成しPMDAに提出すること。

④　システム保守

受注者は本調達で導入した情報システムのハードウェア保守、設計事項、製品仕様に関する保守を行うこと。

（２）　成果物の期日等

納入成果物は以下の2回に分けて提出しPMDAの承認を得ること。PMDAの資料確認、確認結果による修正等の期間を考慮して提出すること。

表 3.1　納入成果物の提出期限

項番	納入成果物の対象作業	期限
1	業務用PC全台のキッティング作業に関する作業	令和9年5月31日
2	項番1以外の作業	令和9年4月30日

ただし、設計や導入作業のようなシステム構成の把握、評価に必要なドキュメントは各工程でPMDAの要求に応じて提出すること。

ドキュメントは以下の要件を満たして作成すること。

1. PDF形式及びMicrosoft 365 Office及びVisioで扱える形式とすること。ただし、PMDAが別に形式を定めて提出を求めた場合はこの限りではない。文章が主体となるドキュメントはMarkdown形式としても良い。
2. 各納入成果物は日本語により作成すること。製品マニュアルについては日本語または英語によるものとする。
3. CD-RまたはDVD-Rによる正副2部及び電子メールにより納入すること。
4. 本業務を実施する上で必要となる一切の機器納入物等は受注者の責任で手配するとともに費用を負担すること。
5. 各工程の納入成果物も含め、本調達に係る全ての資料を納入すること。

４　作業の実施体制・方法に関する事項

（１）　作業実施体制

① 本調達の導入作業に係るリーダとしてプロジェクトマネージャを設定すること。
② プロジェクトマネージャは本調達の導入作業における各作業の遅延が発生しないように作業体制を整えること。
③ システム設計・導入等を複数業者が連携（再委託を含めて）して実施する等の場合は、参画する各業者の役割分担等を明示すること。

（２） 作業場所

① 受注業務の作業場所（サーバ設置場所等を含む）は、（再委託も含めて）PMDA 内、又は日本国内で PMDA の承認した場所で作業すること。
② 受注業務で用いるサーバ、データ等は日本国外に持ち出さないこと。
③ PMDA 内での作業においては、必要な規定の手続を実施し承認を得ること。
④ 必要に応じて PMDA 職員は現地確認を実施できることとする。

５ 作業の実施に当たっての遵守事項

（１） 基本事項

受注者は、次に掲げる事項を遵守すること。

① 本業務の遂行に当たり、業務の継続を第一に考え、善良な管理者の注意義務をもって誠実に行うこと。

② 本業務に従事する要員は、PMDA と日本語により円滑なコミュニケーションを行う能力と意思を有していること。

③ 本業務の履行場所を他の目的のために使用しないこと。

④ 本業務に従事する要員は、履行場所での所定の名札の着用等、従事に関する所定の規則に従うこと。

⑤ 要員の資質、規律保持、風紀及び衛生・健康に関すること等の人事管理並びに要員の責めに起因して発生した火災・盗難等不祥事が発生した場合の一切の責任を負うこと。

⑥ 受注者は、本業務の履行に際し、PMDA からの質問、検査及び資料の提示等の指示に応じること。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。

⑦ 次回の本業務調達に向けた現状調査、PMDA が依頼する技術的支援に対する回答、助言を行うこと。

⑧ 本業務においては、業務終了後の運用等を、受注者によらずこれを行うことが可能となるよう詳細にドキュメント類の整備を行うこと。

（２） 機密保持、資料の取扱い

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおり。

① 受注者は、受注業務の実施の過程で PMDA が開示した情報（公知の情報を除く。以下同じ。）、他の受注者が提示した情報及び受注者が作成した情報を、本受注業務の目的以外に使用又は第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。

② 受注者は、本受注業務を実施するにあたり、PMDA から入手した資料等については管理簿等により適切に管理し、かつ、以下の事項に従うこと。

- 複製しないこと。
- 用務に必要がなくなり次第、速やかに PMDA に返却又は消去すること。
- 受注業務完了後、上記①に記載される情報を削除又は返却し、受注者において該当情報を保持しないことを誓約する旨の書類を PMDA に提出すること。

③ 応札希望者についても上記①及び②に準ずること。

④ 「独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程」の第 52 条に従うこと。

⑤ 「秘密保持等に関する誓約書」を別途提出し、これを遵守しなければならない。

⑥ 機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

（3） 遵守する法令等

本業務を実施するにあたっての遵守事項は、以下のとおり。

① 受注者は、最新の「政府機関の情報セキュリティ対策のための統一基準」、「府省庁対策基準策定のためのガイドライン」、「医療情報システムの安全管理に関するガイドライン」及び「独立行政法人　医薬品医療機器総合機構情報サイバーセキュリティポリシー」（以下、「セキュリティポリシー」という。）に遵守すること。セキュリティポリシーは非公表であるが、「政府機関の情報セキュリティ対策のための統一基準群（令和 5 年度版）」に準拠しているので、必要に応じ参照すること。セキュリティポリシーの開示については、契約締結後、受注者が担当職員に「秘密保持等に関する誓約書」を提出した際に開示する。

② PMDA へ提示する電子ファイルは事前にウイルスチェック等を行い、悪意のあるソフトウェア等が混入していないことを確認すること。

③ 民法、刑法、著作権法、不正アクセス禁止法、個人情報保護法等の関連法規を遵守することはもとより、下記の PMDA 内規程を遵守すること。

- 独立行政法人 医薬品医療機器総合機構 情報システム管理利用規程
- 独立行政法人 医薬品医療機器総合機構 個人情報管理規程

④ 受注者は、本業務において取り扱う情報の漏洩、改ざん、滅失等が発生することを防止する観点から、情報の適正な保護・管理対策を実施するとともに、これらの実施状況について、PMDA が定期又は不定期の検査を行う場合においてこれに応じること。万一、情報の漏洩、改ざん、滅失等が発生した場合に実施すべき事項及び手順等を明確にするとともに、事前に PMDA に提出すること。また、そのような事態が発生した場合は、PMDA に報告するとともに、当該手順等に基づき可及的速やかに修復すること。

６　成果物の取扱いに関する事項

（１）　知的財産権の帰属

知的財産の帰属は、以下のとおり。

① 本件に係り作成・変更・更新されるドキュメント類及びプログラムの著作権（著作権法第 21 条から第 28 条に定めるすべての権利を含む。）は、受注者が本件のシステム導入の従前より権利を保有していた等の明確な理由により、あらかじめ書面にて権利譲渡不可能と示されたもの以外、PMDA が所有する等現有資産を移行等して発生した権利を含めてすべて PMDA に帰属するものとする。

② 本件に係り発生した権利については、受注者は著作者人格権（著作権法第 18 条から第 20 条までに規定する権利をいう。）を行使しないものとする。

③ 本件に係り発生した権利については、今後、二次的著作物が作成された場合等であっても、受注者は原著作物の著作権者としての権利を行使しないものとする。

④ 本件に係り作成・変更・修正されるドキュメント類及びプログラム等に第三者が権利を有する著作物が含まれる場合、受注者は当該著作物の使用に必要な費用負担や使用許諾契約に係る一切の手続きを行うこと。この場合は事前に PMDA に報告し、承認を得ること。

⑤ 本件に係り第三者との間に著作権に係る権利侵害の紛争が生じた場合には、当該紛争の原因が専ら PMDA の責めに帰す場合を除き、受注者の責任、負担において一切を処理すること。この場合、PMDA は係る紛争の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者にゆだねる等の協力措置を講ずる。
なお、受注者の著作又は一般に公開されている著作について、引用する場合は出典を明示するとともに、受注者の責任において著作者等の承認を得るものとし、PMDA に提出する際は、その旨併せて報告するものとする。

（２）　契約不適合責任

① 本業務の最終検収後 1 年以内の期間において、委託業務の納入成果物に関して本システムの安定稼動等に関わる契約不適合の疑いが生じた場合であって、PMDA が必要

と認めた場合は、受注者は速やかに契約不適合の疑いに関して調査し回答すること。調査の結果、納入成果物に関して契約不適合等が認められた場合には、受注者の責任及び負担において速やかに修正を行うこと。なお、修正を実施する場合においては、修正方法等について、事前に PMDA の承認を得てから着手すると共に、修正結果等について、PMDA の承認を受けること。

② 受注者は、契約不適合責任を果たす上で必要な情報を整理し、その一覧を PMDA に提出すること。契約不適合責任の期間が終了するまで、それら情報が漏洩しないように、ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本産業標準）に従い、また個人情報を取り扱う場合には JISQ15001（日本産業標準）に従い、厳重に管理をすること。また、契約不適合責任の期間が終了した後は、速やかにそれら情報をデータ復元ソフトウェア等を利用してもデータが復元されないように完全に消去すること。データ消去作業終了後、受注者は消去完了を明記した証明書を作業ログとともに PMDA に対して提出すること。なお、データ消去作業に必要な機器等については、受注者の負担で用意すること。

（３） 検収

納入成果物については、適宜、PMDA に進捗状況の報告を行うとともに、レビューを受けること。最終的な納入成果物については、納入成果物が揃っていること及びレビュー後の改訂事項等が反映されていることを、PMDA が確認し、これらが確認され次第、検収終了とする。

なお、以下についても遵守すること。

① 検査の結果、納入成果物の全部又は一部に不合格品を生じた場合には、受注者は直ちに引き取り、必要な修復を行った後、PMDA の承認を得て指定した日時までに修正が反映されたすべての納入成果物を納入すること。

② 納入成果物に規定されたもの以外にも、必要に応じて提出を求める場合があるので、作成資料等を常に管理し、最新状態に保っておくこと。

③ PMDA の品質管理担当者が検査を行った結果、不適切と判断した場合は、品質管理担当者の指示に従い対応を行うこと。

7 入札参加資格に関する事項

（１） 入札参加要件

応札希望者は、以下の条件を満たしていること。

① ISO9001 又は CMMI レベル 2 以上の認定を取得していること。

② ISO/IEC27001 認証（国際標準）又は JISQ27001 認証（日本産業標準）のいずれかを取得していること。

③ 応札時には、導入作業毎に十分に細分化された工数、概算スケジュールを含む見積り根拠資料の即時提出が可能であること。なお、応札後に PMDA が見積り根拠資料の提出を求めた際、即時に提出されなかった場合には、契約を締結しないことがある。

（2） 入札制限

情報システムの調達の公平性を確保するために、以下に示す事業者は本調達に参加できない。

① PMDA の CIO 補佐が現に属する、又は過去 2 年間に属していた事業者等

② 各工程の調達仕様書の作成に直接関与した事業者等

③ 設計・開発等の工程管理支援業者等

④ ①～③の親会社及び子会社（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社をいう。以下同じ。）

⑤ ①～③と同一の親会社を持つ事業者

⑥ ①～③から委託を請ける等緊密な利害関係を有する事業者

8 情報セキュリティの履行状況の確認に関する事項

本調達に係る業務の遂行における情報セキュリティ対策の履行状況を確認するため、PMDA の年次情報セキュリティ監査実施時などで PMDA が本件受注者に対して情報セキュリティ履行状況の確認が必要であると判断した場合は、以下の対応を求めるものとする。

① 情報セキュリティ履行状況の報告

PMDA がその報告内容と提出期限を定めて情報セキュリティ履行状況の報告を求めるものとする。

② 情報セキュリティ監査の実施

PMDA がその実施内容（監査内容、対象範囲、実施等）を定めて、情報セキュリティ監査を行う（PMDA が選定した事業者による監査を含む。）ものとする。

受注者は、あらかじめ情報セキュリティ監査を受け入れる部門、場所、時期、条件等を「情報セキュリティ監査対応計画書」等により提示すること。

受注者は自ら実施した外部監査についても PMDA へ報告すること。

受注者は、情報セキュリティ監査の結果、本調達における情報セキュリティ対策の履行状況について PMDA が改善を求めた場合には、PMDA と協議の上、必要な改善策を立案して速やかに改善を実施するものとする。

情報セキュリティ監査の実施については、本項に記載した内容を上回る措置を講ずることを妨げるものではない。

９　再委託に関する事項

① 受注者は、受注業務の全部又は主要部分を第三者に再委託することはできない。

② ①における「主要部分」とは、以下に掲げるものをいう。

1. 総合的企画、業務遂行管理、手法の決定及び技術的判断等。
2. SLCP-JCF2013 の 2.3 開発プロセス、及び 2.4 ソフトウェア実装プロセスで定める各プロセスで、以下に示す要件定義・基本設計工程に相当するもの。

・ 2.3.1 プロセス開始の準備

・ 2.3.2 システム要件定義プロセス

・ 2.3.3 システム方式設計プロセス

・ 2.4.2 ソフトウェア要件定義プロセス

・ 2.4.3 ソフトウェア方式設計プロセス

ただし、以下の場合には再委託を可能とする。

・ 補足説明資料作成支援等の補助的業務

・ 機能毎の工数見積において、工数が比較的小規模であった機能に係るソフトウェア要件定義等業務

③ 受注者は、再委託する場合、事前に再委託する業務、再委託先等を PMDA に申請し、承認を受けること。申請にあたっては、「再委託に関する承認申請書」の書面を作成の上、受注者と再委託先との委託契約書の写し及び委託要領等の写しを PMDA に提出すること。受注者は、機密保持、知的財産権等に関して本仕様書が定める受注者の責務を再委託先業者も負うよう、必要な処置を実施し、PMDA に報告し、承認を受けること。なお、第三者に再委託する場合は、その最終的な責任は受注者が負うこと。

④ 再委託先が、更に再委託を行う場合も同様とする。

⑤ 再委託における情報セキュリティ要件については以下のとおり。

・ 受注者は再委託先における情報セキュリティ対策の実施内容を管理し PMDA に報告すること。

・ 受注者は業務の一部を委託する場合、本業務にて扱うデータ等について、再委託先またはその従業員、若しくはその他の者により意図せざる変更が加えられないための管理体制を整備し、PMDA に報告すること。

・ 受注者は再委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関して、PMDA から求めがあった場合には情報提供を行うこと。

・ 受注者は再委託先にて情報セキュリティインシデントが発生した場合の再委託先における対処方法を確認し、PMDA に報告すること。

・ 受注者は、再委託先における情報セキュリティ対策、及びその他の契約の履行状況の確認方法を整備し、PMDA へ報告すること。
・ 受注者は再委託先における情報セキュリティ対策の履行状況を定期的に確認すること。また、情報セキュリティ対策の履行が不十分な場合の対処方法を検討し、PMDA へ報告すること。
・ 受注者は、情報セキュリティ監査を実施する場合、再委託先も対象とするものとする。
・ 受注者は、再委託先が自ら実施した外部監査についても PMDA へ報告すること。
・ 受注者は、委託した業務の終了時に、再委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

１０ その他特記事項

（１） 環境への配慮

環境への負荷を低減するため、以下に準拠すること。

① 本件に係る納入成果物については、最新の「国等による環境物品等の調達の推進等に関する法律（グリーン購入法）」に基づいた製品を可能な限り導入すること。

② 導入する機器等がある場合は、性能や機能の低下を招かない範囲で、消費電力節減、発熱対策、騒音対策等の環境配慮を行うこと。

（２） その他

PMDA 全体管理組織（PMO）が担当課に対して指導、助言等を行った場合には、受注者もその方針に従うこと。

本業務を応札するにあたり必要となる情報を開示するので、希望する者は別紙 4 を参照すること。

１１ 附属文書

（１） 要件定義書

別紙 1 概略スケジュール
別紙 2 システム概要図
別紙 3 システム詳細要件

１２ 窓口連絡先

独立行政法人　医薬品医療機器総合機構　情報化統括推進室

共用 LAN システム担当者

電話：03 (3506) 9485

Email：sa_infragr_xj●pmda.go.jp

※迷惑メール防止対策をしているため、●を半角のアットマークに置き換えること。

別紙１　概略スケジュール

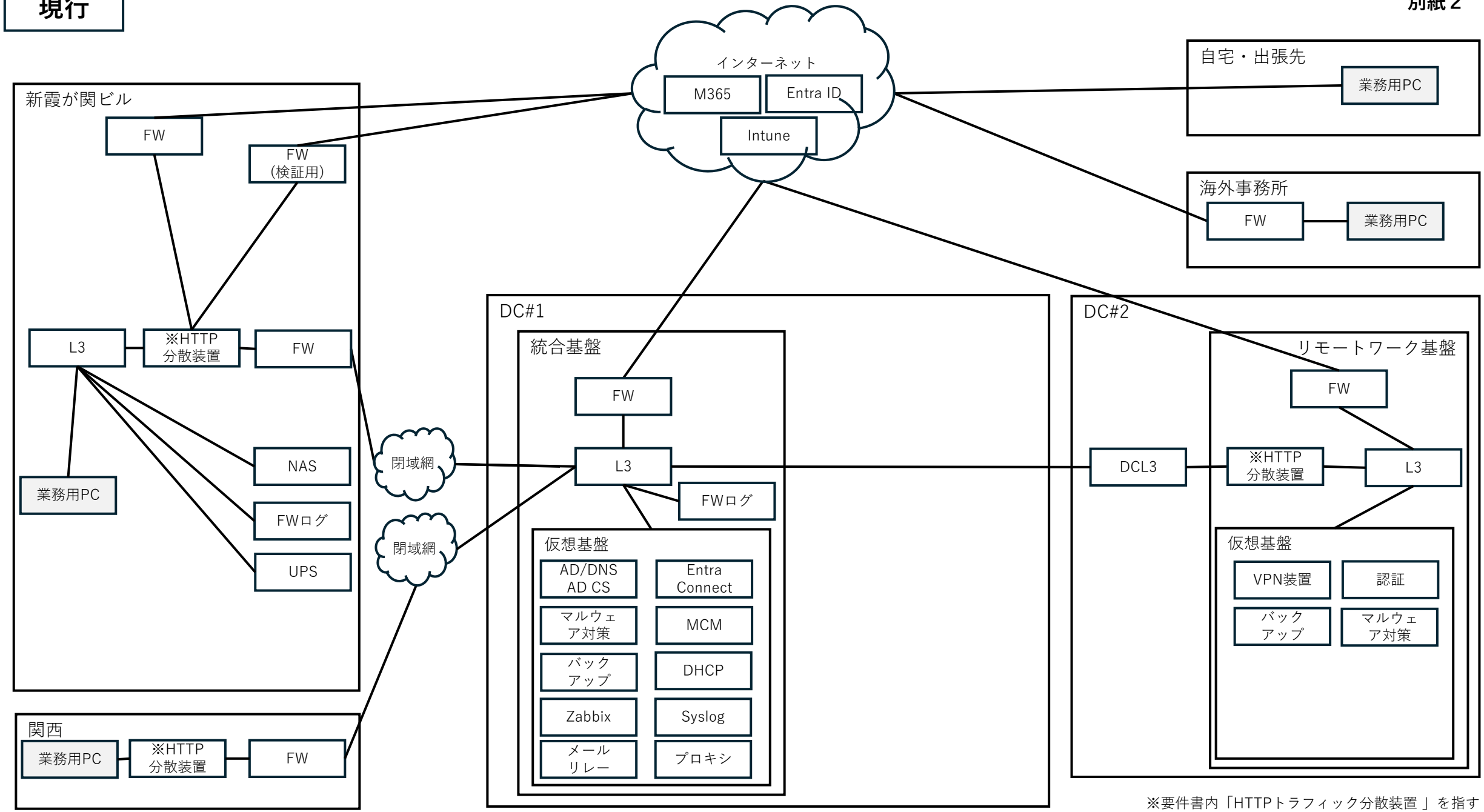
	2025年									2026年												2027年					▼				
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月
基盤																														
機器手配																														
基盤設計・構築																														
PC設計・構築																														
PC動作確認																														
デプロイ・PC交換																														
新旧環境並行稼働期間																														
保守（2032年5月末まで）																														

	2025年									2026年												2027年					▼				
	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月
PC																														
機器手配																														
納品																														
保守（2032年5月末まで）																														

※PCの納入スケジュールは本件受注者のスケジュール都合で前後する可能性がある

別紙２

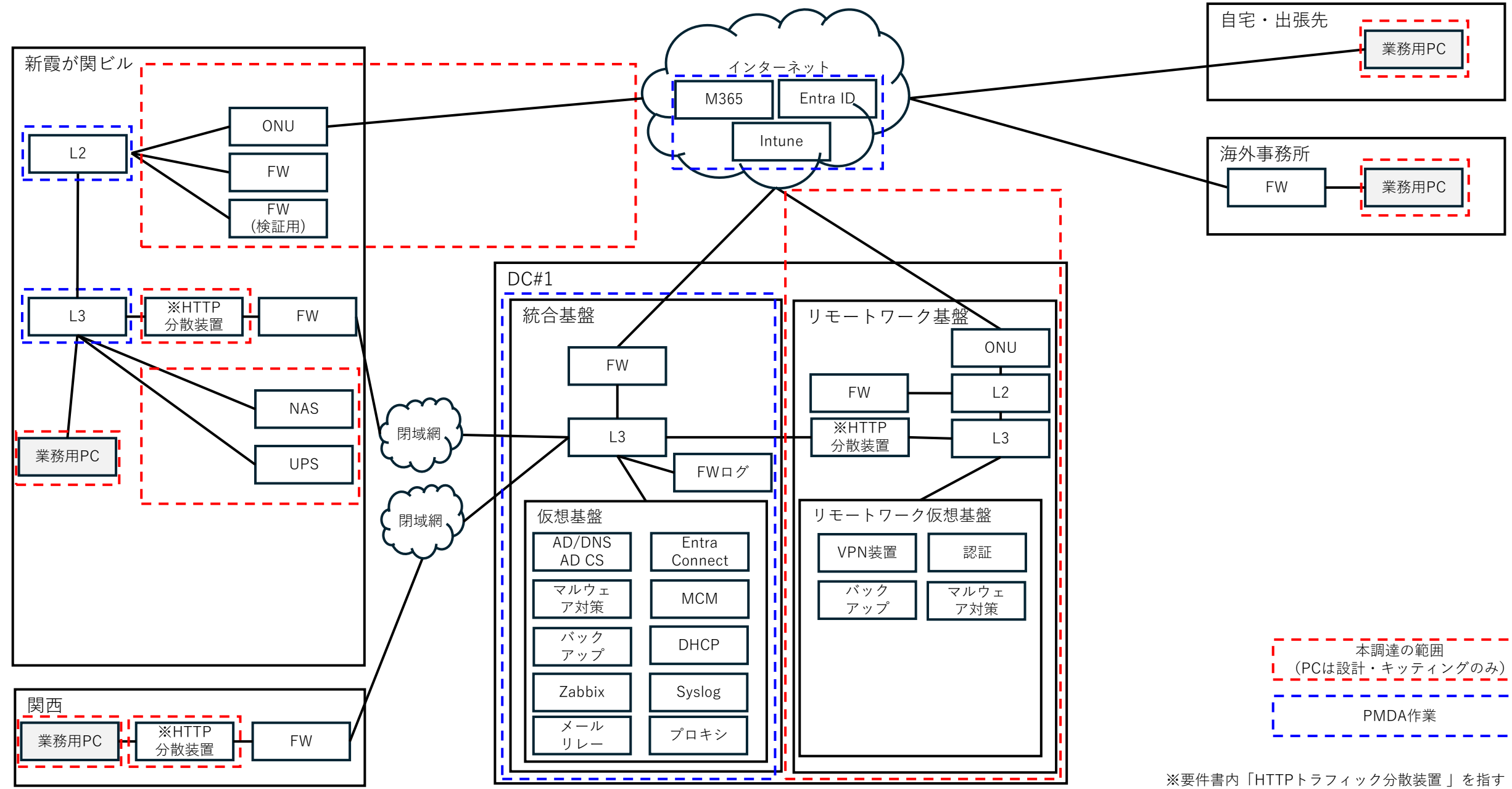
現行



※要件書内「HTTPトラフィック分散装置 」を指す

次期構成案（論理接続イメージ）

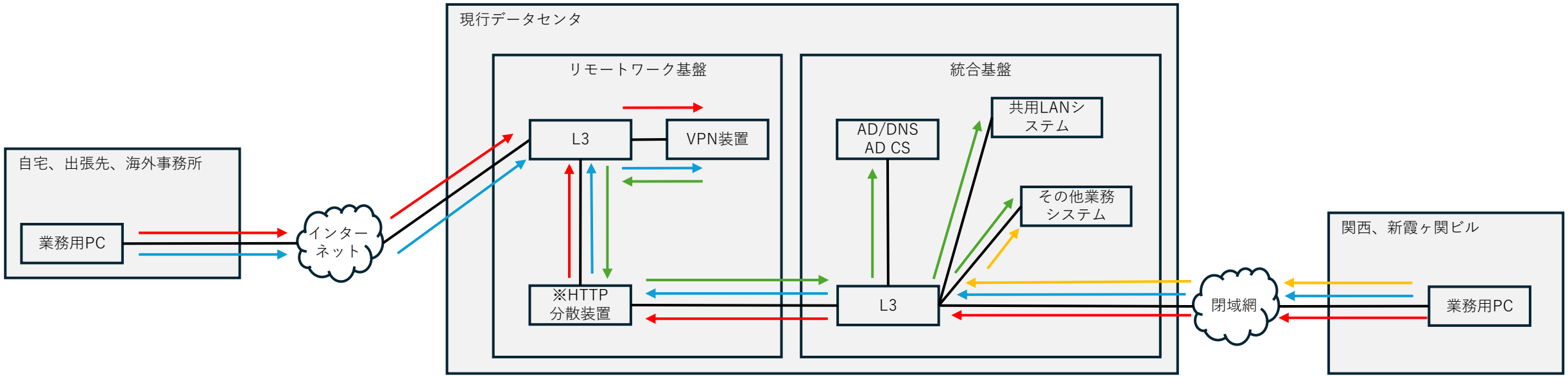
別紙２



※要件書内「HTTPトラフィック分散装置 」を指す

リモートワーク接続イメージ

別紙２



【接続概要】

- 業務用PCにインストールしたクライアントがOS起動時にVPN装置へ接続（赤色矢印）
- VPN装置への接続が確立されると業務用PCに仮想NICが割当たり業務用PC-VPN装置間でVPNトンネルを張る（青色矢印）
- VPNトンネル経由で基盤内のL3ルーティングに従い各システム等宛先に接続する（緑色矢印）
- VPNトンネルではなく実NICから通信する宛先もあり、クライアントが取得するVPN装置のポリシーにて制御される（黄色矢印、図の宛先は例）

※要件書内「HTTPトラフィック分散装置 」を指す

共用 LAN システム　リモートワーク環境の更新

別紙 3　システム詳細要件

1.　プロジェクト要件

1.1.　プロジェクト計画

受注者は本調達の全工程の基本的な進め方を検討し、文書にまとめてプロジェクト開始時に PMDA と合意すること。

1.1.1.　プロジェクト計画に関するドキュメント

受注者はプロジェクトのスケジュール、進行方法を記したプロジェクト実施計画書を作成し、PMDA の承認を得ること。プロジェクト実施計画書に最低限記載が必要な事項は以下の通り。

- プロジェクトスコープ
- プロジェクト体制表
- WBS (受注者と PMDA の作業分担を含めること)
- プロジェクト管理要領(文書管理要領、セキュリティ管理要領、品質管理要領、変更管理要領)
- 会議体

1.2.　設計

受注者は調達仕様書に記載の要件を満たすための設計を行い、その内容を記したシステム設計書を作成すること。

1.2.1.　特に留意すべき非機能要件

1.2.1.1.　可用性及び保守性

突発的な障害だけでなく、ソフトウェアアップデート等の計画作業時であってもユーザの利用に関する性能・体感的な性能縮退が可能な限り最小になるように構成、運用設計を行うこと。

1.2.1.2.　情報セキュリティ設計

業務用 PC に起因した情報セキュリティリスクが最小となるように設計すること。あわせてシステム運用管理に必要な管理用アカウント、管理用インターフェースへのアクセスも最小となるように設計すること。逸脱した利用を可能な限り捕捉できるようにシステムログの出力、アラート設計を行うこと。

管理用アカウントは極力共有アカウントを避け、運用者数量分のアカウントを作成・運用できるように構成すること。

1.2.2. 設計に関するドキュメント

1.2.2.1. 基本設計書

システムの基本的な構成、各設計の意図を記すこと。最低限以下の内容を含めること。

- システムの各構成要素の役割と設計の意図及び実装概略
- システム全体の概要及び他システムとの接続点が分かるシステム全体構成図
- 物理装置間の接続情報を記したシステム物理構成図
- L3 ベースのシステム論理構成図
- システムのリソース情報
- 業務用 PC 利用時の認証、通信フロー
- 障害ポイント及びシステム異常時の動作
- 主要な動作アプリケーション及びサービス、ジョブの一覧
- ネットワークアドレス、IP アドレスの一覧
- システムアカウント及び用途の一覧
- 導入製品の個体識別が可能な一覧（ハードウェア、ソフトウェア、ライセンスをすべて含む。）

1.2.2.2. 詳細設計書

具体的なパラメータ、設定ファイル内容、システム構成要素の詳細情報を記すこと。

1.2.2.3. 運用設計書

本調達で導入するシステムを運用するための手順を作成すること。最低限以下の内容を含めること。

- システムが正常に稼働していることを確認するための手順
- 本書で求めている具体的な製品操作手順
- 機能障害発生時の通知に応じた対応方法
- 定められたソフトウェアアップデート手順がある場合はその手順

1.2.2.4. 導入・移行設計書

本調達で導入するシステムの構築フローを利用者影響、運用管理影響、システム構成等の要素から段階化し、各段階におけるシステムの状態、周囲のシステムと接続、運用状態を時系列で図示すること。既存システムから移行が必要な要素については特に留意すること。

尚、既存のシステムに動作影響がある場合、動作影響発生の 3 週間前に PMDA に影響範囲を報告し合意すること。

1.2.2.5. テスト設計書

本調達で導入するシステムの各機能及び運用が正常に動作することを確認するためのテスト設計を行うこと。テスト設計書にはテストの実施有無、意図、粒度、方法、使用するテストデータを記載すること。テスト設計は以下の内容に留意して行うこと。

- 全使用機能の正常動作
- 冗長構成における部分障害時の動作
- リソース負荷を考慮した性能試験

1.3. 導入

受注者は本システムを実現するために必要な製品を導入する作業を行う。各製品には設計フェーズで定まった内容の設定を行い、システムが正常に稼働するように構成すること。構成後は動作テストを行い意図した動作となることを確認すること。

導入作業に応じて設計内容に変更が生じる場合、PMDA と合意の上でプロジェクト計画に定めた変更管理要領に基づき設計に関するドキュメントの修正を行うこと。

1.3.1. 導入に関するドキュメント

1.3.1.1. テスト結果報告書

テスト設計書に基づきシステム動作テストを実施した結果を一覧化して PMDA に報告すること。必ずしも全テストの結果報告を同じタイミングで実施する必要はないが、重要になる移行段階では移行可否を判断する移行判定を行う。この場合、移行の前に当該部分の詳細なテスト結果報告書を求めることがある。

1.4. 引継ぎ

受注者は本調達で導入するシステムの運用方法を PMDA に引継ぐこと。引継ぎは必ずしも対面での説明を求めるものではないが、PMDA が対面の説明を求めた場合はこれに対応すること。

1.4.1. 引継ぎに関するドキュメント

1.4.1.1. 運用手順書

運用手順書には以下の内容を記載すること。

- 各製品が設計の通り動作していることを確認する方法
- 業務用 PC の交換やアカウントの管理等、定常的に発生すると考えられる内容の業務手順
- 本紙に記載している各構成要素の操作方法
- 各構成要素の保守体制
- 受注者に対する保守依頼を行うための方法とサービス定義内容

1.5. 進捗報告

受注者はプロジェクト設計書に基づき、本調達の進捗状況を最低限 2 週間に 1 回報告するための会議体を設定すること。会議帯には少なくとも以下の内容を含めること。

- 実績を記載した WBS の説明
- 課題の対応状況
- 翌 2 週間以内の作業予定の報告

受注者は会議の議事録を作成し、当該会議後 3 営業日以内に PMDA に提出すること。PMDA から議事録の内容に指摘があった場合、必要に応じて修正を行うこと。

2. 関連システムや用語

本書内で表現される関連システムや用語について以下に示す。

用語	説明
統合基盤	機構の各システムが横断的に利用する NW やストレージ、仮想基盤等のインフラ、及び監視サービスやバックアップシステム等のアプリケーション群
業務用 PC	職員が通常業務に利用する PC の総称、リモートワーク（テレワーク）も本端末を用いて行う
共用 LAN システム	業務用 PC の所属ドメインを管理する Active Directory やファイルサーバ、メールシステム等の総称、リモートワーク時には業務用 PC から本システムやその他業務システムへ接続する 統合基盤のインフラ上に構成されている
現行データセンタ	統合基盤における各インフラが収容されているデータセンタ
新霞が関ビル	機構職員が勤務する東京のオフィスビル
関西支部	機構職員が勤務する関西のオフィスビル

3. 主な構成要素

システム構成のうち主な構成要素とその役割は以下に示す通り。

3.1. リモートワークインフラ物理ロケーション

本システムでは VPN のような通信技術によりリモートワーク時の業務用 PC と PMDA を接続す

る。リモートワークインフラ物理ロケーションには導入機器を稼働させるためのスペース、電源、物理的な管理が含まれる。リモートワークインフラ基盤用に準備している現行のデータセンタ内のラック 1 本を利用して構成すること。

3.2. リモートワークインフラ基盤

業務用 PC のリモート接続の制御、リモート接続状況の可視化、統合基盤との接続を行い、それぞれの機能を維持するためのサーバ、ネットワーク機器等を指す。

3.3. リモートワーク端末通信制御装置

業務用 PC と暗号通信接続を構成する終端装置及びこれらの機能を維持管理するための装置を指す。本装置は業務用 PC からの接続要求に応じて暗号通信を確立し、業務用 PC の状態によって許可する通信ルールを動的に変動させる。これによりリモートワーク中に PC の状態が一定の基準を下回った場合に自動的に接続を切り離す。

リモートワーク時に接続するネットワークのセキュリティは担保されないため、接続したネットワークが PMDA の管理ネットワークであるか自動的に判断し、ユーザに対して透過的に必要なセキュリティポリシを適用する。リモートワーク時には必要最小限の通信しか許可せず、例えば自宅ネットワーク内に接続されている NAS 等の装置とは一切の通信を禁止する。

3.4. HTTP トラフィック分散装置

本装置では業務用 PC が発する通信のうち、一部の HTTP トラフィックに対して特別な処理を行う。特に、許可された Office365 テナントにのみ接続可能とする通信制限（HTTP ヘッダーへの許可テナント情報の挿入）、動的に更新される Office365 の接続先情報を用いた送信トラフィックの識別および送信元 IP アドレスの NAT 変換、HTTP ログの収集を行う。

3.5. 新霞が関ビル内 Office365 通信用装置

本装置では新霞が関ビル内で利用する業務用 PC が発する通信のうち、HTTP トラフィック分散装置が NAT 変換した送信元 IP アドレスからの Office365 向けの通信をインターネット対して送信する。これを実現するためのインターネット回線およびネットワーク機器等を指す。

3.6. 業務用 PC

PMDA 執務室内及びリモートワーク時に使用する PC を指す。PC ハードウェアは PMDA が別途調達して支給する。この PC ハードウェアを使用して本件受注者は設計した内容を実現するためのキッティング作業を行う。

3.7. 業務端末管理システム

共用 LAN システムでは既存の業務用 PC を運用管理するための一機能として本システムを運用している。受注者はこれらの設備を使用して本件で設計した業務用 PC の運用に必要な制御を行うこと。主要な制御項目として、USB インターフェースを使用して接続する記憶装置の制限、マルウェアチェック及びアラート発報、ソフトウェアコントロール、リモートコントロール、PC 操作ログの記録といったものがある。これらの機能に関わる設定作業は本調達の作業範囲に含まない。

3.8. PC マスタイメージ展開用 MECM

業務端末管理システムで運用中のものとは別建ての業務用 PC のイメージ展開用の MECM サーバを指す。受注者は業務用 PC に対してマスタイメージから PXE ブートによるイメージ展開が可能な環境を構築すること。サーバ OS および MECM サーバ利用に必要なライセンスは PMDA で準備するため本調達には含まない。受注者はサーバ OS の準備に必要なスペック情報等について情報提供をすること。

3.9. その他の既存システム

共用 LAN システムではシステムの運用管理に以下の製品を使用している。本調達で構築する各システムの運用設計に使用して良い。製品の設定は基本的に PMDA が行うため設定に必要な情報を提供すること。ただし本調達で導入した機器等に対する必要な設計、設定およびエージェント等のインストールは本調達の作業範囲に含む。

- Microsoft 社 Active Directory
- Zabbix 社 Zabbix
- ManageEngine 社 Netflow Analyzer
- Rsyslog (OSS)

4. 各要素の要件

本項目では必要最小限の機能を記載している。各機能を実現するために必要なものを構成に含めること。各機器の設置に伴い棚板等必要な部材が発生する場合は、本件受注者が準備すること。

4.1. リモートワークインフラ物理ロケーション

リモートワークインフラ基盤を構成する物理機器について、新霞が関ビル、関西支部に設置する機器を除きリモートワークインフラ物理ロケーション内に設置する。本ロケーション内には本システム用のラックを 1 架 PMDA が準備する。本ラックには 42U まで機器が搭載可能となっている。

4.2. リモートワークインフラ基盤

本項で記載するリモートワークインフラ基盤の要件は参考値として 3 Tier 構成想定で記載している

が、機能・性能要件を満たす場合はハイパーコンバージドインフラストラクチャ(HCI)構成としてもよい。また、本調達で導入する WindowsOS のサーバについては既存の Active Directory のドメインに参加させることを想定すること。

4.2.1. リモートワーク仮想基盤

4.2.1.1. 機能・性能要件

1. 本書に記載する各機能を実現するためのサーバを稼働させられる仮想基盤システムであること。アプライアンスや別途物理サーバである必要のあるものは仮想基盤システム上に構成しなくても良い。
2. 仮想基盤の物理ホストに搭載する CPU は本書に記載する各機能を実現するために十分な性能を備えていること。
3. 仮想基盤上の仮想マシンの仮想 CPU は少なくともリモート接続の品質に影響するノードについてはオーバコミットしないようなリソースを備えていること。
4. 物理ホストの物理ディスクは RAID5 相当のディスク障害耐性を備えていること。
5. 物理ホストの物理ディスクはディスク障害時に自動的に使用開始されるホットスペアディスクを 1 個備えていること。もしくは 1 台のホストの稼働が停止した場合やディスク交換によりホストの停止が必要となった場合でも、残りのホストにより本基盤機能が維持され縮退状態とならない構成とすること。
6. 物理ホストと共有ストレージを接続するインターフェースは Fiber Channel(FC)、もしくは Internet Small Computer System Interface(iSCSI)により 1 インターフェースあたり 25Gbps 以上のスループットを備えていること。
7. FC 接続先 SAN スイッチ、もしくは iSCSI 接続先 NW スイッチ(以下、iSCSI 用スイッチと記す)の冗長構成が可能なこと。
8. 共有ストレージとの接続インターフェースを FC とする場合、SAN スイッチには SAN スイッチの設定、状態を管理可能な専用物理インターフェースを備え、IP 通信による情報取得が可能なこと。iSCSI とする場合、iSCSI 用スイッチにて同等の機能を有すること。
9. 共有ストレージのコントローラは冗長構成が可能なこと。1 台のコントローラは冗長化された SAN スイッチ、もしくは iSCSI 用スイッチからのインターフェース接続を全て収容可能なこと。
10. 共有ストレージのディスクは SSD ベースとすること。HDD と組み合わせるハイブリッド構成でも良いが、各機能の利用に十分な I/O 性能を備えること。
11. 共有ストレージの物理ディスクは RAID6 相当のディスク障害耐性を備えていること。
12. 共有ストレージには共有ストレージの設定、状態を管理可能な専用物理インターフェースを備え、IP 通信による情報取得が可能なこと。
13. 仮想基盤のディスク容量は、各機能を維持しログ等の中長期的に保存するデータを要件の通りに保存した場合に使用率が 65%以下となるようなディスク容量を備えていること。仮想基盤

の構成に共有ストレージを使用する場合、物理ホストに格納される最低限の仮想マシン構成ファイルはこの数値の計算外として良い。

14. 仮想基盤システムを構成する物理ホストは冗長構成とし、物理ホストが 1 台使用できない状態になった場合でも、リモートワーク仮想基盤上で動作する全ての仮想マシンが性能劣化することなく動作可能なコンピューティングリソースを備えていること。さらにこの状態であっても物理ホストの物理メモリの使用量が原則として 60%を超えないような物理メモリを備えていること。
15. 物理ホストのネットワーク接続は管理者の運用管理用途とするもの以外は 10Gbps のスループットを持つインターフェースを使用可能なこと。
16. 物理ホストのネットワーク接続は接続先のネットワーク機器を分ける冗長接続が可能なこと。冗長接続は LACP またはスタティックリンクアグリゲーションを設定したネットワーク機器と接続可能なこと。
17. DVD-R 等の光学ディスクを読み取り可能なドライブを備えていること。
18. 物理ホストの状態を管理可能な専用物理インターフェースを備え、IP 通信による情報取得が可能なこと。
19. 仮想基盤上の物理ホストを操作可能な KVM コンソールを備えていること。
20. 物理ホストの障害発生時、障害が発生した物理ホスト上で動作していた仮想マシンが自動的に他の物理ホストで動作する HA 機能を備えていること。
21. 稼働中の仮想マシンを仮想マシンの動作を停止させずに別の物理ホストに移動させる機能を備えていること。
22. 仮想基盤に設定するネットワーク設定は各物理ホストで共有され、行った設定が各物理ホストに反映可能なこと。
23. 各物理装置は 19 インチラックに搭載可能なこと。
24. 物理ホスト、SAN スイッチまたは iSCSI 用スイッチ、共有ストレージは電源冗長が可能なこと。
25. 物理ホストは電源に関する省エネ対策が施されていること。
26. 仮想基盤上で数量無制限に構築可能な OS ライセンスはなくても良い。このようなライセンスを用いない場合は各要素で必要になる OS ライセンスを構成に含めること。
27. 仮想基盤上で動作している仮想マシンの仮想マシンレベルのバックアップを取得可能なこと。バックアップは増分によるもので良い。

4.2.1.2. 構成要件

1. 仮想基盤の構成方法に応じて各要件を満たすように仮想基盤を構成すること。構成に必要な配線等に使用する部材や作業も含む。
2. 物理ホスト、SAN スイッチまたは iSCSI 用スイッチ、ストレージコントローラが冗長接続され、これらの要素に単一障害点がないように構成すること。

3. SAN スイッチのゾーニングは原則としてソフトゾーニングで構成すること。
4. 仮想マシンが利用可能な仮想ディスクを格納するデータ領域の最大容量は、仮想マシンの用途や種別ごとに分けるように構成し、共有ストレージで単一の論理ボリュームのみを使用しない構成とすること。
5. 外部からのリモート接続の着通信と PMDA 内に向けた通信は異なる物理 NIC が使用し、各物理 NIC は 10Gbps 以上のスループットを備えるように構成すること。PMDA 内からのリモート接続の着通信は上記のどちらかの NIC を兼用して良い。
6. 仮想基盤の機能利用のために専用物理 NIC を使用する場合、10Gbps 以上のスループットを備えるように構成すること。
7. 仮想基盤の運用管理のための NIC は 10Gbps 以上のスループットを備えるように構成すること。
8. 物理 NIC は用途ごとに冗長接続できるように構成し、冗長化したネットワーク機器と接続すること。
9. 物理ホスト、SAN スイッチまたは iSCSI 用スイッチ、共有ストレージの状態をネットワーク経由で管理できるように構成すること。
10. リモート接続の品質に影響を与える可能性のある仮想マシンは、仮想マシンが動作する物理ホストが変更されにくくなるように構成すること。
11. 仮想マシンが動作している物理ホストに障害が発生した場合、当該仮想マシンが自動的に他の物理ホストで動作を開始できるように構成すること。
12. 仮想基盤を管理するための管理システムを利用する際のユーザ認証では、既存で PMDA が運用する Active Directory 上の特定アカウントが使用可能となるように構成すること。
13. 各機能の実現に仮想基盤を構成する物理ホスト以外にハードウェアを使用する場合、そのハードウェアもネットワーク接続すること。
14. 仮想基盤で動作する仮想マシンの OS レベルの増分バックアップを取得すること。バックアップ頻度及び保持世代数は原則週 1 回、3 世代保持とする。ただしバックアップ取得時のリモート接続品質影響がなく、さらにログを保持することを目的としている仮想マシンのバックアップ頻度及び保持世代数は毎日、7 世代保持とする。各バックアップの具体的なスケジュールはリモート接続品質への影響を最小とするように設計すること。
15. 取得したバックアップを用いてリストアが可能となるように構成すること。
16. 仮想マシン以外のバックアップについて、受注者はリストアに必要な情報を明確化し保守対応が継続的に可能になるように構成すること。
17. 各要素の障害発生を PMDA が検出できるように設定を行うこと。実際の通知には既存で PMDA が運用する Zabbix やメール配送サーバを使用しても良い。Zabbix では Zabbix Agent、SNMP、SNMP Trap での監視が可能だが、可能な限り SNMP Trap を使用せず SNMP での状態取得による監視構成とすること。
18. バックアップの成否を通知する仕組みを構成すること。

19. 物理ホスト、SAN スイッチまたは iSCSI 用スイッチ、共有ストレージの電源は冗長構成とすること。

4.2.1.3. 運用・保守要件

1. 共有ストレージの論理ボリューム作成手順を作成すること。作成した論理ボリュームを使用するために SAN スイッチまたは iSCSI 用スイッチの設定が必要な場合、その作業内容も手順に含めること。
2. バックアップスケジュールの変更、バックアップ処理の一時的な停止、新しいバックアップスケジュール作成を行うための手順を作成すること。
3. バックアップの成否を確認するための手順を作成すること。
4. 仮想基盤物理ホストの障害を検出するための手順を作成すること。
5. ハードウェア保守は平日 9 時～17 時オンサイト保守とすること。保守作業にはケーブリング等の物理作業、設定復元、ソフトウェアインストール等の設定作業を含み、正常構成に復帰させるように対応すること。
6. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。
7. メール、電話を使用した本装置の仕様に関する技術的な問い合わせに対応すること。

4.2.2. マルウェア対策

4.2.2.1. 機能・性能要件

1. リモートワークインフラ基盤で動作する Windows や Linux 系 OS のような汎用サーバ上でマルウェアを自動的に検出し、隔離、駆除が可能なこと。
2. マルウェアのシグネチャファイルは自動更新が可能なこと。
3. 検出対象外ディレクトリ、ファイルを指定可能なこと。
4. マルウェア検出及び対応状況を集中管理するための Web インターフェースを備えていること。

4.2.2.2. 構成要件

1. マルウェア対策にエージェントソフトウェアのインストールが必要な場合はインストールを行うこと。
2. マルウェア検出時に通知を行うように構成すること。既存で PMDA が運用している Zabbix やメール配送サーバを使用しても良い。
3. 集中管理用の Web インターフェースを提供するサーバは本調達で構築する仮想基盤上に構成すること。
4. 当該サーバのバックアップは本調達で構築する OS バックアップを使用すること。

4.2.3. バックアップ・リストア

4.2.3.1. 機能・性能要件

1. リモートワークインフラ基盤内で動作する仮想マシン、物理サーバのマシン単位のバックアップおよびリストアが可能なこと。
2. バックアップ処理は基本的に日次での実行を想定しており、バックアップおよびリストア可能な世代数は 7 世代とすること。
3. バックアップおよびリストア作業を集中管理するための Web インターフェースを備えていること。
4. バックアップデータは暗号化可能なこと。

4.2.3.2. 構成要件

1. バックアップおよびリストアにエージェントソフトウェアのインストールが必要な場合はインストールを行うこと。
2. バックアップ失敗等エラー発生時に通知を行うように構成すること。既存で PMDA が運用している Zabbix やメール配送サーバを使用しても良い。
3. 集中管理用の Web インターフェースを提供するサーバは本調達で構築するする仮想基盤上に構成すること。
4. 当該サーバのバックアップは本調達で構築する OS バックアップを使用すること。

4.2.3.3. 運用・保守要件

1. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。
2. メール、電話を使用した本装置の仕様に関する技術的な問い合わせに対応すること。

4.2.4. ネットワーク構成

4.2.4.1. リモートワーク基盤ファイアウォール

4.2.4.1.1. 機能・性能要件

1. 20Gbps 以上のファイアウォールスループットを備えていること。
2. リモート接続に必要な L4 通信を処理しきれること。
3. 19 インチラックに搭載可能なこと。

4.2.4.1.2. 構成要件

1. 2 台で Active-Standby による冗長構成とすること。
2. トラフィックログ、システムログを格納するための専用アプライアンスを新規で用意し、これにログを送信するように構成すること。
3. 外部、内部、DMZ ゾーンを作成し、ゾーン間の IP 通信のフィルタリング設定を行うこと。
4. 本装置を経由する同一ゾーン内の通信は明示的に許可したもの以外は通信を禁止するように

構成すること。

5. ゾーンごとに物理インターフェースは占有するように構成すること。
6. L3 通信は基本的にスタティック、コネクトルーティングにより構成すること。
7. リモートワーク基盤 L3 スイッチと接続すること。接続インターフェースを使用するゾーンごとに 1Gbps インターフェース 2 ポートを Active-Active 構成で接続すること。
8. リモートワーク基盤 L2 スイッチと接続すること。接続インターフェースは使用するゾーンごとに 1Gbps インターフェース 2 ポートを Active-Active 構成で接続すること。
9. 全体の構成の整合性を取るために VDOM を使用しても良い。VDOM を使用する場合、それぞれの VDOM で使用するゾーンが同一用途と判断できる場合はトラフィックが分散されていると判断し、リモートワーク基盤 L3 スイッチとの接続物理インターフェースは 1 ポートずつでも良い。
10. システム管理用のローカルアカウントを PMDA の指定する運用者数分作成すること。

4.2.4.1.3. 運用・保守要件

1. 装置の HA 状態を変更するための条件、手順を作成すること。
2. 装置状態を確認するための手順を作成すること。
3. システム管理用のローカルアカウントを CLI から作成、無効化、削除、設定変更するためのコマンド情報を提供すること。
4. システム異常は可能な限り SNMP Trap ではなく SNMP による状態取得により検出できるように設計すること。
5. ハードウェア保守は平日 9 時～17 時オンサイト保守とすること。保守作業にはケーブリング等の物理作業、設定復元等の設定作業を含み、正常構成に復帰させるように対応すること。
6. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。
7. メール、電話を使用した本装置の仕様に関する技術的な問い合わせに対応すること。

4.2.4.2. リモートワーク基盤 L3 スイッチ

4.2.4.2.1. 機能・性能要件

1. L3 スイッチとして動作し、スタティックルーティング、コネクトルーティング、OSPF に対応していること。
2. L3、L4 ベースのポリシベースルーティングに対応していること。
3. 複数台のスイッチを論理的に 1 台で構成可能なスタックに対応していること。本書に示す各機能はスタックを構成した状態でも利用可能なこと。
4. スイッチ内で論理的に装置を分割可能な VRF に対応していること。
5. VRF ごとにそれぞれルーティングテーブルを保持可能なこと。
6. 10GBASE-SR に対応した物理インターフェースを 1 台あたり 20 ポート以上有すること。当該ポートは 1000Base-SX、1000Base-LX、1000Base-T 用ポートとしても使用可能なこと。

7. 全ポートを全二重通信においてフルワイヤーレートで使用可能なこと。
8. SNMP により物理ポートのトラフィック量を取得可能なこと。
9. sFlow または NetFlow 送信機能を有すること。
10. 19 インチラックに搭載可能なこと。
11. 電源冗長が可能なこと。

4.2.4.2.2. 構成要件

1. 2 台でスタック構成とすること。
2. スタックマスタ障害時にユーザのリモート接続品質が極力低下しないように構成すること。
3. リモートワークインフラ基盤内の内部ゾーンに分類される通信の L3 通信が行われるように構成すること。L3 通信は基本的にスタティック、コネクトルーティングにより構成すること。
4. HTTP トラフィック分散装置 1 台とスタック構成とした本装置を 20Gbps で通信できるように接続すること。
5. リモートワーク基盤ファイアウォールと要件を満たすために必要な構成で接続すること。
6. リモートワーク仮想基盤と要件を満たすために必要な構成で接続すること。
7. その他必要な物理装置があればネットワーク接続すること。
8. DMZ ゾーンの通信は本装置では L2 通信のみ行うように構成し、DMZ ゾーン内の L3 通信はリモートワーク基盤ファイアウォールで制御するように構成すること。
9. サービス系と運用管理系の通信を分けるための VRF を構成すること。既存データセンタ内の L3 ネットワーク機器では同様に VRF が設定されており、同一用途の VRF 同士で通信可能となるように構成すること。必要であれば HTTP トラフィック分離装置の分散分割も行うこと。
10. 既存で PMDA が運用する Zabbix から SNMP 監視できるように構成すること。Zabbix の設定は PMDA が行う。
11. システムログを既存で PMDA が運用する Syslog サーバに送信するように構成すること。
12. sFlow または NetFlow を既存で PMDA が運用するフローコレクタに送信するように構成すること。
13. システム管理用のローカルアカウントを PMDA の指定する運用者数分作成すること。

4.2.4.2.3. 運用・保守要件

1. スタックの状態を確認するための手順を作成すること。
2. システム管理用のローカルアカウントを CLI から作成、無効化、削除、設定変更するためのコマンド情報を提供すること。
3. システム異常は可能な限り SNMP Trap ではなく SNMP による状態取得により検出できるように設計すること。
4. ハードウェア保守は平日 9 時～17 時オンサイト保守とすること。保守作業にはケーブリング等の物理作業、設定復元等の設定作業を含み、正常構成に復帰させるように対応すること。

5. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。
6. メール、電話を使用した本装置の仕様に関する技術的な問い合わせに対応すること。

4.2.4.3. リモートワーク基盤 WAN L2 スイッチ

4.2.4.3.1. 機能・性能要件

1. L2 スイッチとして利用可能なこと。
2. 複数台のスイッチを論理的に 1 台で構成可能なスタックに対応していること。
3. 1Gbps で接続可能な物理インターフェースを 1 台あたり 24 ポート以上有すること。
4. 全ポートを全二重通信においてフルワイヤーレートで使用可能なこと。
5. SNMP により物理ポートのトラフィック量を取得可能なこと。
6. sFlow または NetFlow 送信機能を有すること。
7. 19 インチラックに搭載可能なこと。
8. 電源冗長が可能なこと。

4.2.4.3.2. 構成要件

1. 2 台でスタック構成とすること。
2. スタックマスタ障害時にユーザのリモート接続品質が極力低下しないように構成すること。
3. リモートワーク基盤ファイアウォールと要件を満たすために必要な構成で接続すること。
4. 利用者からのリモート接続通信用のインターネット回線を収容する回線終端装置と可能な限り冗長性が保たれる形でネットワーク接続すること。
5. その他必要な物理装置があればネットワーク接続すること。
6. 既存で PMDA が運用する Zabbix から SNMP 監視できるように構成すること。Zabbix の設定は PMDA が行う。
7. システムログを既存で PMDA が運用する Syslog サーバに送信するように構成すること。
8. sFlow または NetFlow を既存で PMDA が運用するフローコレクタに送信するように構成すること。
9. システム管理用のローカルアカウントを PMDA の指定する運用者数分作成すること。

4.2.4.3.3. 運用・保守要件

1. スタックの状態を確認するための手順を作成すること。
2. システム管理用のローカルアカウントを CLI から作成、無効化、削除、設定変更するためのコマンド情報を提供すること。
3. システム異常は可能な限り SNMP Trap ではなく SNMP による状態取得により検出できるように設計すること。
4. ハードウェア保守は平日 9 時～17 時オンサイト保守とすること。保守作業にはケーブリング等の物理作業、設定復元等の設定作業を含み、正常構成に復帰させるように対応すること。

5. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。
6. メール、電話を使用した本装置の仕様に関する技術的な問い合わせに対応すること。

4.2.4.4. リモートワーク基盤インターネット回線

4.2.4.4.1. 機能・性能要件

1. 構成に応じて 1Gbps 帯域保証の回線を選択すること。
2. 本回線用としてグローバル IP アドレスを 16 個以上使用可能なこと。
3. 回線は Active-Standby で冗長化されており、回線サービスや回線終端装置の障害時に自動的に Standby 側回線が Active 状態に遷移すること。

4.2.4.4.2. 構成要件

1. リモートワーク基盤 WAN L2 スイッチと要件を満たすように接続すること。

4.2.4.4.3. 運用・保守要件

1. 回線の計画メンテナンス作業がある場合、メンテナンスの 14 日以上前にメールで通知する体制とすること。本回線のメンテナンスであることを識別するための情報を PMDA に提供すること。
2. 回線障害時、メールによる障害発生通知が可能なこと。
3. 回線終端装置の障害発生時は平日 9 時～17 時オンサイトによる交換が可能なこと。

4.3. リモートワーク端末通信制御装置

各機能を実現するために必要なサーバ、アプリケーション、ネットワークを構成すること。本システムで新規導入する各構成要素の他に、既存で PMDA が運用中の Active Directory に関する各機能を使用しても良い。

4.3.1. リモート接続機能

4.3.1.1. 機能・性能要件

1. PMDA 執務室外から PMDA のネットワークに安全に接続するための暗号化された通信経路を確立できること。この通信経路内では原則としてすべての IP アドレス、TCP/UDP 通信が可能なこと。
2. 通信の暗号化技術は CRYPTREC に定められている電子政府推奨暗号リストに含まれたものを使用していること。
3. 暗号通信を確立するための認証方法として Active Directory 上のユーザアカウントによる認証が使用可能なこと。認証トラフィックは暗号化されていること。
4. PMDA 内の各リソースと通信可能なデバイスを制限可能なこと。

5. 接続デバイス、OS 製品(Windows、macOS 等)、OS のバージョン、レジストリ値、Windows 更新プログラムの適用状態、特定プロセスの実行状態、特定パスの特定ファイルの有無、Windows ファイアウォールの動作状態をもとに、リモート接続を遮断可能なこと。
6. アクセス先 IP アドレス、アクセス先 FQDN、L4 ポート、通信アプリケーションを通信制御内容、スプリットトンネルとして設定可能なこと。また、暗号通信が PMDA 執務室内外のどちらから行われたかを自動的に判別し、適用する通信制御内容を自動的に変更可能なこと。
7. 業務用 PC を PMDA 執務室外で使用する際、通信可能な宛先を最小限にする仕組みを備えていること。L3、L4 ベースのみの制御は許容しない。通信を行うソフトウェアやサービスによる制御が可能なこと。
8. 暗号通信を受け付けるノードは基本的に全て Active 状態で稼働させること。接続先はノードの負荷状態に応じて自動的に負荷分散する仕組みを有すること。
9. ある特定のノードにリモート接続中の業務用 PC を管理者が別のノードに接続するように操作可能なこと。この操作は利用者に透過的に操作可能なこと。移動自体は 5 秒程度以内に完了すること。この時、暗号化通信経路内のアプリケーションセッションの維持の保証はしなくても良い。
10. 暗号通信を受け付けるノードのうち特定のノードについて新規接続を受け付けない状態にできること。
11. 宛先 IP アドレスが NAT された状態であっても業務 PC からの暗号通信の確立が可能なこと。
12. 暗号通信を行う業務用 PC に対して IP アドレスを払い出す DHCP サーバとしてネットワーク到達性のある任意の DHCP サーバを指定可能なこと。
13. ユーザに暗号通信の切断を許容しない構成が可能なこと。
14. 暗号化通信経路内の TCP 通信を最適化する機能を有し、RDP 等の画面転送プロトコルを使用した業務を快適に行うための補助が可能なこと。
15. 暗号化通信を確立した履歴をロギング可能なこと。同一ログ内で接続元 IP アドレスが特定可能なこと。

4.3.1.2. 構成要件

1. 各機能を実現するために必要なノードをリモートワークインフラ基盤に構築すること。
2. 1850 台の業務用 PC が同時接続可能となるように構成すること。また、ユーザの利用に影響を与えないように動作検証を行うための本番環境とは別にテスト用接続装置を構成すること。テスト用接続装置は 10 台程度が接続できれば良い。具体的な接続台数は設計時に PMDA と合意の上決定すること。Active Directory は本番と同様のものを利用することを想定している。
3. システム構成上、障害発生時に利用者のリモート接続操作自体に影響が発生する可能性があるノードについては N+1 構成とすること。N 数はシステム維持に必要な数量を受注者が設計すること。
4. 業務用 PC が接続するリモート接続サーバの FQDN を 2 種類用意し、明示的に 2 系統の接続

機能を構成すること。各系統の接続台数は前述の 1850 台の半分ずつを想定しているが、設計に応じて数量を決定すること。業務用 PC の接続先リモート接続機能は業務用 PC ごとに明示的に定め、業務用 PC 側で接続系統を動的に切り替えられる必要はない。

5. 各リモート接続系統のトンネル通信のスループットは業務用 PC1 台あたり 3Mbps 以上を確保できるように構成すること。このスループットはリモート接続機能のみのものであり WAN 回線等のスループットとの整合性は考慮する必要はない。
6. リモート接続時は業務用 PC のクライアント証明書による認証を自動的に行い、接続完了するように構成すること。
7. 認証に Radius サーバ等が必要な場合はリモートワークインフラ基盤上に構築すること。尚、クライアント証明書と同等の端末認証が行える仕組みがある場合、その構成でも良い。その構成に必要な要素があれば構成に含めること。
8. 各ノードは OS、ミドルウェア、アプリケーションのパッチ適用が可能となるように構成すること。PMDA が既存で運用する WSUS 及び Redhat Satellite を使用しても良い。既存で運用する各サーバの設定は PMDA で行うが、PMDA が受注者に対して設定に必要となる情報を確認する場合があるので、これに対応すること。
9. リモート接続を行う業務用 PC の暗号化通信経路内のデフォルトの L3 通信経路は現行データセンタ内の L3 スイッチに向けられるようにネットワーク構成を行うこと。暗号化通信経路を通った通信が使用するインターネット回線はリモート接続用のインターネット回線とは別の回線を使用することを意図している。
10. 業務用 PC が暗号化通信経路内で通信を行うために必要な IP アドレスは DHCP 構成とすること。DHCP サーバは PMDA が既存で運用する DHCP サーバを使用すること。尚、DHCP サーバは Windows Server2022 の機能を使用しており、2 台でリース情報を共有する冗長構成としている。DHCP サーバの設定は PMDA が行うが、設定する DHCP オプションは受注者の設計事項とする。
11. 業務用 PC が暗号化通信経路内で使用する DNS サーバは既存で運用する DNS サーバを使用すること。
12. 業務用 PC が PMDA 執務室内外どちらの NW を利用している場合でも、本機能の制御下に置くこと。
13. 業務用 PC からインターネットへの通信は Microsoft365 等の特定宛先以外禁止としている。業務用 PC が PMDA 執務室内の NW を利用している場合に、本機能を利用するため必要なノードへ通信する際はノードのプライベート IP アドレスに着信する等、適切な経路となるよう構成すること。
14. 業務用 PC が発する通信の宛先が同一の宛先 URL、IP アドレスであってもリモート接続を行う場所が PMDA 執務室内外でスプリットトンネルの有効可否を自動的に選択するように構成すること。
15. 暗号化通信経路内の TCP 通信を最適化し、利用者が快適な快適に利用できる環境を構築する

こと。主要な通信プロトコルは RDP、SMB、HTTP(S)、PCoIP(S)で一部には音声、動画が含まれる。

16. Microsoft 社が提供する Office365 向けの URL、IP アドレスを自動的に取得し通信制御単位として使用できるように構成すること。
17. リモート接続を行う業務用 PC が接続しているローカルネットワーク上のノードや任意のインターネットサイトにアクセスできないように構成すること。DNS 等、リモート接続を確立するために必要最小限の通信の開放は許容するが、L3、L4 レベルのみの制御ではなく通信可能なソフトウェアやサービスを制限すること。
18. リモート接続を行う業務用 PC が発する Office365 向けの通信先のうち、主要なトラフィックの出力先はスプリットトンネルとなるように構成すること。尚、この制御は業務用 PC に行う設定と整合性を確保するように構成すること。
19. 業務用 PC をリモートワーク端末通信制御装置に通信到達性のないクローズドネットワークで使用した場合であってもクローズドネットワーク上の任意のノードと通信が不可となるように構成すること。
20. リモートワーク端末通信制御装置による通信制御から外れる操作を一般利用者が行えないように構成すること。
21. リモート接続を試みた業務用 PC で管理者が指定した Windows 更新プログラムが適用されていない場合、NAC(Network Access Control)相当の機能により利用者に状況、対応方法を知らせるメッセージを表示させること。表示内容は PMDA と合意の上、決定すること。メッセージを表示させると同時に、当該業務用 PC にあらかじめ定めたレベルのフラグを指定可能なこと。
22. リモート接続を試みた業務用 PC に管理者が指定したファイルがない場合、NAC 相当の機能により利用者に状況、対応方法を知らせるメッセージを表示させること。表示内容は PMDA と合意の上、決定すること。メッセージを表示させると同時に、当該業務用 PC にあらかじめ定めたフラグを指定可能なこと。
23. NAC により指定されたフラグに応じてアクセス可能なノードが制限可能になるように通信ルールを構成すること。

4.3.1.3. 運用・保守要件

1. 暗号化通信経路内、スプリットトンネルにより直接通信を行う通信内容の変更が可能なようにポリシ設計を行い、ポリシ変更方法を手順化すること。
2. Office365 が使用する URL、IP アドレスが変わった時に必要になる対応を手順化すること。
3. リモート接続機能が正常に動作していることを確認するための方法を手順化すること。障害発生に可能な限り早く気が付けるように監視方法を設計すること。
4. リモート接続機能を提供する各ノードの役割を明確化し、障害発生時の影響範囲として想定される事項を一覧化すること。

5. 管理外の端末がリモート接続を行っていることを把握するための方法を手順化すること。
6. 本機能を構成する各ノードのソフトウェアアップデートを行う際の作業手順を作成すること。作業手順は可能な限り一般利用者への影響が小さくなるような方法にすること。アップデート作業は PMDA が行う。
7. ハードウェアで構成する場合は、平日 9 時～17 時オンサイト保守とすること。保守作業にはケーブリング等の物理作業、設定復元等の設定作業を含み、正常構成に復帰させるように対応すること。
8. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。

4.3.2. 端末認証機能

許可された業務用 PC のみリモート接続が可能となるような構成とするために Radius サーバのような認証サーバが必要な場合は認証サーバを構築すること。

4.3.2.1. 機能・性能要件

1. 特定の装置からの認証のみ受け付けられるように構成すること。制限は IP アドレスベースでも良い。

4.3.2.2. 構成要件

1. 2 台構成とすること。
2. 2 台のサーバは Active-Acitve で稼働するように構成し、アクセスはロードバランス可能なように構成すること。機能があれば HTTP トラフィック分散装置のロードバランス機能を使用して良い。

4.3.2.3. 運用・保守要件

1. 認証機能が正常に動作していることを確認するための方法を手順化すること。障害発生に可能な限り早く気が付けるように監視方法を設計すること。
2. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。

4.3.3. リモート接続状況可視化

4.3.3.1. 機能・性能要件

1. リモート接続の履歴を業務用 PC のハードウェア単位で過去 62 日以上確認可能なこと。
2. リモート接続中に業務用 PC から発生したネットワークトラフィック量を可視化できること。可視化は暗号化通信経路内だけでなくスプリットトンネル側に発生したものも可能なこと。
3. 業務用 PC 上のアプリケーション単位でネットワークトラフィックを可視化できること。
4. 特定の宛先 IP アドレス、FQDN をベースとしてトラフィックを発生させた業務用 PC をリスト化可能なこと。

5. 各情報は Web ブラウザから確認可能なこと。

4.3.3.2. 構成要件

1. 各機能を実現するために必要なノードをリモートワークインフラ基盤に構築すること。
2. 本機能の冗長化は必須としない。
3. 各ノードは OS、ミドルウェア、アプリケーションのパッチ適用が可能となるように構成すること。PMDA が既存で運用する WSUS 及び Redhat Satellite を使用すること。既存で運用する各サーバの設定は PMDA で行うが、PMDA が受注者に対して設定に必要となる情報を確認する場合があるので、これに対応すること。

4.3.3.3. 運用・保守要件

1. リモート接続状況可視化が正常に動作していることを確認するための方法を手順化すること。障害発生に可能な限り早く気が付けるように監視方法を設計すること。
2. 本機能を構成する各ノードのソフトウェアアップデートを行う際の作業手順を作成すること。アップデート作業は PMDA が行う。
3. ハードウェアで構成する場合は、平日 9 時～17 時オンサイト保守とすること。保守作業にはケーブリング等の物理作業、設定復元等の設定作業を含み、正常構成に復帰させるように対応すること。
4. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。

4.3.4. DHCP ログ可視化

4.3.4.1. 機能・性能要件

1. 期間、IP アドレスを指定することで、指定した期間中に当該 IP アドレスを使用していた可能性のあるデバイスを特定可能な WebGUI を備えること。
2. 期間、デバイス名を指定することで、指定した期間中に当該デバイスが使用していた可能性のある IP アドレスを特定可能な WebGUI を備えること。
3. 過去 366 日以上の履歴を確認可能なこと。
4. 利用者を制限するための認証機能を備えていること。認証方式は LDAP 及び LDAPS が使用可能なこと。
5. LDAP 及び LDAPS 認証使用時、WebGUI にログイン可能なユーザが所属すべき Active Directory 上のセキュリティグループを指定可能なこと。

4.3.4.2. 構成要件

1. リモートワークインフラ基盤上に構成すること。
2. 本機能の冗長化は必須としない。
3. 可能な限り欠損なく可視化できるように構成すること。本機能が何らかの原因により使用でき

ない場合、後から当該時間帯の DHCP ログを可視化対象とできれば良い。

4. DHCP サーバにエージェント等のソフトウェアインストールが必要な場合、インストール作業は PMDA が実施する。インストーラとインストール手順を PMDA に提供すること。

4.3.4.3. 運用・保守要件

1. リモート接続状況可視化が正常に動作していることを確認するための方法を手順化すること。障害発生に可能な限り早く気が付けるように監視方法を設計すること。
2. 本機能を構成する各ノードのソフトウェアアップデートを行う際の作業手順を作成すること。アップデート作業は PMDA が行う。
3. ハードウェアで構成する場合は、平日 9 時～17 時オンサイト保守とすること。保守作業にはケーブリング等の物理作業、設定復元等の設定作業を含み、正常構成に復帰させるように対応すること。
4. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。

4.4. HTTP トラフィック分散装置

各機能を実現するために必要なサーバ、アプリケーション、ネットワークを構成すること。

4.4.1. 機能・性能要件

1. 業務用 PC に対して透過的な HTTP プロキシサーバとして動作すること。
2. Microsoft 社が公開する Office365 が使用する URL、IP アドレスを自動的に取得し、通信制御の要素として使用可能なこと。
3. Office365 が使用する通信先とマッチする通信のみ送信元 IP アドレスを NAT する機能を有すること。NAT 後に使用する IP アドレスは複数指定可能なこと。送信元 IP アドレスにより異なる NAT 用 IP アドレスが使用可能なこと。
4. Office365 が使用する通信先とマッチする通信のみ L3 通信のネクストホップアドレスを変更可能なこと。
5. Office365 にログインする際のテナントを制限するための HTTP ヘッダを必要最小限の HTTP 通信にのみ挿入可能なこと。これに必要な SSL 復号化機能を有すること。SSL 復号化はハードウェア処理であること。
6. HTTP アクセスログを Syslog サーバに送信可能なこと。
7. L3 ネットワーク機器として動作可能なこと。
8. HA 機能を備えており、Active-Standby として動作すること。
9. リモートワークインフラ基盤、新霞ヶ関ビルに設置する本装置は 10Gbps 以上のスループットを維持可能なこと。
10. 関西支部に設置する本装置は 5Gbps 以上のスループットを維持可能なこと。尚、関西支部の同時利用端末は 30 台を想定すること。

11. リモートワークインフラ基盤、新霞ヶ関ビルに設置する本装置は本装置を論理的に分割し、設定、管理をそれぞれ行う機能を有すること。
12. リモートワークインフラ基盤に設置する本装置は L4 ベースファイアウォール機能を有すること。
13. 19 インチラックに搭載可能なハードウェアアプライアンスであること。
14. 装置管理用のネットワークインターフェースを 1 ポート保持すること。

4.4.2. 構成要件

4.4.2.1. 各箇所の共通要件

1. 業務用 PC が本装置を経由することにより主に Office365 向けのトラフィックの経路制御を行えるように構成すること。設置場所はリモートワークインフラ基盤、新霞ヶ関ビル、関西拠点とする。尚、業務用 PC には HTTP プロキシは設定しない。
2. PMDA が指定するテナントのみ Office365 の認証が可能となるようにすること。
3. L3 通信可能なようにネットワーク設計を行うこと。
4. 2 台による冗長構成とすること。
5. 装置管理用のインターフェースはサービス系と異なるネットワークアドレスとなるように構成すること。
6. 1 台当たり 1RU で設置可能なこと。

4.4.2.2. リモートワークインフラ基盤に配置する装置の要件

1. リモートワークインフラ基盤内に設置すること。
2. 既存データセンタの L3 ネットワーク機器統合基盤 L3 スイッチと接続すること。統合基盤 L3 スイッチはスタックによる冗長化を行っている。統合基盤 L3 スイッチ側トランシーバの準備、接続及び接続部材の準備は必要に応じて受注者が行うこと。
3. 統合基盤 L3 スイッチと本装置間はスタティックルートによる L3 接続を行うこと。統合基盤 L3 スイッチの設定は PMDA が行う。
4. HA による二重化を行うこと。
5. L3、L4 ファイアウォール機能によりリモートワークインフラ基盤と既存の PMDA ネットワーク間の通信制御をステートフルに行うこと。
6. リモートワークインフラ基盤システム内の各サーバに RDP、SSH をはじめとした管理アクセス可能な PMDA の既存システムの送信元 IP アドレスを、L4 ファイアウォール機能により制限すること。

4.4.2.3. 新霞ヶ関ビルに配置する装置の要件

1. 新霞ヶ関ビル内の新規ックに設置すること。
2. 新霞ヶ関ビル内の L2 スイッチ(サーバ L2 スイッチ)とファイアウォール(内部ファイアウォー

ル)に 1000Base-T x2 で接続すること。接続及び接続部材の準備は受注者が行うこと。

3. 新霞ヶ関ビルの L3 スイッチ(新霞ヶ関ビル L3 スイッチ)、内部ファイアウォールとスタティックルートによる L3 接続を行うこと。サーバ L2 スイッチ、新霞ヶ関ビル L3 スイッチ、内部ファイアウォールの設定は PMDA が行う。
4. HA による二重化を行うこと。
5. 業務 PC 用の透過プロキシとして構成すること。プロキシ機能に関する要件はリモートワーク用基盤のものと同等とする。

4.4.2.4. 関西支部に配置する装置の要件

1. 関西支部内の既設ラックに設置すること。
2. 関西支部内の L2 スイッチ(サーバ L2 スイッチ)とファイアウォール(内部ファイアウォール)に 1000Base-T x2 で接続すること。接続及び接続部材の準備は受注者が行うこと。
3. 関西支部 L3 ネットワーク機器とスタティックルートによる L3 接続を行うこと。サーバ L2 スイッチと内部ファイアウォールの設定は PMDA が行う。
4. HA による二重化を行うこと。
5. 業務 PC 用の透過プロキシとして構成すること。プロキシ機能に関する要件はリモートワーク用基盤のものと同等とする。

4.4.2.5. 運用・保守要件

1. 宛先が Office365 の通信の場合に指定する NAT 用 IP アドレス、L3 ルーティング用のネクストホップアドレスの変更手順を作成すること。
2. 宛先が Office365 であっても接続を禁止するための設定手順を作成すること。
3. Office365 で認証可能なテナントの変更手順を作成すること。
4. L4 ファイアウォールルールの変更手順を作成すること。
5. 装置の HA 状態を変更するための条件、手順を作成すること。
6. 装置状態を確認するための手順を作成すること。
7. システム異常は可能な限り SNMP Trap ではなく SNMP による状態取得により検出できるように設計すること。
8. ハードウェア保守は平日 9 時～17 時オンサイト保守とすること。保守作業にはケーブリング等の物理作業、設定復元等の設定作業を含み、正常構成に復帰させるように対応すること。
9. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。
10. メール、電話を使用した本装置の仕様に関する技術的な問い合わせに対応すること。

4.5. 新霞が関ビル内 Office365 通信用装置

新霞が関ビル内の HTTP トラフィック分散装置で分離した Office 向け通信で利用する目的でインターネット回線を利用しておりこれを構成する機器も更新する。本項では特に必要となる要件につい

て記す。

4.5.1. Office365 等コミュニケーションツール用回線

4.5.1.1. 機能要件

1. 2.5Gbps 帯域確保型であること。
2. Active-Standby での冗長回線であること。回線の通信キャリアは同一でも構わない。
3. Active 回線に障害が発生した際は自動的に Standby 回線を利用するように切り替わること。
4. グローバル IP アドレスを 16 個以上使用可能なこと。

4.5.1.2. 構成要件

1. ONU または ONU とあわせて導入する通信機器を PMDA の既設 L2 スイッチに接続すること。
2. 回線の引き込み作業を行うこと。
3. ONU を収容するスイッチやルータを導入する場合、高さは 1RU とすること。

4.5.1.3. 保守要件

1. ONU、ルータ、スイッチに障害が発生した際のハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
2. 回線の計画メンテナンスがある場合、メンテナンス日の 14 日以上前にメンテナンスの実施を PMDA にメールで通知すること。
3. 不測の回線障害が発生した際、120 分以内に障害発生を PMDA にメールで通知すること。障害状況を確認するための WebUI の提供でも良い。

4.5.2. ファイアウォール

4.5.2.1. 機能・性能要件

1. 1.5Gbps 以上のファイアウォールスループットを備えていること。
2. 150,000 以上の L4 コネクションを維持可能なこと。
3. 2 台の装置で Active-Standby 構成にて HA 構成が可能なこと。Active 機の障害発生時には自動的に Standby 機が Active 状態に遷移可能なこと。
4. HA による切り替わりが発生したことは SNMP Trap またはメール通知可能なこと。
5. ファイアウォールを通過するパケットを走査し、通信がどの SaaS で使用するものか可視化する機能を有すること。
6. 現在ファイアウォール上でコネクションを維持している通信の一覧を表示可能なこと。
7. TLS 通信において脆弱性のあるブロック暗号化モードを検出可能なこと。
8. スクリプトベースの HTTP アクセスで装置状態を取得可能な API を備えていること。
9. トラフィックログをログ管理システムに送信可能なこと。
10. 1000Base-T に対応した物理インターフェースを 4 ポート以上備えていること。

11. IP 通信可能な専用の物理インターフェースを備えていること。
12. 100V 電源で動作可能なこと。
13. 最大消費電力は 300W 以下であること。
14. 電源冗長が可能なこと。
15. 19 インチラックに搭載可能なこと。

4.5.2.2. 構成要件

1. 装置 2 台で HA による冗長構成とすること。
2. PMDA が指定する L3 ネットワーク機器に対して内部向けのルーティング設定を行うこと。ルーティングはスタティックルートを想定している。
3. Office365 等コミュニケーションツール用回線を使用してインターネットと通信するようにルーティング、NAT 設定を行うこと。尚、内部向けの通信とあわせて PMDA の既存 L2 スイッチ、L3 ネットワーク機器の設定変更は PMDA が行うことを想定している。
4. 特定の送信元 IP アドレスのみインターネットと通信可能なようにファイアウォールポリシを構成すること。
5. ログをログ管理システムに送信する設定を行うこと。
6. PMDA の既存 L2 スイッチと装置あたり 1000Base-T 2 本で接続し、LACP によるリンクアグリゲーションを設定すること。
7. 既存 L2 スイッチとの接続に必要なネットワークケーブルの配線作業を行うこと。本装置設置場所と既存 L2 スイッチは同じ部屋にあり、フリーアクセス床の下で配線が可能になっている。想定している距離は 20m 程度。
8. 電源冗長を行うこと。
9. 新設する 19 インチラックに搭載すること。

4.5.2.3. 運用・保守要件

1. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。オンサイト対応時はケーブル接続を含む物理対応、設定の復元等の現状復帰に必要な対応を行うこと。
2. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
3. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。
4. 装置の起動、停止手順書を作成すること。

4.6. UPS

4.6.1. 機能・性能要件

1. 常時インタラクティブ方式で動作すること。
2. 100Base-TX または 1000Base-T に対応する物理インターフェースを備え、UPS の状態を Web

ブラウザから確認可能な WebUI を有すること。

3. 入力電源の障害を検出時、出力電源に接続されている機器のシャットダウン可能なこと。この動作は自動的に行われるように構成可能なこと。
4. 入力電源の障害を検出後、指定した時間経過以内に入力電源が復旧した場合、出力電源に接続されている機器のシャットダウン処理が行われないような仕組みを有すること。
5. 入力電源は PMDA の電源タップの 5-15R または 5-20R に接続可能な形状であること。
6. 19 インチラックに搭載可能なこと。

4.6.2. 構成要件

1. 既存 L2 スイッチとの接続に必要なネットワークケーブルの配線作業を行うこと。本装置設置場所と既存 L2 スイッチは同じ部屋にあり、フリーアクセス床の下で配線が可能になっている。想定している距離は 20m 程度。
2. 入力電源異常検出時にハードウェアを自動的にシャットダウンする仕組みを構成すること。外部にサーバが必要な場合は構築すること。PMDA の既存仮想基盤システムを使用して良い。OS は受注者が用意すること。OS デプロイ、基本的なネットワーク設定は PMDA が行うが、OS 設計及び UPS の制御に必要なソフトウェアインストール、ソフトウェア設定、ソフトウェア利用のために行う OS 設定は受注者が行うこと。

4.6.3. 保守要件

1. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。オンサイト対応時はケーブル接続を含む物理対応、設定の復元等の現状復帰に必要な対応を行うこと。
2. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
3. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。
4. 装置の起動、停止手順書を作成すること。

   運用中、少なくとも 1 回バッテリ交換が可能なこと。バッテリ交換はオンサイトで受注者が行うこと。尚、連絡体制、オンサイト対応共に PMDA とメーカが直接連絡を行う体制でも良い。

4.7. NAS

4.7.1. 機能・性能要件

1. 業務用 PC の配布するアプリケーションや更新プログラムを配置可能な NAS を 1 台構成に含めること。
2. NAS 上のデータアクセスに SMB、CIFS、FTP が使用可能なこと。

4.7.2. 構成要件

1. NAS は 30TB 以上の実効ディスク容量を有するように構成すること。

2. 物理ディスク 1 本に障害が発生してもデータアクセスに問題が生じないように RAID 構成を行うこと。RAID グループが分かれても構わないが、RAID グループごとに 4TB 以上の実効容量を持つように RAID レベルから設計すること。
3. ディスク障害時に自動的に活性状態になるスペアディスクを 1 本以上搭載すること。
4. エラー発生時に通知を行うように構成すること。既存で PMDA が運用している Zabbix やメール配送サーバを使用しても良い。
5. NAS へのアクセスは既存で PMDA が運用する Active Directory を使用した Windows 認証を構成し、OS ログオンとシングルサインオン可能なようにすること。
6. 物理ディスクを暗号化し、物理ディスクからのデータ復元を困難とすること。
7. NAS 装置上のデータバックアップの考慮は不要とする。
8. 本装置設置場所と同じ部屋にある既存の L2 スイッチと 1000Base-T により接続すること。必要な配線作業も実施すること。配線はフリーアクセス床の床下に行うこと。L2 スイッチとの距離は 10m 程度を想定すること。尚、L2 スイッチの設定は PMDA が行う。
9. 新霞ヶ関ビルの既設の 19 インチラック内に設置すること。
10. 1RU で設置可能なこと。
11. 100V 電源で利用可能なこと。
12. 最大消費電力は 250W 以下であること。

4.7.3. 保守要件

1. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。オンサイト対応時はケーブル接続を含む物理対応、設定の復元等の現状復帰に必要な対応を行うこと。
2. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
3. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。
4. 装置の起動、停止手順書を作成すること。
5. 保守作業に必要となる情報を事前に PMDA と共有し、情報保持の方法を手順化すること。

4.8. 業務用 PC

4.8.1. キッティング作業に関する要件

4.8.1.1. 基本作業

1. 本システムで設計した内容を実現できるようにクライアント PC のキッティングを行うこと。業務用 PC として使用するハードウェアは PMDA から支給する。今回の作業対象になる PC の台数は以下の通り
    - 業務用 PC：1650 台（指紋認証用センサ有、3 モデルを想定）
2. 今後の PC 運用に使用するためのマスタ PC 及びマスタイメージを作成すること。マスタの種類は PC モデルごとに 1 個ずつとする。ただし設計上、複数のマスタが必要になった場合は必

要数分作成すること。

3. 基本的なキッティング作業は受注者が用意したスペースで行うこと。
4. ドメイン参加や初期動作テストの確認等、PMDA のネットワークに接続する必要のある作業については新霞ヶ関ビル内のスペースを使用して良い。尚、このスペースは基本的に平日 18 時～22 時、土日休日 9 時～20 時までの利用とする。30 名程度であれば一般的な PC 設定を行えるスペースを想定している。尚、このスペースは他の用途にも使用しているので必ずしも全ての日程で使用できるわけではないことに留意すること。
5. 関西支部での PC 配布時、受注者は現地の配布作業に立ち会うこと。配布作業は 1 日を想定している。
6. キッティング時に業務用 PC の有線 LAN、無線 LAN NIC の MAC アドレスをリスト化し、業務用 PC のユーザ配布前にリストを PMDA に提出すること。
7.

4.8.1.2. 業務用 PC に対する物理作業

1. 本調達で使用する業務用 PC は受注者の事業所等に納品する。受注者は必要に応じて倉庫等を準備しキッティング作業を行うこと。倉庫の利用に関わる費用が発生する場合、見積もりに含めること。
2. 本調達でキッティングする新業務用 PC を配布次第、現在 PMDA 職員が使用している現業務用 PC は回収する。新霞ヶ関ビル、関西支部内の現業務用 PC は各拠点内の PMDA が指定する場所に集積すること。
3. 業務用 PC には個体を識別するためのハードウェアシリアル、ホスト名、用途等を記したシール及び剥離防止の保護シールを貼付すること。これらのシールは受注者が用意すること。マウス等の添付品にも同様の情報が記載されたシールを貼付すること。こちらには保護シールは不要とする。
4. 業務用 PC には PMDA の指定する資産管理用のシールを貼付すること。

4.8.2. 構成要件

4.8.2.1. OS

1. Windows11 Enterprise を使用すること。Windows11 Enterprise を使用するための Microsoft365 ライセンスは PMDA が支給する。
2. Windows11 のバージョンは構築の際、PMDA と合意の上決定すること。
3. OS に付属するニュース閲覧機能等、業務上不要と考えられる表示領域は極力表示しないように設定すること。

4.8.2.2. BIOS/UEFI

1. BIOS/UEFI のパスワードを設定し、一般ユーザがハードウェア構成の変更が行えないようにすること。
2. ユーザの業務用 PC の通常利用時にこれらのパスワードの入力を求められないように構成する

こと。

4.8.2.3. OS ログオン・アカウント

1. 指定する業務用 PC では Windows Hello for Business を構成し、PIN または指紋またはパスワードによる認証が可能となるように構成すること。Windows Hello for Business をユーザがセットアップする際の本人認証に使用する SMS や認証用アプリケーションは PMDA がユーザに支給するので考慮の必要はない。Windows Hello for Business を構成するデバイスが明示的に分かるように Active Directory を構成すること。尚、Active Directory の設定作業自体は PMDA が行うので設定すべき作業内容を提供すること。
2. PMDA が準備した FIDO2 デバイスを 2 要素認証の 1 つとして利用できるよう設計および設定すること。PMDA が保有する既存設備に必要な設定は PMDA が実施するので設定に必要な情報を提供すること。
3. 管理用途としてローカルアカウントを設定すること。

4.8.2.4. ネットワーク設定

1. ホスト名を設定すること。
2. 各 NIC の IP アドレスは DHCP による取得とすること。DHCP サーバはリモートワーク端末通信制御装置で使用しているものを使用して構成すること。
3. 有線 LAN と無線 LAN に同時に接続した場合、有線 LAN を使用して通信するように構成すること。
4. 新霞ヶ関ビルに配置する業務用 PC には PMDA の指定する無線 LAN ESSID に接続できるように構成すること。この ESSID ではコンピュータアカウントによる IEEE802.1x 認証を行っている。
5. 一般利用者が接続する SSID を任意に指定可能なように構成すること。
6. 手動インポートが必要な CA 証明書をインポートすること。Active Directory の機能を使用しても良い。
7. ネットワーク隣接 PC の探索を禁止するように構成すること。
8. 既存の Active Directory ドメインに参加させること。
9. リモートワーク端末通信制御装置と暗号通信経路を確立できるように構成すること。

4.8.2.5. アプリケーション

1. Microsoft365 Office アプリケーションをインストールすること。Office アプリケーションを使用するために必要な Microsoft365 ライセンスは PMDA が支給する。
2. Office アプリケーションのアドイン管理方式を設計すること。
3. その他に PMDA の指定するアプリケーションをインストールすること。インストール方法は PMDA が指示するが特に複雑な手順を要するものはない。また、特段の断りがない限り受注者がこれらのアプリケーションライセンスを用意する必要はない。
4. Windows ストアアプリの利用制限を行うこと。
5. 不要なプリインストールアプリケーションを定め、PMDA と合意の上削除すること。

4.8.2.6. ディスク暗号化

1. BitLocker によりディスク暗号化を行うこと。
2. 回復キーの保管方法を検討し PMDA と合意の上で保管すること。

4.8.2.7. HTTP プロキシ

1. 業務用 PC には直接 HTTP プロキシや PAC ファイルを構成しないように構成すること。

4.8.2.8. Windows Update / Office Update

1. 業務端末管理システムを構成する MECM で Windows 及び Office の更新プログラム適用を管理できるように構成すること。
2. 特に必要がない限り、デュアルスキャンを無効化しインターネットから更新プログラムを取得しないように構成すること。
3. ユーザがリモート接続を行っている際の Windows Update の運用をネットワークトラフィック量の観点から設計すること。
4. 信頼するパブリックな CA 証明書を自動更新するように構成すること。

4.8.2.9. Web ブラウザ

1. Microsoft Edge を標準 Web ブラウザとして構成すること。

4.8.2.10. マルウェア検出

1. Windows Defender を有効化し、マルウェアの検出、駆除するように構成すること。ただし Microsoft365 E5 の機能である ATP に相当する機能は使用しない。

4.8.2.11. その他

1. 他にユーザ利用における利便性向上、システム保護のために必要な設定を行うこと。

4.8.3. 運用・保守要件

1. マスタ PC からイメージを作成、および展開する手順を作成すること。
2. 業務用 PC の破損等により発生する PC 交換に関してシステム面における手順を設計し、具体的な交換フロー、手順を PMDA と合意の上で作成すること。手順は管理者向けのものとすること。利用者向けの手順は PMDA が作成するため、必要に応じて情報提供を行うこと。
3. 業務用 PC のハードウェア保守は本調達の対象外とする。業務用 PC にはハードウェア交換保守を準備しており、PMDA から受注者に保守手順を共有する。この保守手順を PC 交換手順に反映させること。

4.9. PC マスタイメージ展開用 MECM

4.9.1. 機能・性能要件

1. 業務用 PC のマスタイメージを PXE ブートで展開可能であること。
2. タスクシーケンスを用いて業務用 PC キッティングの一連の作業を自動実行可能であること。

4.9.2. 構成要件

1. 機能要件を満たすために必要なスペックを保持すること。サーバ OS は PMDA が準備するため、必要なスペックおよび設定に関わる情報を提供すること。
2. MECM サーバは OS、ミドルウェア等のパッチ適用が可能となるように構成すること。PMDA が既存で運用する WSUS を使用しても良い。既存で運用する各サーバの設定は PMDA で行うが、PMDA が受注者に対して設定に必要となる情報を確認する場合があるので、これに対応すること。
3. エラー発生時に通知を行うように構成すること。既存で PMDA が運用している Zabbix やメール配送サーバを使用しても良い。
4. MECM へのアクセスは既存で PMDA が運用する Active Directory を使用した Windows 認証を構成し、OS ログオンとシングルサインオン可能なようにすること。
6. マスタ PC の OS イメージ等の実データの配置場所は本調達で導入する NAS を利用可能とする。
7. 作成するマスタのうち 1 機種について、OS マスタイメージ展開用のタスクシーケンスを作成すること。
8. マスタ展開等に利用可能な USB メモリを 5 本納品すること。USB メモリは Type-C 接続かつ 256GB 以上の容量を有すること。

4.9.3. 運用・保守要件

1. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。
2. MECM が OS イメージ展開に利用する Windows PE 環境や OS マスタイメージの更新手順書を作成すること。
3. タスクシーケンスの利用方法について手順書を作成すること。

5. 移行要件

5.1. 現行リモートワークインフラ基盤から新環境への移行

リモートワーク基盤を日常業務として利用する業務用 PC は現状約 1700 台程度あり、システムの移行に際して業務影響を最小限となるように移行設計を行うこと。

移行に際しての現状においての想定は以下のとおりとする。

・現行 PC は現行リモートワークインフラ基盤と接続、新 PC は新リモートワークインフラ基盤と接続を基本とするが、約 2 か月程度並行稼働期間を設け、現新どちらの基盤にも接続可能とする。

5.2. 新業務 PC の配布準備

新業務用 PC の配布スケジュール及び方法を PMDA と合意の上で作成すること。新 PC の一般利用

者への配布作業は PMDA が行う。一般利用者向けに新業務用 PC の初期セットアップ手順、現業務用 PC の取り扱い手順を作成すること。

5.3. NAS のデータ移行

新霞が関ビルで運用中の NAS に格納されたデータについて、本調達で導入する NAS にデータの移行を行うこと。

6. 現行システム終了時要件

現行リモートワークインフラ基盤機器等のシステム終了時の対応に関して記載する。データ消去は原則設置場所で行い、データ消去後はデータ消去が完了したことを示す書類を提出すること。なおデータ消去に必要な機器やソフトウェアは受注者が準備すること。

6.1. 現行リモートワークインフラ基盤機器

移行を完了した現行リモートワークインフラ基盤機器等について、データ消去を行い PMDA の指定する場所まで運搬すること。作業対象機器のリストは機密保持誓約書提出後に開示する。

6.2. 新霞が関ビル設置機器

移行を完了した現行リモートワークインフラ基盤機器等について、データ消去を行い PMDA の指定する場所まで運搬すること。作業対象機器のリストは機密保持誓約書提出後に開示する。また現行利用中の PC 約 1480 台のデータ消去を行うこと。

6.3. 関西支部設置機器

移行を完了した現行リモートワークインフラ基盤機器等について、データ消去を行い PMDA の指定する場所まで運搬すること。作業対象機器のリストは機密保持誓約書提出後に開示する。また現行利用中の PC 約 20 台のデータ消去を行うこと。

7. その他

7.1. サーバ証明書

インターネット経由で接続する可能性のあるサーバのうち、サーバ証明書が必要なものがある場合は必要数、用途を明確化した上で受注者が必要数分用意すること。サーバ証明書は EV 証明書とすること。ワイルドカード証明書は不可とする。サーバ証明書の更新が必要な場合、更新スケジュール及び更新手順書を作成すること。

7.2. 総合テスト

本システムを使用した業務正常性確認テストを総合テストとして実施する。業務正常性の確認主体は PMDA で行う。その結果に問題がある場合は PMDA から総合テストの結果を受けて、本システムの設計、設定に問題がないか受注者が確認を行い、修正が必要な場合は PMDA と協議の上で修正作業を行うこと。