業務システム統合基盤の構築及び保守
調達仕様書

令和５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 2
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 4
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 6
（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 8
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 9
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

業務システム統合基盤の構築及び保守

（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。

（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、役職員が業務を行うための基幹システム(共用 LAN システム)、特定業務システムを整備し運用している。

各システムを動作させるための仮想サーバ基盤、ネットワーク、セキュリティ装置等のシステムインフラを業務システムごとに構築する形をとっている。この方式でのインフラ構築は各業務システムに特化した構成を取りやすい反面、全体としての構成品の重複によるコスト高、システム運用のサイロ化等のデメリットもある。

各業務システムで必要とされるシステムインフラはある程度共通していることから、各業務システムを動作させるためのシステムインフラを一括で構成し、システムインフラ全体のコスト低減、セキュリティレベルの統一、運用ノウハウの集約を行う。本調達ではこれに必要なハードウェア、ソフトウェア、サービス、システム保守を導入する。

また、本調達で構築するシステムインフラ上に現行システムで運用している共用 LAN システムの機能を移行する。

（４）　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２ 概略スケジュール案」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	外部公開 DNS サービスリプレイス(仮)	
2	インターネット閲覧環境の構築(仮)	-
3	セキュリティログ基盤の構築(仮)	-
4	現行データセンタのラック利用継続(仮)	-
5	共用 LAN サブシステム 1 の移行(仮)	-

（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 外部公開 DNS サービスリプレイス(仮)

PMDA が運用するドメインの DNS レコードを管理するシステムの更新を行うことを計画している。本調達で導入する一部のシステムはインターネットに公開することから DNS レコードの登録が必要になる。これらの DNS レコードはこの調達案件で構築する DNS サービスに登録を行う。

② インターネット閲覧環境の構築(仮)

PMDA のクライアント端末がインターネット上のリソースにアクセスする際に使用するリモートデスクトップ環境。既に構築済みの環境だが、現行システムではインターネットとの境界になるファイアウォール装置とインターネット閲覧環境の間で IPsec VPN による接続を行っている。本調達で構成するインターネットとの境界になる装置でも IPsec VPN による接続を行う。尚、Microsoft Active Directory を使用したドメイン環境も構成されており、本調達の作業対象のドメイン環境と信頼関係を結んでいる。

③ セキュリティログ基盤の構築(仮)

本調達で導入する構成品のうち、主にセキュリティ機能の動作ログを管理するためのログ基盤を構築する。本調達ではこれらのログを汎用的な Syslog サーバに格納することを想定している。この調達案件ではこれらのログをログ基盤に転送するための仕組みを導入する。

④　現行データセンタのラック利用継続(仮)

本調達では本調達で導入する機器を設置するデータセンタと現行データセンタ間の通信を行うための閉域 WAN 回線を構成する。この回線を現行データセンタで収容するためのラックスペースが必要になることから、本案件では現行システムで利用しているラックの一部を継続的に利用できるようにする。

⑤　共用 LAN サブシステム 1 の移行(仮)

共用 LAN システムで運用しているサブシステムの一つを移行する。このサブシステムは現行システムのデータセンタのネットワーク機器を経由して独自のシステムインフラが構築されている。このシステムは令和 4 年の運用開始であることから本調達でのシステム構築後も継続的に使用するため、サブシステムのハードウェアを全て新しいデータセンタに移設し、システム接続を行う。

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。各別紙を確認し、内容を十分に理解した上で作業を行うこと。また、本システムのネットワーク要件に関しては要件や構成を詳細に記載していることからセキュリティ確保を目的として公開はしない。本調達に関する機密保持契約書を提出した応札者に送付する。

①　統合基盤システムの設計及び構築

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作業を行うこと。

②　共用 LAN システムのシステム移行

受注者は現行の仮想基盤システム上で動作している共用 LAN システムの機能、データ移行を行うこと。

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	システムインフラの設計、構築	2024 年 3 月 31 日
2	業務システム構築に関係のない現行の共用 LAN システムの移行	2024 年 11 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 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「政府機関のサイバー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、「政府機関のサイバーセキュリティ対策のための統一基準群（令和３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 システム全体概要図
別紙 2 概略スケジュール
別紙 3 システム詳細要件
別紙 4 業務システムネットワークアーキテクチャ
別紙 5 IP ネットワーク詳細構成 (機密保持誓約書を提出後に提供する。)

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：cm-kyoyolan●pmda.go.jp

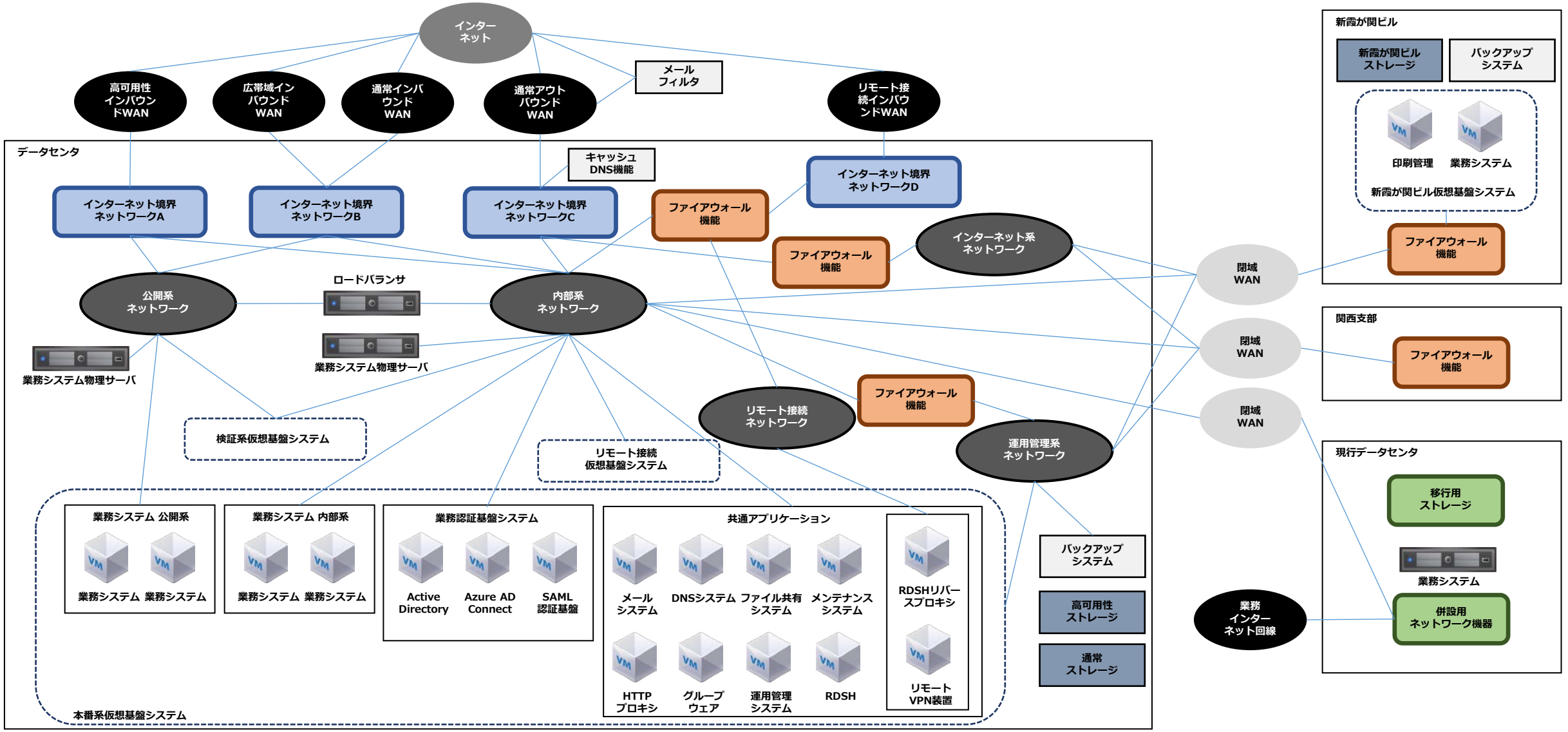
※迷惑メール防止対策をしているため、●を半角のアットマークに置き換えること。

業務システム統合基盤の構築及び保守

調達仕様書

別紙1 システム全体概要図

システム全体概要図


インターネット
高可用性インバウンドWAN
広帯域インバウンドWAN
通常インバウンドWAN
通常アウトバウンドWAN
メールフィルタ
リモート接続インバウンドWAN
データセンタ
キャッシュDNS機能
インターネット境界ネットワークA
インターネット境界ネットワークB
インターネット境界ネットワークC
インターネット境界ネットワークD
ファイアウォール機能
ファイアウォール機能
インターネット系ネットワーク
公開系ネットワーク
ロードバランサ
内部系ネットワーク
業務システム物理サーバ
業務システム物理サーバ
検証系仮想基盤システム
リモート接続ネットワーク
ファイアウォール機能
運用管理系ネットワーク
リモート接続仮想基盤システム
業務システム 公開系
業務システム 業務システム
業務システム 内部系
業務システム 業務システム
業務認証基盤システム
Active Directory
Azure AD Connect
SAML認証基盤
共通アプリケーション
メールシステム
DNSシステム
ファイル共有システム
メンテナンスシステム
RDSHリバースプロキシ
HTTPプロキシ
グループウェア
運用管理システム
RDSH
リモートVPN装置
本番系仮想基盤システム
バックアップシステム
高可用性ストレージ
通常ストレージ
閉域WAN
閉域WAN
閉域WAN
業務インターネット回線
新霞が関ビル
新霞が関ビルストレージ
バックアップシステム
印刷管理
業務システム
新霞が関ビル仮想基盤システム
ファイアウォール機能
関西支部
ファイアウォール機能
現行データセンタ
移行用ストレージ
業務システム
併設用ネットワーク機器

業務システム統合基盤の構築及び保守 調達仕様書

別紙2 概略スケジュール案

項番	項目	日程																								
		2023年									2024年												2025年	2026年	2027年	2028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	-			8月	9月	10月
	現行システム運用期間																											
	設計・構築・テスト																											
	既存システムの移行 (※1)																											
	PMDAによるシステム構築 (※2)																											
	基盤システム納品 (※)																											
	基盤システムの正常性テスト																											
	運用テスト																											
	システム保守の提供期間																											
	システムカットオーバ (※3)																											
	併設用ストレージの接続																											
	併設用ネットワーク機器の接続																											
	全体の正常性テスト																											
	閉域WAN回線Eの利用期間 (開始日程は構築方式による)																											

(※1)共用LANシステム及び現行の仮想基盤システム上の一部業務システムの移行を行う。現行の仮想基盤システムの運用期間中かつそれらに対する業務アクセスが停止しない限り、この期間を使用して移行作業を行って良い。

(※2)PMDAが構築を行うこととしているサブシステムを統合基盤システム上に構築する。

(※3)業務システム管理者が統合基盤システム上に業務システムの構築を開始できる状況を指す。

業務システム統合基盤の構築及び保守

調達仕様書 別紙 3 システム詳細要件

1. システム全体概要

1.1. システム概要

本調達で構築するシステムはPMDAの業務システムを稼働させるためのシステムインフラになる(以後、統合基盤システムと表記する。)。統合基盤システムでは統合基盤システムを使用して業務システムを構築する業務システム管理者に対して以下の汎用的なシステムインフラ機能を提供する。

- 仮想マシンの作成機能及びその稼働リソースとなるCPU、メモリ、ディスクの提供
- 仮想マシンの運用機能
- 物理サーバを設置するためのファシリティ
- 物理サーバを接続するためのネットワーク基盤
- 業務システムにアクセスするためのIPネットワーク機能
- 仮想マシン、物理サーバに対するロードバランス機能
- 公開システムに対するネットワークセキュリティ機能
- 仮想マシン、物理サーバに対するマルウェア駆除機能
- 仮想マシン、物理サーバのシステムバックアップ及びリストア機能
- 業務システム管理のための認証基盤
- 汎用的な通信アプリケーション機能

本調達では業務システム管理者に対するこれらの機能の画一的な提供を行うための仕組みを構築する。統合基盤システムの構成は以下のサブシステムで構成される。

- システムファシリティ
- 業務仮想基盤システム
- IPネットワークシステム
- バックアップシステム
- 業務認証基盤システム
- 共通アプリケーション

システムファシリティはシステムを構成するハードウェア等を設置する物理ロケーション、ラック、電源等の設備である。大部分のハードウェアはオンプレミス環境のデータセンタに設置することを想定しているが、一部の設備はPMDAの執務室内に設置する。データセンタではシステムを稼働させるために必要なラックスペース、電源、空調等の設備を借用する。PMDAの執務室に設置する機器を搭載するラックも納品対象になるが一部のハードウェアはPMDAの既設ラックに搭載する。

各サブシステムは業務システムに対してシステムインフラ機能を提供し、業務システムの構築

者はこれらの機能を使用して業務システムを統合基盤システム上に構築する。統合基盤システムでは業務システム構築者がなるべく汎用的な形で業務システムを構築できるような共通サービス機能の提供を目的とする。また、一部の機能は業務システムごとのカスタマイズ、運用管理が必要になることから、機能動作状況の参照、機能自体の設定権限を付与することで業務システム構築者に運用を委任する。

業務仮想基盤システムは業務システムの仮想マシンを構築、運用するための仮想サーバ基盤である。この仮想サーバ基盤は複数の業務システム管理者が使用することから、管理可能な仮想基盤システム上のオブジェクト及びその操作に関する権限を準備し、業務システム管理者が担当業務システムの範囲内で操作が可能となるような認証の仕組みを構成する。尚、仮想サーバ基盤を構成する物理ホストは複数の業務システムで共有し、特定の物理ホストを特定の業務システムに割り当てないものとする。

IP ネットワークシステムは統合基盤システム及び業務システムの各ノード、PMDA のクライアント端末、インターネットと相互に IP 通信をするためのネットワーク基盤である。セキュリティを確保するため、業務システム間、業務システム内で適切な L2、L3 通信境界を構成できるようなネットワーク構成を実装する。他に業務システム間通信のファイアウォール機能による通信制御、負荷分散を必要とするノードに対するロードバランス、IPS、WAF によるネットワークセキュリティ機能を提供する。また、物理サーバを必要とする業務システムのために物理サーバを収容できるネットワーク環境も整備する。

バックアップシステムは業務システムの仮想マシン、物理サーバのシステムバックアップ機能及びリストア機能を提供する。バックアップは業務システムに大きな問題が発生した際の復旧手段になることから、確実にバックアップ処理、リストア処理が機能するようにシステムを構成する。

業務認証基盤システムは PMDA 職員が業務にかかわるデバイスや機能の使用のために必要とする認証を行うための基盤システムである。認証データベースとしての Microsoft 社 Active Directory 及び Azure Active Directory を中核としており、現状でも共用 LAN システムにおいて運用している。全体管理者、業務システム担当者に統合基盤システムを利用する際の適切な権限を付与するため、業務認証基盤システムを構成する。

共通アプリケーションは汎用的なインフラアプリケーションである。メール配送機能や HTTP プロキシ機能、ファイル共有機能等を提供しており、統合基盤システムでは各業務システムがこれらの機能を使用できるようにサービスを提供する。多くの機能は共用 LAN システムが既に提供しているものであり、本調達ではこれらの機能を移行した上で、機能や性能の向上を行う。

リモート接続基盤システムは特定用途向けの VDI 及びリモートデスクトップホストシステムである。共用 LAN システムでは既に一定のリモートワーク環境を提供しているが、特定の立場や用

途において使用する VDI も提供している。本システムではこれらの機能を継続して提供するための VDI システムを構築する。

1.2. 統合基盤システム上での業務システムの構築

1.2.1. 概要

統合基盤システムの運用者は本調達で構築する全サブシステムを管理する全体管理者、本システム上に業務システムを構築する業務システム管理者に分けられる。業務システム管理者は業務システムごとに異なる。業務システム管理者は統合基盤システム上に業務システムを構築する。

業務システム管理者は構築対象ノードのネットワーク配置(公開、内部)、形式(仮想、物理)を検討し、統合基盤システム上にシステム構成を反映させる。統合基盤システムは構築対象ノードの性質に応じてセキュリティ機能や負荷分散機能、管理機能を提供し、業務システム管理者はこれらの機能を構築対象ノードに適用する。統合基盤システムでは可能な限り画一的なシステムアーキテクチャ、機能を提供することで、業務システム管理者が業務システムのアーキテクチャ設計、機能実装を効率的に行えるようにする。業務システムの正常稼働のため業務システム管理者が細かいチューニングを行うべきと考えられる要素の管理は業務システム管理者に委任できるような仕組みを目指す。一方、業務システム管理者の作業が他の業務システムや統合基盤システム全体の稼働に可能な限り影響を与えないような堅牢性の確保も行い、適切な権限委任、管理体制を構築する。

本調達の受注者は統合基盤システムがこうした運用を目的としたシステムであることを考慮して設計、構築を行うこと。

1.2.2. 業務システム構築フローのイメージ

業務システム管理者は全体管理者と連携し以下の流れで統合基盤システム上に業務システムを構築する。

項番	手順	内容
1	ネットワークアーキテクチャ検討	業務システムのノードを統合基盤システムのネットワークアーキテクチャに適用するための検討を行う。
2	ノードアーキテクチャ検討	ノードの冗長性、リソースの検討を行う。
3	利用機能の検討	業務システムのノードの性質に応じて統合基盤システムが提供する機能の利用有無を検討する。
4	管理アカウントの払い出し	業務システムの構築、運用の体制により必要なアカウント、権限を検討し、全体管理者から払い出しを受ける。
5	サーバリソースの払い出し	ノードアーキテクチャに沿ってリソースを申請し、全体管理者から払い出しを受ける。
6	仮想マシンの作成	仮想マシンの管理機能から仮想マシンを作成する。

7	IP 通信設定	必要に応じて L3 ルーティング、ファイアウォール設定を行い基本的な IP 通信の到達性を確保する。
8	物理サーバの接続	物理サーバをラックに搭載し、ネットワーク及びストレージに接続する。
9	ロードバランス設定	ロードバランス設定(TLS 復号化を含む)を行う。
10	セキュリティ機能設定	IPS、WAF、マルウェア対策の設定を申請し、全体管理者が設定を行う。
11	管理機能設定	システム監視やネットワークトラフィック監視の設定を行う。
12	システムバックアップ設定	仮想マシン、物理サーバのバックアップ設定を行う。
13	業務システム運用開始	運用を開始する。
14	チューニング	運用実態にあわせて設定をチューニングする。

このフローは現時点での想定であり、本調達の設計、構築にあわせて詳細な PMDA が構築フローを作成する。構築フローの策定にあたり、応札者の設計、構築範囲に関しては構成の説明やシステム利用方法の詳細を確認することがある。また、一部の提供機能に関連する構成要素は本調達の受注者ではなく PMDA が構築する。

1.2.3. ネットワークアーキテクチャ

統合基盤システム上の業務システムのネットワークアーキテクチャは「別紙 4 業務システムネットワークアーキテクチャ」に示す通り。ネットワークアーキテクチャの要点は以下の通り。

- 複数の異なる業務システムが同種のネットワークアーキテクチャを採用し、画一的なシステムを構成する。
- 業務システムのノードはインターネットに公開する公開系、内部から使用する内部系に分かれる。その分類により統合基盤システム上のネットワーク配置、セキュリティ機能が変わる。
- 業務システムのノードは公開系、内部系の中で仮想マシン、物理サーバの形式に分かれる。ノードの形式により統合基盤システム上のネットワーク配置が異なる。
- 公開システム向けのインバウンドインターネット回線を用意する。
- 業務システムが個別に用意する物理サーバを接続するための環境を提供する。物理サーバの性質にあわせたネットワーク配置環境を用意する。
- インターネットにアクセスするノードのためのアウトバウンドインターネット回線を用意する。
- 内部から公開システムにアクセスするための接続を用意する。
- 業務システムのノードをメンテナンスするための運用管理ネットワークを提供する。

1.2.4. システムリソース

統合基盤システムでは業務システムの仮想マシンのための CPU、メモリ、ディスク、物理サーバのためのファシリティ、物理ネットワーク接続環境、ディスクをリソースとして提供する。業務システム管理者は全体管理者が準備した申請フローに基づき、必要なリソース量と必要に応じてその形式を申請する。全体管理者は申請に基づきリソースを払い出す。業務システム管理者は払い出されたリソースを使用してシステムを構築する。

尚、本調達の要件に記載している各リソースサイズは統合基盤システムの利用を想定している業務システムのリソースサイズから算出したものになっており、実際の業務システム構築で使用できるリソースの最大値は限られている。

1.2.5. システムアカウント

統合基盤システムは全体管理者だけでなく複数の業務システム管理者が使用する。作業ミス等を起因とした統合基盤システム全体や管理対象外の業務システムへの影響を極小化するため、管理対象外のリソースに関する読み取り、書き込みの権限を可能な限り最小限とするように作業用アカウントとその権限設定を行う。

また、ディレクトリサービスを使用したアカウントの集中管理により可能な限り発行するアカウントの数を減らし、作業者のアカウント管理負荷を軽減する。同一業務システムであっても管理者の立場によって異なる権限が必要になることもある。これらのアカウントは可能な限り業務認証基盤システムと連携できる構成とするように設計、構築を行う。

1.2.6. IP 通信、ロードバランス設定

業務システムにはあらかじめ業務システムが利用可能なネットワークアドレスを払い出しており、業務システム管理者はこのネットワークアドレスから必要なネットワーク構成を切り出して使用する。同一の業務システムであっても複数の L3 ネットワークセグメントを使用する場合があるため、統合基盤システムでは業務システム内での L3 ルーティングを行えるような環境を提供する。

業務システム管理者は必要なネットワークアドレスの申請を行い、全体管理者はそのネットワーク環境の準備をする。ダイナミックルーティングを使用することで、ネットワーク機器の手動設定を必要とする作業内容を低減させる。業務システムのノード間が IP 通信を行うための L3 ルーティング設定及び付随する L2 設定は原則として全体管理者が行い、業務システム管理者にとってノード間の通信経路はある程度透過的な運用とする。

業務システムのノードによってはロードバランス及び TLS 復号化、再暗号化が必要になることがある。統合基盤システムではこれらのノードに対するロードバランス機能と TLS 処理機能を提供する。業務システムに関するこれらの設定は詳細なチューニングが必要になる場合があるため、設定は基本的に業務システム管理者が行う。ただし、前述の通り IP 通信に関わる基本的なネット

ワーク設定は全体管理者が可能な限り行う。

1.2.7. ネットワーク・エンドポイントセキュリティ機能

統合基盤システムでは公開系ノード向けのネットワークセキュリティ機能として IPS 及び WAF による不正通信の遮断機能と仮想マシン、物理サーバ向けのエンドポイントセキュリティ機能としてマルウェア対策機能を提供する。これらの機能を利用する場合、業務システム管理者はフローに基づいて利用を申請し全体管理者が設定する。除外ルール等の設定値チューニングは運用状況や業務システム個別の状況に応じて全体管理者が行う。

これらのセキュリティ機能による通信遮断ログを集積し、それぞれ閲覧できるような仕組みを構築するが、ログ閲覧機能の構築に関しては本調達の作業対象外とする。

1.2.8. システムバックアップ・リストア機能

統合基盤システムでは統合基盤システム上の仮想マシン、接続された物理サーバに対するシステム及びファイルレベルのバックアップ及びリストア機能を提供する。バックアップ設定、バックアップ成否確認、リストア作業は業務システム管理者が行う。システムアカウントを利用し、管理対象ノードのみを作業対象とすることが可能なように権限設定を行う。

バックアップ及びリストアは業務システムの稼働継続における重要な要素になり得る上、統合基盤システム上では複数の業務システムが稼働することからバックアップデータの保護を可能な限り高い安全性で行えるようにする。そのためデータセンタ内だけでなく別拠点でのバックアップデータの保全、不審なバックアップデータ更新の検出、バックアップデータへのアクセス制限を行う。

2. サブシステムの構成

2.1. システムファシリティ

2.1.1. 物理ロケーション

統合基盤システムを稼働させる物理ロケーションと役割は以下の通り。

名称	説明
データセンタ	統合基盤システムの主要なハードウェアを設置するデータセンタ。
現行データセンタ	現行の共用 LAN システムが稼働しているデータセンタ。
新霞が関ビル	PMDA の執務室。
関西支部	PMDA の執務室。

特段の記載がない限り、以降に記す導入品はデータセンタに設置する。

本調達で構築するハードウェアの大部分はデータセンタに設置する。現行データセンタでは一部のファシリティ条件が現在のハードウェアの設置、稼働に対して必ずしも適していないため、データセンタの変更を行う。

データセンタは立地、災害時体制、導入機器の排熱、エアフロー、耐荷重、消費電力、拡張性等の要件を考慮する。

尚、一部のシステムは現行データセンタで稼働を続けるため、現行データセンタと通信を行うための通信回線を準備する。

2.1.2. ラック

2.1.2.1. データセンタ

データセンタに設置するハードウェアを搭載するためのラックを構成に含める。ラックの用途は以下の通り。

ラック名	用途
WAN 収容ラック	インターネット回線、閉域 WAN を収容する ONU、WAN 回線を収容する L2 スイッチ、ネットワークセキュリティ装置を搭載する。
ネットワークラック	主要な L3 スイッチ、L2 スイッチを搭載する。
業務仮想基盤ラック	仮想基盤システムの物理ホスト、バックアップシステム及び一部の運用管理装置を搭載する。
ストレージラック	仮想基盤システムが使用する共有ストレージ、Fiber Channel スイッチを搭載する。

物理サーバラック	業務システム、特定用途の物理サーバを搭載する。
リモート接続基盤ラック	リモート接続基盤システムに関連する各装置を搭載する。
特定システム用ラック	本システムと接続する特定のシステムを搭載する。

データセンタに搭載する機器は標準では 200V 電源を使用する。100V しか対応していない機器には個別で対応する。

2.1.2.2. 新霞が関ビル

新霞が関ビルのハードウェアはビル内の 2 か所に設置する。設置場所、搭載情報は以下の通り。

設置場所	搭載
設置場所 1	データセンタとの接続に使用する閉域 WAN を収容する ONU、新霞が関ビルの通信境界になるファイアウォールを設置する。既設の 19 インチラックに搭載する。
設置場所 2	新霞が関ビルに設置する仮想基盤システムとそれらをネットワーク接続するネットワーク機器を設置する。24RU 程度以下のハーフサイズの 19 インチラックを構成に含める。

設置場所 1 では 100V 電源のみ使用できる。設置場所 2 では 200V を使用できるが、可能な限り 100V 電源の機器を使用する。200V を使用する場合、電源工事が必要になるため電源が必要になる時期の 6 か月以上前に PMDA にその旨を伝達すること。

2.1.2.3. 関西支部

関西支部のハードウェアは既設の 19 インチラックに搭載する。電源は 100V のみ使用できる。

2.1.2.4. 現行データセンタ

データセンタと現行データセンタを接続する閉域 WAN を収容する ONU、後述する併設用ネットワーク機器、併設用ストレージを設置する。現行機器を搭載しているラックに搭載する。

2.2. 業務仮想基盤システム

業務仮想基盤システムは以下に記す種類の仮想基盤システム及び物理サーバで構成される。

名称	説明
本番系仮想基盤システム	業務システムのプロダクション及びステージング環境の仮想マシンを稼働させるための仮想基盤システム。
検証系仮想基盤システム	本番系仮想基盤システムの設定変更の動作テスト、新規システムの概念検証を行うための仮想基盤システム。
新霞が関ビル仮想基盤システム	新霞が関ビルに設置する小規模の仮想基盤システム。業務システムのプロダクション環境を稼働させる。

物理サーバ	業務システムが特定用途に用意する物理サーバ。

2.2.1. 本番系仮想基盤システム

2.2.1.1. 基本構成

ハイパーバイザ型の仮想基盤管理ソフトウェア、物理ホスト、Fiber Channel(FC)接続する共有ストレージにより構成する。仮想マシンに使用できる OS として Windows Server2019、2022、Red Hat Enterprise Linux(RHEL)8、9 を提供する。これらの OS を使用した仮想マシンは数量無制限に構築できるような OS ライセンスを用意する。

2.2.1.2. 仮想基盤物理ホスト

仮想基盤物理ホストには汎用的なサーバを使用する。実際に稼働する仮想マシンの OS は Windows Server と RHEL で偏りが想定されることから、Windows Server 用の物理ホスト、RHEL 用の物理ホストに分ける。物理ホストの CPU、メモリリソース量の検討は PMDA が行った結果を要件としている。物理ホスト数量は Windows Server 用を 11 台、RHEL 用を 4 台とする。冗長性能としてそれぞれ N+2、N+1 を想定している。

2.2.1.3. 仮想基盤システムを管理するための Web インターフェース

仮想基盤システムの仮想マシン、ディスク領域、ネットワーク接続等のオブジェクトを管理するための Web インターフェースサーバ(仮想基盤管理サーバ)を導入する。

仮想基盤管理サーバの機能利用にはユーザ認証を必須とし、業務認証基盤システムと連携して認証及び参照、操作内容の権限管理を行う。

仮想基盤管理サーバは少なくとも 2 台で冗長化し、可用性を向上させる。

2.2.1.4. 共有ストレージ

本番系仮想基盤システムが使用する共有ストレージと FC スイッチを経由して接続する。共有ストレージはストレージを利用する仮想マシン、物理サーバの要件に対応するため複数種類で構成する。共有ストレージの種別は以下の通り。

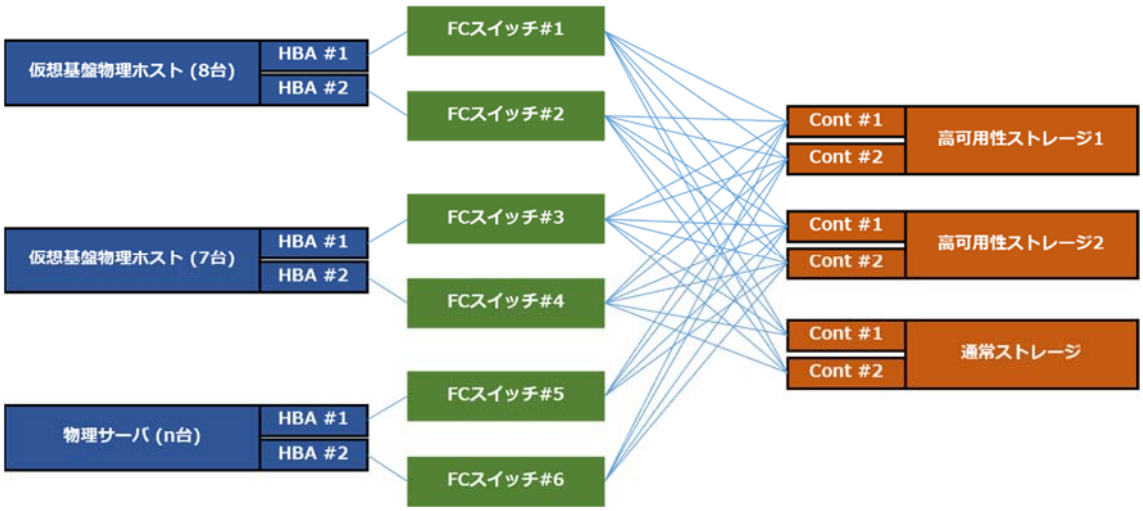
名称	説明
高可用性ストレージ 1	プロダクション環境の仮想マシンの仮想ディスク、データを格納する。
高可用性ストレージ 2	プロダクション環境の仮想マシンの仮想ディスク、データを格納する。
通常ストレージ	特段の高い可用性を必要としないデータや一部のバックアップファイル、アーカイブデータを格納する。

高可用性ストレージは 2 台で構成し、並列で構成する。2 台の高可用性ストレージ間では特にデータレプリケーション等は行わず、システム構築時に仮想マシン及び物理サーバの配置先を 2 台の高可用性ストレージから選択することでストレージレベルの冗長性を確保できるようにする。尚、必ずしも冗長構成の仮想マシンのみが使用するわけではない。

高可用性ストレージ 1、高可用性ストレージ 2 を制御するコントローラは二重化し、コントローラ障害時にも可能な限り早く SCSI 通信を再開するためコントローラは Active-Active で動作可能なことを要件とする。コントローラ片系障害時の性能縮退は許容する。

通常ストレージを制御するコントローラは二重化し、コントローラが Active-Standby で動作することを要件とする。

仮想基盤物理ホストには Host Bus Adapter(HBA)を 2 個搭載し、FC スイッチとマルチパス接続する。各 FC 接続インターフェースの帯域は 32Gbps とする。SAN 接続の構成イメージは以下の通り。



2.2.1.5. 共有ストレージのボリューム

各共有ストレージでは用途に応じて仮想基盤システム、物理サーバから利用可能なボリュームを設定する。具体的なボリューム構成はシステム設計の際に決定する。

2.2.1.6. ネットワーク接続

仮想基盤物理ホストは IP ネットワークシステムで構成するサーバ接続 L2 スイッチ A、サーバ接続 L2 スイッチ B、サーバ接続 L2 スイッチ C、管理 L2 スイッチと接続する。各ネットワーク接続の情報は以下の通り。

接続スイッチ	用途	メディア	本数
サーバ接続 L2 スイッチ A	仮想マシンのサービストラフィック	10GBase-SR	2

サーバ接続 L2 スイッチ B	仮想基盤システムの運用トラフィック	10GBase-SR	2
サーバ接続 L2 スイッチ C	運用管理、バックアップトラフィック	10GBase-SR	2
管理ポート L2 スイッチ	IPMI インターフェース	100/1000Base-T	1

サーバ接続 L2 スイッチ B に接続する NIC は仮想マシンの物理ホスト移動等、仮想基盤特有の操作に伴い発生するトラフィックに割り当てる。

複数接続するインターフェースではリンクアグリゲーションに相当する機能を使用し、両接続を Active として使用できるように構成する。

2.2.1.7. 仮想マシンのネットワーク構成

業務仮想基盤システム上で動作する仮想マシンに求められるセキュリティレベルは異なるため、仮想マシンの L3 セグメントを適切に構成した上で、L4 フィルタリングを行えることを必須とする。ネットワーク構成の要件の詳細は「2.3IP ネットワークシステム」に記載しているのでそちらを参照すること。IP ネットワークシステムとの通信の整合性を取るため、仮想基盤システム側でも必要なネットワーク設定を行う。

2.2.1.8. 物理サーバの接続

本番系仮想基盤システムでは業務システムの物理サーバの接続環境を提供する。物理サーバは物理サーバ用の FC スイッチを介して高可用性ストレージに接続する。FC 接続は以下の通り。

帯域 / メディア	本数	HBA 構成
32Gbps (マルチモード光ファイバ)	2	2 個の HBA を使用しそれぞれ 1 本ずつ FC 接続する。

物理サーバのネットワーク物理接続は以下の通り。

用途	メディア	本数	接続スイッチ
仮想マシンのサービストラフィック	10GBase-SR	2	サーバ接続 L2 スイッチ D
運用管理、バックアップトラフィック	10GBase-SR	2	サーバ接続 L2 スイッチ E
IPMI インターフェース	100/1000Base-T	1	管理 L2 スイッチ

ネットワーク論理接続は「2.3IP ネットワークシステム」に記載する。

本システムにおいて業務システムの物理サーバを以下ように分類する。

物理サーバの種別	用途
公開物理サーバ	インターネットに公開するシステムのユーザインターフェースサーバ。

公開物理サーバ連携物理サーバ	インターネットに公開するシステムのユーザインターフェースサーバが物理サーバの場合にその物理サーバが連携する物理サーバ。
公開仮想マシン連携物理サーバ	インターネットに公開するシステムのユーザインターフェースサーバが仮想マシンの場合にその仮想マシンが連携する物理サーバ。
内部物理サーバ	内部向けのシステムのユーザインターフェースサーバ。
内部物理サーバ連携物理サーバ	内部向けのシステムのユーザインターフェースサーバが物理サーバの場合にその物理サーバが連携する物理サーバ。
内部仮想マシン連携物理サーバ	内部武家のシステムのユーザインターフェースサーバが仮想マシンの場合にその仮想マシンが連携する物理サーバ。

各物理サーバはロードバランスの対象となることがある。

2.2.1.9. KVM コンソール

本番系仮想基盤システムの物理ホストが搭載されているラック全てにディスプレイ、キーボード、ポインティングデバイス機能を有する KVM コンソールを設置し、基本的なローカル作業を行えるようにする。操作対象の物理ホストを切り替えられる機能を持つことを要件とする。

2.2.2. 検証系仮想基盤システム

2.2.2.1. 基本構成

検証系仮想基盤システムは基本的に本番系仮想基盤システム自体の検証環境として運用することを想定しているため、基本的に本番系仮想基盤システムと同等の構成とする。ただし、システムサイズは本番系と同等である必要はないため、仮想基盤物理ホストの数量や共有ストレージの容量は本番系仮想基盤システムより小さく設計する。

2.2.2.2. 仮想基盤物理ホスト

仮想基盤物理ホストには汎用的なサーバを使用する。仮想基盤物理ホストは 3 台で構成し、全ての物理ホストの仮想マシンが数量無制限で Windows Server2019、2022、RHEL8、9 を使用できるような OS ライセンスを用意する。

2.2.2.3. 仮想基盤システムを管理するための Web インターフェース

仮想基盤システムの仮想マシン、ディスク領域、ネットワーク接続等のオブジェクトを管理するための Web インターフェースサーバ(仮想基盤管理サーバ)を導入する。本番系仮想基盤システムとは別個に作成する。

仮想基盤管理サーバの機能利用にはユーザ認証を必須とし、業務認証基盤システムと連携して認証及び参照、操作内容の権限管理を行う。

仮想基盤管理サーバは少なくとも 2 台で冗長化し、可用性を向上させる。

2.2.2.4. 共有ストレージ

検証系仮想基盤システムが使用する共有ストレージと FC スイッチを経由して接続する。共有ストレージは検証用仮想基盤システム専用のストレージを構成する。ストレージのファームウェアアップデートのテスト等、ストレージレベルのテストも行うため、本番系仮想基盤システムの高可用性ストレージと同じモデルのストレージを使用する。FC スイッチも検証系仮想基盤システム用に用意する。検証系仮想基盤システムで使用するストレージの種別は以下の通り。

名称	説明
検証用ストレージ	統合基盤の検証、新規システムの PoC に使用する。

仮想基盤物理ホストには Host Bus Adapter(HBA)を 2 個搭載し、FC スイッチとマルチパス接続する。各 FC 接続インターフェースの帯域は 32Gbps とする。SAN 接続の構成イメージは以下の通り。

2.2.2.5. 共有ストレージのボリューム

具体的なボリューム構成はシステム設計の際に決定する。

2.2.2.6. ネットワーク接続

仮想基盤物理ホストは IP ネットワークシステムで構成するサーバ接続 L2 スイッチ G、管理 L2 スイッチと接続する。各ネットワーク接続の情報は以下の通り。

接続スイッチ	用途	メディア	本数
サーバ接続 L2 スイッチ G	仮想マシンのサービストラフィック	10GBase-SR	2
サーバ接続 L2 スイッチ G	仮想基盤システムの運用トラフィック	10GBase-SR	2
サーバ接続 L2 スイッチ G	運用管理、バックアップトラフィック	10GBase-SR	2
管理 L2 スイッチ	IPMI インターフェース	100/1000Base-T	1

複数接続するインターフェースではリンクアグリゲーションに相当する機能を使用し、両接続を Active として使用できるように構成する。

2.2.2.7. 仮想マシンのネットワーク構成

業務仮想基盤システム上で動作する仮想マシンに求められるセキュリティレベルは異なるため、仮想マシンの L3 セグメントを適切に構成した上で、L4 フィルタリングを行えることを必須とする。ネットワーク構成の要件の詳細は「2.3IP ネットワークシステム」に記載しているのでそちら

を参照すること。IP ネットワークシステムとの通信の整合性を取るため、仮想基盤システム側でも必要なネットワーク設定を行う。

2.2.2.8. KVM コンソール

検証系仮想基盤システムの物理ホストに対して基本的なローカル作業を行うためのディスプレイ、キーボード、ポインティングデバイス機能を有する KVM コンソールを設置する。ただし、検証系仮想基盤システムの物理ホストが本番系仮想基盤システムと同じラックに搭載されている場合は本番系仮想基盤システムの KVM コンソールと兼用しても良い。操作対象の物理ホストを切り替えられる機能を持つことを要件とする

2.2.3. 新霞が関ビル仮想基盤システム

2.2.3.1. 基本構成

PMDA では新霞が関ビルで執務を行う職員が多いことから、ネットワークトラフィックのやり取りの効率性を上げるため一部のサーバを新霞が関ビルに配置している。新霞が関ビル仮想基盤システムはそれらのサーバを稼働させるための基盤として構成する。ただしこの仮想基盤システムで動作する仮想マシンは少ないことが想定されるため、本番系仮想基盤システムと比べてシンプルなシステム構成とする。また、新霞が関ビルでは設備のメンテナンスを目的とした電源の停止が定期的に発生するため、システム停止及び再稼働をなるべく簡易に行えるような構成とする。

2.2.3.2. 仮想基盤物理ホスト

仮想基盤物理ホストは 3 台で構成する。Windows Server2019 または Windows Server2022 を 8 台、RHEL8 または 9 を 4 台利用可能になる OS ライセンスを用意する。

2.2.3.3. 仮想基盤システムを管理するための Web インターフェース

仮想基盤システムの仮想マシン、ディスク領域、ネットワーク接続等のオブジェクトを管理するための Web インターフェースサーバ(仮想基盤管理サーバ)を導入する。ただし、本番系仮想基盤システムと共通化できる場合、本番系仮想基盤システムの仮想基盤管理サーバを使用しても良い。その場合、異なる仮想基盤システムとして管理できるように仮想基盤システムとしてのクラスタリング構成を分割すること。

仮想基盤管理サーバの機能利用にはユーザ認証を必須とし、業務認証基盤システムと連携して認証及び参照、操作内容の権限管理を行う。

2.2.3.4. 共有ストレージ

新霞が関ビル仮想基盤システムでは共有ストレージと iSCSI で接続する。物理ホスト及び共有ストレージは iSCSI 用にサーバ接続 L2 スイッチ I と 10GBase-SR で接続し、10Gbps の帯域を確保する。新霞が関ビル仮想基盤システムで使用するストレージの種別は以下の通り。

名称	説明

新霞が関ビルストレージ	新霞が関ビル仮想基盤システムのプロダクション環境の仮想マシン、データを格納する。

通常ストレージを制御するコントローラは二重化する。冗長方式は Active-Active、Active-Standby どちらでも良いものとする。

2.2.3.5. 共有ストレージのボリューム

各共有ストレージでは用途に応じて仮想基盤システム、物理サーバから利用可能なボリュームを設定する。具体的なボリューム構成はシステム設計の際に決定する。

2.2.3.6. ネットワーク接続

仮想基盤物理ホストは IP ネットワークシステムで構成するサーバ接続 L2 スイッチ I、既設 L2 スイッチ B と接続する。各ネットワーク接続の情報は以下の通り。

接続スイッチ	用途	メディア	本数
サーバ接続 L2 スイッチ I	仮想マシンのサービストラフィック	10GBase-SR	2
サーバ接続 L2 スイッチ I	仮想基盤システムの運用トラフィック	10GBase-SR	2
サーバ接続 L2 スイッチ I	iSCSI トラフィック	10GBase-SR	2
サーバ接続 L2 スイッチ I	運用管理、バックアップトラフィック	10GBase-SR	2
既設 L2 スイッチ B	IPMI インターフェース	100/1000Base-T	1

10GBase-SR 接続は Direct Attach Cable を使用しても良い。その場合はサーバ接続 L2 スイッチ I との接続実績を考慮すること。

複数接続するインターフェースではリンクアグリゲーションに相当する機能を使用し、両接続を Active として使用できるように構成する。

2.2.3.7. 仮想マシンのネットワーク構成

仮想マシンのデフォルトゲートウェイは内部ファイアウォール D を指定する。仮想マシンの数や種類は少ないため、新霞が関ビル仮想基盤システムのネットワークは単純な L2 接続のみとし、仮想マシン間の L3 通信制御は内部ファイアウォール D、L2 通信制御はサーバ接続 L2 スイッチ I で行う。

2.2.3.8. KVM コンソール

新霞が関ビル仮想基盤システムの物理ホストが搭載されているラック全てにディスプレイ、キーボード、ポインティングデバイス機能を有する KVM コンソールを設置し、基本的なローカル作業を行えるようにする。操作対象の物理ホストを切り替えられる機能を持つことを要件とする。

2.2.3.9. UPS による電源保護とシャットダウン連携

新霞が関ビルの電源設備に意図しない停止があった場合に新霞が関ビル仮想基盤システムに対する電源供給を UPS により一定時間保護し、あらかじめ定めた時間内に入力電源が復旧しない場合は自動的に仮想マシン及び新霞が関ビル仮想基盤システムを自動的に停止させる仕組みを導入する。

2.3. IP ネットワークシステム

2.3.1. 概要

本システムの各ノード間の IP 通信を制御するためのネットワークシステムを構成する。既存のネットワークシステムの更新ではなく、本システム向けに新たに作成するネットワークであることに留意すること。

業務システムに対して画一的なネットワーク構成を提供できるようにネットワークを構成する。

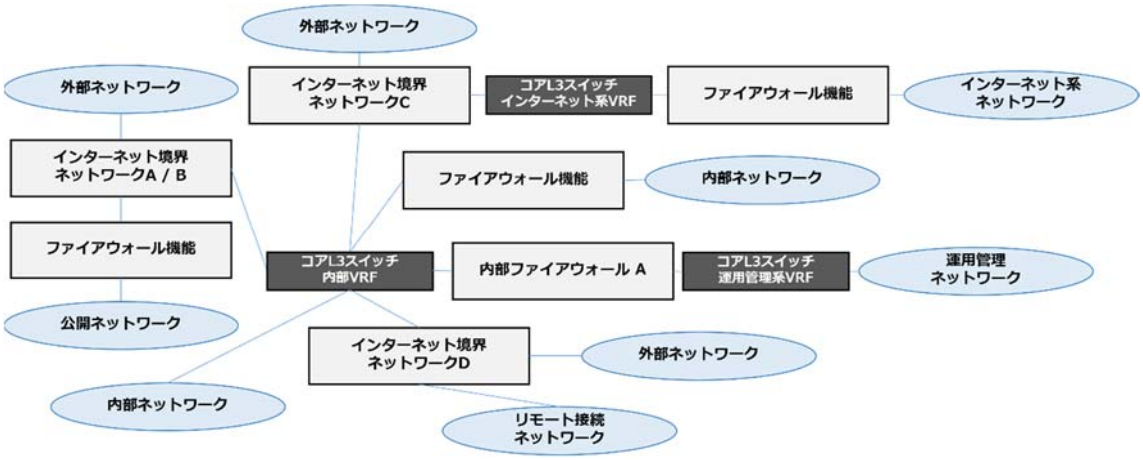
2.3.2. ネットワーク分類と分類間の通信制御

ネットワークは以下の 6 個に分類され、具体的なネットワークアドレスはいずれかのネットワーク分類に所属する。異なるネットワーク分類間が通信を行う場合は L3/L4 フィルタリングが可能な装置を経由する必要がある。

ネットワーク分類は以下の通り。

- 内部ネットワーク
- 公開ネットワーク
- 運用管理ネットワーク
- インターネット系ネットワーク
- リモート接続ネットワーク
- 外部ネットワーク

ネットワーク分類間の通信はおおむね以下の構成を想定している。詳細な構成は受注者と PMDA の設計合意の上で決定する。



各ネットワーク分類の説明は以下に記載する通り。

内部ネットワークは本システムを構成する各サーバ、本システム上に構築する業務システムの各サーバが構成する提供サービスのうち、インターネットへの公開を行わないサービスを提供することを目的としたノードと内部で使用するクライアント端末を収容するネットワークを指す。ノードの形態は仮想、物理を問わない。

公開ネットワークは本システムを構成する各サーバ、本システム上に構築する業務システムの各サーバが構成する提供サービスのうち、インターネットへの公開を行うサービスを提供することを目的としたノードを収容するネットワークを指す。サーバの形態は仮想、物理を問わない。ただし、このネットワーク分類に所属しているノード全てがインターネットに直接公開されるわけではなく、例えばインターネットに公開するサーバが参照するデータベースサーバのようなノードもここに配置することがある。公開システムネットワークはデータセンタに構成する。

運用管理ネットワークは本システムを構成する各サーバ、本システム上に構築する業務システムのメンテナンス作業及びバックアップトラフィックのためのネットワークを指す。運用管理ネットワークは基本的に運用管理ネットワーク内で通信が完結するように構成するが、必要最低限の通信のみファイアウォールを経由して許可する。運用管理ネットワークはデータセンタ、新霞が関ビル、関西支部に構成する。

リモート接続ネットワークはリモート接続基盤システムに接続するためのネットワークを指す。リモート接続基盤システムの VDI やリモートデスクトップホスト自体のトラフィックはこのネットワーク分類ではなく内部ネットワークに所属する。

インターネット系ネットワークは一部を除いて他のネットワークと切り離されており直接インターネットに接続しているネットワークを指す。インターネットに接続するクライアント端末以外に、本調達で構成する仮想基盤システム上の一部のサーバもこのネットワークに所属する。インターネット系ネットワークはデータセンタ、新霞が関ビル、関西支部に構成する。

外部ネットワークはインターネット上の不特定多数のノードが存在しているネットワークを指す。外部ネットワークは本システムの制御対象外であるため、必要最低限の通信のみ外部ネットワークと通信するような構成とし、外部ネットワークとの出入りを制御する。

2.3.3. インターネット回線

本システムではインターネット回線を用途に応じて複数構成する。構成したインターネット回線は後述するインターネット境界ネットワークに収容する。構成するインターネット回線は以下の通り。

名称	用途
高可用性インバウンド回線	可用性が重視される公開システム向けの回線
広帯域インバウンド回線	帯域を必要とする公開システム向けの回線
通常インバウンド回線	特段の要件のない公開システム向けの回線
リモート接続インバウンド回線	VDI 等のリモート接続を行うための回線。
通常アウトバウンド回線	Web 閲覧、メール、システムトラフィック向けの回線

2.3.4. インターネット境界ネットワーク

インターネットとの境界ではセキュリティ維持のための機能、公開システム向けの負荷分散機能を構成する。障害時の影響範囲の局所化、トラフィック分散を目的とし、回線種別に応じて複数系統のインターネット境界ネットワークを構成する。

名称	用途
インターネット境界ネットワーク A	高可用性インバウンド回線を収容する。
インターネット境界ネットワーク B	帯域確保インバウンド回線、通常インバウンド回線、リモート接続回線を収容する。
インターネット境界ネットワーク C	アウトバウンド回線を収容する。
インターネット境界ネットワーク D	リモート接続基盤システム上の VDI、RDSH と接続するためのインバウンド回線を収容する。

2.3.4.1. インバウンド回線

インターネット境界ネットワーク A、B は公開システム向けに以下の機能を提供することを要件とする。

- L3/L4 フィルタリング
- IPS
- Web アプリケーションファイアウォール(WAF)
- ロードバランス

IPS 及び WAF によるフィルタを行う際、対象トラフィックが TLS により暗号化されている場合は復号化してフィルタが可能な構成とする。各セキュリティ機能によるフィルタを終えた後は負荷分散対象のノードが収容されている L3 ネットワーク機器に向けてトラフィックを転送する。この時、復号化した TLS トラフィックの再暗号化の有無を宛先に応じて選択可能とする。

インターネット境界ネットワークはそれぞれ複数の異なる回線を収容する(インターネット境界ネットワーク A は現状では 1 種別回線のみの収容だが、今後拡張する可能性がある)。それらのトラフィックをルーティングするため、公開システムの分類に応じてインターネット境界ネットワークでは複数のルーティングテーブルを持つ装置を使用する。

インターネット境界ネットワーク D は外部ネットワーク、内部クライアントネットワークからリモート接続基盤システム上の VDI、RDSH に接続するために使用する。セキュリティを考慮し、この接続には L3/L4 フィルタリング機能を要件とする。

2.3.4.2. アウトバウンド回線

インターネット境界ネットワーク C はアウトバウンド回線を収容することから、以下のセキュリティ機能を要件とする。

- L3/L4 フィルタリング
- 不正な FQDN の名前解決に対する DNS 通信のブロック
- Web/URL フィルタリング
- トラフィックのクラウドアプリケーション分析

外部ネットワークにアクセス可能な送信元 IP アドレス、L4 ポート情報を最小限となるように構成し、不要な端末が直接インターネットに接続できないようにする。

アウトバウンド回線を追加する時に備え、複数のルーティングテーブルを持つ装置を使用する。

2.3.4.3. インターネット境界ネットワークの構成

インターネット境界ネットワークの具体的な構成は「2.3.7L3 ネットワーク構成」に記載している。

2.3.5. 閉域 WAN 回線

各拠点を閉域回線で接続する。閉域回線の一覧は以下の通り。

名称	用途
閉域 WAN 回線 A	データセンタと新霞が関ビルを接続し、サービス系トラフィックの転送に使用する。
閉域 WAN 回線 B	データセンタと新霞が関ビルを接続しバックアップトラフィック及び運用管理トラフィックの転送に使用する。

閉域 WAN 回線 C	データセンタと関西支部を接続し、サービス系トラフィック、運用管理トラフィックの転送に使用する。
閉域 WAN 回線 D	データセンタと現行データセンタを接続し、新霞が関ビル、関西支部からデータセンタを経由して現行データセンタ上のサービス利用に使用する。
閉域 WAN 回線 E	データセンタと現行データセンタを接続し､本調達及び業務システムのデータ移行用の回線として使用する。

各閉域 WAN 回線では広域イーサネットを使用し、IEEE802.1Q タグ VLAN を使用できることを要件とする。

閉域 WAN 回線 E は 2025 年 12 月 31 日までの運用とする。

2.3.6. 業務システムのネットワーク接続

本システム上に構築する業務システムのサーバが他のノードと通信を行う際は同じネットワーク分類のノード同士であっても原則として L3/L4 フィルタリングが可能な装置を経由するものとする。業務システムのサーバは内部ネットワークだけでなく、運用管理ネットワーク、インターネット系ネットワークでも稼働する。

2.3.7. L3 ネットワーク構成

この節では本システムのネットワーク構成の詳細な説明、意図を記載する。システム運用におけるセキュリティ維持のため必要な手続きを行った応札者にのみ提供する。手続きについては調達仕様書本紙を参照すること。

2.4. バックアップシステム

2.4.1. 概要

本調達で構築する仮想基盤システム上の仮想マシン、物理サーバ(それぞれ業務システムサーバを含む)のバックアップ及びリストアが可能な仕組みを構成する｡バックアップは 2 種類取得する。一つ目はデータセンタで取得(1 次バックアップ)し、二つ目は 1 次バックアップで取得したバックアップデータを新霞が関ビルに設置したバックアップシステムにコピーする(2 次バックアップ)。

バックアップシステムではバックアップ設定、バックアップ動作、リストア操作は各業務システム担当者が行える仕組みを構成する。管理対象外のノードに対する操作を誤って行えないような権限設定も行う。

2.4.2. バックアップ処理の基本要件

バックアップシステムで取得するバックアップの粒度は業務システムの仮想マシン、物理サーバのマシンレベルのバックアップを基本とする。ただし、このバックアップデータからのリストアはシステムレベルだけでなくファイル単位でのリストアが可能となるようにバックアップデー

タを取得する。

1 次バックアップは前回バックアップ時との差分をバックアップデータとして取得する増分バックアップを毎日取得し、14 世代のバックアップデータを確保する(一部、週に 1 回取得にする等、スケジュールが異なるものもある)。バックアップ対象のデータ総量はフルバックアップと 14 日の増分バックアップ全てを合算して 500TB を前提とする。1 次バックアップは夜間に動作させることを想定しており、6 時間 30 分以内に完了させられるようなバックアップ処理性能を確保する。

2 次バックアップには 1 次バックアップをコピーする。2 次バックアップは 1 次バックアップの完全なコピーとし、 1 次バックアップと同じ粒度、世代でのバックアップデータを保持する。

業務システム管理者が用意する独自のバックアップデータは業務仮想基盤システムの通常ストレージに格納する。

2.4.3. リストア処理の想定

データセンタ及びデータセンタに構築した統合基盤システムの機能の大部分が利用可能である場合、1 次バックアップデータからのリストア処理を行う。リストア操作は業務システム管理者が行う。

1 次バックアップデータが利用不可の場合、2 次バックアップからリストア処理を行う。例えば災害等でデータセンタ自体の利用が困難な状況を想定する。この時にデータセンタやシステム稼働に必要なハードウェアは使用できない可能性が高いが、それらのハードウェアの準備は本調達の保守の範囲内で復旧を行うものとし、その他に必要となるものがある場合は別途の検討とする。バックアップシステムはこれらのハードウェアやシステムインフラが整っていることを前提とした場合のリストアデータを提供する。ただし、2 次バックアップからのリストアは 2 次バックアップ側のデータからのみで行えるようにすることを要件とする。例えば、2 次バックアップに対応する 1 次バックアップデータがない場合にリストアができないような構成は認めない。

2.4.4. バックアップシステムの基本構成

バックアップシステムは以下の要素で構成する。

構成品	説明
バックアップ取得サーバ	本番系仮想基盤システム、物理サーバの日常的なシステムバックアップを 1 次バックアップとして取得し、2 次バックアップデータ格納サーバと連携して 2 次バックアップの保全処理を行う。 動作テスト等を目的として検証系仮想基盤システムの仮想マシンを対象とすることもある。

新霞が関ビルバックアップ取得サーバ	新霞が関ビル仮想基盤システム上の仮想マシンの日常的なバックアップを 1 次バックアップとして取得する。
2 次バックアップデータ格納サーバ	2 次バックアップのデータを保管するサーバ。

バックアップを取得するためのバックアップサーバをデータセンタに構成する。バックアップサーバが仮想マシンであるか物理装置であるかの指定はしないが、要件に記載のバックアップ処理機能、性能を持つ構成とする。

バックアップシステムを物理装置で構成する場合、バックアップ処理を行うネットワークインターフェースをサーバ接続 L2 スイッチ H に接続してバックアップ処理を行う。バックアップトラフィックの帯域を考慮し、サーバ接続 L2 スイッチ H とは物理装置 1 台あたり 10Gbps 以上の帯域を確保できるように接続する。

バックアップシステムを仮想マシンで構成する場合、バックアップシステム用の物理サーバを業務仮想基盤システムの物理ホストとして追加で用意し、その物理サーバの OS、マルウェア対策、ネットワーク接続、バックアップデータ格納用のストレージを用意すること。

バックアップ取得サーバで新霞が関ビルバックアップ取得サーバの機能を包含しても良い。新霞が関ビルバックアップ取得サーバを個別に構成する場合、新霞が関ビルの仮想マシンをバックアップするための物理サーバを構成し、サーバ接続 L2 スイッチ I に 10Gbps 以上の帯域を確保できるように接続する。

2 次バックアップデータ格納サーバはサーバ接続 L2 スイッチ I に 10Gbps 以上の帯域を確保できるように接続する。新霞が関ビルバックアップ取得サーバと機能を兼用しても良い。データセンタと新霞が関ビル間のバックアップトラフィック転送には閉域 WAN C を使用する。

2.4.5. バックアップ対象

1 次バックアップ対象は以下の通り。

- 本番系仮想基盤システムの仮想マシンの構成ファイルと仮想ディスク
- 検証系仮想基盤システムの仮想マシンの構成ファイルと仮想ディスク
- データセンタに設置する物理サーバのシステム構成情報とディスクデータ
- 新霞が関ビル仮想基盤システムの仮想マシンの構成ファイルと仮想ディスク

バックアップ対象の OS は Windows Server2019、Windows Server2022、RHEL8、RHEL9 とする。必要であればバックアップ対象サーバにエージェントソフトウェアをインストールすることを前提として良い。

2 次バックアップ対象は 1 次バックアップ対象のデータ全てだが、新霞が関ビル仮想基盤シス

テムの仮想マシンの 2 次バックアップは取得しなくても良い。

2.4.6. バックアップシステムの責任囲外の要素

バックアップシステムではデータベースのトランザクションログレベルのバックアップ取得機能を業務システム管理者には提供しない。トランザクションログの保全が必要な場合は業務システム管理者が独自に構築するものとする。ただし、業務システム管理者が構築したトランザクションログを取得するサーバのシステムバックアップの取得はバックアップシステムにて取得する。

2.4.7. バックアップ設定及び動作の管理

業務システム管理者は自身の管理対象ノードのバックアップ設定、バックアップ成否の確認、バックアップ再実行、リストアのような運用作業を行う。このため、業務システム管理者がバックアップシステムの管理インターフェースにログインする際は管理対象ノード以外の操作ができないような構成とする。

2.4.8. バックアップデータの保護

統合基盤システムでは業務システムのデータ保護を行うことから、バックアップデータ自体の保護を可能な限り行う。バックアップデータ自体の暗号化、ファイルシステムの書き込み制限、バックアップデータに対する IP アクセス制御のような機能によりバックアップデータを保護する。

2.4.9. ランサムウェア被害からの復旧

バックアップシステムでは災害等の広範囲に及ぶ事由によるシステム破壊からの復旧以外に、例えばランサムウェアによるシステム破壊、データ損失から業務システムを可能な限り保護する手段を用意する。そのため、バックアップシステムではランサムウェアによるバックアップデータの不審な更新差分検出を要件とする。

2.5. 業務認証基盤システム

2.5.1. Active Directory

現行システムでも稼働しており、PMDA で使用している大部分のユーザアカウント、クライアント端末、サーバのアカウントを格納し、動作制御を行っている。多くのサーバに対する Kerberos 認証のコンポーネントとして機能しており、一部のシステムからは LDAP(S)接続も行っている。本調達でもこの仕組みは継続して使用する。現行の Active Directory は Windows Server2016 上で稼働しており、機能レベルは 2016 になっている。

2.5.2. プライベート認証局

Active Directory を構成しているサーバ上で Windows Server の機能を使用したプライベート認証局を構成している。この機能も継続指定使用する。

2.5.3. Azure AD Connect

PMDA では Microsoft Office365 を使用しており、そのために Active Directory 上のアカウントを

Azure AD Connect を介して Azure AD に同期している。本調達でも Azure AD Connect による同期の仕組みを継続使用する。

クライアント端末は Hybrid Azure AD 参加をしており、これらをはじめとした現行の Azure AD Connect の設定も移行対象とする。

2.5.4. SAML 認証基盤

現行システムでは SAML 認証は行っていないが、本調達では試験的に一部の運用管理サーバを対象に SAML 認証を行う。SAML 認証の ID ソースとしては Active Directory または Azure AD 上のユーザアカウントを使用する。試験的な導入ということもあり、今回の運用では限定的なユーザ、限定的なシングルサインオン対象として構築する。必要な IdP サーバを構築し、シングルサインオン対象のサーバを SP として登録する。

2.5.5. 外部専門委員用 Active Directory

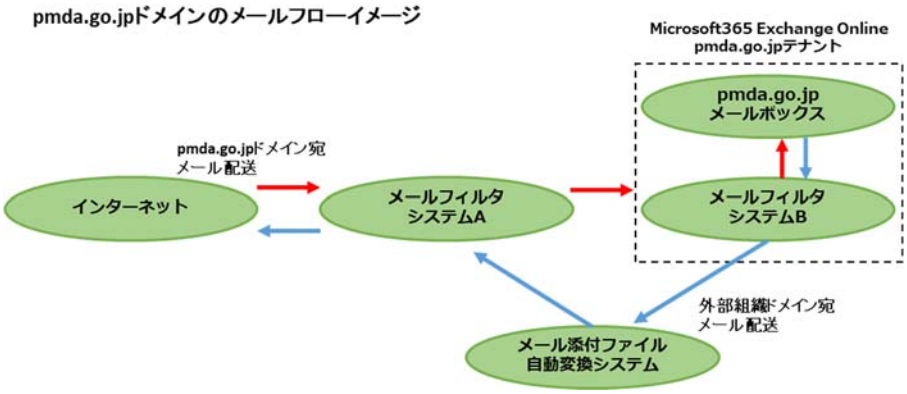
現行システムでも稼働しており、外部専門委員リモート接続システムで使用するアカウントを格納している。「2.5.1Active Directory」の Active Directory とは異なるドメイン環境ではあるが、ドメイン間の信頼関係がある。

2.6. 共通アプリケーション

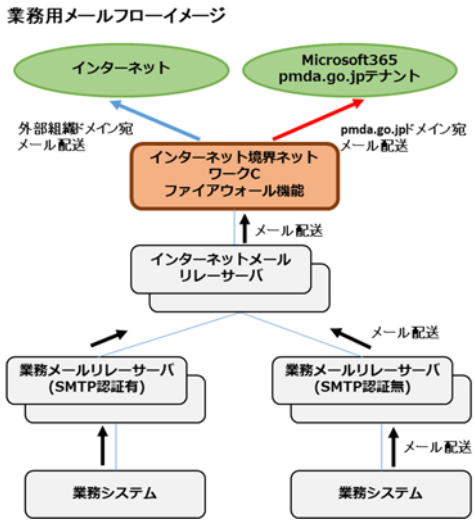
2.6.1. メールシステム

PMDA では、PMDA 職員が外部組織とコミュニケーションをとる手段、業務システムからの通知や通報を受け取るための手段として電子メールを利用している。電子メールに対するスパム、マルウェア対策や添付ファイルの自動変換システム、業務用メールリレーシステムを構成する。

pmda.go.jp ドメインのメールアドレスを持つメールボックスは現行システムとして稼働中の Microsoft365 Exchange Online 上で管理されており、pmda.go.jp ドメイン宛メールアイテムの最終的な配送先となる。



業務用メールリレーシステムではインターネットメールリレーサーバから通常アウトバウンド回線を利用してメールを配送する。



2.6.1.1. メールフィルタシステム A

主に PMDA 職員が外部組織(pmda.go.jp 以外)と電子メールを交換する際に利用するメールサービスとなる。メールドメインは pmda.go.jp ドメインであり、pmda.go.jp ドメインの MX レコードは本システム上で稼働する MTA サーバを指定する。

本システムを通過するメールのスパム、マルウェアを検査し脅威メールフィルタリングを行う。

2.6.1.2. メールフィルタシステム B

主に PMDA 職員が職員同士、または外部組織と電子メールを交換する際に利用する MTA サーバとなる。

本システムを通過する pmda.go.jp ドメイン宛メールのスパム、マルウェアを検査し脅威メールのフィルタリングを行う。脅威検知の確度を上げるため、メールフィルタシステム A とは異なるセキュリティデータベース、エンジンによるメールフィルタリングの二重化を目的とする。

本システムは現行システムとして稼働中の Microsoft 365 Exchange Online による実装とする。

2.6.1.3. メール添付ファイル自動変換システム

PMDA では、電子メールのファイル添付機能を使用したファイルデータ送信を行っている。PMDA 職員が外部組織宛にファイルデータを送信する際にファイル保護が必要となる。

本システムを通過する外部組織宛のメールに対し、添付ファイルデータを自動的に外部ストレージへ保存、URL へ変換し宛先に送信する構成とする。受信者は送信された URL へアクセスし、添付ファイルデータを取得する。

2.6.1.4. 業務用メールリレーシステム

PMDA では、サービス監視における障害検知やウイルス検知時の通報メール、業務システムの

ジョブ処理結果通知メールを PMDA システム担当者(pmda.go.jp)や外部組織へ送信している。通報メール、通知メールを集約しインターネット向けにメールを配送するためのメールリレーシステムを Postfix で構成する。

2.6.1.4.1. インターネットリレーサーバ

下位 MTA の業務メールリレーサーバから配送された電子メールを受け付け、インターネット向けにメールを配送する上位 MTA サーバとなる。宛先は PMDA システム担当者、外部組織、どちらも存在する。また IP アドレス、ネットワーク指定による配送元制限を行う。

インターネットリレーサーバは 2 台構成とし、汎用ロードバランサで負荷分散する。

2.6.1.4.2. 業務メールリレーサーバ(SMTP 認証有)

各業務システムから配送された電子メールを受け付け、上位 MTA のインターネットリレーサーバへ配送する。また SMTP 認証を設定し、配送元を制限する。

業務メールリレーサーバ(SMTP 認証有)は 2 台構成とし、汎用ロードバランサで負荷分散する。

2.6.1.4.3. 業務メールリレーサーバ(SMTP 認証無)

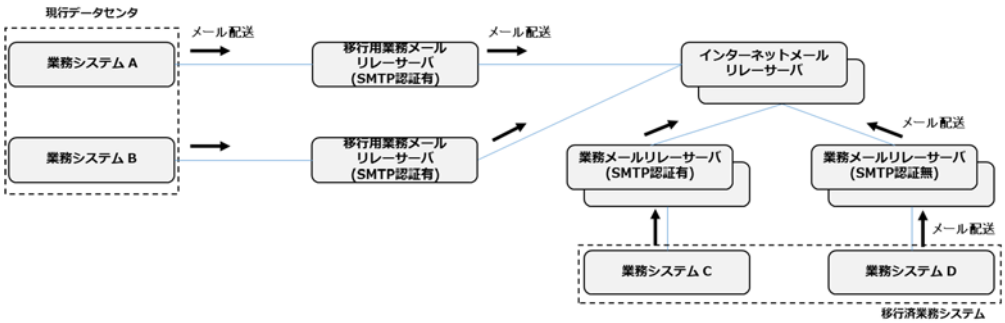
各業務システムから配送された電子メールを受け付け、上位 MTA のインターネットリレーサーバへ配送する。また IP アドレス、ネットワーク指定による配送元制限を行う。

業務メールリレーサーバ(SMTP 認証無)は 2 台構成とし、汎用ロードバランサで負荷分散する。

2.6.1.4.4. 併設用業務メールリレーサーバ

現行データセンタで稼働を続ける業務システム用に併設用業務メールリレーサーバを構成する。本サーバは現行の業務メールリレーサーバから IP アドレスを移行し、本番系仮想基盤システム上に作成する。

現行データセンタで稼働中の業務システムから本サーバへのメール配送には、併設用ネットワーク機器を利用する



2.6.2. DNS システム

2.6.2.1. 内部 DNS システム

内部システム向けに公開される pmda.go.jp ドメインのゾーン情報を管理している。ドメインの参加有無にかかわらず PMDA 内で名前解決が必要なシステムや機器の大部分は本システムを DNS サーバとして指定する。

特定ゾーンについては条件付きフォワーダを明示し問い合わせ先ネームサーバを指定している。管理下にないゾーンへの名前解決はキャッシュ DNS システムへ再帰的な問い合わせを行い、本システムが直接ルートヒントへ問い合わせることはしない。

現行システムでは Windows Server 標準機能で構成されており、Active Directory と同居している。本調達でも同等のシステムを要求する。

2.6.2.2. キャッシュ DNS システム

インターネット上のルートヒントへ再帰的問い合わせを行う。現行システムではデータセンタのオプション機能として提供されており、本調達でも同等のシステムを通常アウトバウンド回線のオプション機能として要求する。

2.6.3. HTTP プロキシシステム

シグネチャの更新やアップデートファイルの取得のため、インターネット上のリソースと通信が必要なサーバ向けの HTTP プロキシサーバ。一般的なクライアント端末はこのプロキシサーバは使用しない。

2.6.4. ファイル共有システム

ファイル共有システムでは用途別のファイルサーバを構築する。ファイルサーバは Windows Server のファイル共有機能及び DFS を使用する。ファイルサーバは部門用ファイルサーバ 1 台、個人用ファイルサーバ 2 台、特定用途ファイルサーバ 1 台、システム資源ファイルサーバ 1 台を構成する。

部門用ファイルサーバ、個人用ファイルサーバ、特定用途ファイルサーバは現行システムで運用している。現行システムで運用中のデータ、アクセス権を引き継いで使用する。システム資源ファイルサーバは本システムで新しく導入するサーバで、システムログや設定情報、調査用資料を格納する。

2.6.5. 印刷管理システム

新霞が関ビル内に設置されている複合機を共有するためのプリントサーバ。クライアント端末は印刷管理システム上で共有された複合機を指定することで、個々に複合機のドライバをインストールすることなく印刷を行える。Windows Server の標準機能で構成する。

2.6.6. グループウェア

Microsoft Sharepoint2016 で構成されており、現行システムで使用している。フロントエンド Web サーバ 2 台、データベースサーバ 1 台で構成されており、フロントエンド Web サーバ 2 台はロードバランサで負荷分散を行う。

2.6.7. 運用管理システム

2.6.7.1. システム状態監視サーバ

Zabbix Zabbix で構成する。本システム及び業務システムを対象としてエージェントソフトウェア及び SNMP による監視を行う。

2.6.7.2. sFlow コレクタサーバ

本システムのネットワーク機器からネットワークフロー情報を取得し、統計情報を表示する。

2.6.7.3. Windows Server アップデート管理サーバ

本システムで導入する Windows Server を使用した仮想マシンの Windows Update を管理する。Microsoft Windows Server Updater Services(WSUS)を使用する。Windows10 等、クライアント OS はこのサーバを使用しない。

2.6.7.4. Linux OS パッケージ管理サーバ

本システムで導入する Linux OS を使用した仮想マシンのパッケージ管理を行う。Red Hat Satellite を使用する。

2.6.7.5. サーバ構成管理サーバ

本システムで導入する主に Linux OS を使用した仮想マシンの構成管理を行う。Red Hat Ansible Tower を使用する。

2.6.7.6. クライアント端末ログ管理サーバ

既存のクライアント端末及びリモート接続仮想基盤システム上の VDI のクライアント操作ログの取得、USB デバイスの制限を行う。現行システムで同等の機能を SKY Skysea Client View Light Edition で実現しており、本システムでも現行のシステムを継続利用する。

2.6.7.7. クライアント端末状態管理サーバ

既存のクライアント端末の状態把握、ソフトウェア配信、セキュリティ機能の集約管理を行う。現行システムで同等の機能を Microsoft Microsoft Endpoint Configuration Manager(MECM)で実現しており、本システムでも現行のシステムを継続利用する。

2.6.7.8. サーバマルウェア対策サーバ

本システムで構築する仮想マシン、物理サーバ、本システムを利用する業務システムを対象としてマルウェア検査及び駆除を行う。

2.6.7.9. VDI マルウェア対策サーバ

リモート接続仮想基盤システム上に構成する VDI を対象としてマルウェア検査及び駆除を行う。

2.6.7.10. 汎用 Syslog サーバ

本システムで構築する各要素のログ設計において Syslog 送信するものを対象としたログサーバ。rsyslog で構成する。

2.6.7.11. ファイルサーバログ管理サーバ

本システムで構築するファイル共有システムを対象として、アクセスログを収集する。

2.6.7.12. ファイアウォール管理サーバ

本システムで構築するファイアウォールの管理を集約的に行う。ログの収集、ファイアウォールポリシ、オブジェクトの集中管理を行う。

2.6.8. リモート接続仮想基盤システム

PMDA では、基本的に業務用 PC を自宅へ持ち帰りリモートワークを実施しているが、特段の理由等により業務用 PC の持ち帰りが困難となっている職員が存在する。それらの職員、もしくは持ち帰らなかった職員がリモートワークを実施できるよう私物 PC 等から接続可能な環境を構成している。本調達においても、同様のリモート接続仮想基盤システムを構成する。

2.6.8.1. 基本構成

ハイパーバイザ型の仮想基盤管理ソフトウェア、物理ホスト、Fiber Channel(FC)接続する共有ストレージにより構成する。本仮想基盤には VDI 以外の仮想マシンを稼働させない。

2.6.8.2. 仮想基盤物理ホスト

仮想基盤物理ホストには汎用的なサーバを使用する。物理ホストの CPU、メモリリソース量は本基盤で稼働させる VDI の要求リソース、最大稼働数、最大同時接続数から検討する。

VDI 情報は以下の通り。また冗長性能としては N+1 を想定している。

VDI 種類	vCPU	仮想メモリ	仮想ディスク	稼働数	同時接続数
VDI A	2 コア	16GB	150GB	50 台	50
VDI B	2 コア	6GB	100GB	150 台	100

2.6.8.3. 仮想基盤システムを管理するための Web インターフェース

仮想基盤システムの仮想マシン、ディスク領域、ネットワーク接続等のオブジェクトを管理するための Web インターフェースサーバ(仮想基盤管理サーバ)を導入する。

仮想基盤管理サーバの機能利用にはユーザ認証を必須とし、業務認証基盤システムと連携して認証及び参照、操作内容の権限管理を行う。仮想基盤管理サーバは冗長化し、可用性を向上させ

る。これらの仮想基盤管理サーバは本番系仮想基盤システムで構成されるものを使用してもよい。その場合、管理単位を分割し本仮想基盤の仮想マシンが本番兼仮想基盤ホストのリソースを参照しないよう構成すること。

2.6.8.4. ストレージの接続

通常ストレージと接続する。通常ストレージへは本番系仮想基盤システムと同じ FC スイッチを経由して Fiber Channel で接続する。

2.6.8.5. ネットワーク構成

仮想基盤物理ホストは IP ネットワークシステムで構成するサーバ接続 L2 スイッチ F、管理 L2 スイッチと接続する。ホスト 1 台あたりの想定本数、各ネットワーク接続の情報は以下の通り。

接続スイッチ	用途	メディア	本数
サーバ接続 L2 スイッチ F	仮想マシンのサービストラフィック	10GBase-SR	2
	仮想基盤システムの運用トラフィック	10GBase-SR	2
管理 L2 スイッチ	IPMI インターフェース	100/1000Base-T	1

サーバ接続 L2 スイッチ F に接続する NIC は用途毎にメディアを分ける。仮想マシンのサービストラフィックと、仮想マシンの物理ホスト移動等、仮想基盤特有の操作に伴い発生する運用トラフィックにそれぞれ割り当てる。

複数接続するインターフェースではリンクアグリゲーションに相当する機能を使用し、両接続を Active として使用できるように構成する。

2.6.8.6. 仮想マシンの OS 構成

仮想マシンの OS として Windows10 Enterprise バージョン 21H2 を構成する。仮想マシンの OS ライセンス、またこれらの OS に対してリモート接続を行う上で必要なライセンスを用意する。OS ライセンスはライセンス認証サーバ(KMS)にて認証可能な製品とすること。また本調達で用意したライセンスは既存の Volume Licensing Service Center にて管理、製品ダウンロードが可能となるよう、アカウントを統合する。

仮想マシンは VDI 種類毎に参加するドメインが異なる。VDI A は pmda.go.jp ドメインへ参加し、VDI B はインターネット系システム用のドメインへ参加する。インターネット系システム用ドメインを管理する Active Directory サーバは PMDA が構成する。

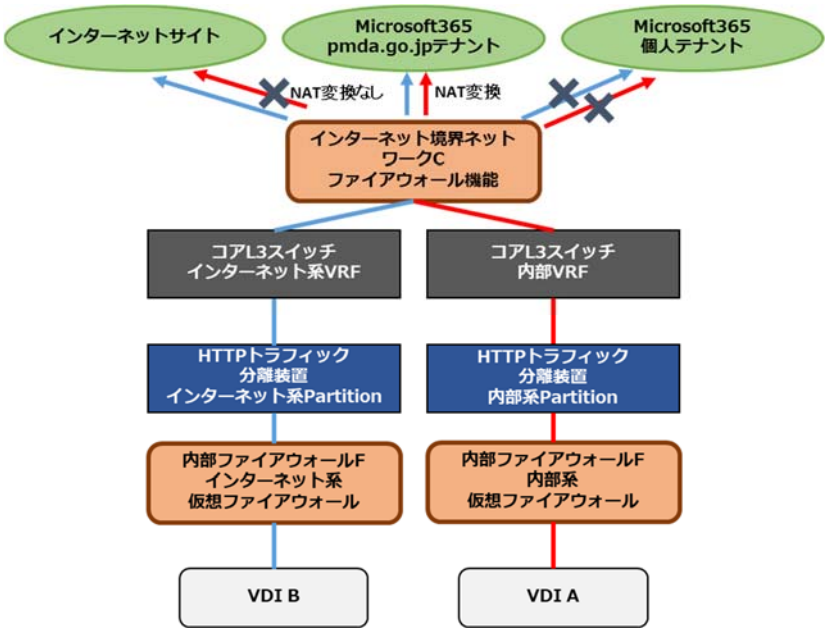
2.6.8.7. 仮想マシンのネットワーク構成

リモート接続仮想基盤システム上で稼働する仮想マシンは、VDI 種類毎に内部システムネットワーク、インターネット系ネットワークをそれぞれ利用する。いずれも内部ファイアウォール F をデフォルトゲートウェイとし、DHCP にて IP アドレスを動的に取得する。

VDI 種類	利用ネットワーク
VDI A	内部システムネットワーク
VDI B	インターネット系ネットワーク

各 VDI は Microsoft365 を利用する。個人用の Microsoft365 テナントへの接続を禁止するため VDI から Microsoft365 に対し発生する HTTPS 通信にアクセス許可テナント情報を付加する機能を構成する必要がある。また内部システムネットワークに所属しつつ Microsoft365 へのアクセスは許可するため、透過的なプロキシを構成する。透過プロキシに要求される機能は Microsoft365 各サービスの宛先 FQDN に動的に追従し、該当の FQDN 宛通信であればソース IP アドレスを NAT 変換し配送する動作となる。

これらの機能を有した HTTP トラフィック分離装置をリモート接続仮想基盤システムとコア L3 スイッチの間に配置する構成とする。



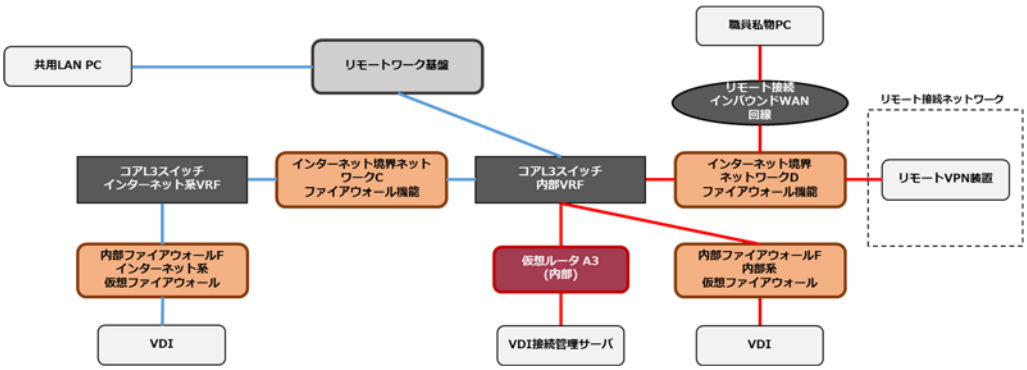
ネットワーク構成の要件の詳細は「2.3IP ネットワークシステム」に記載しているのでそちらを参照すること。

2.6.8.8. リモート VPN 装置

リモート接続仮想基盤システム上で稼働する内部システムネットワークの VDI に対してインターネットから接続する際、リモート VPN 装置を経由する。現行システムでは Absolute Software(旧 NetMotion Software) NetMotion を採用しているが、私物 PC から接続して利用する機会が多いことから、ユーザ利便性を考慮して本調達においても同様の製品にて構成する。

インターネット系ネットワークの VDI は既存の共用 LAN PC からのみ利用する。接続する際は、

リモート VPN 装置を経由せず現行環境のリモートワーク基盤より接続する。



2.6.8.9. VDI 接続管理サーバ

接続先 VDI を管理し、セッションの割り当てを行う VDI 接続管理サーバを構成する。私物 PC から NetMotion に対して VPN 接続した後、内部システムネットワークに所属している VDI 接続管理サーバに着信、VDI へセッションが振り分けられる。

セッション振り分け以降は私物 PC と VDI 間で直接通信する構成とする。

2.6.9. 外部専門員用リモート接続システム

PMDA では、外部機関所属の専門員が私物 PC 等からインターネット経由で、本システム上のサーバにリモートデスクトップ接続し業務を行っている。本調達においても、同様の外部専門員用リモート接続システムを構成する。

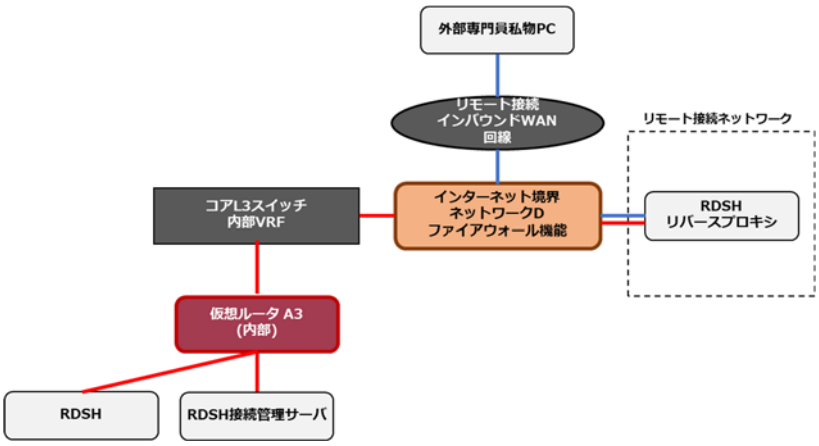
本システムのサーバには複数ユーザから接続するため、Remote Desktop Session Host(以下 RDSH)として構成する。

2.6.9.1. RDSH リバースプロキシ

外部専門員用リモート接続システムでは RDSH に対してインターネットから接続する際、リバースプロキシを経由する。現行システムでは VMware Unified Access Gateway(以下 UAG)、を採用しているが、基本的に私物 PC から接続して利用する機会が多いことから、ユーザ利便性を考慮して本調達においても同様の製品にて構成する。

私物 PC から UAG に対して接続した後、UAG を経由し内部システムネットワークに所属している RDSH 接続管理サーバに着信、RDSH へセッションが振り分けられる。

セッション振り分け以降も私物 PC と RDSH 間の通信は UAG を経由する。



2.6.9.2. RDSH 接続管理サーバ

接続先 RDSH を管理し、セッションの割り当てを行う RDSH 接続管理サーバを構成する。私物 PC から RDSH サーバまでの接続は必ず UAG を介して転送される構成とする。

2.6.9.3. RDSH サーバ

複数ユーザがリモートデスクトップ接続可能な RDSH サーバを構成する。本サーバに対し外部専門員がリモートデスクトップ接続を行い、本サーバ上に格納された資料を閲覧する。

2.6.10. データセンタ

2.6.11. メンテナンスシステム

本調達で構成する各要素のメンテナンス作業を行うためのシステム。メンテナンス作業用に以下のノードを作成する。

ノード内容	用途
メンテナンス作業用仮想マシン	RDP や SSH などの作業を行うためのメンテナンス用仮想マシン。業務システムごとに作成し、複数人が同時に使用できるような構成とする。
調査用物理サーバ	リモートパケット収集装置、コンソールインターフェース管理装置を収容する作業用サーバ。調査やメンテナンス作業用のアプリケーションのインストールを行い、作業を円滑に進められるように構成する。
リモートパケット収集装置	ネットワーク機器のミラーリングパケットを受信し、内容を調査できるようにする。リモートパケット収集装置ではパケットの保存を要件としない。

コンソールインターフェース管理装置	ハードウェアの管理コンソールインターフェースを集約し、ネットワーク疎通ができない場合に調査を行える環境を作る。

2.7. 本調達の範囲で移行するその他の既存業務システム

現行仮想基盤システムで稼働している業務システム仮想マシンの移行を行う。受注者は本調達で構築する仮想基盤システムに V2V で移行すること。業務システムの動作確認は PMDA が行う。

2.7.1. 業務システム 1

業務システム 1 は OS を Windows Server とした仮想マシン 1 台で構成されており、インターネットに公開している。本システムでは通常インバウンド WAN を使用してインターネットに公開する。この移行に伴う公開 DNS サーバのレコード変更は PMDA が行う。尚、業務システム 1 にはプライベート IP アドレスが設定されており、途中のネットワーク機器で宛先 IP アドレスの NAT を行っている。本システムのネットワーク設計によって業務システム 1 の IP アドレスの変更は許容される。変更作業は PMDA が行う。

業務システム 1 に対するセキュリティ機能として IPS 及び TLS 復号化を行っている。インターネット境界ネットワーク B で IPS 及び TLS 復号化及び再暗号化を行い、さらに WAF の対象とすること。サーバ証明書と秘密鍵は提供する。

このシステムには内部ネットワークからのアクセスも発生する。コア L3 スイッチ、インターネット境界ネットワーク B を経由して業務システム 1 にアクセスできるように構成すること。尚、この時に使用する L4 ポートは外部ネットワークからのアクセス時とは異なるものを使用する。

2.7.2. 業務システム 2

業務システム 2 は OS を Windows Server とした仮想マシン 1 台で構成されており、内部ネットワークからのみ使用する。本システムのネットワーク設計によって業務システム 1 の IP アドレス変更は許容される。変更作業は PMDA が行う。

2.7.3. 業務システム 3

業務システム 3 は OS を Windows Server とした仮想マシン 1 台で構成されており、内部ネットワークからのみ使用する。本システムのネットワーク設計によって業務システム 1 の IP アドレス変更は許容される。変更作業は PMDA が行う。このシステムは HTTP プロキシ経由で通常アウトバウンド WAN を使用してインターネットにアクセスする。

2.7.4. 業務システム 4

業務システム 4 は OS を Windows Server とした仮想マシン 4 台で構成されており、内部ネットワークからのみ使用する。現行のネットワークアドレスを変更せずに移行する必要がある。

2.7.5. 業務システム 5

業務システム 5 は OS を Windows Server とした仮想マシン 6 台で構成されており、内部ネットワークからのみ使用する。現行のネットワークアドレスを変更せずに移行する必要がある。

2.8. 移行用ストレージ

現行のシステムで運用している仮想基盤システム(VMware ESXi をハイパーバイザとしている)の共有ストレージは 2024 年 12 月 31 日に運用を終了する。この共有ストレージでは一部の業務システムのデータが格納されており、その業務システムは前述の日程以降も一定期間、現行データセンタで稼働を続けこのデータを使用する。これに対応するため、本調達では移行用のストレージを構成する。予期困難な不具合の発生確率を低減させるため、移行用ストレージは現行ストレージと同一メーカの同等あるいは類似モデルを使用する。

現行の共有ストレージは業務システムが管理する仮想基盤システムの物理ホストと FC スイッチ経由で接続されている。移行用ストレージをこの既存 FC スイッチに接続し、仮想基盤システムから移行用ストレージの LUN を使用できるように構成する。既存 FC スイッチは現行の装置を継続利用できるため、FC スイッチ購入は本調達の範囲外とする。

移行用ストレージを搭載するためには現行システムのハードウェアの一部をラックから取り外す必要がある。取り外したハードウェアは現行データセンタの別ラックに搭載する。これらのハードウェアは本調達のシステム構築、既存システムの移行作業の進行にあわせて停止できる。受注者はこれらを考慮した移行スケジュールの作成を行う。

移行用ストレージの LUN を使用するための仮想基盤システムの設定、既存データストアからの仮想ディスク移行は PMDA が実施する。想定している作業と作業分担は以下の通り。

作業	担当
移行用ストレージの基本設定、LUN 作成 (LUN 構成は基本的に現行を踏襲する。)	受注者
既存 FC スイッチとの接続、配線	受注者
既存 FC スイッチの設定	受注者
仮想基盤システム上のデータストア作成	PMDA
ストレージ利用最適化のための ESXi 用の VIB ソフトウェア提供	受注者
VIB ソフトウェアのインストール	PMDA
ストレージ vMotion によるデータ移行	PMDA

現行システムのハードウェアは以下の通り。

製品区分	製品名
FC スイッチ	SN3000B

共有ストレージ	HPE Nimble Storage CS3000

3. 要件範囲外の関連要素

3.1. 公開 DNS サーバ

PMDA ではインターネットにリソースを公開するためのドメインとして「pmda.go.jp」ドメインを運用している。このドメインに対する名前解決に応答するための権威 DNS サーバは本調達外で用意をしている。権威 DNS サーバにレコード登録が必要な場合は PMDA が作業を行うので、受注者は必要なレコード内容、意図を PMDA に対して事前に提供すること。

4. 構築要件

本調達におけるシステム構築の要件を記す。これまでの記載事項を満たすような構成品の選定、設計、設定を行うこと。

4.1. 共通の構成要件

4.1.1. 基本的な機能の設計

4.1.1.1. ホスト名

1. 本システムではホスト名の命名規則はあらかじめ定めたものを使用する。この命名規則は IP アドレスを持つノードに対して少なくとも 1 個指定する。命名は PMDA が行うので、受注者はホスト名を指定する必要のあるノードを設計時に提示すること。

4.1.1.2. 時刻同期

1. 基本的に業務認証基盤システムで構築する Active Directory の 3 台を時刻同期サーバとして使用する。この Active Directory は外部の NTP サーバと時刻同期する。受注者は現行の設定を確認し、時刻同期設定を行い、外部の NTP サーバとの時刻同期通信設定を行うこと。Active Directory との IP 到達性がないノードがある場合、そのノードの時刻同期は個別に検討する。特定のネットワークアドレスのノード全てがこれに該当する場合、時刻同期を中継するための NTP サーバの構築も検討し、必要に応じて構築すること。

4.1.1.3. NIC の構成

1. 本システムで構築するサーバはアプリケーションの制約がない限り、原則としてサービス系ネットワークに接続する NIC と運用管理系ネットワークに接続する NIC を持つ。デフォルトルートはサービス系ネットワーク側に指定することを基本とし、運用管理系ネットワークには必要なスタティックルートを指定すること。
2. 特段の理由がなければ IPv6 を無効化すること。

4.1.1.4. インターネット上のリソースの名前解決

1. 通常アウトバウンド WAN の機能に求めるキャッシュ DNS 機能を使用してインターネット上のリソースの名前解決を行えるように構成すること。

4.1.2. システム監視設計

4.1.2.1. システム正常性の定義

1. 本システムで導入する各サブシステムの正常稼働状態を定義し、正常稼働中であることを確認するための監視項目、確認項目のリストを作成すること。
2. システム正常性の監視は PMDA が行うが、PMDA が監視設定を行うにあたり、監視すべき項目の詳細情報を求めることがある。受注者はこれに対応し、製品や設計に関する情報を提供する

こと。

4.1.2.2. ハードウェア監視設計

1. 仮想基盤システムの物理ホストの各ハードウェアに障害が発生した際、メールや SNMP による通報が可能になるように構成すること。
2. ネットワーク機器やアプライアンスのハードウェア障害が発生した際、可能な限りメール、SNMP による通報が可能になるように構成すること。
3. PowerShell や Python 等の汎用的なスクリプトからの HTTP 接続を想定した API を有しておりメーカが API のリファレンス等の情報を提供している場合、それらを提供すること。

4.1.3. Windows Server の OS 設計

1. 本システムで導入する Windows Server の OS 設計を行うこと。本書に記載していない設定に関しては PMDA にヒアリングを行い協議の上決定すること。

4.1.3.1. ディスク構成

1. 特段の理由がなければシステム領域とデータ領域を異なるドライブレターで構成すること。
2. システム領域のディスクサイズを Windows Update や一時的なログの格納を考慮して設計すること。これらは Windows Server2019、Windows Server2022 で個別に検討すること。

4.1.3.2. Active Directory ドメイン

1. 特記事項がなければ、本システムで構築する Windows Server は原則として業務認証基盤システムの Active Directory ドメインに参加させる。ドメイン参加は、ホスト名決定後に PMDA がコンピュータアカウント作成を行った上で、ドメイン参加作業用のアカウントを受注者に払い出すので、そのアカウントを使用してドメイン参加作業を行うこと。尚、コンピュータアカウントの所属 OU 設計は PMDA が行う。

4.1.3.3. WSUS の指定

1. 特記事項がなければ、本システムで構築する Windows Server の Windows Update は本システムで PMDA が構築する WSUS を使用して行う。受注者は構築した Windows Server に対して WSUS の指定を行うこと。WSUS に対象サーバが登録されたことは PMDA が確認するが、登録されない場合、Windows Server 側の設定に問題がないかを受注者が確認すること。また、インターネット上の Windows Update リソースにアクセスしないように構成すること。

4.1.3.4. 信頼するルート証明機関

1. GPO 等により手動で追加する CA 証明書を除き、信頼する CA 証明書を更新する仕組みを構成すること。ただし、原則としてインターネット上のリソースに直接アクセスすることは運用ポ

リシ上不可であるため、設計時に更新方法を PMDA と協議し決定すること。

4.1.3.5. Windows ファイアウォール

1. 原則として Windows ファイアウォールは無効化すること。

4.1.3.6. PowerShell ロギング設定

1. PowerShell のロギング設定を行い、PowerShell の実行内容がロギングされるように構成すること。

4.1.4. Red Hat Enterprise Linux の OS 設計

1. 本システムで導入する RHEL の OS 設計を行うこと。基本的な設定に関しては PMDA にヒアリングを行い協議の上決定すること。

4.1.4.1. ディスク構成

1. 特段の理由がなければシステム領域とデータ領域を異なるディスクで構成すること。特にデータ領域は LVM を構成すること。
2. 受注者が構築する各サーバのディスク構成について事前に PMDA の承認を受けること。

4.1.4.2. RHEL サブスクリプションの登録

1. 本システムで構築した RHEL サーバのサブスクリプション登録を行うこと。Red Hat Portal と通信ができないサーバ向けのサブスクリプション登録方法を検討すること。
2. virt-who サービスを稼働させる RHEL サーバを検討し PMDA と合意した上で virt-who サービスを構築すること。本システムで構築する Linux OS パッケージ管理サーバに virt-who サービスを構築する形としても良いが、その場合は PMDA が設定を行うので、必要な作業内容を PMDA に連携すること。

4.1.4.3. 信頼する CA 証明書

1. ca-certificate の更新を検討し、定期的に信頼する CA 証明書を最新化する方法を設計すること。

4.1.4.4. SELinux

1. 特段の理由がなければ SELinux は無効とすること。

4.1.4.5. Active Directory との連携

1. SSSD を導入し、RHEL サーバを Active Directory ドメインに参加させること。ドメイン参加した RHEL サーバにログインする際、Active Directory ドメインユーザを利用可能とすること。認証方式として Kerberos または LDAPS が利用可能とすること。

4.1.4.6. SSH 接続

1. ユーザ ID と公開鍵認証による接続が可能となるように構成すること。
2. Active Directory のアカウントを使用して SSH 接続できるように構成すること。
3. Active Directory で特定のセキュリティグループに所属しているアカウントのみ SSH 接続できるように構成すること。全ての要件の成立に問題がある場合、構成を PMDA と合意した上で構築を行うこと。

4.1.4.7. firewalld

1. 特段の理由がなければ firewalld は停止させること。

4.1.4.8. ソフトウェアインストール

1. メンテナンスを目的として以下のソフトウェアをインストールすること。依存関係上必要になるソフトウェアがある場合はそのインストールも行うこと。
   - curl
   - wget
   - tcpdump
   - lsof
   - nfs-utils
   - cifs-utils
   - samba-common
   - samba-client
   - python3.x (構築時最新)
   - vim

設計時にインストールソフトウェアは追加されることがある。これらにも対応すること。インストールにあたり、ソースコードからのインストールを必要とするようなソフトウェアは本作業には想定していない。

4.1.4.9. sudo

1. sudo 実効を許可するユーザを限定すること。

4.1.5. 物理サーバ

1. 仮想基盤システムの物理ホスト及び物理サーバでは、搭載しているハードウェアを正常に利用するためのドライバ等の基本的なソフトウェア及び一時的にシステムを起動するための OS を記録した起動メディアを納入すること。

4.1.6. ハードウェアの管理インターフェースの接続

1. IP 通信により装置を管理するインターフェースは管理ポート L2 スイッチに接続すること。
2. イーサネットスイッチ等で IP 通信可能な管理インターフェースがない場合、可能な限り通信ポートを 1 ポート管理インターフェースに転用すること。L3 スイッチのように動作に影響を与える可能性がある場合は必ずしもこの接続は必須としない。

4.1.7. 管理アカウント設計

1. 業務システム管理者が利用するシステムを始めとして、受注者が構築を行う導入製品の各管理機能に対するログインに使用できるアカウントの設計を行うこと。アカウントの ID ソースには可能な限り業務認証基盤システムを使用すること。
2. 受注者が構築を行う導入製品の各管理機能の権限設定を検証し、PMDA が行うシステム運用設計に対する情報提供を行うこと。

4.1.1. 管理機能へのアクセス制限

1. 本調達で導入する各製品の管理アクセスが可能な接続元 IP アドレスを制限できるようにネットワーク設計を行うこと。必要に応じて製品自体の機能を使用して管理アクセスを制限すること。

4.1.2. 配線

1. 本調達の作業で想定される主要な配線については各構成要素で個別に記載しているが、特段の記載がない場合でも必要な配線作業を行うこと。
2. 配線を行う際、システム拡張時の配線の取り扱いを簡易化するため、ラックをまたぐ場合は原則としてマルチモードの光ケーブルで接続すること。同一ラック内の配線には UTP を使用して良い。ただし、リモートパケット収集システム、コンソールインターフェース管理装置に対してはラックをまたぐ場合であっても必要に応じて UTP を使用して良い。
3. 配線作業を行う際にはラック内の配線経路を設計し、ハードウェアとの物理的な干渉を極力小さくすること。必要に応じて配線を束ねるパネルをラックに設置し、整理された形で配線を行うこと。
4. 現行データセンタ、新霞が関ビル、関西支部においても必要な配線を行うこと。
5. 機器に接続するケーブルには両端に示名条片を貼り付け、接続元機器名、接続元インターフェース名、接続先機器名、接続先インターフェース名が分かるようにすること。
6. ケーブルを識別するための命名規則を検討し、ケーブルの両端に示名条片を貼り付けケーブルを識別できるようにすること。

4.2. システムファシリティ

4.2.1. データセンタ

1. 本調達で導入する各ハードウェアを収容するためのデータセンタ利用を構成に含めること。

4.2.2. ラック

4.2.2.1. データセンタラック共通要件

1. 本調達で導入する各ハードウェアを収容するためのラックを構成に含めること。必ずしも隣接ラックである必要はない。
2. ラック 1 台は 42RU 以上の高さを有すること。
3. 各ラックの電源は系統を分離し、1 系統の電源障害により電源冗長が可能な搭載機器の動作停止が発生しないようにすること。

4.2.2.1.1. WAN 収容ラック

1. インターネット回線、閉域 WAN を収容する回線終端装置及び付随機器、インターネット L2 スイッチ、インターネット境界ネットワーク A、B、C、D、閉域 WAN L2 スイッチを収容すること。
2. 回線終端装置等を配置するためのラック搭載可能な棚板を本調達で導入する機器に必要なものに加えて 2 枚構成に含めること。棚板をラックに固定するための部材も含めること。
3. インターネット回線や WAN 回線の追加に備え、連続した 6RU の空きスペースを 1 か所確保可能な構成とすること。

4.2.2.1.2. ネットワークラック

1. 特に設置場所の指定のない各 L3 スイッチ、L2 スイッチ、ファイアウォールを収容すること。
2. 機器の増設に備え、連続した 8RU の空きスペースを 1 か所確保可能な構成とすること。

4.2.2.1.3. 業務仮想基盤ラック

1. 本番系仮想基盤システム、検証系仮想基盤システムの物理ホストを収容すること。
2. 機器の増設に備え、連続した 6RU の空きスペースを 1 か所確保可能な構成とすること。

4.2.2.1.4. ストレージラック

1. 高可用性ストレージ 1、高可用性ストレージ 2、通常ストレージ、検証ストレージ、バックアップシステムのハードウェアを収容すること。

4.2.2.1.5. 物理サーバラック

1. 物理サーバラックとして 42U 以上のラックを 1 架構成に含めること。
2. 物理サーバラックは最大電力 5000VA 以上(200V)、耐荷重 800kg を収容可能とすること。

4.2.2.1.6. リモート接続基盤ラック

1. インターネット境界ネットワーク D、内部ファイアウォール F、HTTP トラフィック分離装置、

サーバ接続 L2 スイッチ F、リモート接続基盤システムの物理ホストを収容すること。

4.2.2.1.7. 特定システム用ラック

1. 特定システム用ラックとして 42 以上のラックを 3 架構成に含めること。ラックのスペックは業務仮想基盤ラックと同等とすること。

4.2.2.2. 新霞が関ビルのラック

1. 新霞が関ビルの設置場所 2 に配置する機器を収容するラックを構成に含めること。最大で 2 架までのラックを設置できる。
2. ラックは 20～24RU の高さとすること。
3. ラックの転倒防止対策にスタビライザを取り付けること。

4.3. 業務仮想基盤システム

4.3.1. 仮想基盤システムの基本構成

4.3.1.1. 構成要件

1. 仮想基盤システムをハイパーバイザ型で構成すること。ハイパーバイザとして使用する製品バージョンは PMDA と協議の上、可能な限り最新版とすること。
2. 仮想基盤システムを管理するための Web インターフェースサーバ(仮想基盤管理サーバ)を構築すること。仮想基盤管理サーバは冗長構成とすること。
3. 同一の仮想基盤管理サーバから本番系業務仮想基盤システム、新霞が関ビル仮想基盤システムを管理可能なように構成すること。検証系仮想基盤システム用の仮想基盤管理サーバを別途構築すること。
4. 異なる種別の仮想基盤システムの物理ホストを共有リソースとして使用できないように構成すること。
5. 仮想マシンの稼働状態、リソース使用状況のレポーティングが可能な Web インターフェースサーバ(仮想基盤監視サーバ)を構築すること。
6. 本番系業務仮想基盤システム、検証系業務仮想基盤システムに対して発生した IP トラフィックのトラフィックログを後から確認可能なログサーバを構築すること。
7. 仮想基盤システム上のトラフィック、ファイアウォール機能の統計情報を可視化可能な Web インターフェースサーバ(仮想基盤トラフィック監視サーバ)を構築すること。
8. 各監視系サーバへのログインには業務認証基盤システムの Active Directory 上のアカウントを使用可能なように構成すること。また、ログインした際に業務システム管理者は自身の管理する仮想マシン以外の状態は見られないように構成すること。

4.3.2. 本番系仮想基盤システム

4.3.2.1. 構成要件

4.3.2.1.1. 基本構成

1. 仮想マシンを稼働させる物理ホストは Windows Server 用の物理ホスト 11 台、RHEL 用の物理ホスト 4 台で構成すること。ただし、本番系仮想基盤システムにバックアップシステムのバックアップ処理を行うサーバを構成する場合は Windows Server 用の物理ホストを最低でも 1 台追加し、必要なリソースをまかなうこと。他のホスト同様の各ライセンスを構成に含めること。
2. ハイパーバイザには仮想 L3 ネットワークを構成可能な製品を使用すること。
3. 物理ホストでは Hyper Threading を有効にすること。
4. 物理ホストに 2 個の HBA を搭載して FC スイッチとマルチパス接続し、高可用性ストレージ、通常ストレージを利用可能な構成とすること。
5. 物理ホストのネットワークインターフェースはサービス系、仮想基盤管理系、運用管理系で物理ポートを占有させること。それぞれのネットワークインターフェースは 10GBase-SR とすること。チーミングを行い、サーバ接続 L2 スイッチ A、サーバ接続 L2 スイッチ B、サーバ接続 L2 スイッチ C に冗長接続すること。
6. 物理ホストを管理するための IPMI インターフェースを管理ポート L2 スイッチに接続すること。
7. 物理ホストが障害等により停止した際、その物理ホストで稼働していた仮想マシンが自動的に別の物理ホストで動作を復旧するように構成すること。
8. データセンタの 19 インチラックに搭載すること。
9. 電源を二重化し、電源冗長を行うこと。

4.3.2.1.2. 仮想マシンの CPU、メモリ

1. 各業務システム向けの CPU、メモリリソースを予約した領域を構成すること。各リソースは設計時に PMDA から要望を提示したものをベースに、システム構成上の実効性、妥当性を検討し、最終的な構成を PMDA と合意すること。
2. 仮想マシンの物理ホスト配置を手動で変更可能なように構成すること。

4.3.2.1.3. 仮想マシンの OS、基本構成

1. Windows Server2019、Windows Server2022、RHEL は本番系業務仮想基盤システム内で作成可能に数量制限のないライセンスで構成すること。
2. Windows Server2019、Windows Server2022、RHEL8 及び RHEL9 の仮想マシンテンプレートを作成すること。仮想マシンテンプレートは OS の設計内容を反映させた状態で作成すること。

4.3.2.1.4. ストレージアクセス構成

1. 高可用性ストレージ、通常ストレージで作成したボリュームに対応するストレージ領域を構成

すること。

4.3.2.1.5. ネットワーク構成

1. 物理ネットワークの L3 ネットワーク境界となる仮想ルータを構成すること。サービス系のネットワークインターフェースを使用して内部システム向け、公開システム向けの仮想ルータ両方が通信可能となるように構成すること。IP ネットワークシステムに記載する構成と整合性をとれるように仮想ネットワークを構成すること。
2. 物理ホスト間で共有可能な仮想イーサネットスイッチを構成し、仮想イーサネットスイッチの操作を一度行うことで全物理ホストに設定が反映されるようにすること。
3. 仮想イーサネットスイッチの構成、所属させるネットワークは PMDA と協議の上で決定すること。
4. テンプレートを使用した仮想マシン展開時に、必要に応じて仮想基盤システムの OS の基本パラメータのカスタマイズが可能となるように構成すること。
5. 仮想イーサネットスイッチから本調達で構築するフローコレクタにネットワークフロー情報を送信するように構成すること。
6. 仮想マシン間で L3 通信するための仮想ルータを構成すること。
7. PMDA が指定した仮想マシンは仮想ルータを経由せず、仮想イーサネットスイッチから直接物理ネットワークに通信可能なように構成すること。

4.3.2.2. 管理機能

1. 仮想基盤システム上のオブジェクトの操作権限を設定したロールを構成すること。ロールは全体管理者、業務システム管理者向けに作成すること。業務システム管理者向けのロールは 8 種類程度を想定しているが、各ロールに付与する権限内容自体はほぼ同等とする。
2. 仮想マシン、ストレージ領域、ネットワーク設定に対する操作権限を付与するためのグルーピング設定を行うこと。
3. グルーピングに対してロールの割り当て及びロールに割り当てられた権限を持つユーザ割り当てを行うこと。
4. 冗長構成の仮想マシンのように同一の物理ホストで動作することが好ましくない仮想マシンが異なる物理ホストで稼働することを強制するためのルール設計を行うこと。

4.3.2.3. 移行要件

1. 現行システムから V2V 対象の仮想マシンの移行を行うこと。移行対象の仮想マシンと動作確認要件は本システムの構成にそれぞれ記載がある。

4.3.2.4. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。

2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 物理ホストのオンサイト対応時、ハイパーバイザのインストール、仮想基盤システムへの機能的な合流までを行うこと。仮想マシンの再配置が必要な場合、その操作は PMDA が行う。

4.3.3. 新霞が関ビル仮想基盤システム

4.3.3.1. 構成要件

4.3.3.1.1. 基本構成

1. 仮想マシンを稼働させる物理ホストは 3 台で構成すること。
2. 物理ホストでは Hyper Threading を有効にすること。
3. 物理ホストをサーバ接続 L2 スイッチ C 経由で新霞が関ビル共有ストレージと iSCSI 接続すること。iSCSI 接続の帯域は 20Gbps 以上確保すること。
4. 物理ホストのネットワークインターフェースはサービス系、仮想基盤管理系で物理ポートを占有させること。それぞれのネットワークインターフェースは 10GBase-SR とすること。チーミングを行い、スタック構成のサーバ接続 L2 スイッチ C に冗長接続すること。
5. 物理ホストを管理するための IPMI インターフェースを既設 L2 スイッチ B に接続すること。
6. 物理ホストが障害等により停止した際、その物理ホストで稼働していた仮想マシンが自動的に別の物理ホストで動作を復旧するように構成すること。
7. 本調達で導入する 19 インチラックに搭載すること。
8. 電源を二重化し、電源冗長を行うこと。
9. UPS を用意し、UPS の入力電源に異常が発生した際に可能な限り新霞が関ビル仮想基盤システム上の仮想マシン、物理ホストが自動的に正常なシャットダウン処理を通して停止するように構成すること。処理を行うためのサーバ等が必要な場合、本番系仮想基盤システムを使用しても良い。

4.3.3.1.2. 仮想マシンの CPU、メモリ

1. 各業務システム向けの CPU、メモリリソースを予約した領域を構成すること。各リソースは設計時に PMDA から要望を提示したものをベースに、システム構成上の実効性、妥当性を検討し、最終的な構成を PMDA と合意すること。
2. 仮想マシンの物理ホスト配置を手動で変更可能なように構成すること。

4.3.3.1.3. 仮想マシンの OS、基本構成

1. Windows Server2019、2022 の仮想マシンを新霞が関ビル仮想基盤システム内に 16 個以上作成

可能なライセンスで構成すること。

2. RHEL8 及び 9 の仮想マシンを新霞が関ビル仮想基盤システム内に 6 個以上作成可能なライセンスで構成すること。
3. Windows Server2022、RHEL8 及び RHEL9 の仮想マシンテンプレートを作成すること。仮想マシンテンプレートは OS の設計内容を反映させた状態で作成すること。特段の理由がなければ本番系仮想基盤システムで作成したものと同じ構成で良いが、新霞が関ビルのネットワーク構成により変更が必要な部分は変更を行うこと。

4.3.3.1.4. ストレージアクセス構成

1. 新霞が関ビルで作成したボリュームに対応するストレージ領域を構成すること。

4.3.3.1.5. ネットワーク構成

1. 物理ホスト間で共有可能な仮想イーサネットスイッチを構成し、仮想イーサネットスイッチの操作を一度行うことで全物理ホストに設定が反映されるようにすること。
2. 仮想イーサネットスイッチの構成、所属させるネットワークは PMDA と協議の上で決定すること。
3. 物理ネットワークと必要な L2 通信が可能となるように構成すること。
4. IPMI インターフェースを新霞が関ビル既設 L2 スイッチ B に接続すること。必要な配線を行うこと。

4.3.3.1.6. 管理機能

1. 仮想基盤システム上のオブジェクトの操作権限を設定したロールを構成すること。ロールは全体管理者、業務システム管理者向けに作成すること。業務システム管理者向けのロールは 8 種類程度を想定しているが、各ロールに付与する権限内容自体はほぼ同等とする。この構成は本番系仮想基盤システムと同じ構成として良い。
2. 仮想マシン、ストレージ領域、ネットワーク設定に対する操作権限を付与するためのグルーピング設定を行うこと。
3. グルーピングに対してロールの割り当て及びロールに割り当てられた権限を持つユーザ割り当てを行うこと。

4.3.3.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 物理ホストのオンサイト対応時、ハイパーバイザのインストール、仮想基盤システムへの機能的な合流までを行うこと。

4.3.4. 検証系仮想基盤システム

4.3.4.1. 構成要件

4.3.4.1.1. 基本構成

1. 仮想マシンを稼働させる物理ホストは 3 台で構成すること。
2. ハイパーバイザには仮想 L3 ネットワークを構成可能な製品を使用すること。
3. 物理ホストでは Hyper Threading を有効にすること。
4. 物理ホストを FC スイッチとマルチパス接続し、検証用ストレージを利用可能な構成とすること。
5. 物理ホストのネットワークインターフェースはサービス系、仮想基盤管理系、運用管理系で物理ポートを占有させること。それぞれのネットワークインターフェースは 10GBase-SR とすること。チーミングを行い、スタック構成のサーバ接続 L2 スイッチ G に冗長接続すること。
6. 物理ホストを管理するための IPMI インターフェースを管理ポート L2 スイッチに接続すること。
7. 物理ホストが障害等により停止した際、その物理ホストで稼働していた仮想マシンが自動的に別の物理ホストで動作を復旧するように構成すること。
8. データセンタの 19 インチラックに搭載すること。
9. 電源を二重化し、電源冗長を行うこと。

4.3.4.1.2. 仮想マシンの CPU、メモリ

1. 本番系仮想基盤と同等の構成を作成すること。ただし検証系仮想基盤システムには本番環境の業務システムは稼働させないため、受注者が作成するテストサーバで動作確認を行うこと。

4.3.4.1.3. 仮想マシンの OS、基本構成

2. Windows Server2019、Windows Server2022、RHEL は検証系業務仮想基盤システム内で作成可能に数量制限のないライセンスで構成すること。
3. Windows Server2019、Windows Server2022、RHEL8 及び RHEL9 の仮想マシンテンプレートを作成すること。仮想マシンテンプレートは OS の設計内容を反映させた状態で作成すること。特段の理由がなければ本番系仮想基盤システムで作成したものと同じ構成で良い。

4.3.4.1.4. ストレージアクセス構成

1. 検証用ストレージで作成したボリュームに対応するストレージ領域を構成すること。

4.3.4.1.5. ネットワーク構成

1. 物理ネットワークの L3 ネットワーク境界となる仮想ルータを構成すること。サービス系のネットワークインターフェースを使用して内部システム向け、公開システム向けの仮想ルータ両方が通信可能となるように構成すること。
2. 物理ホスト間で共有可能な仮想イーサネットスイッチを構成し、仮想イーサネットスイッチの操作を一度行うことで全物理ホストに設定が反映されるようにすること。
3. 仮想イーサネットスイッチの構成、所属させるネットワークは PMDA と協議の上で決定すること。
4. 仮想イーサネットスイッチから本調達で構築するフローコレクタにネットワークフロー情報を送信するように構成すること。
5. 仮想マシン間で L3 通信するための仮想ルータを構成すること。

4.3.4.1.6. 管理機能

1. 仮想基盤システム上のオブジェクトの操作権限を設定したロールを構成すること。ロールは全体管理者、業務システム管理者向けに作成すること。業務システム管理者向けのロールは 8 種類程度を想定しているが、各ロールに付与する権限内容自体はほぼ同等とする。この構成は本番系仮想基盤システムと同じ構成として良い。
2. 仮想マシン、ストレージ領域、ネットワーク設定に対する操作権限を付与するためのグルーピング設定を行うこと。
3. グルーピングに対してロールの割り当て及びロールに割り当てられた権限を持つユーザ割り当てを行うこと。

4.3.4.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 物理ホストのオンサイト対応時、ハイパーバイザのインストール、仮想基盤システムへの機能的な合流までを行うこと。

4.3.5. 共有ストレージ

4.3.5.1. 高可用性ストレージ

4.3.5.1.1. 構成要件

1. 本装置を 2 台導入すること。

2. コントローラは 2 台以上で冗長構成とし、全てのコントローラを Active 状態で動作させること。
3. 本装置 1 台あたり、実効容量として 180TB 以上を確保すること。
4. ディスクは全て NVMe SSD で構成すること。
5. 2 個までのディスク同時障害耐性を持つように構成すること。
6. FC スイッチと FC インターフェースで接続し、本番系仮想基盤システム、物理サーバから本装置にアクセス可能な構成とすること。接続はコントローラ、FC スイッチ、FC インターフェースの単一障害時の SCSI トラフィックに対する影響範囲を留められるよう冗長接続とすること。尚、SAN 接続の構成上、他の仮想基盤システムから本装置にアクセスが可能であっても良い。
7. 構築時に PMDA から提示する論理ボリューム構成案をもとにボリューム構成を検討し、ボリューム設定を行うこと。
8. ディスク暗号化を行うこと。暗号鍵の保管場所を検討し、管理者のみアクセス可能な場所に格納すること。
9. 本装置で発生したシステムイベントを本調達で構築する汎用 Syslog サーバに送信すること。
10. 電源は 2 系統以上の冗長構成とすること。
11. データセンタの 19 インチラックに搭載すること。

4.3.5.1.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 記憶媒体の障害及び障害予兆を検出するリモート監視体制を構築すること。これらの症状を検出した場合、リモート監視体制側から PMDA にメールまたは電話による連絡を行った上で記憶媒体の交換が可能であること。
6. 記憶媒体の障害時のような比較的定型的なオンサイト対応の場合、オンサイト対応を行う作業者は日本語によるコミュニケーションが可能であり、PMDA 担当者が機器の設置場所に赴かなくても、機器設置ロケーションの入館、保守対応が可能なこと。
7. 本調達の契約終了 2 週間前から契約終了日までに、本装置の記憶媒体のデータ消去作業を行うこと。データが格納されたディスクはデータセンタから持ち出さずに作業を行うこと。ただし、記憶媒体単位での消去作業を行わずにデータ消去を行える機能がある場合はその機能を使用しても良い。
8. 新しく論理ボリュームを作成するための手順書を作成すること。この手順書には仮想基盤システムから論理ボリュームを使用可能となるまでの必要作業手順を含めること。

4.3.5.2. 通常ストレージ

4.3.5.2.1. 構成要件

1. 本装置を 1 台導入すること。
2. コントローラは 2 台冗長構成で動作すること。動作方式は Active-Standby 構成、Active-Active 構成どちらでも良い。
3. 本装置 1 台あたり、実効容量として 300TB 以上を確保すること。
4. ディスクは NVMe SSD と HDD の混在構成で SSD をキャッシュアクセス専用に使用可能な構成とすること。現行システムでは総容量の 20%程度をキャッシュとして使用している。尚、主な記憶領域全てを NVMe SSD で構成しても良い。
5. 2 個までのディスク同時障害耐性を持つように構成すること。
6. FC スイッチと FC インターフェースで接続し、本番系仮想基盤システムから本装置にアクセス可能となるように構成すること。接続はコントローラ、FC スイッチ、FC インターフェースの単一障害時の SCSI トラフィックに対する影響範囲を留められるよう冗長接続とすること。尚、SAN 接続の構成上、他の仮想基盤システムから本装置にアクセスが可能であっても良い。
7. 構築時に PMDA から提示する論理ボリューム構成案をもとにボリューム構成を検討し、ボリューム設定を行うこと。
8. ディスク暗号化を行うこと。暗号鍵の保管場所を検討し、管理者のみアクセス可能な場所に格納すること。
9. 本装置で発生したシステムイベントを本調達で構築する汎用 Syslog サーバに送信すること。
10. 電源は 2 系統以上の冗長構成とすること。
11. データセンタの 19 インチラックに搭載すること。

4.3.5.2.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 記憶媒体の障害及び障害予兆を検出するリモート監視体制を構築すること。これらの症状を検出した場合、リモート監視体制側から PMDA にメールまたは電話による連絡を行った上で記憶媒体の交換が可能であること。
6. 記憶媒体の障害時のような比較的定型的なオンサイト対応の場合、オンサイト対応を行う作業者は日本語によるコミュニケーションが可能であり、PMDA 担当者が機器の設置場所に赴かなくても、機器設置ロケーションの入館、保守対応が可能なこと。

7. 本調達の契約終了 2 週間前から契約終了日までに、本装置の記憶媒体のデータ消去作業を行うこと。データが格納されたディスクはデータセンタから持ち出さずに作業を行うこと。ただし、記憶媒体単位での消去作業を行わずにデータ消去を行える機能がある場合はその機能を使用しても良い。
8. 新しく論理ボリュームを作成するための手順書を作成すること。この手順書には仮想基盤システムから論理ボリュームを使用可能となるまでの必要作業手順を含めること。

4.3.5.3. 検証用ストレージ

4.3.5.3.1. 構成要件

1. 本装置を 1 台導入すること。
2. コントローラは 2 台以上で冗長構成とし、全てのコントローラを Active 状態で動作させること。
3. 本装置 1 台あたり、実効容量として 50TB 以上を確保すること。
4. ディスクは全て NVMe SSD で構成すること。
5. RAID6 相当のディスク障害耐性を持つように構成すること。
6. FC スイッチと FC インターフェースで接続し、本番系仮想基盤システム、物理サーバから本装置にアクセス可能な構成とすること。接続はコントローラ、FC スイッチ、FC インターフェースの単一障害時の SCSI トラフィックに対する影響範囲を留められるよう冗長接続とすること。尚、SAN 接続の構成上、他の仮想基盤システムから本装置にアクセスが可能であっても良い。
7. 構築時に PMDA から提示する論理ボリューム構成案をもとにボリューム構成を検討し、ボリューム設定を行うこと。
8. ディスク暗号化を行うこと。暗号鍵の保管場所を検討し、管理者のみアクセス可能な場所に格納すること。
9. 本装置で発生したシステムイベントを本調達で構築する汎用 Syslog サーバに送信すること。
10. 電源は 2 系統以上の冗長構成とすること。
11. データセンタの 19 インチラックに搭載すること。

4.3.5.3.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 記憶媒体の障害及び障害予兆を検出するリモート監視体制を構築すること。これらの症状を検出した場合、リモート監視体制側から PMDA にメールまたは電話による連絡を行った上で記

憶媒体の交換が可能であること。

6. 記憶媒体の障害時のような比較的定型的なオンサイト対応の場合、オンサイト対応を行う作業者は日本語によるコミュニケーションが可能であり、PMDA 担当者が機器の設置場所に赴かなくても、機器設置ロケーションの入館、保守対応が可能なこと。
7. 本調達の契約終了 2 週間前から契約終了日までに、本装置の記憶媒体のデータ消去作業を行うこと。データが格納されたディスクはデータセンタから持ち出さずに作業を行うこと。ただし、記憶媒体単位での消去作業を行わずにデータ消去を行える機能がある場合はその機能を使用しても良い。

4.3.5.4. 新霞が関ビル共有ストレージ

4.3.5.4.1. 構成要件

1. 本装置を 1 台導入すること。
2. コントローラは 2 台冗長構成で動作すること。動作方式は Active-Standby 構成、Active-Active 構成どちらでも良い。
3. 本装置 1 台あたり、実効容量として 40TB 以上を確保すること。ただし、バックアップシステムの 2 次バックアップデータ格納サーバの記憶領域として本装置と共用する場合は、その用途に必要な分も構成に含めること。
4. RAID6 相当のディスク障害耐性を持つように構成すること。
5. サーバ接続 L2 スイッチ I と 10GBase-SR 2 本以上で接続し、新霞が関ビル仮想基盤システムから iSCSI 接続可能なように構成すること。
6. 構築時に PMDA から提示する論理ボリューム構成案をもとにボリューム構成を検討し、ボリューム設定を行うこと。
7. ディスク暗号化を行うこと。暗号鍵の保管場所を検討し、管理者のみアクセス可能な場所に格納すること。
8. 本装置で発生したシステムイベントを本調達で構築する汎用 Syslog サーバに送信すること。
9. 電源は 2 系統以上の冗長構成とすること。
10. 新霞が関ビルの本調達で導入する 19 インチラックに搭載すること。
11. UPS を用意し、UPS の入力電源に異常が発生した際に可能な限り自動的に正常なシャットダウン処理を通して停止するように構成すること。処理を行うためのサーバ等が必要な場合、本番系仮想基盤システムを使用しても良い。新霞が関ビル仮想基盤システムの UPS の仕組みを流用しても良い。

4.3.5.4.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。

3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 記憶媒体の障害及び障害予兆を検出するリモート監視体制を構築すること。これらの症状を検出した場合、リモート監視体制側から PMDA にメールまたは電話による連絡を行った上で記憶媒体の交換が可能であること。
6. 記憶媒体の障害時のような比較的定型的なオンサイト対応の場合、オンサイト対応を行う作業者は日本語によるコミュニケーションが可能であり、PMDA 担当者が機器の設置場所に赴かなくても、機器設置ロケーションの入館、保守対応が可能なこと。
7. 本調達の契約終了 2 週間前から契約終了日までに、本装置の記憶媒体のデータ消去作業を行うこと。データが格納されたディスクは新霞が関ビルから持ち出さずに作業を行うこと。ただし、記憶媒体単位での消去作業を行わずにデータ消去を行える機能がある場合はその機能を使用しても良い。
8. 新しく論理ボリュームを作成するための手順書を作成すること。この手順書には仮想基盤システムから論理ボリュームを使用可能となるまでの必要作業手順を含めること。

4.3.6. FC スイッチ

4.3.6.1. 本番系 FC スイッチ

4.3.6.1.1. 構築要件

1. 1 台の物理ホストが 2 台の FC スイッチと接続するように構成すること。本番系 FC スイッチは 4 台で構成し、本番系仮想基盤システムとリモート接続基盤システムの物理ホストを分散して接続すること。
2. 高可用性ストレージ 1、高可用性ストレージ 2、通常ストレージと FC 接続すること。各ストレージに対する接続に冗長性を持たせるため、各 FC スイッチから各ストレージの異なるコントローラに FC 接続を行うこと。
3. ソフトゾーニングを行うこと。
4. 本調達で構築するシステム状態監視サーバから SNMP アクセス可能なように構成すること。
5. FC インターフェース全てにマルチモード光ファイバを使用可能なトランシーバを接続して納入すること。
6. 本調達で本番系 FC スイッチに接続する物理ホストが使用可能となるようなライセンスを構成に含めること。

4.3.6.1.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。

3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.3.6.2. 検証系 FC スイッチ

4.3.6.2.1. 構築要件

1. 本番系 FC スイッチと別筐体で構成すること。
2. 1 台の物理ホストが 2 台の FC スイッチと接続するように構成すること。
3. 検証用ストレージと FC 接続すること。ストレージに対する接続に冗長性を持たせるため、各 FC スイッチからストレージの異なるコントローラに FC 接続を行うこと
4. ソフトゾーニングを行うこと。
5. 本調達で構築するシステム状態監視サーバから SNMP アクセス可能なように構成すること。
6. 本調達で検証系 FC スイッチに接続する物理ホストが使用可能となるようなライセンスを構成に含めること。

4.3.6.2.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.3.6.3. 物理サーバ用 FC スイッチ

4.3.6.3.1. 構築要件

1. 1 台の物理サーバが 2 台の FC スイッチと接続するように構成すること。業務システムが準備する物理サーバがこの FC スイッチを使用できるように構成すること。
2. 高可用性ストレージ 1、高可用性ストレージ 2 と FC 接続すること。
3. ソフトゾーニングを行うこと。
4. 本調達で構築するシステム状態監視サーバから SNMP アクセス可能なように構成すること。
5. FC インターフェース全てにマルチモード光ファイバを使用可能なトランシーバを接続して納入すること。
6. 物理サーバ用 FC スイッチ全ポートを使用可能となるようなライセンスを構成に含めること。

4.3.6.3.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。

2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.4. IP ネットワークシステム

「別紙 5 IP ネットワーク詳細構成」を参照の上、製品選定、システム構築を行うこと。

4.4.1. IP ルーティング

1. 内部システムネットワークと運用管理ネットワーク内では基本的に OSPF によるルーティングを構成すること。
2. ネットワーク構成、拡張性の観点から OSPF のエリア設計を行い、PMDA と設計を合意した上で構成すること。
3. OSPF の設計時はデフォルトルートの取り扱い、再配布に関する設計を行い、PMDA と合意すること。必ずしも全ての L3 ネットワーク機器で OSPF を使用することを要件とはしないが、ネットワークの変更時の作業、ヒューマンエラー発生頻度の低減を図れるように設計を行うこと。
4. 本調達の設計範囲外の既存ネットワークアドレスについても必要な通信が可能となるように設計すること。
5. 仮想基盤システムのトラフィックが通過するネットワーク機器ではフラグメントが発生しないようにジャンボフレームを構成すること。ジャンボフレームとして指定するサイズは仮想基盤システムのネットワーク使用効率を最大化できるように構成すること。
6. 本調達で導入する動作確認用物理サーバを使用して各種別の物理サーバを模した L3 ルーティング、セキュリティ機能、ロードバランスの動作正常性を確認すること。ロードバランスを行う際は動作確認用物理サーバに簡易的な Web サーバを構成して HTTP 及び HTTPS 通信による動作確認を行うこと。このテストに必要なネットワークケーブルを用意すること。

4.4.2. コア L3 スイッチ

4.4.2.1. 構成要件

1. 本装置を 2 台用意し、2 台スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 内部系、運用管理系、インターネット系、追加システム向けの VRF を構成すること。
4. OSPF を設定し、各ネットワークの経路情報を動的に交換すること。
5. 必要な L2、L3 設定を行うこと。
6. 各要件を満たすために必要なネットワーク物理接続を行うこと。

7. 必要に応じてアクセスリストを設定しトラフィックフィルタを行うこと。
8. リンクアグリゲーションを構成する場合、接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
9. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
10. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
11. 運用管理システムで構築するシステム sFlow コレクタサーバにネットワークフロー情報を送信するように構成すること。
12. データセンタの 19 インチラックに搭載すること。
13. 電源を二重化し、電源冗長を行うこと

4.4.2.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、スタティックルート設定、OSPF 動作インターフェース変更、経路フィルタ及び経路再配布設定の変更、OSPF 状態確認、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.3. サーバ接続 L2 スイッチ A

4.4.3.1. 構成要件

1. 本装置を 4 台用意し、スタック構成で 2 組構成すること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。
4. 本番系仮想基盤システムの物理ホストを接続すること。
5. 本番系仮想基盤システム、リモート接続仮想基盤システムのサービス系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続すること。
6. コア L3 スイッチと 40GBase-SR で接続し、本装置 1 組あたり 80Gbps の帯域を確保すること。
7. サーバ接続 L2 スイッチ D と 10GBase-SR で接続し、本装置 1 組あたり 20Gbps の帯域を確保すること。ただし、公開仮想マシン連携物理サーバ、内部仮想マシン連携物理サーバとの通信

制御に物理的なファイアウォールを使用する場合は要件となる帯域を確保した上で接続すること。

8. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
9. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
10. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
11. データセンタの 19 インチラックに搭載すること。
12. 電源を二重化し、電源冗長を行うこと。

4.4.3.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション状態、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.4. サーバ接続 L2 スイッチ B

4.4.4.1. 構成要件

1. 本装置を 4 台用意し、スタック構成で 2 組構成すること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。
4. 本番系仮想基盤システムの物理ホストを接続すること。
5. 本番系仮想基盤システム、リモート接続仮想基盤システムの仮想基盤管理系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続すること。
6. コア L3 スイッチと 40GBase-SR で接続し、本装置 1 組あたり 80Gbps の帯域を確保すること。
7. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
8. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
9. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能

になるように構成すること。

10. データセンタの 19 インチラックに搭載すること。
11. 電源を二重化し、電源冗長を行うこと。

4.4.4.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.5. サーバ接続 L2 スイッチ C

4.4.5.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。
4. 本番系仮想基盤システムの物理ホストを接続すること。
5. 本番系仮想基盤システムの運用管理系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続すること。
6. コア L3 スイッチと 40GBase-SR で接続し、本装置 1 組あたり 80Gbps の帯域を確保すること。
7. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
8. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
9. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
10. データセンタの 19 インチラックに搭載すること。
11. 電源を二重化し、電源冗長を行うこと。

4.4.5.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最

新設定情報の保持は PMDA が行うものとする。

3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、VLAN 設定、L2-L4 拡張 ACL 設定、ミラーリング設定、装置の物理状態確認」

4.4.6. サーバ接続 L2 スイッチ D

4.4.6.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。
4. 業務システムの物理サーバのサービス系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理サーバ 1 台あたり計 2 本)接続できるようにすること。
5. 内部ファイアウォール B と 10GBase-SR で接続し、10Gbps の帯域を確保すること。
6. 内部ファイアウォール C と 10GBase-SR で接続し、10Gbps の帯域を確保すること。
7. サーバ接続 L2 スイッチ A と 10GBase-SR で接続し、本装置 1 組あたり 20Gbps の帯域を確保すること。ただし、公開仮想マシン連携物理サーバ、内部仮想マシン連携物理サーバとの通信制御に物理的なファイアウォールを使用する場合は要件となる帯域を確保した上で接続すること。
8. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
9. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
10. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
11. データセンタの 19 インチラックに搭載すること。
12. 電源を二重化し、電源冗長を行うこと。
13. サーバ接続 L2 スイッチ D で使用可能な 10GBase-SR を 24 個納入すること。

4.4.6.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～

17 時に対応可能なこと。

4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.7. サーバ接続 L2 スイッチ E

4.4.7.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。
4. 業務システムの物理サーバの運用管理系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理サーバ 1 台あたり計 2 本)接続できるようにすること。
5. コア L3 スイッチと 10GBase-SR で接続し、20Gbps の帯域を確保すること。
6. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
7. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
8. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
9. データセンタの 19 インチラックに搭載すること。
10. 電源を二重化し、電源冗長を行うこと。

4.4.7.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 拡張ベース設定、パケットミラーリング設定、装置の物理状態確認」

4.4.8. サーバ接続 L2 スイッチ F

4.4.8.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。
4. リモート接続基盤システムの物理ホストのサービス系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。
5. リモート接続基盤システムの物理ホストの仮想基盤管理系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。
6. HTTP トラフィック分離装置と 10GBase-SR で接続し、10Gbps の帯域を確保すること。
7. 内部ファイアウォール F と 10GBase-SR で接続し、10Gbps の帯域を確保すること。
8. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
9. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
10. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
11. データセンタの 19 インチラックに搭載すること。
12. 電源を二重化し、電源冗長を行うこと。

4.4.8.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.9. サーバ接続 L2 スイッチ G

4.4.9.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構

成すること。

3. 必要な L2 設定を行うこと。
4. 検証系仮想基盤システムの物理ホストのサービス系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。
5. 検証系仮想基盤システムの物理ホストの仮想基盤管理系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。
6. 検証系仮想基盤システムの物理ホストの運用管理系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。
7. コア L3 スイッチと 10GBase-SR で接続し、20Gbps の帯域を確保すること。
8. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
9. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
10. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
11. データセンタの 19 インチラックに搭載すること。

4.4.9.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.10. サーバ接続 L2 スイッチ H

4.4.10.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。
4. データセンタに設置するバックアップシステムのハードウェアを 10GBase-SR(物理ホスト 1 台あたり計 2 本)で接続できるようにすること。

5. コア L3 スイッチと 40GBase-SR で接続し、80Gbps の帯域を確保すること。
6. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
7. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
8. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
9. データセンタの 19 インチラックに搭載すること。
10. 電源を二重化し、電源冗長を行うこと。

4.4.10.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース設定、パケットミラーリング設定、装置の物理状態確認」

4.4.11. サーバ接続 L2 スイッチ I

4.4.11.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。
4. 新霞が関ビル仮想基盤システムの物理ホストのサービス系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。
5. 新霞が関ビル仮想基盤システムの物理ホストの仮想基盤管理系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。
6. 新霞が関ビル仮想基盤システムの物理ホストの運用管理系トラフィック用ポートとスタック構成の本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。
7. 新霞が関ビル仮想基盤システムの物理ホストの iSCSI トラフィック用ポートとスタック構成の

本装置に 10GBase-SR で 1 本ずつ(物理ホスト 1 台あたり計 2 本)接続できるようにすること。

8. 新霞が関ビル共有ストレージの iSCSI トラフィック用ポートとスタック構成の本装置に 10GBase-SR で接続し、20Gbps 以上の帯域を確保すること。
9. 既設 L2 スイッチ C と 1000Base-T で接続し、20bps の帯域を確保すること。
10. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
11. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
12. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
13. 新霞が関ビルの本調達で導入する 19 インチラックに搭載すること。
14. 電源を二重化し、電源冗長を行うこと。

4.4.11.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.12. インターネット境界ネットワーク

4.4.12.1. インターネット境界ネットワーク A

4.4.12.1.1. 構成要件

1. 各要件を満たせるように必要な要素を構成すること。複数の製品を使用して実現して良い。
2. ファイアウォール機能によるステートレスな L3/L4 フィルタリング機能を構成し、必要最低限の情報のみ外部ネットワークに公開する構成とすること。
3. 公開システムの 1IP アドレスごとに一つのフィルタルールを作成すること。同一フィルタルール内に複数の L4 条件を設定して良い。
4. 既存の遮断 IP アドレスを移行すること。数量は 3000 個程度を想定すること。
5. 公開システムのグローバル IP アドレスをプライベート IP アドレスに NAT すること。
6. 収容しているインターネット回線に対するデフォルトルートをはじめ、必要な L3 ルーティング設定を行うこと。
7. 高可用性インバウンド WAN を収容する構成とすること。

8. インターネット回線を 1 回線追加可能な拡張性を有すること。回線が追加されることを前提とした設定を本件の構築段階で行うこと。ルーティングやネットワークアドレスの構成は想定のもので良い。物理ネットワーク接続が必要な場合、その接続も行うこと。
9. 内部ネットワーク、インターネット境界ネットワーク B からインターネット境界ネットワーク A を経由して公開システムにアクセスするためのルーティング設定を行うこと。
10. IPS 機能を構成すること。対象トラフィックが TLS により暗号化されている場合、復号化した上で IPS 機能を適用すること。
11. 本システムの管理トラフィック等、明らかに攻撃とは無関係と判断できる通信パターンを検知除外登録すること。
12. 運用中に除外パターンを追加する際、定型的な手順で除外設定が可能になるように手順を整備すること。
13. WAF 機能を構成すること。対象トラフィックが TLS により暗号化されている場合、復号化した上で WAF 機能を適用すること。
14. L3/L4 フィルタリング機能の許可トラフィック、遮断トラフィックをファイアウォール管理サーバに送信すること。
15. IPS 機能の遮断トラフィックを汎用 Syslog サーバに送信すること。
16. WAF 機能の遮断トラフィックを汎用 Syslog サーバに送信すること。
17. TLS 復号化に失敗したことを示すログを汎用 Syslog サーバに送信すること。
18. 装置・経路障害、冗長機能の状態変化を SNMP、Syslog で検出可能なように構成すること。製品の管理装置との連携でも良い。
19. 公開システムに対してロードバランスが可能となるように構成すること。
20. セキュリティ機能適用のために TLS 復号化したトラフィックを宛先 IP アドレスに応じて再暗号化してロードバランスするもの、再暗号化せずにロードバランスするものを分けて構成すること。
21. 業務システム管理者がロードバランス設定を行うための管理画面にアクセスする際、自身が管理するシステム向けのロードバランス設定のみ行うことが可能で、他の業務システム管理者が管理画面にアクセスしてもその設定を表示させないように業務システム単位で独立した管理画面及びロードバランスが可能なように構成すること。
22. 対象の公開システムが収容されている業務仮想基盤システムの仮想ルータ A、内部ファイアウォール B に対してルーティング設定を行うこと。
23. インターネット境界ネットワークを構成する要素は二重化し、経路、筐体いずれも単一障害点がないように構成すること。
24. インターネット境界ネットワークで公開しているサービスに PMDA 内部からアクセスする際にもインターネットからのアクセスと同様のセキュリティ機能が適用されるようにネットワークを構成すること。
25. インターネットスイッチ A と 1000Base-T または 1000Base-SX で接続し、2Gbps 以上の帯域を

確保すること。

26. コア L3 スイッチと 10GBase-SR で接続し、10Gbps 以上の帯域を確保すること。この接続はインターネット境界ネットワーク A から公開システムに対する通信で占有すること。
27. 内部ネットワークから公開システムにアクセスするため、コア L3 スイッチと 1000Base-SX で接続し、1Gbps 以上の帯域を確保すること。この接続にはインターネットスイッチ A を使用しても良い。
28. 各機能を業務システム管理者向けに提供する際、物理インターフェースを共有できない場合、共有できない機能に関しては作成する業務システム管理者数もしくは収容するインターネット回線の種別と同数分、要件同様の物理接続を行うこと。
29. L3/L4 フィルタリング機能は 3Gbps 以上のスループットを確保可能なこと。
30. IPS 機能は 1Gbps 以上のスループットを確保可能なこと。TLS 復号化を行うことでスループットが低下する場合、低下後のスループットで確保可能なこと。
31. WAF 機能は 500Mbps 以上のスループットを確保可能なこと。TLS 復号化を行うことでスループットが低下する場合、低下後のスループットで確保可能なこと。
32. ロードバランス処理機能は 10Gbps 以上のスループットを確保可能なこと。
33. 可能な限り電源を二重化し、電源冗長を行うこと。

4.4.12.1.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、HA 状態確認、L3/L4 フィルタ設定変更、IPS 除外、WAF 除外、基本的な L4 ロードバランス設定の流れ、基本的な L7 ロードバランスの流れ(詳細な L7 設定手順は不要)、L7 ロードバランスにおけるサーバ証明書のインポート及び更新、TLS 復号化及び再暗号化」

4.4.12.2. インターネット境界ネットワーク B

4.4.12.2.1. 構成要件

1. 各要件を満たせるように必要な要素を構成すること。複数の製品を使用して実現して良い。
2. ファイアウォール機能によるステートレスな L3/L4 フィルタリング機能を構成し、必要最低限の情報のみ外部ネットワークに公開する構成とすること。
3. 公開システムの 1IP アドレスごとに一つのフィルタルールを作成すること。同一フィルタルール内に複数の L4 条件を設定して良い。

4. 既存の遮断 IP アドレスを移行すること(この IP アドレスはインターネット境界ネットワーク A と同じ。)。
5. 公開システムのグローバル IP アドレスをプライベート IP アドレスに NAT すること。
6. 収容しているインターネット回線に対するデフォルトルートをはじめ、必要な L3 ルーティング設定を行うこと。
7. 広帯域インバウンド WAN、通常インバウンド WAN を収容可能な構成とすること。
8. インターネット回線を 1 回線追加可能な拡張性を有すること。回線が追加されることを前提とした設定を本件の構築段階で行うこと。ルーティングやネットワークアドレスの構成は想定のもので良い。物理ネットワーク接続が必要な場合、その接続も行うこと。
9. 内部ネットワーク、インターネット境界ネットワーク A からインターネット境界ネットワーク B を経由して公開システムにアクセスするためのルーティング設定を行うこと。
10. IPS 機能を構成すること。対象トラフィックが TLS により暗号化されている場合、復号化した上で IPS 機能を適用すること。
11. 本システムの管理トラフィック等、明らかに攻撃とは無関係と判断できる通信パターンを検知除外登録すること。
12. 運用中に除外パターンを追加する際、定型的な手順で除外設定が可能になるように手順を整備すること。
13. WAF 機能を構成すること。対象トラフィックが TLS により暗号化されている場合、復号化した上で WAF 機能を適用すること。
14. L3/L4 フィルタリング機能の許可トラフィック、遮断トラフィックをファイアウォール管理サーバに送信すること。
15. IPS 機能の遮断トラフィックを汎用 Syslog サーバに送信すること。
16. WAF 機能の遮断トラフィックを汎用 Syslog サーバに送信すること。
17. TLS 復号化に失敗したことを示すログを汎用 Syslog サーバに送信すること。
18. 装置・経路障害、冗長機能の状態変化を SNMP、Syslog で検出可能なように構成すること。製品の管理装置との連携でも良い。
19. 公開システムに対してロードバランスするように構成すること。
20. セキュリティ機能適用のために TLS 復号化したトラフィックを宛先 IP アドレスに応じて再暗号化してロードバランスするもの、再暗号化せずにロードバランスするものを分けて構成すること。
21. 業務システム管理者がロードバランス設定を行うための管理画面にアクセスする際、自身が管理するシステム向けのロードバランス設定のみ行うことが可能で、他の業務システム管理者が管理画面にアクセスしてもその設定を表示させないように業務システム単位で独立した管理画面及びロードバランスが可能なように構成すること。
22. 対象の公開システムが収容されている業務仮想基盤システムの仮想ルータ A、内部ファイアウォール B に対してルーティング設定を行うこと。

23. インターネット境界ネットワークを構成する要素は二重化し、経路、筐体いずれも単一障害点がないように構成すること。
24. インターネット境界ネットワークで公開しているサービスに PMDA 内部からアクセスする際にもインターネットからのアクセスと同様のセキュリティ機能が適用されるようにネットワークを構成すること。
25. インターネットスイッチ B と 1000Base-T または 1000Base-SX で接続し、2Gbps 以上の帯域を確保すること。
26. コア L3 スイッチと 10GBase-SR で接続し、10Gbps 以上の帯域を確保すること。この接続はインターネット境界ネットワーク B から公開システムに対する通信で占有すること。
27. 内部ネットワークから公開システムにアクセスするため、コア L3 スイッチと 1000Base-SX で接続し、1Gbps 以上の帯域を確保すること。この接続にはインターネットスイッチ B を使用しても良い。
28. 現行データセンタで稼働している業務システム B の公開システムと通信するための専用の物理接続としてコア L3 スイッチと 1000Base-SX で接続し、1Gbps 以上の帯域を確保すること。この接続にはインターネットスイッチ B を使用しても良い。
29. 各機能を業務システム管理者向けに提供する際、物理インターフェースを共有できない場合、共有できない機能に関しては作成する業務システム管理者数もしくは収容するインターネット回線の種別と同数分、要件同様の物理接続を行うこと。
30. L3/L4 フィルタリング機能は 7Gbps 以上のスループットを確保可能なこと。
31. IPS 機能は 2Gbps 以上のスループットを確保可能なこと。TLS 復号化を行うことでスループットが低下する場合、低下後のスループットで確保可能なこと。
32. WAF 機能は 1Gbps 以上のスループットを確保可能なこと。TLS 復号化を行うことでスループットが低下する場合、低下後のスループットで確保可能なこと。
33. ロードバランス処理機能は 30Gbps 以上のスループットを確保可能なこと。
34. 可能な限り電源を二重化し、電源冗長を行うこと。

4.4.12.2.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、HA 状態確認、L3/L4 フィルタ設定変更、IPS 除外、WAF 除外、基本的な L4 ロードバランス設定の流れ、基本的な L7 ロードバランスの流れ(詳細な L7 設定手順は不要)、L7 ロードバランスにおけるサ

ーバ証明書のインポート及び更新、TLS 復号化及び再暗号化」

4.4.12.3. インターネット境界ネットワーク C

4.4.12.3.1. 構成要件

1. 各要件を満たせるように必要な要素を構成すること。
2. インターネット系ネットワークと他のネットワークからのアウトバウンド通信を個別に制御できるように L3/L4 フィルタリング機能を提供する装置は個別にルーティングテーブルを保持できるように構成すること。
3. L3/L4 フィルタリング機能を構成し、アウトバウンド通信を最小限とすること。
4. 内部系ネットワークとインターネット系ネットワークの L3 ネットワーク境界として構成し、それぞれのネットワーク間が通信を行うための L3 ルーティング設定を行うこと。
5. 既存の遮断 IP アドレスを移行すること(この IP アドレスはインターネット境界ネットワーク A と同じ。)。
6. URL フィルタリングを設定し、悪意あるサイトへのアクセスをブロックすること。
7. URL フィルタリングを適用しない通信を送信元 IP アドレス、宛先 IP アドレスに基づいて指定できるように構成すること。
8. URL フィルタリング、不正な名前解決結果による通信遮断が発生した場合、ユーザの Web ブラウザに表示するエラー画面を設定すること。表示内容をカスタマイズし、ユーザが次に行う行動が分かりやすくなるようにすること。
9. リスクのあるグローバル IP アドレスとの通信が発生したことが分かるように構成すること。可視化はファイアウォール管理サーバを使用しても良い。
10. インターネット上のノードと通信できるように NAT 設定を行うこと。
11. 収容しているインターネット回線に対するデフォルトルートをはじめ、必要な L3 ルーティング設定を行うこと。
12. 通常アウトバウンド WAN を収容する構成とすること。
13. インターネット回線を 1 個追加可能な拡張性を有すること。
14. 各セキュリティ機能の許可トラフィック、遮断トラフィックをファイアウォール管理サーバに送信すること。
15. 装置・経路障害、冗長機能の状態変化を SNMP、Syslog で検出可能なように構成すること。製品の管理装置との連携でも良い。
16. コア L3 スイッチと 10GBase-SR で接続し、10Gbps の帯域を確保すること。仮想ファイアウォール機能を使用時、異なる仮想ファイアウォールで物理インターフェースを占有できない場合、それぞれの仮想ファイアウォールに 10GBase-SR 接続を行うこと。
17. 各機能を業務システム管理者向けに提供する際、物理インターフェースを共有できない場合、共有できない機能に関しては作成する業務システム管理者数もしくは収容するインターネット回線の種別と同数分、要件同様の物理接続を行うこと。

18. インターネット境界ネットワークを構成する要素は二重化し、経路、筐体いずれも単一障点がないように構成すること。
19. インターネットスイッチ C と 1000Baes-T または 1000Base-SX で接続し、1Gbps 以上の帯域を確保すること。
20. 各セキュリティ機能を使用した場合のスループットは 1.5Gbps 以上を確保できるように構成すること。
21. PMDA が運用しているリモートサービスの VPN ゲートウェイと IPsec VPN による接続を行うこと。
22. 可能な限り電源を二重化し、電源冗長を行うこと。

4.4.12.3.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、HA 状態確認、L3/L4 フィルタリング変更方法、URL フィルタリング設定変更方法」

4.4.12.4. インターネット境界ネットワーク D

4.4.12.4.1. 構成要件

1. 外部ネットワークからリモート接続インバウンド WAN を経由してリモート接続基盤システムのリモート VPN 装置、RDSH リバースプロキシに接続できるように構成すること。
2. ファイアウォール機能によるステートレスな L3/L4 フィルタリング機能を構成し、必要最低限の情報のみ外部ネットワークに公開する構成とすること。
3. リモート VPN 装置に接続したクライアント端末、RDSH リバースプロキシが内部ネットワークの必要なノードと通信可能になるように L3、L4 設定を行うこと。
4. リモート VPN 装置、RDSH リバースプロキシの L3 ゲートウェイとして構成すること。
5. 公開システムの 1IP アドレスごとに一つのフィルタルールを作成すること。同一フィルタルール内に複数の L4 条件を設定して良い。
6. 既存の遮断 IP アドレスを移行すること(この IP アドレスはインターネット境界ネットワーク A と同じ。)。運用中に遮断 IP アドレスを追加する際、定型的な手順で追加が可能になるよう手順を整備すること。
7. 公開システムのグローバル IP アドレスをプライベート IP アドレスに NAT すること。
8. L3/L4 フィルタリング機能の許可トラフィック、遮断トラフィックをファイアウォール管理サ

ーバに送信すること。

9. 装置・経路障害、冗長機能の状態変化を SNMP、Syslog で検出可能なように構成すること。製品の管理装置との連携でも良い。
10. インターネットスイッチ C と 1000Base-T または 1000Base-X で接続し、1Gbps 以上の帯域を確保すること。
11. コア L3 スイッチと 10GBase-SR で接続し、10Gbps 以上の帯域を確保すること。
12. L3/L4 フィルタリング機能は 2Gbps 以上のスループットを確保可能なこと。
13. 可能な限り電源を二重化し、電源冗長を行うこと。

4.4.12.4.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、HA 状態確認、L3/L4 フィルタ設定変更」

4.4.13. インターネット回線

4.4.13.1. 高可用性インバウンド WAN

4.4.13.1.1. 構成要件

1. 2 系統の回線が Active-Active で動作する冗長構成とすること。
2. 1 系統の回線障害が発生した際に公開システムに対する通信が自動的に継続されるように冗長設計を行うこと。
3. インターネット境界ネットワーク A と接続して公開システムがインターネットと通信できるように構成すること。
4. グローバル IP アドレスとプライベート IP アドレスの NAT に関する設計、設定を行うこと。
5. 回線終端装置をインターネットスイッチ A に接続すること。回線終端装置は 2 台で構成し、インターネットスイッチ A の異なる筐体にそれぞれ接続すること。

4.4.13.1.2. 保守要件

1. 回線に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.13.2. 広帯域インバウンド WAN

4.4.13.2.1. 構成要件

1. インターネットに接続するための通信経路を冗長構成とすること。
2. 1 系統の通信経路に障害が発生した際でも 2 系統側の回線を使用して通信を継続できるように構成し、公開システムに対する通信が継続可能となるような冗長設計を行うこと。
3. インターネット境界ネットワーク B と接続して公開システムがインターネットと通信できるように構成すること。
4. グローバル IP アドレスとプライベート IP アドレスの NAT に関する設計、設定を行うこと。
5. 回線終端装置をインターネットスイッチ B に接続すること。回線終端装置は 2 台で構成し、インターネットスイッチ B の異なる筐体にそれぞれ接続すること

4.4.13.2.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.13.3. 通常インバウンド WAN

4.4.13.3.1. 構成要件

1. インターネットに接続するための通信経路を冗長構成とすること。
2. 1 系統の通信経路に障害が発生した際でも 2 系統側の回線を使用して通信を継続できるように構成し、公開システムに対する通信が継続可能となるような冗長設計を行うこと。
3. インターネット境界ネットワーク B と接続して公開システムがインターネットと通信できるように構成すること。
4. グローバル IP アドレスとプライベート IP アドレスの NAT に関する設計、設定を行うこと。
5. 回線終端装置をインターネットスイッチ B に接続すること。回線終端装置は 2 台で構成し、インターネットスイッチ B の異なる筐体にそれぞれ接続すること。

4.4.13.3.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.13.4. 通常アウトバウンド WAN

4.4.13.4.1. 構成要件

1. インターネットに接続するための通信経路を冗長構成とすること。
2. 1 系統の通信経路に障害が発生した際でも 2 系統側の回線を使用して通信を継続できるように構成し、公開システムに対する通信が継続可能となるような冗長設計を行うこと。
3. インターネット境界ネットワーク C と接続して各ノードがインターネット接続できるように設計、設定を行うこと。
4. 回線終端装置をインターネットスイッチ C に接続すること。回線終端装置は 2 台で構成し、イ

ンターネットスイッチ C の異なる筐体にそれぞれ接続すること。

5. PMDA 側の送信元 IP アドレスの所属(内部ネットワーク、インターネット系ネットワーク)に応じて PMDA 側への L3 ルーティングのネクストホップアドレスを変えることで、内部系ネットワーク、インターネット系ネットワークが本回線を使用してインターネットに接続できるように構成すること。
6. PMDA のキャッシュ DNS サーバがインターネット上のリソースの名前解決を行えるようなキャッシュ DNS 機能を構成すること。

4.4.13.4.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.13.5. リモート接続インバウンド WAN

4.4.13.5.1. 構成要件

1. インターネットに接続するための通信経路を冗長構成とすること。
2. 1 系統の通信経路に障害が発生した際でも 2 系統側の回線を使用して通信を継続できるように構成し、公開システムに対する通信が継続可能となるような冗長設計を行うこと。
3. インターネット境界ネットワーク D と接続してインターネットからリモート VPN 装置、RDSH リバースプロキシに接続できるように設計、設定を行うこと。
4. 回線終端装置をインターネットスイッチ C に接続すること。回線終端装置は 2 台で構成し、インターネットスイッチ C の異なる筐体にそれぞれ接続すること。
5. グローバル IP アドレスとプライベート IP アドレスの NAT に関する設計、設定を行うこと。

4.4.13.5.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.14. 仮想基盤システム上のネットワーク

4.4.14.1. 仮想基盤ネットワーク管理サーバ

4.4.14.1.1. 構成要件

1. 仮想基盤システム上のネットワーク構成を管理できる管理サーバを構築すること。
2. 管理サーバは 3 台以上で冗長構成とすること。全 Active 構成とし、クライアントからの接続を負荷分散可能な構成とすること。

4.4.14.1.2. 保守要件

1. 仮想基盤システムの保守内容に準ずるものとする。

4.4.14.2. 仮想ルータ A

4.4.14.2.1. 構築要件

1. 作成する仮想ルータ A の数量、備えるリソースを PMDA と合意の上、設計すること。
2. OSPF により L3 経路情報を自動的に交換するように構成すること。
3. 2 台冗長構成とすること。冗長構成を踏まえた L3 経路設計を行うこと。
4. 冗長化した仮想ルータ A が同一の仮想基盤物理ホストに配置されないように構成すること。
5. 仮想マシンと仮想マシン連携物理サーバ(内部、公開両方)間の通信の L3 ネットワーク境界として動作するように構成すること。
6. L3/L4 ベースのファイアウォール機能が動作するように構成すること。

4.4.14.2.2. 保守要件

1. 仮想基盤システムの保守内容に準ずるものとする。

4.4.14.3. 仮想ルータ B

4.4.14.3.1. 構成要件

1. 作成する仮想ルータ B の数量、備えるリソースを PMDA と合意の上、設計すること。
2. OSPF により L3 経路情報を自動的に交換するように構成すること。
3. 冗長構成とすること。
4. L3/L4 ベースのファイアウォール機能が動作するように構成すること。

4.4.14.3.2. 保守要件

1. 仮想基盤システムの保守内容に準ずるものとする。

4.4.15. 内部ファイアウォール A

4.4.15.1. 構成要件

1. 内部ネットワークと運用管理ネットワークの L3、L4 境界となるように構成すること。
2. Active-Standby による 2 台冗長構成とすること。
3. コア L3 スイッチを 10GBase-SR にて 2 本で接続し、20Gbps の帯域を確保すること。
4. 運用管理ネットワークとその他のネットワークの通信を必要最低限とするようにファイアウォールポリシを構成すること。
5. OSPF を構成し、動的に L3 経路情報を交換できるように構成すること。
6. 広告不要な L3 経路情報がある場合、経路フィルタを行うこと。
7. 必要であれば再配布設定を行うこと。
8. トラフィックログをファイアウォール管理サーバに送信すること。
9. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。

10. 冗長構成の状態に変化があった時、その変化内容を通知する方法を設計すること。
11. データセンタの 19 インチラックに搭載すること。
12. 電源を二重化し、電源冗長を行うこと。

4.4.15.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、HA 状態確認、OSPF 状態確認」

4.4.16. 内部ファイアウォール B

4.4.16.1. 構成要件

1. 公開ネットワークの物理サーバの通信を制御するための境界として構成すること。
2. Active-Standby による 2 台冗長構成とすること。
3. 本装置とコア L3 スイッチを 10GBase-SR で接続し、10Gbps の帯域を確保すること。
4. サーバ接続 L2 スイッチ D と 10GBase-SR で接続し、10Gbps の帯域を確保すること。
5. 独立したルーティングテーブルを持つ仮想ファイアウォールを 5 個構成すること。異なる仮想ファイアウォールが物理インターフェースを共有できない場合、必要な物理接続を用意すること。ただし、この場合サーバ接続 L2 スイッチ D に対する接続は仮想ファイアウォール 1 個あたり 2Gbps の帯域を確保する構成で良い。サーバ接続 L2 スイッチ D のポート数が不足する場合、サーバ接続 L2 スイッチ D の数量を増やすことで対応すること。
6. インターネット境界ネットワーク A、インターネット境界ネットワーク B を経由して公開物理サーバにアクセスできるように L2、L3 ネットワークを構成すること。
7. 各仮想ファイアウォールではゾーンを作成し業務システムの通信を制御すること。
8. トラフィックログをファイアウォール管理サーバに送信すること。ただし、一部の運用トラフィックのみのログは対象外とする。対象外ポリシは PMDA と合意の上決定すること。
9. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
10. 冗長構成の状態に変化があった時、その変化内容を通知する方法を設計すること。
11. データセンタの 19 インチラックに搭載すること。
12. 電源を二重化し、電源冗長を行うこと。

4.4.16.2. 保守用件

1. 平日 9 時～17 時オンサイト保守を行うこと。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、ファイアウォールポリシの設定変更方法」

4.4.17. 内部ファイアウォール C

4.4.17.1. 構成要件

1. 内部ネットワークの物理サーバの通信を制御するための境界として構成すること。
2. Active-Standby による 2 台冗長構成とすること。
3. 本装置とコア L3 スイッチを 10GBase-SR で接続し、10Gbps の帯域を確保すること。
4. サーバ接続 L2 スイッチ D と 10GBase-SR で接続し、10Gbps の帯域を確保すること。
5. 独立したルーティングテーブルを持つ仮想ファイアウォールを 5 個構成すること。異なる仮想ファイアウォールが物理インターフェースを共有できない場合、必要な物理接続を用意すること。ただし、この場合サーバ接続 L2 スイッチ D に対する接続は仮想ファイアウォール 1 個あたり 2Gbps の帯域を確保する構成で良い。サーバ接続 L2 スイッチ D のポート数が不足する場合、サーバ接続 L2 スイッチ D の数量を増やすことで対応すること。
6. 各仮想ファイアウォールではゾーンを作成し業務システムの通信を制御すること。
7. トラフィックログをファイアウォール管理サーバに送信すること。ただし、一部の運用トラフィックのみのログは対象外とする。対象外ポリシは PMDA と合意の上決定すること。
8. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
9. 冗長構成の状態に変化があった時、その変化内容を通知する方法を設計すること。
10. データセンタの 19 インチラックに搭載すること。
11. 電源を二重化し、電源冗長を行うこと。

4.4.17.2. 保守用件

1. 平日 9 時～17 時オンサイト保守を行うこと。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、ファイアウォールポリシの設定変更方法」

4.4.18. 内部ファイアウォール D

4.4.18.1. 構成要件

1. 新霞が関ビルの設置場所 1 に設置し、新霞が関ビルとデータセンタのネットワーク境界として構成すること。
2. Active-Standby による 2 台冗長構成とすること。
3. 既設 L2 スイッチ A と 1000Base-T で接続し、データセンタ側のインターフェースで 2Gbps の帯域を確保すること。
4. 既設 L2 スイッチ A と 1000Base-T で接続し、新霞が関ビルの既設 LAN 側のインターフェースで 2Gbps の帯域を確保すること。
5. 独立したルーティングテーブルを持つ仮想ファイアウォールを 3 個作成し、内部系、運用管理系、インターネット系の仮想ファイアウォールとして構成すること。異なる仮想ファイアウォールが物理インターフェースを共有できない場合、必要な物理接続を用意すること。その場合、既設 L2 スイッチ A の使用可能ポート数が不足することから、既設 L2 スイッチ A と内部ファイアウォール D の間に L2 スイッチを追加すること。この L2 スイッチが単一障害点にならないように構成すること。
6. 各仮想ファイアウォールではゾーンを作成し通信を制御すること。
7. トラフィックログをファイアウォール管理サーバに送信すること。ただし、一部の運用トラフィックのみのログは対象外とする。対象外ポリシは PMDA と合意の上決定すること。
8. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
9. 冗長構成の状態に変化があった時、その変化内容を通知する方法を設計すること。
10. 新霞が関ビルの設置場所 1 の既設 19 インチラックに搭載すること。
11. 電源を二重化し、電源冗長を行うこと。

4.4.18.2. 移行要件

1. 本調達の内部ファイアウォール D に相当する既設ファイアウォール(Fortinet Fortigate501E)のポリシを参考に、必要なポリシを移行すること。
2. 一部の業務システムを収容するためのゾーンがあり、既存ネットワークのゾーンとのポリシ設定がある移行完了後、既設ファイアウォールをラックから取り外し、新霞が関ビル内の指定エリアに運ぶこと。あわせて不要になったネットワークケーブルを破棄すること。

4.4.18.3. 保守用件

1. 平日 9 時～17 時オンサイト保守を行うこと。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、ファイアウォールポリシの設定変更方法」

4.4.19. 内部ファイアウォール E

4.4.19.1. 構成要件

1. 関西支部に設置し、関西支部とデータセンタのネットワーク境界として構成すること。
2. Active-Standby による 2 台冗長構成とすること。
3. 既設 L2 スイッチ C と 1000Base-T で接続し、データセンタ側のインターフェースで 1Gbps の帯域を確保すること。
4. 既設 L2 スイッチ C と 1000Base-T で接続し、関西支部の既設 LAN 側のインターフェースで 1Gbps の帯域を確保すること。
5. 独立したルーティングテーブルを持つ仮想ファイアウォールを 3 個作成し、内部系、運用管理系、インターネット系の仮想ファイアウォールとして構成すること。異なる仮想ファイアウォールが物理インターフェースを共有できない場合、必要な物理接続を用意すること。
6. 各仮想ファイアウォールではゾーンを作成し通信を制御すること。
7. トラフィックログをファイアウォール管理サーバに送信すること。ただし、一部の運用トラフィックのみのログは対象外とする。対象外ポリシは PMDA と合意の上決定すること。
8. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
9. 冗長構成の状態に変化があった時、その変化内容を通知する方法を設計すること。
10. 関西支部の既設 19 インチラックに搭載すること。
11. 電源を二重化し、電源冗長を行うこと。

4.4.19.2. 移行要件

1. 本調達の内部ファイアウォール E に相当する既設ファイアウォール(Paloalto PA220)のポリシを参考に、必要なポリシを移行すること。一部の業務システムを収容するためのゾーンがあり、既存ネットワークのゾーンとのポリシ設定がある移行完了後、既設ファイアウォールをラックから取り外し、関西支部内の指定エリアに運ぶこと。あわせて不要になったネットワークケーブルを破棄すること。

4.4.19.3. 保守用件

1. 平日 9 時～17 時オンサイト保守を行うこと。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、ファイアウォールポリシの設定変更方法」

4.4.20. 内部ファイアウォール F

4.4.20.1. 構成要件

1. リモート接続基盤システム上の VDI の L3 ゲートウェイとなるように構成すること。
2. Active-Standby による 2 台冗長構成とすること。
3. サーバ接続 L2 スイッチ F と 10GBase-SR で接続し、10Gbps の帯域を確保すること。
4. 独立したルーティングテーブルを持つ仮想ファイアウォールを 2 個作成し、内部系、インターネット系の仮想ファイアウォールとして構成すること。異なる仮想ファイアウォールが物理インターフェースを共有できない場合、必要な物理接続をそれぞれの仮想ファイアウォールで用意すること。
5. トラフィックログをファイアウォール管理サーバに送信すること。ただし、一部の運用トラフィックのみのログは対象外とする。対象外ポリシは PMDA と合意の上決定すること。
6. リモート接続仮想基盤システム上の VDI 向けの DHCP リレーを構成すること。
7. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
8. 冗長構成の状態に変化があった時、その変化内容を通知する方法を設計すること。
9. データセンタの 19 インチラックに搭載すること。
10. 電源を二重化し、電源冗長を行うこと。

4.4.20.2. 保守用件

1. 平日 9 時～17 時オンサイト保守を行うこと。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

5. 以下の内容が分かる手順書を作成すること。「ログイン、アカウント追加・削除、ファイアウォールポリシの設定変更方法」

4.4.21. HTTP トラフィック分離装置

4.4.21.1. 構成要件

1. リモート接続仮想基盤システム上の VDI A、B が本装置を透過プロキシとして使用できるよう構成すること。
2. VDI A、VDI B の通信が本装置を経由するように L2、L3 設定を行うこと。
3. コア L3 スイッチを経由して通常アウトバウンド WAN を使用してインターネットに接続できるように L2、L3 設定を行うこと。
4. Microsoft 社が公開している Microsoft365 サービスの宛先 FQDN、IP アドレスを自動的に取得、通信制御の設定に利用可能な構成とすること。
5. 本装置を通過するトラフィックの宛先が Microsoft365 サービスの場合、送信元 IP アドレスを NAT 変換すること。NAT 変換対象の送信元 IP アドレスは VDI A のみとすること。
6. アクセス先 Microsoft365 テナント制限のため HTTP ヘッダ情報を HTTP 通信に挿入すること。
7. HTTP ヘッダ情報挿入に必要な SSL 復号化、暗号化を本装置上で実施するよう構成すること。
8. HTTP アクセスログを汎用 Syslog サーバに送信すること。
9. 独立したルーティングテーブルを持つ仮想的な装置を構成すること。
10. 仮想的な装置は VDI A、VDI B 用に構成すること。
11. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
12. Active-Standby で動作する冗長構成とすること。
13. 冗長構成の状態に変化があった時、その変化内容を通知する方法を設計すること。
14. データセンタの 19 インチラックに搭載すること。
15. 電源を二重化し、電源冗長を行うこと。

4.4.21.2. 保守用件

1. 平日 9 時～17 時オンサイト保守を行うこと。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 以下の内容が分かる手順書を作成すること。「HA 状態確認、HTTP ヘッダ挿入設定の変更方法、通信制御設定の変更方法」

4.4.22. 閉域 WAN 回線

4.4.22.1. 閉域 WAN 回線 A

4.4.22.1.1. 構成要件

1. 新霞が関ビルとデータセンタを接続するように構成すること。
2. 1 系統の通信経路に障害が発生した際でも 2 系統側の回線を使用して通信を継続できるように構成し、公開システムに対する通信が継続可能となるような冗長設計を行うこと。
3. 回線終端装置を新霞が関ビルの設置場所 1 に設置し、既設 L2 スイッチ A と接続すること。
4. 回線終端装置をデータセンタの閉域 WAN L2 スイッチと接続すること。
5. 内部ファイアウォール D の内部系仮想ファイアウォール、インターネット系仮想ファイアウォールのトラフィックを転送するように構成すること。

4.4.22.1.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.22.2. 閉域 WAN 回線 B

4.4.22.2.1. 構成要件

1. 新霞が関ビルとデータセンタを接続するように構成すること。
2. 回線終端装置を新霞が関ビルの設置場所 1 に設置し、既設 L2 スイッチ A と接続すること。
3. 回線終端装置をデータセンタの閉域 WAN L2 スイッチと接続すること。
4. 内部ファイアウォール D の運用管理系仮想ファイアウォールのトラフィックを転送するように構成すること。

4.4.22.2.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.22.3. 閉域 WAN 回線 C

4.4.22.3.1. 構成要件

1. 関西支部とデータセンタを接続するように構成すること。
2. 関西支部の既設ラックに設置し、既設 L2 スイッチ C と接続すること。
3. 回線終端装置をデータセンタの閉域 WAN L2 スイッチと接続すること。
4. 内部ファイアウォール E の全ての仮想ファイアウォールのトラフィックを転送するように構成すること。

4.4.22.3.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.22.4. 閉域 WAN 回線 D

4.4.22.4.1. 構成要件

1. データセンタと現行データセンタを接続するように構成すること。
2. 1 系統の通信経路に障害が発生した際でも 2 系統側の回線を使用して通信を継続できるように構成し、公開システムに対する通信が継続可能となるような冗長設計を行うこと回線終端装置をデータセンタの閉域 WAN L2 スイッチと接続すること。
3. 回線終端装置を現行データセンタの既設ラックに設置すること。
4. 現行データセンタの L3 スイッチと 1000Base-T で接続すること。移行状況によって併設用 L2 スイッチに接続しなおすこと。
5. 現行データセンタの L3 スイッチの 10GBase-R インターフェースを 1000Base-T インターフェースとして使用可能なトランシーバを必要数分構成に含めること。L3 スイッチのモデルは HPE 5940 である。

4.4.22.4.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.22.5. 閉域 WAN 回線 E

4.4.22.5.1. 構成要件

1. データセンタと現行データセンタを接続するように構成すること。
2. 回線終端装置を現行データセンタの既設ラックに設置すること。
3. 現行データセンタの L3 スイッチと 1000Base-T で接続すること。移行状況によって併設用 L2 スイッチに接続しなおすこと。
4. 現行データセンタの L3 スイッチの 10GBase-R インターフェースを 1000Base-T インターフェースとして使用可能なトランシーバを必要数分構成に含めること。L3 スイッチのモデルは HPE 5940 である。
5. 2025 年 12 月 31 日まで稼働できるように構成すること。

4.4.22.5.2. 保守要件

1. 通信に障害が発生した際、メールや電話で PMDA に連絡を行うこと。

4.4.23. 閉域 WAN L2 スイッチ

4.4.23.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L2 設定を行うこと。

4. 各閉域 WAN の回線終端装置を 1000Base-T で接続すること。
5. コア L3 スイッチと 10GBase-SR で接続し、20Gbps 以上の帯域を確保すること。
6. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
7. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
8. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
9. データセンタの 19 インチラックに搭載すること。

4.4.23.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.24. インターネットスイッチ A

4.4.24.1. 構成要件

1. 本装置をそれぞれ 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L２設定を行うこと。
4. 高可用性インバウンド WAN 回線の回線終端装置を 1000Base-T で接続すること。回線冗長のため回線終端装置が複数ある場合、スタックを構成する異なるインターネットスイッチに接続することで冗長性を確保すること。
5. インターネット境界ネットワーク A と 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
6. コア L3 スイッチと 1000Base-SX で接続し、2Gbps の帯域を確保すること。
7. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
8. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
9. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能

になるように構成すること。

10. データセンタの 19 インチラックに搭載すること。
11. 電源を二重化し、電源冗長を行うこと。

4.4.24.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.25. インターネットスイッチ B

4.4.25.1. 構成要件

1. 本装置をそれぞれ 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L２設定を行うこと。
4. 広帯域インバウンド WAN 回線、通常インバウンド WAN 回線の回線終端装置を 1000Base-T で接続すること。回線冗長のため回線終端装置が複数ある場合、スタックを構成する異なるインターネットスイッチに接続することで冗長性を確保すること。
5. インターネット境界ネットワーク B と 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
6. コア L3 スイッチと 1000Base-SX で接続し、2Gbps の帯域を確保すること。
7. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
8. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
9. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
10. データセンタの 19 インチラックに搭載すること。
11. 電源を二重化し、電源冗長を行うこと。

4.4.25.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.26. インターネットスイッチ C

4.4.26.1. 構成要件

1. 本装置をそれぞれ 2 台用意し、スタック構成とすること。
2. スタックを構成する本装置に対する各機器の物理接続は接続、筐体の冗長構成となるように構成すること。
3. 必要な L２設定を行うこと。
4. 通常アウトバウンド WAN 回線、リモート接続インバウンド WAN 回線の回線終端装置を 1000Base-T で接続すること。回線冗長のため回線終端装置が複数ある場合、スタックを構成する異なるインターネットスイッチに接続することで冗長性を確保すること。
5. インターネット境界ネットワーク C と 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
6. インターネット境界ネットワーク D と 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
7. コア L3 スイッチと 1000Base-SX で接続し、2Gbps の帯域を確保すること。
8. リンクアグリゲーションの構成では接続装置のリンクアグリゲーション設定を考慮し、トラフィックがなるべく分散されるように構成すること。
9. 装置への管理ログインイベントを汎用 Syslog サーバに Syslog 送信できるように構成すること。
10. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
11. データセンタの 19 インチラックに搭載すること。
12. 電源を二重化し、電源冗長を行うこと。

4.4.26.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最

新設定情報の保持は PMDA が行うものとする。

3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容が分かるマニュアルを作成すること。「ログイン、アカウント追加・削除、物理インターフェース状態、リンクアグリゲーション設定、VLAN 設定、L2-L4 ベース ACL 設定、パケットミラーリング設定、装置の物理状態確認」

4.4.27. 汎用ロードバランサ

4.4.27.1. 構成要件

1. 必要な L2、L3 設定を行うこと。
2. Active-Standby による冗長構成とすること。
3. コア L3 スイッチと 10GBase-SR で接続し、10Gbps の帯域を確保すること。
4. サーバ接続 L2 スイッチ D と 10GBase-SR で接続し、10Gbps の帯域を確保すること。
5. 内部ネットワークの仮想マシン、各物理サーバのロードバランスが行えるように構成すること。
6. 筐体内に独立したルーティングテーブルを持つ仮想的なロードバランサを構成し、各物理サーバ、内部ネットワークの仮想マシンの管理管轄に応じて仮想的なロードバランサでロードバランスを行えるように構成すること。
7. ロードバランス設定には必要に応じてパーシステンス設定を行うこと。
8. ロードバランス対象のサーバの仮想 IP アドレスに対して、送信元 IP アドレスによるアクセス制限を行うこと。
9. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
10. 冗長構成の状態に変化があった時、その変化内容を通知する方法を設計すること。
11. データセンタの 19 インチラックに搭載すること。
12. 電源を二重化し、電源冗長を行うこと。

4.4.27.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 次の内容がわかる手順書を作成すること。「ログイン、アカウント追加・削除、HA 状態の確認方法」

4.4.28. 併設用ネットワーク機器

4.4.28.1. 併設用 L3 スイッチ

4.4.28.1.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. 併設用ファイアウォールの業務システム B 向けインターフェースと 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
3. 併設用ファイアウォールの業務システム C 向けインターフェースと 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
4. 併設用 L2 スイッチと 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
5. 業務システム A の 2 台の既存ネットワーク機器と 1000Base-SX で接続すること。
6. 業務システム B の 2 台の既存ネットワーク機器 A と 10GBase-SR で接続すること。
7. 業務システム B の 2 台の既存ネットワーク機器 B と 1000Base-T で接続すること。
8. 業務システム C の 2 台の既存ネットワーク機器と 10GBase-SR で接続すること。
9. 業務システム D の 2 台の既存ネットワーク機器 A と 1000Base-T で接続すること。併設用 L3 スイッチ 1 台あたり 2 ポートをこの接続に使用すること。
10. 業務システム D の 2 台の既存ネットワーク機器 B と 1000Base-T で接続すること。併設用 L3 スイッチ 1 台あたり 2 ポートをこの接続に使用すること。
11. 上記の接続とは別に 1000Base-LR 接続を行うために必要なトランシーバ 2 個、1000Base-T 接続を行うために必要なトランシーバ 12 個を用意すること。これらの接続は移行状況に応じて共用 LAN システムの既存ネットワーク機器と接続するために使用する。配線には併設用 L3 スイッチに敷設されている既存のケーブルを使用すること。
12. 各業務システムの内部システム、公開システムと通信できるように L2、L3 設定を行うこと。
13. 閉域 WAN 回線 D、閉域 WAN 回線 E を使用してデータセンタと通信できるように L2、L3 設定を行うこと。
14. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
15. 運用管理システムで構築するシステム sFlow コレクタサーバにネットワークフロー情報を送信するように構成すること。
16. 現行データセンタの 19 インチラックに搭載すること。
17. 電源を二重化し、電源冗長を行うこと。

4.4.28.1.2. 移行要件

1. 現行システムで運用している L3 スイッチ(現行 DCL3 スイッチ)を本装置に更新すること。ただし、基本的には本装置への交換は現行システムの移行対象システムが全て移行された後に行

うこと。

2. 現行システムの物理配線を継続利用するため、現行 DCL3 スイッチが設置されているラックに搭載すること。
3. 現行 DCL3 スイッチから取り外した現行システムの物理配線を本スイッチに接続すること。

4.4.28.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.4.28.3. 併設用ファイアウォール

4.4.28.3.1. 構成要件

1. 本装置を 2 台用意し、Active-Standby による冗長構成とすること。
2. ルーティングテーブルを独立して保持できる仮想的なファイアウォールを筐体内に 2 個作成し、それぞれ業務システム B と業務システム D の公開システム用に割り当てること。
3. 業務システム B 向けに併設用 L3 スイッチと 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
4. 業務システム D 向けに併設用 L3 スイッチと 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
5. 業務システム B の公開システムが通常インバウンド WAN を使用してインターネットからのアクセスを受け付けられるように L2、L3 設定を行うこと。
6. 業務システム D の公開システムが業務システムインターネット 1 と業務システムインターネット 2 を使用してインターネットからのアクセスを受け付けられるように L2、L3 設定を行うこと。
7. 業務システム D のインターネットからのアクセスに対する応答トラフィックは業務システム D の IP アドレスに応じて L3 ルーティングのネクストホップを業務システムインターネット 1 と業務システムインターネット 2 に変えるようなポリシベースルーティング設定を行うこと。
8. 仮想ファイアウォールの片方はインターネット回線にデータセンタのアウトバウンド回線を使用するように構成すること。もう片方の仮想ファイアウォールでは現行データセンタのインターネット回線を使用すること。現行インターネットのインターネット回線は複数あるため、業務システムの送信元 IP アドレスによって使用するインターネット回線を変えるようにポリシベースルーティングを構成すること。
9. 業務システム B、業務システム D の公開システムに対するインバウンドトラフィックには IPS

機能を適用すること。IPS 機能を適用する際、TLS により暗号化されたトラフィックの場合は本装置で復号化して適用し、適用後に再暗号化すること。

10. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
11. 運用管理システムで構築するシステム sFlow コレクタサーバにネットワークフロー情報を送信するように構成すること。
12. 現行データセンタの 19 インチラックに搭載すること。
13. 電源を二重化し、電源冗長を行うこと。

4.4.28.3.2. 移行要件

1. 現行システムのファイアウォールに設定されている通信遮断 IP アドレスのポリシ及びアドレスオブジェクトを移行すること。

4.4.28.3.3. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.4.28.4. 併設用 L2 スイッチ

4.4.28.4.1. 構成要件

1. 本装置を 2 台用意し、スタック構成とすること。
2. 併設用 L3 スイッチと 1000Base-T または 1000Base-SX で接続し、2Gbps の帯域を確保すること。
3. 閉域 WAN 回線 D、閉域 WAN 回線 E の回線終端装置を接続すること。
4. 業務システム D の業務インターネット回線 1 と業務インターネット回線 2 のネットワーク機器を 1000Base-T で接続すること。現行のラックに敷設されているケーブルを使用すること。
5. 各併設用ネットワーク機器が IP 接続可能な管理インターフェースを有している場合、併設用 L2 スイッチに接続すること。
6. 各要件を満たす L2 設定を行うこと。
7. 運用管理システムで構築するシステム状態監視サーバから SNMPv2 または v3 アクセスが可能になるように構成すること。
8. 現行データセンタの 19 インチラックに搭載すること。
9. 電源を二重化し、電源冗長を行うこと。

4.4.28.4.2. 保守要件

1. 平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.5. バックアップシステム

4.5.1. 構成要件

1. バックアップ取得対象のバックアップを取得可能なように構成すること。
2. 本調達で構成する仮想マシン、物理サーバのバックアップを取得するようにバックアップ設定を行うこと。
3. バックアップ可能な物理サーバの台数に制限がある場合、25 台のバックアップを取得可能な構成とすること。
4. 対象のバックアップ処理をバックアップ処理時間中に終えられるような性能を保持できるハードウェア構成とすること。
5. バックアップ対象のデータを保持できる記憶領域を含めること。
6. ランサムウェア対策として、バックアップデータの不審な更新を検出した場合にアラートを発行できるように構成すること。
7. 複数の業務システム管理者が使用することを前提としたバックアップ対象のグルーピング、権限の設計、構築を行うこと。
8. 管理対象のサーバ以外のバックアップ設定ができないような権限設定を行うこと。
9. 要件を満たすようにバックアップシステムをネットワーク接続すること。
10. 2 次バックアップデータにアクセス可能な送信元 IP アドレスが最小となるようにネットワーク制御を行うこと。
11. 新霞が関ビルに設置するハードウェア用に UPS を用意し、UPS の入力電源に異常が発生した際に可能な限り自動的に正常なシャットダウン処理を通して停止するように構成すること。処理を行うためのサーバ等が必要な場合、本番系仮想基盤システムを使用しても良い。新霞が関ビル仮想基盤システムの UPS の仕組みを流用しても良い

4.5.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。

3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.6. 業務認証基盤システム

4.6.1. Active Directory

4.6.1.1. 構成要件

1. 本番系仮想基盤システム上に構築すること。現行システムではドメインコントローラが 4 台あり、現行データセンタの 2 台、新霞が関ビルの印刷管理システム上の 2 台で構成されている。本システムでは業務仮想基盤システム上に 3 台のドメインコントローラを構築すること。既存の 4 台のドメインコントローラはドメインコントローラとして利用を継続する予定はない。
2. OS を最新化した上で、現行の Active Directory 構成を移行すること。

4.6.1.2. 移行要件

1. OS を Windows Server2022 で構成しなおすこと。移行方法の検討も行うこと。
2. FSMO の移行を行うこと。
3. 不要なドメインコントローラは降格作業を行うこと。
4. OU 設計を行うこと。OU 構成は基本的に現行踏襲とするが、本調達で導入するシステムの管理を行うためのシステム管理アカウントの OU 配置に制限がある場合、必要に応じて再設計を行うこと。
5. 既存 GPO の動作テストを行うこと。正常確認が PMDA でのみ行えるものもあるため、確認作業の役割分担を行い、漏れのないように確認すること。特にクライアント証明書の配布設定に関しては十分に注意すること。

4.6.1.3. 保守要件

1. 設計内容に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4.6.2. プライベート認証局

4.6.2.1. 構成要件

1. 本システムで構築するいずれかのドメインコントローラ上に構成すること。認証局はエンタープライズモードで構築すること。

4.6.2.2. 移行要件

1. 現行の認証局の発行済み証明書を移行すること。
2. 現行の認証局のハッシュアルゴリズム SHA-1 をよりセキュリティ強度の高いものに変更する

こと。これに伴い、プライベート認証局のドメイン範囲においてクライアント側に信頼するルート CA の追加が必要になる場合は GPO や手動追加により対応すること。尚、既存システムに対して手動追加が必要になる場合は PMDA が対応する。

4.6.2.3. 保守要件

1. 設計内容に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4.6.3. Azure AD Connect

4.6.3.1. 構成要件

1. 業務仮想基盤システム上にサーバを 1 台構築し、Azure AD Connect のインストールを行うこと。

4.6.3.2. 移行要件

1. 既存の Azure AD Connect による同期構成と矛盾なく同期が継続されるように移行作業を行うこと。

4.6.3.3. 保守要件

1. 設計内容に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4.6.4. SAML 認証基盤

4.6.4.1. 構成要件

1. IdP サーバは業務認証基盤システム上に構築すること。
2. IdP サーバを冗長構成とすること。必要であれば汎用ロードバランサを構成すること。
3. SP として Zabbix サーバを構築し、SAML 認証により Zabbix にログインできることを確認すること。この Zabbix サーバは本番運用では使用しない。
4. PMDA が構築する Zabbix サーバを SP として登録する際の技術的支援を行うこと。
5. 本調達で導入する sFlow コレクタを SP として登録する際の技術的支援を行うこと。

4.6.4.2. 保守要件

1. 設計内容に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4.6.5. 外部専門委員用 Active Directory

4.6.5.1. 構成要件

1. リモート接続仮想基盤システム上に構築すること。現行システムではドメインコントローラが 2 台あり、現行データセンタで稼働している。本システムでは 2 台のドメインコントローラを構築すること。
2. OS を最新化した上で、現行の Active Directory 構成を移行すること。

4.6.5.2. 移行要件

1. OS を Windows Server2022 で構成しなおすこと。移行方法の検討も行うこと。
2. FSMO の移行を行うこと。
3. 不要なドメインコントローラは降格作業を行うこと。
4. OU 設計を行うこと。OU 構成は基本的に現行踏襲とするが、本調達で導入するシステムの管理を行うためのシステム管理アカウントの OU 配置に制限がある場合、必要に応じて再設計を行うこと。
5. 既存 GPO の動作テストを行うこと。

4.7. 共通アプリケーション

4.7.1. メールシステム

4.7.1.1. メールフィルタシステム A

4.7.1.1.1. 構成要件

1. Microsoft365 Exchange Online と連携し、pmda.go.jp ドメインの送受信メールが本システムを経由して配送されるよう経路を設定すること。Microsoft365 Exchange Online 側に設定が必要な場合、実施すること。
2. 外部組織から pmda.go.jp ドメインへの配送メールに対してスパムメール検査、フィルタリングを行うこと。
3. 外部組織、pmda.go.jp ドメイン間における双方向の配送メールに対してマルウェアメール検査、フィルタリングを行うこと。
4. IP アドレス、メールアドレス、メールドメインを指定したメール受信拒否、許可を行うこと。
5. 本システムのフィルタリング処理にて受信拒否、廃棄、隔離された場合に、ユーザが検知可能なよう構成すること。
6. 本システム上の MTA は 2 台以上の冗長構成となっていること。
7. メール配送ログを 90 日間保持すること。
8. 本システムの管理画面に対するログイン、操作ログを 90 日間保持すること。
9. 5000 アカウント(メールアドレス)が本システムを利用可能な構成とすること。

4.7.1.1.2. 移行要件

1. pmda.go.jp ドメインのメールアドレスが本システムを利用する上で必要な DNS レコードを提示すること。DNS レコードの設定は PMDA が行う。
2. 現行システムのフィルタリングルールにて明示的に指定している受信拒否、許可の対象情報を移行すること。対象情報にはメールサーバ IP アドレス、メールアドレス、メールドメインが含まれる。移行対象は約 1600 件となっており、テキストベースでの提供が可能。
3. 現行システムに登録されている利用者アカウントを新システムにも登録すること。対象アカウントの情報は PMDA が提示する。

4.7.1.1.3. 保守要件

1. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
2. 日本語による問い合わせ対応が可能なこと。
3. 以下の内容が分かる手順書を作成すること。「アカウント登録・削除、フィルタルール作成・編集、削除、ログ確認方法」

4.7.1.2. メールフィルタシステム B

4.7.1.2.1. 構成要件

1. 現行システムにて利用中の Microsoft365 Exchange Online を使用すること。
2. 脅威ポリシは基本現行のままでよいが、本調達において新規導入するメールシステムに合わせた設定が必要な場合は構成すること。

4.7.1.2.2. 移行要件

1. 本調達において新規導入するメールシステムに合わせた配送経路を設定すること。

4.7.1.3. メール添付ファイル自動変換システム

4.7.1.3.1. 構成要件

1. Microsoft365 Exchange Online と連携し、pmda.go.jp ドメインから外部組織宛の送信メールが本システムを経由して配送されるよう経路を設定すること。Microsoft365 Exchange Online 側に設定が必要な場合、実施すること。メールフィルタシステム A から配送される構成としてもよい。
2. pmda.go.jp ドメインから外部組織への配送メールに添付されているファイルを自動的に外部ストレージへ保存、URL へ変換し宛先に送信すること。
3. ファイル格納先の外部ストレージは全体で 100GB 用意すること。
4. ファイル格納先へのアクセス URL は有効期限、アクセス可能回数を設定すること。
5. 格納したファイルに対するウイルスチェックを自動的に行うこと。

6. 特定の宛先、宛先ドメイン、もしくは差出人単位で添付ファイル自動変換処理をバイパスする方法を検討すること。
7. 本システム上の MTA は 2 台以上の冗長構成となっていること。
8. 5000 アカウント(メールアドレス)が本システムを利用可能な構成とすること。

4.7.1.3.2. 保守要件

1. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
2. 日本語による問い合わせ対応が可能なこと。
3. 以下の内容が分かる手順書を作成すること。「アカウント登録・削除、ログ確認方法」

4.7.1.4. インターネットリレーサーバ

4.7.1.4.1. 構成要件

1. インターネットリレーサーバは Postfix にて構成する。仮想マシンの作成、Postfix インストール、Postfix 設定は PMDA が行う。
2. サーバは 2 台構成とし、汎用ロードバランサによる負荷分散設定を行う。このロードバランスに関するネットワーク設定について、本システムでのネットワーク設計に合わせた支援を行うこと。ロードバランス設定自体は PMDA が行う。

4.7.1.5. 業務メールリレーサーバ(SMTP 認証有)

4.7.1.5.1. 構成要件

1. 業務メールリレーサーバ(SMTP 認証有) は Postfix にて構成する。仮想マシンの作成、Postfix インストール、Postfix 設定は PMDA が行う。
2. サーバは 2 台構成とし、汎用ロードバランサによる負荷分散設定を行う。このロードバランスに関するネットワーク設定について、本システムでのネットワーク設計に合わせた支援を行うこと。ロードバランス設定自体は PMDA が行う。

4.7.1.6. 業務メールリレーサーバ(SMTP 認証無)

4.7.1.6.1. 構成要件

1. 業務メールリレーサーバ(SMTP 認証無) は Postfix にて構成する。仮想マシンの作成、Postfix インストール、Postfix 設定は PMDA が行う。
2. サーバは 2 台構成とし、汎用ロードバランサによる負荷分散設定を行う。このロードバランスに関するネットワーク設定について、本システムでのネットワーク設計に合わせた支援を行うこと。ロードバランス設定自体は PMDA が行う。

4.7.1.7. 併設用業務メールリレーサーバ

4.7.1.7.1. 構成要件

1. 併設用業務メールリレーサーバは Postfix にて構成する。仮想マシンの作成、Postfix インストール、Postfix 設定は PMDA が行う。

4.7.1.7.2. 移行要件

1. 本サーバは現行の業務メールリレーサーバから IP アドレスを移行する。現行データセンタから本サーバに対しての通信には併設用ネットワーク機器を利用する。併設用ネットワーク機器を経由したメール配送経路確保のため L3 ルーティング設定を行うこと。

4.7.2. DNS システム

4.7.2.1. 内部 DNS システム

4.7.2.1.1. 構成要件

1. 内部 DNS システムは Windows 標準機能を利用し、Active Directory サーバ上に構成すること。
2. 管理するゾーンは pmda.go.jp ドメインとすること。
3. 各 Active Directory サーバ間でゾーン情報を同期、共有される構成とすること。
4. フォワード先は本システムで構成するキャッシュ DNS システムを指定すること。

4.7.2.1.2. 移行要件

1. pmda.go.jp ゾーンの移行を行うこと。

4.7.2.2. キャッシュ DNS システム

4.7.2.2.1. 構成要件

1. 通常アウトバウンド WAN 回線のオプション機能により提供されること。

4.7.2.2.2. 保守要件

1. サービス仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4.7.3. HTTP プロキシシステム

4.7.3.1. 構成要件

1. HTTP プロキシサーバはオープンソースのプロキシソフトウェア Squid を使用して PMDA が構築する。Squid をインストールした RHEL サーバ 2 台で構成し、汎用ロードバランサで負荷分散を行う。このロードバランスに関するネットワーク設定について、本システムでのネットワーク設計に合わせた支援を行うこと。ロードバランス設定自体は PMDA が行う。

4.7.4. ファイル共有システム

4.7.4.1. 構成要件

1. DFS 名前空間の設定を行うこと。DFS 名前空間は現行システムでは Active Directory に設定しているが、必ずしも Active Directory に設定する必要はない。
2. 各ファイルサーバは次に示す実効容量で構成すること。
   部門用ファイルサーバ : 20TB
   個人用ファイルサーバ(1 台あたり) : 40TB
   特定用途ファイルサーバ : 25TB
   システム資源ファイルサーバ : 10TB
3. 現行システムでは DFS 名前空間の設定により、クライアント端末では「¥¥ドメイン名¥DFS ルート」を指定することで共有対象ファイルサーバの共有フォルダが全て表示される形としている。本システム移行後でも現行とファイルパスを変えずに運用するため、同様の方法でアクセス可能なように構成すること。尚、新設するシステム資源ファイルサーバは別の DFS 名前空間で構成すること。
4. 本システムで構成するファイルサーバログ管理システムと連携するように構成すること。
5. Volume Shadow Copy Service を構成すること。取得したスナップショットを格納する専用領域を構成すること。
6. スナップショットは毎日 12 時 30 分に取得し、14 日前までの履歴を保持すること。

4.7.4.2. 移行要件

1. 既存のファイルサーバからパス構成を変えずにフォルダ、ファイルを移行すること。
2. アクセス権を現行システム同様となるように移行すること。
3. 既存のファイルサーバに設定されているファイル容量クオータを移行すること。

4.7.5. 印刷管理システム

4.7.5.1. 構成要件

1. プリントサーバとして 2 台の Windows Server を新霞が関ビル仮想基盤システム上に構築すること。
2. 複合機のドライバは PMDA が提供する。印刷テストも PMDA が行うが、印刷の挙動に問題がある場合はプリントサーバ側に問題がないか受注者が確認すること。

4.7.5.2. 移行要件

1. 2 台の Windows Server には異なる複合機が共有設定されている(冗長化はしていない)。その設定を移行すること。

4.7.5.3. 保守要件

1. 設計内容に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4.7.6. グループウェア

4.7.6.1. 移行要件

1. 現行のグループウェアを構成する Web サーバ 2 台、データベースサーバを V2V により移行すること。
2. 汎用ロードバランサでフロントエンド Web サーバ向けのロードバランス設定を行うこと。ロードバランス設定は単純な L4 ロードバランスで良い。Web サーバは HTTP(非暗号通信)で通信を行うように構成されている。

4.7.6.2. 保守要件

1. 移行内容に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。

4.7.7. 運用管理システム

4.7.7.1. システム状態監視サーバ

4.7.7.1.1. 作業要件

1. PMDA が Zabbix Zabbix で構成する。アプリケーションインストール、監視設定は PMDA が行う。Zabbix をインストールする OS も PMDA が構築するが、仮想基盤システムで設計した RHEL テンプレートを使用する。そのため本件に関する受注者作業は特にない。

4.7.7.1.2. 保守要件

1. Zabbix サーバ 2 台冗長構成、1 台構成を 6 組、合計 8 台を構成することを前提に、PMDA が直接ソフトウェアサポートにメール問い合わせが可能な保守体制を整えること。

4.7.7.2. sFlow コレクタサーバ

4.7.7.2.1. 構成要件

1. インターフェース監視の場合、500 インターフェースを監視可能なライセンスを納入すること。デバイス監視の場合、30 デバイスを監視可能なライセンスを納入すること。
2. 業務認証基盤システム上に OS 構築及び sFlow コレクタのインストールを行い、SAML 認証基盤の SP として登録しシングルサインオン動作が可能なことを確認すること。その他のアプリケーション設定は PMDA が行う。
3. 別途データベース製品が必要な場合、構成に含めること。

4.7.7.2.2. 保守要件

1. PMDA が直接ソフトウェアサポートにメール問い合わせが可能な保守体制を整えること。

4.7.7.3. Windows Server アップデート管理サーバ

4.7.7.3.1. 構成要件

1. 仮想マシンの作成、アプリケーションインストール、アプリケーション設定は PMDA が行うため、受注者の作業はない。

4.7.7.4. Linux OS パッケージ管理サーバ

4.7.7.4.1. 構成要件

1. Red Hat Satellite で 200 台のサーバを管理可能なライセンスを納入すること。
2. Satellite を稼働させる仮想マシンは本番系仮想基盤システム上に PMDA が構築する。
3. 本調達の Linux サーバで受注者が構築するサーバは、ソフトウェアパッケージを Satellite から入手できるように構成すること。実行が必要なスクリプトファイルや設定は PMDA から指示する。

4.7.7.4.2. 保守要件

1. PMDA が直接ソフトウェアサポートにメール問い合わせが可能な保守体制を整えること。

4.7.7.5. サーバ構成管理サーバ

4.7.7.5.1. 構成要件

1. Red Hat Ansible Tower で 200 台のサーバを管理可能なライセンスを納入すること。
2. Ansible Tower を稼働させる仮想マシンは本番系仮想基盤システム上に PMDA が構築する。
3. 本調達の Linux サーバで受注者が構築するサーバは、Ansible の Playbook が動作するように構成すること。実行が必要なスクリプトファイルや設定は PMDA から指示する。

4.7.7.5.2. 保守要件

1. PMDA が直接ソフトウェアサポートにメール問い合わせが可能な保守体制を整えること。

4.7.7.6. クライアント端末ログ管理サーバ

4.7.7.6.1. 構成要件

1. 現行システムで動作している SKY 社 Skysea Client View Light Edition で使用可能なサーバライセンスを納入すること。管理対象のクライアント数は 2700 とし、内 200 は VDI とすること。クライアントライセンスは 2025 年 12 月 31 日まで利用可能な分を構成に含めること。

4.7.7.6.2. 移行要件

1. 現行システムの仮想基盤上で動作しているサーバを本番系仮想基盤システムに V2V で移行すること。移行後のアプリケーション動作テストは PMDA が行う。現システムの構成は管理サーバ 1 台、ログサーバ 1 台、HTTP ゲートウェイサーバ 1 台で構成されている。

4.7.7.6.3. 保守要件

1. PMDA が直接ソフトウェアサポートにメール問い合わせが可能な保守体制を整えること。

4.7.7.7. クライアント端末状態管理サーバ

4.7.7.7.1. 構成要件

1. 現行システムで動作している MECM で使用可能なライセンスを納入すること。管理対象のクライアント数はデバイスベースで 2500 とすること。

4.7.7.7.2. 移行要件

1. 現行システムの仮想基盤上で動作しているサーバを本番系仮想基盤システムに V2V で移行すること。移行後のアプリケーション動作テストは PMDA が行う。現システムの構成は MECM サーバ 1 台で構成されている。

4.7.7.8. サーバマルウェア対策サーバ

4.7.7.8.1. 構成要件

1. 本番系仮想基盤システム、検証系仮想基盤システム、新霞が関ビル仮想基盤システム上の仮想マシン、物理サーバのマルウェア検出、駆除ができるように構成すること。
2. 仮想基盤システム上の仮想マシンについては仮想マシンの数量の制限なくマルウェア検査対象とできるように構成すること。
3. 物理サーバは 50 台を検査対象とできるようなライセンスを納入すること。
4. Windows Server2019、Windows Server2022、RHEL8、RHEL9 ごとに標準的なマルウェア検出除外設定を作成し、標準的な検出ポリシとして構成すること。
5. 変更監視対象ディレクトリを指定することで、変更監視が可能となるように構成すること。
6. マルウェア検出時、アラートとしてメール通知を行う構成とすること。

4.7.7.8.2. 保守要件

1. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
2. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
3. エージェント側で構成する場合、新規サーバ構築時に監視対象として追加するための手順書を作成すること。

4. マルウェア検出除外設定を行うための手順書を作成すること。

4.7.7.9. VDI マルウェア対策サーバ

4.7.7.9.1. 構成要件

1. リモート接続仮想基盤システムに構成する仮想マシンのマルウェア検出、駆除ができるように構成すること。
2. 仮想マシン 200 台を検査対象とできるようなライセンスを納入すること。
3. マルウェア検出時、アラートとしてメール通知を行う構成とすること。

4.7.7.9.2. 保守要件

1. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
2. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
3. マルウェア検出除外設定を行うための手順書を作成すること。

4.7.7.10. 汎用 Syslog サーバ

4.7.7.10.1. 構成要件

1. 仮想マシンの作成、アプリケーションインストール、アプリケーション設定は PMDA が行うため、受注者の作業はない。

4.7.7.11. ファイルサーバログ管理サーバ

4.7.7.11.1. 構成要件

1. 本システムで構成するファイル共有システムのファイルサーバのアクセスログを取得できるように構成すること。
2. ユーザ名、送信元 IP アドレス、日付、時間帯を条件として対象のファイル、フォルダのアクセスログを検索可能となるように構成すること。

4.7.7.12. ファイアウォール管理サーバ

4.7.7.12.1. 構成要件

1. ハードウェアアプライアンスとして導入すること。
2. コア L3 スイッチまたはサーバ接続 L2 スイッチ C と 1000Base-T または 1000Base-X または 10GBase-R で接続すること。接続経路は冗長化すること。
3. 本調達で導入するファイアウォールアプライアンスのトラフィックログを収集するように構成すること。
4. 本調達で導入するファイアウォールアプライアンスで使用するファイアウォールポリシオブジェクトの共通性を検討し、ファイアウォールポリシの作成・更新を効率的に行えるように構

成すること。

4.7.7.12.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.7.8. リモート接続仮想基盤システム

4.7.8.1. 構成要件

4.7.8.1.1. 基本構成

1. 本システム上で稼働する仮想マシンの要求リソース、最大稼働数、最大同時接続数を元に物理ホスト台数、搭載リソースを構成すること。また物理ホスト 1 台が障害等により停止した場合でも仮想マシンの最大数が縮小することなく、継続稼働可能とすること。
2. 物理ホストでは Hyper Threading を有効にすること。
3. 物理ホストに複数の HBA を搭載して FC スイッチとマルチパス接続し、通常ストレージを利用可能な構成とすること。
4. 物理ホストのネットワークインターフェースはサービス系、仮想基盤管理系で物理ポートを占有させること。それぞれのネットワークインターフェースは 10GBase-SR とすること。チーミングを行い、サーバ接続 L2 スイッチ F に冗長接続すること。
5. 物理ホストが障害等により停止した際、その物理ホストで稼働していた仮想マシンが自動的に別の物理ホストで動作を復旧するように構成すること。

4.7.8.1.2. 仮想マシンの CPU、メモリ

1. 各物理ホスト間で CPU、メモリの消費量がある程度均一となるよう、仮想マシンの配置先物理ホストが動的に変更される構成すること。

4.7.8.1.3. 仮想マシンの OS、基本構成

1. Windows10 Enterprise が 200 台作成可能なライセンスで構成すること。
2. Windows10 Enterprise が初期状態でインストールされた仮想マシンを 1 台作成すること。またその仮想マシンを VDI として展開できること。
3. OS のライセンス認証はライセンス認証サーバ(KMS)を利用可能なこと。
4. 本調達で用意した OS は既存の Volume Licensing Service Center にて管理し、製品ダウンロードが可能なようアカウント統合を行うこと。

5. 仮想マシンは VDI マルウェア対策サーバにて管理すること。また VDI 展開後の OS であってもマルウェア対策機能が稼働すること。
6. 仮想マシンを VDI として構成する際の GPO、KMS、ユーザプロファイル管理サーバ、DHCP サーバは PMDA が作成する。
7. リモート接続 VPN 装置を経由してインターネットから VDI へ接続できること。
8. VDI から Microsoft365 へ HTTP トラフィック分離装置を経由して接続できること。また接続先テナントの制御はホワイトリス形式とすること。
9. Microsoft Office(Word、Excel、PowerPoint、Outlook)が利用可能な永続版ライセンスを、70 台分用意すること。

4.7.8.1.4. ストレージアクセス構成

1. 通常ストレージで作成したリモート接続仮想基盤システム用の論理ボリュームに対応して、物理ホストから接続可能な構成とすること。

4.7.8.1.5. ネットワーク構成

1. 物理ホスト間で共有可能な仮想イーサネットスイッチを構成し、仮想イーサネットスイッチの操作を一度行うことで全物理ホストに設定が反映されるようにすること。
2. 仮想イーサネットスイッチの構成、所属させるネットワークは PMDA と協議の上で決定すること。

4.7.8.1.6. リモート VPN 装置構成

1. リモート接続 VPN 装置(NetMotion サーバ)を、本番系仮想基盤システム上に作成すること。
2. NetMotion サーバは 2 台構成とし、製品機能による冗長設定を行うこと。
3. NetMotion サーバは 150 台のデバイスを管理可能なライセンスで構成すること。
4. インターネットから NetMotion サーバへはインターネット境界ネットワーク D を介して接続できる構成とすること。FQDN は PMDA が策定する。
5. NetMotion サーバ接続時の認証方法はユーザ認証とすること。認証プロトコルは NTML バージョン 2 とすること。
6. 認証可能なユーザは Active Directory の特定セキュリティグループに所属するアカウントのみとすること。セキュリティグループ情報は PMDA が策定する。
7. NetMotion サーバに設定する接続ポリシは PMDA と協議の下、決定すること。
8. VPN 接続後にクライアントが接続する VDI 接続管理サーバを本番系仮想基盤システム上に作成すること。
9. VDI 接続管理サーバは 1 台構成とすること。
10. VDI に対して同時接続数が 150 接続許容可能なライセンスで構成すること。
11. VDI 接続管理サーバの FQDN に対して発行できる商用の証明書を用意すること。FQDN は

PMDA が策定する。

12. 商用証明書は本システムの稼働期間中、利用可能な有効年数分を購入すること。
13. VDI 接続管理サーバの設定は PMDA と協議の下、決定すること。

4.7.8.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 物理ホストのオンサイト対応時、ハイパーバイザのインストール、仮想基盤システムへの機能的な合流までを行うこと。仮想マシンの再配置が必要な場合、その操作は PMDA が行う。

4.7.9. 外部専門委員用リモート接続システム

4.7.9.1. 構成要件

1. RDSH リバースプロキシ(UAG)は本番系仮想基盤システム上に作成すること。
2. UAG は 1 台構成とすること。
3. インターネットから UAG へはインターネット境界ネットワーク D を介して接続できる構成とすること。FQDN は PMDA で策定する。
4. UAG の FQDN に対して発行できる商用の証明書を用意すること。
5. 商用証明書は本システムの稼働期間中、利用可能な有効年数分を購入すること。
6. RDSH 接続管理サーバを本番系仮想基盤システム上に作成すること。
7. RDSH 接続管理サーバは 1 台構成とすること。
8. RDSH 接続管理サーバは Active Directory で管理するドメインに参加すること。
9. RDSH 接続管理サーバに設定する各ポリシは PMDA と協議の下、決定すること。
10. RDSH サーバは本番系仮想基盤システム上に作成すること。OS バージョンは Windows Server2022 とすること。
11. RDSH サーバは 1 台構成とすること。
12. RDSH サーバは外部専門員用 Active Directory で管理するドメインに参加すること。
13. RDSH サーバに対して複数ユーザがリモートデスクトップ接続可能な構成とすること。
14. UAG を経由してインターネットから RDSH へリモートデスクトップ接続できること。
15. RDSH サーバに対して同時接続数が 30 接続許容可能なライセンスで構成すること。

4.7.9.1.1. 保守要件

1. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～

17 時に対応可能なこと。

2. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.7.10. メンテナンスシステム

4.7.10.1. メンテナンス用仮想マシン

4.7.10.1.1. 構成要件

1. 本番系仮想基盤システムに構築すること。作成するメンテナンス用仮想マシンの数は PMDA と協議の上決定すること。
2. Windows Server2022 で構成すること。
3. メンテナンス用仮想マシンは運用管理ネットワークに構築した仮想ルータ A、仮想ルータ B に接続すること。
4. メンテナンス用仮想マシンには 3 人以上が同時にリモートデスクトップ接続できるように構成すること。必要なライセンスサーバを構築すること。RDS CAL は PMDA が提供する。
5. メンテナンス用仮想マシンにはメンテナンス作業用のソフトウェアをインストールすること。インストールするソフトウェアは設計の際に PMDA から提供する。
6. メンテナンス用仮想マシンの仮想マシンテンプレートを作成すること。

4.7.10.2. 調査用物理サーバ

4.7.10.2.1. 構成要件

1. リモートパケット収集装置、コンソールインターフェース管理装置を集約できる物理サーバを構築すること。
2. OS には RHEL9 を使用すること。
3. GNOME 環境を構成すること。
4. 通常ストレージに FC 接続できるように、本番系 FC スイッチに接続すること。
5. 物理サーバとしてサーバ接続 L2 スイッチ D、サーバ接続 L2 スイッチ E に接続すること。
6. リモートパケット収集システムを接続するための NIC を搭載すること。この接続は最大 20Gbps の帯域を確保すること。
7. バックアップシステムにより調査用物理サーバのバックアップを取得すること。

4.7.10.2.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。

4.7.10.3. リモートパケット収集装置

4.7.10.3.1. 構成要件

1. 本調達で導入するコア L3 スイッチ、インターネット境界ネットワーク A の回線トラフィック、インターネット境界ネットワーク B の回線トラフィックのパケットを収集可能になるように構成すること。
2. 調査用物理サーバと接続し、各ネットワーク機器のミラーリングパケットを調査用物理サーバに保存可能となるように構成すること。
3. データセンタの 19 インチラックに搭載すること。

4.7.10.3.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること

4.7.10.4. コンソールインターフェース管理装置

4.7.10.4.1. 構成要件

1. 本調達で導入するハードウェアのうちデータセンタに設置するもののコンソールインターフェースを集約接続すること。
2. 調査用物理サーバから各機器のコンソールインターフェースにアクセスできるように構成すること。
3. 19 インチラックに搭載すること。集約対象の装置が搭載された全ラックに本装置を 1 台ずつ接続し、運用管理 L2 スイッチ B に 1000Base-T(100Base-TX も可)で接続すること。

4.7.10.4.2. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること

4.8. その他の移行作業

4.8.1. 業務システム 1 の移行

4.8.1.1. 移行要件

1. 対象の仮想マシンを V2V で移行すること。
2. TLS 復号化、再暗号化を行い、復号化されたトラフィックに対して IPS、WAF によるセキュリティチェックが正常に動作することを確認すること。

4.8.2. 業務システム 2 の移行

1. 対象の仮想マシンを V2V で移行すること。

4.8.3. 業務システム 3 の移行

1. 対象の仮想マシンを V2V で移行すること。

4.8.4. 業務システム 4 の移行

1. 対象の仮想マシンを V2V で移行すること。

4.8.5. 業務システム 5 の移行

2. 対象の仮想マシンを V2V で移行すること。

4.8.6. 移行用ストレージの構築

4.8.6.1. 構成要件

1. ストレージコントローラを冗長化すること。
2. 現行のストレージと同等の LUN 及びバックアップ領域の LUN(2 個程度を想定)を作成すること。
3. 作成した LUN を業務システム管理者が運用する仮想基盤システムが利用するために必要な情報を提供すること。
4. 正常にストレージを使用するために必要になる VMware ESXi 向けの VIB ソフトウェアがある場合はソフトウェア及びインストール手順を提供すること。
5. 現行データセンタに搭載されている 2 台の FC スイッチとマルチパス接続すること。FC スイッチと接続するためのケーブルは受注者が用意すること。

4.8.6.2. 移行要件

1. 移行用のストレージの設置スケジュールを検討し、現行データセンタのラックの空きスペースを考慮して設置すること。
2. 2025 年 12 月中に移行用ストレージのデータ削除作業を現行データセンタで行うこと。ただし、記憶媒体単位での消去作業を行わずにデータ消去を行える機能がある場合はその機能を使用

しても良い。

3. データ削除作業完了後、移行用ストレージを新霞が関ビルに搬送すること。搬送作業は 2025 年 12 月中に完了すること。

4.8.6.3. 保守要件

1. ハードウェアは平日 9 時～17 時オンサイト保守とすること。
2. オンサイト保守対応時、機器の設定情報、冗長構成に関する復元を行うこと。ただし機器の最新設定情報の保持は PMDA が行うものとする。
3. 製品仕様に関する技術的な問い合わせに対応すること。受付、対応時間は少なくとも 10 時～17 時に対応可能なこと。
4. ソフトウェアライフサイクルに関する PMDA からの問い合わせに回答すること。
5. 記憶媒体の障害及び障害予兆を検出するリモート監視体制を構築すること。これらの症状を検出した場合、リモート監視体制側から PMDA にメールまたは電話による連絡を行った上で記憶媒体の交換が可能であること。
6. 記憶媒体の障害時のような比較的定型的なオンサイト対応の場合、オンサイト対応を行う作業者は日本語によるコミュニケーションが可能であり、PMDA 担当者が機器の設置場所に赴かなくても、機器設置ロケーションの入館、保守対応が可能なこと。

4.9. その他の納入品

4.9.1. ソフトウェア

1. Windows Server2022 を 5 サーバ分納入すること。
2. RHEL9 を 4 サーバ分納入すること。
3. Microsoft SQL Server 2019 Enterprise Edition を 4 コア分納入すること。
4. Microsoft SQL Server 2019 Standard Edition を 3 サーバ分納入すること。
5. Windows Server2022 で動作する Oracle Database Enterprise Edition を 1 プロセッサライセンス分納入すること。2028 年 10 月 31 日までのソフトウェアサポートが可能なこと。
6. Microsoft Office(Word、Excel、PowerPoint、Outlook)が利用可能なライセンスを 10 サーバ分納入すること。インターネットオフラインで使用可能なライセンスとすること。

4.9.2. ネットワーク機器

1. コア L3 スイッチの 10GBase-R インターフェースで使用可能な 10GBase-SR トランシーバを 6 個、10GBase-LR トランシーバを 4 個納入すること。ハードウェア保守内容はコア L3 スイッチの内容に準ずる。
2. サーバ接続 L2 スイッチ A の 10GBase-R インターフェースで使用可能な 10GBase-SR トランシーバを 20 個、1000Base-T トランシーバを 4 個納入すること。ハードウェア保守内容はサーバ接続 L2 スイッチ A の内容に準ずる。

4.9.3. 動作確認用物理サーバ

1. 動作確認、テスト用を行うための動作確認用物理サーバを 2 台導入すること。物理サーバの要件は「5.7.2 動作確認用物理サーバ」の動作確認用物理サーバに記載の通りとする。ハードウェア保守は業務仮想基盤システムの物理ホストと同等とする。仮想基盤システムとして使用しないため、ハイパーバイザは不要とする。
2. 動作確認用物理サーバで使用できる 10GBase-SR トランシーバを 12 個構成に含めること。
3. 動作確認用物理サーバが物理サーバ用 FC スイッチ経由で高可用性ストレージにアクセスできるような HBA を 4 個及び FC スイッチの接続に必要なケーブルを構成に含めること。
4. OS には Windows Server2022 を構成に含めインストールすること。

4.9.4. メンテナンス部材

1. PS2 インターフェースに接続可能なキーボード、マウスを 1 式ずつ納品すること。
2. D-SUB インターフェースからサーバの映像を表示可能なディスプレイを 1 式納品すること。このディスプレイは持ち運びを想定しているため、15 インチ程度以下とすること。

4.9.5. テスト用ロードバランサ

1. 汎用ロードバランサと同じメーカのロードバランサをテスト用ロードバランサとして 2 台納入すること。
2. 2Gbps 以上の L7 ロードバランススループットを備えていること。
3. ハードウェアアプライアンスであること。
4. 平日 9 時～17 時センドバック保守を行うこと。
5. 運用期間中、サポート対象の全てのバージョンのソフトウェアの提供が可能なこと。
6. 標準的なソフトウェアバージョンアップ手順書を作成すること。

4.9.6. 物理サーバ用 KVM コンソール

1. 物理サーバラック用に物理サーバ 16 台の操作が可能な KVM コンソールを納入し、物理サーバラックに取り付けること。必要に応じて KVM スイッチを構成に含めること。
2. 物理サーバの映像出力インターフェースやマウス、キーボードと KVM コンソールを接続するためのケーブルを 16 本納入すること。

5. 構成品詳細要件

5.1. システムファシリティ

5.1.1. データセンタ

5.1.1.1. 設備要件

1. 鉄道等の公共交通機関を用いて新霞ヶ関ビルから 2 時間以内に到着できる距離であること。鉄道下車後の移動時間も含む。
2. 洪水、土砂崩れなどの自然災害が発生するおそれの無い場所であること。
3. 行政機関の洪水想定区域外であること。
4. 津波・高潮災害に対する危険が少ない場所であること。
5. 隣接地は急傾斜崩落防止区域外であること。
6. 1970 年以降、津波、高潮、集中豪雨による水害が発生していないこと。
7. N 値 50 相当の異常の地層を支持地盤としており、軟弱地盤のおそれがない場所であること。
8. 行政機関の液状化マップにより液状化発生区域外であることが証明可能なこと。
9. 現行建築基準法に指定される耐火・・延焼防止・耐震性能を有していること。
10. ラックを設置するスペースの床が免震構造であること。
11. 電力会社により特別高圧ループ受電方式、マルチスポット方式、もしくは本線・予備線方式により、複数継投で受電し冗長化対策が施されていること。
12. 電力会社での送電系統に障害が発生したことを想定し、予備電源として 24 時間相当の発電機用燃料を備蓄し、冗長化された自家発電装置により電源冗長が可能なこと。
13. 燃料業者との間で優先供給契約を締結しているか、24 時間分の燃料をデータセンタで保持していること。保管場所がデータセンタ敷地内でなくても良いが、30 ㎞以内の距離にあること。
14. 自家発電装置が稼働するまでの装置の電源供給として N+1 以上の冗長性を持った構成で無停電電源装置を備えていること。これにより、導入機器に対するデータセンタからの給電状況を考慮した無停電電源装置を別途導入する必要がないようにすること。自家発電装置は月 1 回の稼働テストを実施していること。
15. 自家発電装置が敷地内に設置されていること。
16. 導入機器を設置する部屋では火災発生時に導入機器に被害を与えないためのガス消火設備を有していること。ガス消火設備は消防法の基準に準拠していること。
17. 立地 100m 以内に消防法による指定量以上の危険製造設備、火薬製造設備、高圧ガス製造設備がないこと。
18. 内装材は不燃材または難燃材であること。
19. 排水管の配管ルートと機器設置室が分離され漏水対策が施されていること。
20. 機器設置室に漏水検知器が設置されていること。空調機設置室が別にある場合はそちらに漏水検知器が設置されていること。
21. 落雷防止としてデータセンタへの需給電源ケーブルの地中引き込み等の対策が施されている

こと。

22. 落雷による二次被害対策として、雷サージにより電気設備機器の破損防止が可能な構造になっていること。
23. マイクロ回線、レーダ施設、送電線、トランス、強電実験室等から離れており、電界及び磁界の被害を受ける恐れの少ない場所であること。
24. 塩害を受ける恐れの少ない場所であること。
25. 天井・照明器具等の落下防止措置が施されていること。建屋が免震構造の場合、本件は満たしていなくても良い。
26. データセンタの出入り口に施錠機能を有すること。
27. 入退館者の管理・監視を 24 時間 365 日実施していること。
28. 搬入設備は搬入専用の設備があること。
29. 機器設置室内はフリーアクセス床であること。天井配線、架空配線の場合はフリーアクセスでなくても構わないが、それによって本システムの構築、保守に物理的な制約が発生しないこと。

5.1.1.2. ラック要件

1. 機器を搭載するラックは EIA 規格に準拠した 19 インチラックであり、42U 程度の高さを備えていること。

5.1.2. 新霞が関ビル

5.1.2.1. ラック要件

1. 機器を搭載するラックは EIA 規格に準拠した 19 インチラックであり、22U 程度の高さを備えていること。
2. スタビライザによる転倒防止が可能なこと。

5.2. 業務仮想基盤システム

5.2.1. 本番系業務仮想基盤システム

5.2.1.1. 物理ホスト

1. 物理コアを 80 個以上使用可能なこと。複数プロセッサを使用する場合の数値で良い。Hyper Treading による増量は計算に含めない。
2. 物理メモリを 768GB 以上搭載すること。
3. 500GB 以上の実効ディスク容量を備えていること。
4. RAID5 相当のディスク障害耐性を備えていること。
5. ディスクに障害が発生した際に自動的にアクティブになるスペアディスクを搭載すること。
6. 物理ホストのサービスに影響を与えることなくディスク交換が可能なこと。
7. 1 インターフェースあたり 32Gbps 以上の帯域を持つファイバチャネルインターフェースを備えていること。2 ポート以上備えていること。

8. 10GBase-R に対応したネットワークインターフェースを 6 ポート以上備えていること。
9. 1000Base-T に対応したネットワークインターフェースを 2 ポート以上備えていること。
10. 物理ホストの状態を管理可能な専用 Web インターフェースを備えており、Web インターフェースから物理ホストの電源操作、コンソール操作が可能なこと。Web インターフェースにアクセスするための専用の物理ネットワークインターフェースを備えていること。
11. ハードウェア異常を SNMP 通知する仕組みを備えていること。
12. 外部 Syslog サーバに装置内イベントを送信可能なこと。
13. 19 インチラックに搭載可能なこと。
14. 200V 電源に対応しており、電源冗長が可能なこと。
15. 100V 電源に対応しており、電源冗長が可能なこと。

5.2.1.2. ハイパーバイザ

1. 汎用的なサーバにインストール可能なハイパーバイザ型の仮想マシンインフラストラクチャソフトウェアであること。
2. 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他の物理ホストに移動可能なこと。
3. 仮想基盤システム上に仮想的な L3 ネットワークを構成可能なこと。L3 ネットワークは物理 L3 ネットワークと IP 通信が可能なこと。
4. 仮想ネットワーク上では L3/L4 フィルタリングが可能なこと。フィルタリング設定は全物理ホストに同時に適用されること。
5. 仮想ネットワーク上には L4 ロードバランスが可能な仮想ロードバランサを構成可能なこと。

5.2.2. 検証系業務仮想基盤システム

5.2.2.1. 物理ホスト

1. 物理コアを 48 個以上使用可能なこと。複数プロセッサを使用する場合の数値で良い。Hyper Treading による増量は計算に含めない。
2. 物理メモリを 512GB 以上搭載すること。
3. 500GB 以上の実効ディスク容量を備えていること。
4. RAID5 相当のディスク障害耐性を備えていること。
5. ディスクに障害が発生した際に自動的にアクティブになるスペアディスクを搭載すること。
6. 物理ホストのサービスに影響を与えることなくディスク交換が可能なこと。
7. 1 インターフェースあたり 32Gbps 以上の帯域を持つファイバチャネルインターフェースを備えていること。2 ポート以上備えていること。
8. 10GBase-R に対応したネットワークインターフェースを 6 ポート以上備えていること。
9. 1000Base-T に対応したネットワークインターフェースを 2 ポート以上備えていること。
10. 物理ホストの状態を管理可能な専用 Web インターフェースを備えており、Web インターフェースから物理ホストの電源操作、コンソール操作が可能なこと。Web インターフェースにアク

セスするための専用の物理ネットワークインターフェースを備えていること。

11. ハードウェア異常を SNMP 通知する仕組みを備えていること。
12. 外部 Syslog サーバに装置内イベントを送信可能なこと。
13. 19 インチラックに搭載可能なこと。
14. 200V 電源に対応しており、電源冗長が可能なこと。

5.2.2.2. ハイパーバイザ

1. 本番系仮想基盤システムと同等機能を有すること。

5.2.3. 新霞が関ビル業務仮想基盤システム

5.2.3.1. 物理ホスト

1. 物理コアを 16 個以上使用可能なこと。複数プロセッサを使用する場合の数値で良い。Hyper Treading による増量は計算に含めない。
2. 物理メモリを 128GB 以上搭載すること。
3. 500GB 以上の実効ディスク容量を備えていること。
4. RAID5 相当のディスク障害耐性を備えていること。
5. ディスクに障害が発生した際に自動的にアクティブになるスペアディスクを搭載すること。
6. 物理ホストのサービスに影響を与えることなくディスク交換が可能なこと。
7. 1 インターフェースあたり 32Gbps 以上の帯域を持つファイバチャネルインターフェースを備えていること。2 ポート以上備えていること。
8. 物理ホストの状態を管理可能な専用 Web インターフェースを備えており、Web インターフェースから物理ホストの電源操作、コンソール操作が可能なこと。Web インターフェースにアクセスするための専用の物理ネットワークインターフェースを備えていること。
9. ハードウェア異常を SNMP 通知する仕組みを備えていること。
10. 外部 Syslog サーバに装置内イベントを送信可能なこと。
11. 19 インチラックに搭載可能なこと。
12. 100V 電源に対応しており、電源冗長が可能なこと。

5.2.3.2. ハイパーバイザ

1. 汎用的なサーバにインストール可能なハイパーバイザ型の仮想マシンインフラストラクチャソフトウェアであること。
2. 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他の物理ホストに移動可能なこと。

5.2.4. 共有ストレージ

5.2.4.1. 高可用性ストレージ 1、高可用性ストレージ 2

高可用性ストレージ 1 台あたりの要求性能を記載している。

1. コントローラは少なくとも 2 台で冗長化されており全アクティブで動作すること。コントローラ障害時の性能縮退影響は考慮しなくて良いが、障害の発生したコントローラは障害検出後すぐに停止可能なこと。
2. FC インターフェースを 8 ポート以上備え、8 台の FC スイッチからストレージアクセスが可能なこと。コントローラ 1 台の障害時でも 8 台の FC スイッチからストレージアクセスが可能なこと。
3. FC インターフェースの帯域幅は 32Gbps であること。
4. RAID6 相当のディスク障害耐性を備えていること。ディスク交換は活性交換が可能なこと。
5. ディスク暗号化が可能なこと。暗号化した状態で読み取り 100,000 以上、書き込み 60,000 以上の IOPS を同時に発揮可能な性能を備えていること。読み取り、書き込みの比率は 7:3 を想定している。
6. ストレージの状態を管理可能な GUI を備え、Web ブラウザから表示可能なこと。
7. 論理ボリュームごとにデータ容量、IOPS を HTTP で取得可能な API を備えていること。
8. 論理ボリュームをグルーピングし、グループ単位でデータ容量、IOPS を確認可能なこと。
9. ファームウェアのアップデート時、アップデート工程中にサービスを停止するコントローラは自動的に SAN から離脱可能なこと。アップデート完了後は自動的に SAN に復帰可能なこと。
10. 19 インチラックに搭載可能なこと。
11. 200V 電源に対応しており、電源冗長が可能なこと。

5.2.4.2. 通常ストレージ

1. コントローラは冗長化されていること。稼働系のコントローラ障害時は自動的にコントローラの系切替が行われること。
2. FC インターフェースを 4 ポート以上備え、4 台の FC スイッチからストレージアクセスが可能なこと。コントローラ 1 台の障害時でも 4 台の FC スイッチからストレージアクセスが可能なこと。
3. FC インターフェースの帯域幅は 32Gbps であること。
4. RAID6 相当のディスク障害耐性を備えていること。ディスク交換は活性交換が可能なこと。
5. ディスク暗号化が可能なこと。暗号化した状態で読み取り 40,000 以上、書き込み 20,000 以上を同時に発揮可能な IOPS 性能を備えていること。読み取り、書き込みの比率は 7:3 を想定している。
6. SSD によるキャッシュと HDD を組み合わせた記憶ディスク構成であること。全 SSD 構成でも良い。
7. 論理ボリュームをグルーピングし、グループ単位でデータ容量、IOPS を確認可能なこと。
8. ファームウェアのアップデート時、アップデート工程中にサービスを停止するコントローラは自動的に SAN から離脱可能なこと。アップデート完了後は自動的に SAN に復帰可能なこと。
9. 19 インチラックに搭載可能なこと。

10. 200V 電源に対応しており、電源冗長が可能なこと。

5.2.4.3. 検証用ストレージ

1. 高可用性ストレージと同等の機能を有すること。

5.2.4.4. 新霞が関ビル共有ストレージ

1. コントローラは冗長化されていること。稼働系のコントローラ障害時は自動的にコントローラの系切替が行われること。
2. iSCSI 接続が可能であり、コントローラごとに 10GBase-SR 2 本にて接続可能なこと。
3. RAID6 相当のディスク障害耐性を備えていること。ディスク交換は活性交換が可能なこと。
4. ディスク暗号化が可能なこと。暗号化した状態で読み取り 40,000 以上、書き込み 20,000 以上を同時に発揮可能な IOPS 性能を備えていること。
5. SSD によるキャッシュと HDD を組み合わせた記憶媒体構成であること。全 SSD 構成でも良い。
6. ファームウェアのアップデート時、アップデート工程中にサービスを停止するコントローラは自動的に SAN から離脱可能なこと。アップデート完了後は自動的に SAN に復帰可能なこと。
7. 19 インチラックに搭載可能なこと。
8. 100V 電源に対応しており、電源冗長が可能なこと。
9. 搭載しているディスク障害監視をリモートから行えること。障害発生時、障害予兆確認時には監視側からメールで PMDA に連絡するサービスを有すること。

5.2.5. 各 FC スイッチ

1. 32Gbps でリンク可能な FC インターフェースを 24 ポート以上備えていること。
2. FC インターフェースのエラーカウントを可視化可能なこと。
3. SNMPv2 に対応しており、FC インターフェースの死活状態を取得可能なこと。

5.3. IP ネットワークシステム

5.3.1. コア L3 スイッチ

1. 40GBase-R インターフェースを 8 ポート以上備えていること。
2. 10GBase-R インターフェースを 24 ポート以上備えていること。ただし、各ファイアウォール装置の仮想ファイアウォール機能の制限により必要ポート数が増えている場合、その追加ポート数を加えた数を要件とする
3. 1000Base-X インターフェースを 24 ポート以上備えていること。このポートはトランシーバを使用することで 1000Base-T インターフェースとしても使用可能なこと。ただし、各ファイアウォール装置の仮想ファイアウォール機能の制限により必要ポート数が増えている場合、その追加ポート数を加えた数を要件とする。

4. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
5. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
6. 筐体内に論理的な L3 スイッチを構成可能な VRF 機能を有すること。VRF ごとに MAC アドレステーブル、ルーティングテーブル、ARP テーブルを保持可能なこと。
7. VRF は 8 個以上作成可能なこと。
8. L3 経路情報を VRF ごとに 4000 個以上保持可能なこと。
9. 16000 個以上の MAC アドレスを VRF ごとに保持可能なこと。
10. ダイナミックルーティングとして OSPF、BGP、PIM-SM に対応していること。
11. グレースフルリスタート相当の機能を備えていること。
12. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
13. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
14. SNMPv2/v3 に対応していること。
15. sFlow または NetFlow に対応していること。
16. トラフィックミラーリングに対応していること。
17. 電源ユニットは冗長化されていること。

5.3.2. サーバ接続 L2 スイッチ A

1. 40GBase-R インターフェースを 2 ポート以上備えていること。
2. 10GBase-R インターフェースを 24 ポート以上備えていること。このインターフェースはトランシーバ接続により 1000Base-T インターフェースとしても利用可能なこと。
3. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
4. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
5. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
6. 16000 個以上の MAC アドレスを保持可能なこと。
7. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
8. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
9. SNMPv2/v3 に対応していること。
10. sFlow または NetFlow に対応していること。
11. 電源ユニットは冗長化されていること。

5.3.3. サーバ接続 L2 スイッチ B

1. 40GBase-R インターフェースを 2 ポート以上備えていること。
2. 10GBase-R インターフェースを 24 ポート以上備えていること。このインターフェースはトラン

シーバ接続により 1000Base-T インターフェースとしても利用可能なこと。

3. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
4. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
5. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
6. 16000 個以上の MAC アドレスを保持可能なこと。
7. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
8. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
9. SNMPv2/v3 に対応していること。
10. sFlow または NetFlow に対応していること。
11. 電源ユニットは冗長化されていること。

5.3.4. サーバ接続 L2 スイッチ C

1. 40GBase-R インターフェースを 2 ポート以上備えていること。
2. 10GBase-R インターフェースを 24 ポート以上備えていること。このインターフェースはトランシーバ接続により 1000Base-T インターフェースとしても利用可能なこと。
3. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
4. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
5. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
6. 16000 個以上の MAC アドレスを保持可能なこと。
7. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
8. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
9. SNMPv2/v3 に対応していること。
10. sFlow または NetFlow に対応していること。
11. 電源ユニットは冗長化されていること。

5.3.5. サーバ接続 L2 スイッチ D

1. 本調達で導入するネットワーク機器同士の接続以外に、10GBase-R インターフェースを 16 ポート以上使用可能であること。このインターフェースはトランシーバ接続により 1000Base-T インターフェースとしても利用可能なこと。
2. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
3. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能な

スイッチング容量を備えていること。

4. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
5. 16000 個以上の MAC アドレスを保持可能なこと。
6. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
7. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
8. SNMPv2/v3 に対応していること。
9. sFlow または NetFlow に対応していること。
10. 電源ユニットは冗長化されていること。

5.3.6. サーバ接続 L2 スイッチ E

1. 本調達で導入するネットワーク機器同士の接続以外に、10GBase-R インターフェースを 16 ポート以上使用可能であること。このインターフェースはトランシーバ接続により 1000Base-T インターフェースとしても利用可能なこと。
2. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
3. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
4. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
5. 16000 個以上の MAC アドレスを保持可能なこと。
6. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
7. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
8. SNMPv2/v3 に対応していること。
9. sFlow または NetFlow に対応していること。
10. 電源ユニットは冗長化されていること。

5.3.7. サーバ接続 L2 スイッチ F

1. 10GBase-R インターフェースを 24 ポート以上備えていること。このインターフェースはトランシーバ接続により 1000Base-T インターフェースとしても利用可能なこと。
2. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
3. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
4. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
5. 16000 個以上の MAC アドレスを保持可能なこと。
6. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
7. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。

8. SNMPv2/v3 に対応していること。
9. sFlow または NetFlow に対応していること。
10. 電源ユニットは冗長化されていること。

5.3.8. サーバ接続 L2 スイッチ G

1. 10GBase-R インターフェースを 24 ポート以上備えていること。このインターフェースはトランシーバ接続により 1000Base-T インターフェースとしても利用可能なこと。
2. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
3. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
4. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
5. 16000 個以上の MAC アドレスを保持可能なこと。
6. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
7. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
8. SNMPv2/v3 に対応していること。
9. sFlow または NetFlow に対応していること。
10. 電源ユニットは冗長化されていること。

5.3.9. サーバ接続 L2 スイッチ H

1. 10GBase-R インターフェースを 12 ポート以上備えていること。このインターフェースはトランシーバ接続により 1000Base-T インターフェースとしても利用可能なこと。
2. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
3. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
4. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
5. 16000 個以上の MAC アドレスを保持可能なこと。
6. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
7. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
8. SNMPv2/v3 に対応していること。
9. sFlow または NetFlow に対応していること。
10. 電源ユニットは冗長化されていること。

5.3.10. サーバ接続 L2 スイッチ I

1. 10GBase-R インターフェースを 24 ポート以上備えていること。このインターフェースはトラ

ンシーバ接続により 1000Base-T インターフェースとしても利用可能なこと。

2. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
3. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
4. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
5. 16000 個以上の MAC アドレスを保持可能なこと。
6. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
7. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
8. SNMPv2/v3 に対応していること。
9. sFlow または NetFlow に対応していること。
10. 電源ユニットは冗長化されていること。

5.3.11. インターネット境界ネットワーク A

1. インターネット経由の不特定多数からのアクセスに備え、L3/L4 フィルタリング機能を有すること。
2. L3/L4 フィルタリングに使用するフィルタ対象の IP アドレスはインターネット境界ネットワーク A、B、C、D で共有でき、1 回の追加でそれぞれに反映されること。
3. IPS 機能を有し、主要な OS(Windows Server2016 以降、RHEL7 以降)・ミドルウェア(Web サーバ、メール配送サーバ)の脆弱性、プロトコルアノマリ、DoS、Botnet からのトラフィックを検出、遮断可能なこと。
4. IPS 機能に使用するシグネチャファイルは自動的に更新可能なこと。
5. シグネチャファイルが更新された際、そのことを示すログを Syslog 送信可能なこと。
6. IPS 機能の除外トラフィックを設定可能なこと。除外単位には送信元 IP アドレス、送信元ネットワークアドレス、宛先 IP アドレス、宛先ネットワークアドレス、シグネチャ ID を組み合わせて指定可能なこと。
7. IPS 機能により遮断された場合、そのことをログとして Syslog 送信可能なこと。
8. WAF 機能を有し、主要なミドルウェアの脆弱性を突いた攻撃の検出、遮断が可能なこと。
9. WAF 機能は少なくとも SQL インジェクション、クロスサイトスクリプティング、バッファオーバーフロー、ディレクトリトラバーサル、OS コマンドインジェクションの攻撃を検出可能なこと。検出可能な対象 OS として Windows Server2016 以降、RHEL7 以降に対応していること。検出可能なデータベースソフトウェアとして Microsoft SQL Server、Oracle Database、PostgreSQL、MySQL、MariaDB に対応していること。
10. TLS により暗号化された通信を復号化可能なこと。
11. IPS 機能、WAF 機能の適用対象トラフィックが TLS により暗号化されている場合、復号化した上で IPS 機能、WAF 機能を適用可能なこと。

12. TLS 復号化を行った後、宛先 IP アドレスに応じて再暗号化の有無を選択可能なこと。
13. ロードバランスが可能なこと。
14. ロードバランスアルゴリズムとして、ラウンドロビン、重みづけラウンドロビン、最小応答時間に基づくバランス、最小コネクション数に基づくバランスに対応していること。
15. ロードバランス制御には L4 ロードバランス、L7 ロードバランスが可能なこと。
16. ロードバランス機能において HTTP トラフィックの L7 リクエストを 1 秒当たり 450,000 件処理可能なこと。
17. ロードバランス機能において RSA による鍵長 2048 ビットの公開鍵使用時に TLS 通信におけるトランザクションを毎秒 25,000 件以上処理可能なこと。
18. ロードバランス機能において RSA による鍵長 2048 ビットの公開鍵使用時に TLS 通信におけるスループットを 5Gbps 以上備えていること。
19. IPS 機能、WAF 機能の遮断ログに送信元 IP アドレス、宛先 IP アドレス、該当シグネチャを示す情報を付記可能なこと。
20. L3/L4 フィルタリング、IPS、WAF、ロードバランス、TLS 復号化、TLS 暗号化の設定を行うための管理用 WebGUI を有すること。管理用 GUI は機能ごとに異なる画面でも良い。
21. ロードバランス、TLS 復号化、TLS 暗号化の設定を行う管理用 WebGUI では管理対象の業務システムのロードバランス設定はできないような管理画面の分割、権限設定が可能なこと。

5.3.12. インターネット境界ネットワーク B

1. インターネット経由の不特定多数からのアクセスに備え、L3/L4 フィルタリング機能を有すること。
2. L3/L4 フィルタリングに使用するフィルタ対象の IP アドレスはインターネット境界ネットワーク A、B、C、D で共有でき、1 回の追加でそれぞれに反映されること。
3. IPS 機能を有し、主要な OS(Windows Server2016 以降、RHEL7 以降)・ミドルウェア(Web サーバ、メール配送サーバ)の脆弱性、プロトコルアノマリ、DoS、Botnet からのトラフィックを検出、遮断可能なこと。
4. IPS 機能に使用するシグネチャファイルは自動的に更新可能なこと。
5. シグネチャファイルが更新された際、そのことを示すログを Syslog 送信可能なこと。
6. IPS 機能の除外トラフィックを設定可能なこと。除外単位には送信元 IP アドレス、送信元ネットワークアドレス、宛先 IP アドレス、宛先ネットワークアドレス、シグネチャ ID を組み合わせて指定可能なこと。
7. IPS 機能により遮断された場合、そのことをログとして Syslog 送信可能なこと。
8. WAF 機能を有し、主要なミドルウェアの脆弱性を突いた攻撃の検出、遮断が可能なこと。
9. WAF 機能は少なくとも SQL インジェクション、クロスサイトスクリプティング、バッファオーバーフロー、ディレクトリトラバーサル、OS コマンドインジェクションの攻撃を検出可能なこと。検出可能な対象 OS として Windows Server2016 以降、RHEL7 以降に対応しているこ

と。検出可能なデータベースソフトウェアとして Microsoft SQL Server、Oracle Database、PostgreSQL、MySQL、MariaDB に対応していること。

10. TLS により暗号化された通信を復号化可能なこと。
11. IPS 機能、WAF 機能の適用対象トラフィックが TLS により暗号化されている場合、復号化した上で IPS 機能、WAF 機能を適用可能なこと。
12. TLS 復号化を行った後、宛先 IP アドレスに応じて再暗号化の有無を選択可能なこと。
13. ロードバランスが可能なこと。
14. ロードバランスアルゴリズムとして、ラウンドロビン、重みづけラウンドロビン、最小応答時間に基づくバランス、最小コネクション数に基づくバランスに対応していること。
15. ロードバランス制御には L4 ロードバランス、L7 ロードバランスが可能なこと。
16. ロードバランス機能において HTTP トラフィックの L7 リクエストを 1 秒当たり 450,000 件処理可能なこと。
17. ロードバランス機能において RSA による鍵長 2048 ビットの公開鍵使用時に TLS 通信におけるトランザクションを毎秒 25,000 件以上処理可能なこと。
18. ロードバランス機能において RSA による鍵長 2048 ビットの公開鍵使用時に TLS 通信におけるスループットを 15Gbps 以上備えていること。
19. IPS 機能、WAF 機能の遮断ログに送信元 IP アドレス、宛先 IP アドレス、該当シグネチャを示す情報を付記可能なこと。
20. L3/L4 フィルタリング、IPS、WAF、ロードバランス、TLS 復号化、TLS 暗号化の設定を行うための管理用 WebGUI を有すること。管理用 GUI は機能ごとに異なる画面でも良い。
21. ロードバランス、TLS 復号化、TLS 暗号化の設定を行う管理用 WebGUI では管理対象の業務システムのロードバランス設定はできないような管理画面の分割、権限設定が可能なこと。
22. ロードバランス機能において、現行システムで使用している aFlex が利用可能なこと。

5.3.13. インターネット境界ネットワーク C

1. HTTP、HTTPS トラフィックに関する URL フィルタリング機能を有すること。
2. URL フィルタリング機能はフィッシングサイト等の悪意あるサイトに対するアクセスをブロック可能なこと。
3. URL フィルタリングに使用するシグネチャは自動更新可能なこと。
4. URL フィルタリングを適用しない HTTP、HTTPS トラフィックを宛先 IP アドレス、送信元 IP アドレスの情報に基づいて指定可能なこと。
5. URL フィルタリングでブロックされた場合、ユーザの Web ブラウザにブロックされたことを示す画面を表示可能なこと。画面に表示するメッセージはカスタマイズ可能なこと。
6. 通信先のグローバル IP アドレスのリスク評価が可能なこと。高リスク IP アドレスとして判定されたことを視覚的に把握可能なこと。高リスク IP アドレスとの通信が発生した際にメールまたは SNMP Trap アラート通知を設定可能なこと。

7. 各機能を使用した場合にスループットを 1.5Gbps 以上確保可能なこと。

5.3.14. インターネット回線

5.3.14.1. 高可用性インバウンド WAN

1. 300Mbps の帯域が保証されていること。
2. 回線は ISP2 系統で冗長構成になっており、Active-Active で動作すること。必ずしも PMDA に複数系統のグローバル IP アドレスを提供する必要はなく、WAN 回線側で障害時のフェールオーバ動作による変更対応を完結できること。ただし、十分に信頼性の高い ISP である場合、ISP は 1 系統としても良い。この場合、東日本、西日本の IX に接続しており、東日本の IX の接続帯域が 800Gbps 以上であること。インターネットスイッチ A との物理的なネットワーク接続は二重化されていること。
3. PMDA が公開システム向けにグローバル IP アドレスを 20 個以上使用できること。ネットワーク機器に設定するルーティング用の IP アドレスはこの数に含めない。

5.3.14.2. 広帯域インバウンド WAN

1. 500Mbps の帯域が保証されていること。
2. 回線は冗長化されていること。
3. インターネットスイッチ B との物理的なネットワーク接続は二重化されていること。
4. PMDA が公開システム向けにグローバル IP アドレスを 10 個以上使用できること。ネットワーク機器に設定するルーティング用の IP アドレスはこの数に含めない。

5.3.14.3. 通常インバウンド WAN

1. 300Mbps の帯域が確保されていること。
2. 回線は冗長化されていること。
3. インターネットスイッチ B との物理的なネットワーク接続は二重化されていること。
4. PMDA が公開システム向けにグローバル IP アドレスを 30 個以上使用できること。ネットワーク機器に設定するルーティング用の IP アドレスはこの数に含めない。

5.3.14.4. 通常アウトバウンド WAN

1. 400Mbps の帯域が保証されていること。
2. 回線は冗長化されていること。
3. インターネットスイッチ C との物理的なネットワーク接続は二重化されていること。
4. アウトバウンド通信を行うにあたり、送信元 NAT 等に使用できるグローバル IP アドレスを 10 個以上備えていること。
5. PMDA の送信元 IP アドレスに応じて異なるネクストホップのスタティックルートを設定可能なこと。

6. PMDA のキャッシュ DNS サーバからの DNS クエリに応答可能なキャッシュ DNS 機能を備えていること。
7. キャッシュ DNS 機能はインターネット上の FQDN の名前解決が可能なこと。
8. キャッシュ DNS 機能は冗長化されていること。

5.3.15. 内部ファイアウォール A

1. 装置内に複数のルーティングテーブルを持つ仮想的なファイアウォールを 5 個以上構成可能なこと。
2. 10GBase-R インターフェースを 4 ポート以上備えていること。ただし、異なる仮想ファイアウォールで同じインターフェースを使用できない場合は 10 ポート以上備えること。
3. 1000Base-T インターフェースを 8 ポート以上備えていること。
4. ファイアウォールスループットを 8Gbps 以上保持可能なこと。
5. ファイアウォールセッション数を 200 万以上保持可能なこと。
6. 新規のファイアウォールセッションを 1 秒当たり 70,000 セッション以上受付可能なこと。
7. OSPF に対応していること。
8. OSPF により広告する経路のフィルタが可能なこと。
9. L3 経路情報の再配布に対応していること。
10. SNMPv2/v3 に対応していること。

5.3.16. 内部ファイアウォール B

1. 装置内に複数のルーティングテーブルを持つ仮想的なファイアウォールを 5 個以上構成可能なこと。
2. 10GBase-R インターフェースを 4 ポート以上備えていること。ただし、異なる仮想ファイアウォールで同じインターフェースを使用できない場合、一つの仮想ファイアウォールごとにコア L3 スイッチ、サーバ接続 L2 スイッチ D と 1000Base-SX で接続し 2Gbps の帯域を確保する構成で代替しても良い。
3. 仮想ファイアウォールはルーティングテーブル、ARP テーブルを個別に保持可能なこと。
4. ファイアウォールスループットを 4.5Gbps 以上保持可能なこと。
5. ファイアウォールセッション数を 80 万以上保持可能なこと。
6. 新規のファイアウォールセッションを 1 秒当たり 50,000 セッション以上受付可能なこと。
7. OSPF に対応していること。
8. OSPF により広告する経路のフィルタが可能なこと。
9. L3 経路情報の再配布に対応していること。
10. SNMPv2/v3 に対応していること。

5.3.17. 内部ファイアウォール C

1. 装置内に複数のルーティングテーブルを持つ仮想的なファイアウォールを 5 個以上構成可能なこと。
2. 10GBase-R インターフェースを 4 ポート以上備えていること。ただし、異なる仮想ファイアウォールで同じインターフェースを使用できない場合、一つの仮想ファイアウォールごとにコア L3 スイッチ、サーバ接続 L2 スイッチ D と 1000Base-SX で接続し 2Gbps の帯域を確保する構成で代替しても良い。
3. 仮想ファイアウォールはルーティングテーブル、ARP テーブルを個別に保持可能なこと。
4. ファイアウォールスループットを 4.5Gbps 以上保持可能なこと。
5. ファイアウォールセッション数を 80 万以上保持可能なこと。
6. 新規のファイアウォールセッションを 1 秒当たり 50,000 セッション以上受付可能なこと。
7. OSPF に対応していること。
8. OSPF により広告する経路のフィルタが可能なこと。
9. L3 経路情報の再配布に対応していること。
10. SNMPv2/v3 に対応していること。

5.3.18. 内部ファイアウォール D

1. 1000Base-T インターフェースを 8 ポート以上備えていること。
2. 筐体内に仮想ファイアウォールを 2 個以上作成可能なこと。
3. 仮想ファイアウォールはルーティングテーブル、ARP テーブルを個別に保持可能なこと。
4. ファイアウォールスループットを 4Gbps 以上保持可能なこと。
5. ファイアウォールセッション数を 1,000,000 万以上保持可能なこと。
6. 新規のファイアウォールセッションを 1 秒当たり 50,000 セッション以上受付可能なこと。
7. OSPF に対応していること。
8. OSPF により広告する経路のフィルタが可能なこと。
9. L3 経路情報の再配布に対応していること。
10. SNMPv2/v3 に対応していること。

5.3.19. 内部ファイアウォール E

1. 1000Base-T インターフェースを 8 ポート以上備えていること。
2. 筐体内に仮想ファイアウォールを 2 個以上作成可能なこと。
3. 仮想ファイアウォールはルーティングテーブル、ARP テーブルを個別に保持可能なこと。
4. ファイアウォールスループットを 500Mbps 以上保持可能なこと。
5. ファイアウォールセッション数を 50,000 万以上保持可能なこと。
6. 新規のファイアウォールセッションを 1 秒当たり 3,000 セッション以上受付可能なこと。
7. OSPF に対応していること。

8. OSPF により広告する経路のフィルタが可能なこと。
9. L3 経路情報の再配布に対応していること。
10. SNMPv2/v3 に対応していること。

5.3.20. 内部ファイアウォール F

1. 装置内に複数のルーティングテーブルを持つ仮想的なファイアウォールを 2 個以上構成可能なこと。
2. 10GBase-R インターフェースを 4 ポート以上備えていること。
3. 1000Base-T インターフェースを 4 ポート以上備えていること。
4. 仮想ファイアウォールはルーティングテーブル、ARP テーブルを個別に保持可能なこと。
5. ファイアウォールスループットを 2Gbps 以上保持可能なこと。
6. ファイアウォールセッション数を 100,000 万以上保持可能なこと。
7. 新規のファイアウォールセッションを 1 秒当たり 10,000 セッション以上受付可能なこと。
8. OSPF に対応していること。
9. OSPF により広告する経路のフィルタが可能なこと。
10. DHCP リレーに対応していること。
11. L3 経路情報の再配布に対応していること。
12. SNMPv2/v3 に対応していること。

5.3.21. HTTP トラフィック分離装置

1. 10GBase-SR インターフェースを 2 ポート以上備えていること。
2. 通信制御の管理、設定単位を装置内で論理的に分割可能なこと。また論理的な管理、設単位は 2 個以上作成可能なこと。
3. スループットを 2Gbps 以上保持可能なこと。
4. セッション数を 100,000 以上保持可能なこと。
5. L3 ネットワーク機器として動作可能なこと。
6. プロキシ認証機能を備えていること。認証方式として Kerberos、LDAP に対応していること
7. HA 機能を備えており、Active-Standby として動作すること。
8. HTTP アクセスログを Syslog サーバに送信可能なこと。
9. SNMPv2/v3 に対応していること。
10. リモート接続基盤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。
11. 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。

5.3.22. 閉域 WAN 回線

5.3.22.1. 閉域 WAN 回線 A

1. 広域イーサネットであること。

2. 500Mbps の帯域が確保されていること。
3. 回線は冗長化されており、Active-Standby で動作すること。
4. IEEE802.1Q VLAN タグが使用可能で、同時に 30 個以上の VLAN が使用可能なこと。

5.3.22.2. 閉域 WAN 回線 B

1. 広域イーサネットであること。
2. 300Mbps の帯域が確保されていること。
3. IEEE802.1Q VLAN タグが使用可能で、同時に 30 個以上の VLAN が使用可能なこと。

5.3.22.3. 閉域 WAN 回線 C

1. 広域イーサネットであること。
2. 100Mbps の帯域が確保されている。
3. IEEE802.1Q VLAN タグが利用可能で、同時に 30 個以上の VLAN が使用可能なこと。

5.3.22.4. 閉域 WAN 回線 D

1. 広域イーサネットであること。
2. 400Mbps の帯域が確保されていること。
3. 回線は冗長化されており、Active-Standby で動作すること。
4. IEEE802.1Q VLAN タグが利用可能で、同時に 30 個以上の VLAN が使用可能なこと。

5.3.22.5. 閉域 WAN 回線 E

1. 広域イーサネットであること。
2. 1Gbps ベストエフォート回線であること。
3. IEEE802.1Q VLAN タグが利用可能で、同時に 30 個以上の VLAN が使用可能なこと。

5.3.23. 閉域 WAN L2 スイッチ

1. 10GBase-R インターフェースを 2 ポート以上備えていること。
2. 1000Base-T インターフェースを 12 ポート以上備えていること。
3. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
4. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
5. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
6. 16000 個以上の MAC アドレスを保持可能なこと。
7. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
8. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。

9. SNMPv2/v3 に対応していること。
10. sFlow または NetFlow に対応していること。

5.3.24. インターネットスイッチ A、B、C

1. 1000Base-X インターフェースを 4 ポート以上備えていること。
2. 1000Base-T インターフェースを 12 ポート以上備えていること。トランシーバを使用して 1000Base-X インターフェースを 1000Base-T インターフェースに転用する構成としても良い。
3. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
4. 装置の全インターフェースを使用した場合にノンブロッキング、ワイヤーレートで通信可能なスイッチング容量を備えていること。
5. 装置 2 台を 1 台として論理的に束ねるスタック機能に対応していること。
6. 16000 個以上の MAC アドレスを保持可能なこと。
7. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
8. スタックしている装置の物理ポートをリンクアグリゲーションのメンバに含められること。
9. SNMPv2/v3 に対応していること。
10. sFlow または NetFlow に対応していること。

5.3.25. 汎用ロードバランサ

1. 10GBase-R インターフェースを 4 ポート以上備えていること。
2. 1000Base-T インターフェースを 4 ポート以上備えていること。
3. 2 台での冗長機能を有すること。
4. 筐体内で仮想的なロードバランサを作成可能なこと。仮想的なロードバランサは 10 個以上作成可能なこと。
5. 仮想ロードバランサは個別のルーティングテーブルを保持可能なこと。
6. ダイナミックルーティングとして OSPF に対応していること。
7. L4 ロードバランスに対応していること。
8. L7 ロードバランスに対応していること。
9. ロードバランストラフィックの TLS 復号化が可能なこと。
10. ロードバランストラフィックに x-forwarded-for 及び任意の HTTP ヘッダを挿入可能なこと。
11. クライアントからの接続を受け付ける負荷分散対象サーバの仮想 IP アドレスに対して、送信元 IP アドレスによるアクセス制限が可能なこと。
12. リンクアグリゲーション機能を有し、2 ポート以上の物理ポートを束ねられること。
13. 30Gbps 以上のロードバランススループットを備えていること。
14. 電源は冗長構成であること。

5.3.26. 管理ポート L2 スイッチ

1. 100/1000Base-T インターフェースを 20 ポート以上備えていること。
2. 1000Base-X インターフェースを 2 ポート以上備えていること。
3. 装置を管理可能なコンソールインターフェースを備えていること。インターフェース形状は RJ-45 であること。
4. SNMPv2/v3 に対応していること。
5. 装置に対する SSH アクセスにより装置管理が可能なこと。

5.3.27. 併設用 L3 スイッチ

1. 10GBase-R インターフェースを 4 ポート以上備えていること。
2. 1000Base-X インターフェースを 12 ポート以上備えていること。このインターフェースは 1000Baes-T トランシーバを使用することで、1000Base-T インターフェースとしても利用可能なこと。
3. スタック機能を備えていること。
4. 筐体内に仮想的な L3 スイッチを作成する VRF 機能を備えていること。
5. OSPF に対応していること。
6. 全インターフェースを使用時、ノンブロッキング、フルワイヤーレートでスイッチングが可能なこと。
7. リンクアグリゲーション機能を有し、4 ポート以上の物理ポートを束ねられること。
8. SNMPv2/v3 に対応していること。
9. sFlow または NetFlow に対応していること。
10. 電源ユニットは冗長化されていること。

5.3.28. 併設用ファイアウォール

1. 1000Base-T インターフェースを 12 ポート以上備えていること。
2. 2 台構成で Active-Standby による冗長構成が可能なこと。
3. 装置内に仮想的なファイアウォールを構成可能なこと。
4. 送信元 IP アドレス、宛先 IP アドレスを条件として L3 転送におけるネクストホップを変更するポリシベースルーティングに対応していること。
5. L3/L4 ベースのフィルタリング機能を備えていること。
6. IPS 機能を有し、主要な OS・ミドルウェアの脆弱性、プロトコルアノマリ、DoS、Botnet からのトラフィックを検出、遮断可能なこと。
7. IPS 機能に使用するシグネチャファイルは自動的に更新可能なこと。
8. シグネチャファイルが更新された際、そのことを示すログを Syslog 送信可能なこと。
9. IPS 機能の除外トラフィックを設定可能なこと。除外単位には送信元 IP アドレス、送信元ネットワークアドレス、宛先 IP アドレス、宛先ネットワークアドレス、シグネチャ ID を組み合わ

せて指定可能なこと。

10. IPS 機能により遮断された場合、そのことをログとして Syslog 送信可能なこと。
11. IPS 機能の適用対象トラフィックが TLS により暗号化されている場合、本装置で復号化した上で IPS 機能を適用可能なこと。IPS 機能の適用後は再暗号化が可能なこと。
12. TLS 復号化、再暗号化を行った上で IPS 機能を使用した場合でも 300Mbps 以上のスループットを保持可能なこと。
13. SNMP v2/v3 に対応していること。
14. 電源ユニットは二重化されていること。

5.3.29. 併設用 WANL2 スイッチ

1. 1000Base-X インターフェースを 2 ポート以上備えていること。
2. 1000Base-T インターフェースを 24 ポート以上備えていること。
3. 52Gbps 以上のスイッチング容量を備えており、ノンブロッキング、ワイヤーレートで通信可能なこと。
4. 16000 個以上の MAC アドレスを保持可能なこと。
5. SNMPv2/V3 に対応していること。
6. 電源ユニットは冗長化されていること。

5.4. バックアップシステム

1. 仮想基盤システムのハイパーバイザ上で動作する Windows Server2019、Windows Server2022、RHEL8、RHEL9 を OS としている仮想マシンのバックアップを取得可能なこと。
2. Windows Server2019、Windows Server2022、RHEL8、RHEL9 を OS としている物理サーバのバックアップを取得可能なこと。
3. Oracle Database、Microsoft SQL Server のトランザクションログバックアップを取得可能なこと。
4. データ格納における実際のディスク使用量を低減するための重複排除機能を有していること。
5. SMB や NFS のような汎用的なファイルアクセスではなく、製品独自のファイルアクセスプロトコルを有していること。
6. バックアップデータのデータ変更の傾向からランサムウェアによるファイルの暗号化が行われていることを検出する機能を有していること。
7. バックアップ設定、バックアップ成否状態を管理するための Web GUI インターフェースを有していること。
8. Web GUI インターフェースのログインにはバックアップシステムのローカルアカウント、Azure AD 上のアカウントを利用可能なこと。
9. Web GUI インターフェースへのログインアカウントによって表示する管理対象ノードを変更可能なこと。

5.5. 業務認証基盤システム

Active Directory、プライベート認証局、Azure AD Connect については製品を指定するため詳細要件は割愛する。

5.5.1. SAML 認証基盤

1. IdP サーバが Active Directory に対して行うアカウント情報の称号は LDAP(S)、Kerberos が使用可能なこと。
2. 認証と合わせて認可によるアクセス制御が可能なこと。
3. 認可を行うための条件判定として Active Directory のセキュリティグループが利用可能なこと。
4. 認可するサービスの制御条件としてサービスの URL(ワイルドカード含む)を利用可能なこと。
5. フロントエンドとなる IdP サーバの冗長化が可能なこと。

5.6. 共通アプリケーション

5.6.1. 運用管理システム

5.6.1.1. システム状態監視サーバ

1. ソフトウェアサポートのある最新バージョンが利用可能であること。

5.6.1.2. sFlow コレクタサーバ

1. sFlow v4 以上、NetFlow v5 以上のネットワークフロー情報を処理可能なこと。
2. 366 日以上過去のネットワークフロー情報を保存可能なこと。
3. 送信元 IP、送信先 IP、送信元ポート、送信先ポート、トラフィック容量を含んだデータを 2 週間以上確保可能なこと。このデータは 1 分刻みで取得可能なこと。
4. 監視対象デバイス、インターフェースを任意にグルーピング可能なこと。
5. SAML 認証に対応しており SP として登録可能なこと。
6. 管理インターフェースへのログインに Active Directory の ID 情報を利用可能なこと。
7. ログインアカウントごとにフローを確認可能な監視対象デバイスを制限可能なこと。

5.6.1.3. サーバマルウェア対策サーバ

1. 仮想基盤システム上の仮想マシンを対象とした各セキュリティ検査は、仮想マシンの数量に関わらず実行可能なこと。
2. 物理サーバの管理も仮想マシンと同じインターフェースで行えること。
3. 監視対象サーバの OS は Windows Server2016 / 2019 / 2022、RHEL8 / 9 に対応していること。
4. 監視対象のマルウェアの検出、駆除が可能なこと。
5. ファイル単位の変更監視が可能なこと。
6. 監視対象除外ディレクトリが指定可能なこと。
7. セキュリティ機能の設定をまとめたテンプレート設定が可能なこと。
8. 監視対象をグルーピングし、セキュリティ機能のテンプレートを適用することでセキュリティ

設定を一括で行えること。

9. セキュリティ機能が動作した際、メールによるアラート通知が可能なこと。

5.6.1.4. VDI マルウェア対策サーバ

1. 監視対象の OS は Windows10 Enterprise に対応していること。
2. 監視対象のマルウェア検出、駆除が可能なこと。
3. 監視対象除外ディレクトリが指定可能なこと。
4. 管理対象をグルーピングし、セキュリティ機能のテンプレートを適用することでセキュリティ設定を一括で行えること。
5. セキュリティ機能が動作した際、メールによるアラート通知が可能なこと。

5.6.1.5. ファイルサーバログ管理サーバ

1. Windows Server のファイル共有機能で構築されたファイルサーバのファイルにアクセスした日時、ユーザ名、ファイル名、操作種別を記録できること。
2. 特定ユーザの操作をロギング対象から除外できること。
3. ファイルサーバログ管理サーバを管理するための Web GUI を備えていること。
4. Web GUI からユーザ、操作種別を条件にログ検索が可能なこと。
5. ファイルサーバアクセスログを外部にエクスポート可能なこと。

5.6.1.6. ファイアウォール管理サーバ

1. ハードウェアアプライアンスであること。
2. 本調達で導入するファイアウォールアプライアンスのトラフィックログを受信可能なこと(仮想基盤システム上の L3/L4 フィルタリング機能は除外する)。
3. 管理対象のファイアウォールポリシにマッチしたトラフィックのログを集約して記録可能なこと。
4. ログ格納領域として 12TB 以上を備えていること。
5. トラフィックログの検索機能を有し、検索条件としてファイアウォールアプライアンスを指定可能なこと。
6. 管理対象のファイアウォールのファイアウォールポリシに使用するオブジェクトを一括管理する機能を有し、ファイアウォール管理システムで作成したオブジェクトを管理対象のファイアウォールに配布可能なこと。
7. 設定可能なオブジェクトは少なくとも IP/ネットワークアドレス、アドレスグループ、IPS シグネチャを含むこと。
8. 管理対象のファイアウォールに本装置からからファイアウォールポリシを設定可能なこと。
9. 管理対象のファイアウォールのポリシマッチ数、IPS シグネチャマッチ数の定期レポートを作成可能なこと。

10. スクリプトベースの HTTP アクセスによりファイアウォールオブジェクト、ポリシの設定が可能なこと。
11. 管理対象のファイアウォールの操作ログ、システムログを集約して記録可能なこと。
12. 本装置に搭載するディスクは RAID5 相当のディスク障害耐性を備えていること。
13. 19 インチラックに搭載可能なこと。

5.6.2. リモート接続仮想基盤システム

5.6.2.1. 物理ホスト

1. 300GB 以上の実効ディスク容量を備えていること。
2. HDD で構成すること。
3. RAID5 相当のディスク障害耐性を備えていること。
4. ディスクに障害が発生した際に自動的にアクティブになるスペアディスクを搭載すること。
5. 物理ホストのサービスに影響を与えることなくディスク交換が可能なこと。
6. 1 インターフェースあたり 32Gbps 以上の帯域を持つファイバチャネルインターフェースを備えていること。2 ポート以上備えていること。
7. 10GBase-R に対応したネットワークインターフェースを 4 ポート以上備えていること。
8. 物理ホストの状態を管理可能な専用 Web インターフェースを備えており、Web インターフェースから物理ホストの電源操作、コンソール操作が可能なこと。Web インターフェースにアクセスするための専用の物理ネットワークインターフェースを備えていること。
9. ハードウェア異常を SNMP 通知する仕組みを備えていること。
10. 外部 Syslog サーバに装置内イベントを送信可能なこと。
11. 19 インチラックに搭載可能なこと。
12. 200V 電源に対応しており、電源冗長が可能なこと。

5.6.2.2. ハイパーバイザ

1. 汎用的なサーバにインストール可能なハイパーバイザ型の仮想マシンインフラストラクチャソフトウェアであること。
2. 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他の物理ホストに移動可能なこと。

5.6.3. メールシステム

5.6.3.1. メールフィルタシステム A

1. クラウドサービスとして提供されること
2. STARTTLS による経路暗号化が可能なこと。
3. 本システムに配送されるメールが、正当なメールサーバから送信されたことを確認可能なこと。
4. 利用者アカウント(メールアドレス)を一括登録、削除が可能なこと。
5. スパムメールフィルタリングの処理動作としては信拒否、隔離、件名・本文に任意キーワード

を挿入し配送が可能なこと。

6. マルウェアメールフィルタリングの処理動作としてメール受信拒否、破棄、隔離が可能なこと。
7. 受信拒否、許可は合計 2000 件以上登録可能なこと。
8. 1 通あたりのメールサイズ上限が添付ファイル含め 100MB まで設定可能なこと。
9. 送受信メール配送ログが本システムの管理画面よりダウンロード可能なこと。
10. 本システムの管理画面に対してログインアカウント以外の接続制御が可能なこと。
11. メール通過量に対する従量課金制ではないこと。

5.6.3.2. メール添付ファイル自動変換システム

1. クラウドサービスとして提供されること。メールフィルタシステム A のオプション機能でもよい。
2. 添付ファイルの外部ストレージへの保管、保管先 URL の宛先への通知は一連の動作となり、ユーザの操作が発生しないこと。
3. 添付ファイル保管先 URL は有効期間、ファイル取得回数上限を設けた上で第三者がアクセス可能であること。
4. 利用者アカウント(メールアドレス)を一括登録、削除が可能なこと。
5. 格納したファイルの自動削除が設定可能なこと。
6. メール通過量に対する従量課金制ではないこと。

5.6.4. DNS システム

5.6.4.1. キャッシュ DNS システム

1. 内部 DNS システムからの名前問い合わせを受け付け、インターネット上の名前情報を再帰的に回答できること。
2. 複数サーバから DNS フォワードとして参照が可能なこと。
3. キャッシュ DNS サーバは 2 台以上の冗長構成となっていること。

5.6.5. メンテナンスシステム

5.6.5.1. 調査用物理サーバ

1. 物理コアを 16 個以上使用可能なこと。複数プロセッサを使用する場合の数値で良い。Hyper Treading による増量は計算に含めない。
2. 物理メモリを 128GB 以上搭載すること。
3. 500GB 以上の実効ディスク容量を備えていること。
4. RAID5 相当のディスク障害耐性を備えていること。
5. ディスクに障害が発生した際に自動的にアクティブになるスペアディスクを搭載すること。
6. 物理ホストのサービスに影響を与えることなくディスク交換が可能なこと。
7. 1 インターフェースあたり 32Gbps 以上の帯域を持つ FC インターフェースを備えていること。

2 ポート以上備えていること。

8. 10GBase-R に対応したネットワークインターフェースを 8 ポート以上備えていること。
9. 1000Base-T に対応したネットワークインターフェースを 2 ポート以上備えていること。
10. 物理ホストの状態を管理可能な専用 Web インターフェースを備えており、Web インターフェースから物理ホストの電源操作、コンソール操作が可能なこと。Web インターフェースにアクセスするための専用の物理ネットワークインターフェースを備えていること。
11. ハードウェア異常を SNMP 通知する仕組みを備えていること。
12. 外部 Syslog サーバに装置内イベントを送信可能なこと。
13. 19 インチラックに搭載可能なこと。
14. 200V 電源に対応しており、電源冗長が可能なこと。

5.6.5.2. リモートパケット収集装置

1. ミラーパケットの受信を行える 10GBase-SR インターフェースを 6 ポート以上備えていること。
2. ミラーパケットの受信を行える 1000Base-T インターフェースを 12 ポート以上備えていること。
3. 受信したミラーパケットを送出できる 10GBase-SR インターフェースを 4 ポート以上備えていること。
4. 異なる物理ポートで受信したミラーパケットを同時に送出可能なこと。
5. 指定した受信ポートからのミラーパケットのみ送出するように設定可能なこと。
6. 送出するミラーパケットを L3/L4 フィルタリング可能なこと。
7. IP 通信による本装置の死活監視が可能なこと。

5.6.5.3. コンソールインターフェース管理装置

1. 捜査対象機器のコンソール接続を切り替える機能を有すること。
2. コンソール接続を 32 ポート以上使用可能なインターフェースを備えていること。
3. IP 通信により本装置と通信可能な 1000Base-T(100Base-TX でも可)インターフェースを 1 ポート以上備えていること。

5.7. その他

5.7.1. 移行用ストレージ

1. 実効容量として 180TB を確保すること。
2. SSD と HDD のハイブリッドまたは全て SSD で構成すること。ハイブリッド構成の場合、キャッシュ領域として使用できる SSD を全体の 20%程度確保すること。
3. コントローラを二重化し、冗長構成とすること。
4. 既存 FC スイッチ 2 台とマルチパス接続すること。

5.7.2. 動作確認用物理サーバ

1. 物理コアを 8 個以上使用可能なこと。プロセッサ数は 1 個で構成すること。
2. 物理メモリを 32GB 以上搭載すること。
3. 500GB 以上の実効ディスク容量を備えていること。ディスクは SSD で構成すること。
4. RAID5 相当のディスク障害耐性を備えていること。
5. ディスクに障害が発生した際に自動的にアクティブになるスペアディスクを搭載すること。
6. 物理ホストのサービスに影響を与えることなくディスク交換が可能なこと。
7. 1 インターフェースあたり 32Gbps 以上の帯域を持つ FC インターフェースを備えていること。2 ポート以上備えていること。
8. 10GBase-R に対応したネットワークインターフェースを 6 ポート以上備えていること。
9. 物理ホストの状態を管理可能な専用 Web インターフェースを備えており、Web インターフェースから物理ホストの電源操作、コンソール操作が可能なこと。Web インターフェースにアクセスするための専用の物理ネットワークインターフェースを備えていること。
10. 19 インチラックに搭載可能なこと
11. 200V 電源に対応しており、電源冗長が可能なこと。
12. 100V 電源に対応しており、電源冗長が可能なこと。

6. プロジェクト要件

6.1. プロジェクト計画

受注者は本調達の全行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。

6.1.1. プロジェクト計画に関するドキュメント

6.1.1.1. プロジェクト実施計画書

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)
- 設計変更管理方針
- 品質管理方針
- プロジェクトにおける機密保持管理方針
- ドキュメント管理方針
- 会議体
- 設計合意のフロー

尚、会議を行う場合には対面開催以外に Microsoft Teams を使用した Web 会議を使用することも可とする。他のツールの利用は許可しない。

設計合意のフローには本調達で導入するシステムの全要素の詳細を受注者と PMDA で合意するための手順を記載する。この作業は多くの工数を要することが想定されるため、受注者、PMDA 共に効率的にこの行程を行えるような手順を検討すること。

プロジェクト実施計画書は契約後に可能な限り早く作成すること。WBS の設計を経て詳細化できる項目についてはプロジェクトの進行にあわせて詳細化を行う形でも良い。

6.1.1.2. 進捗報告

受注者はプロジェクト設計書に基づき、本調達の進捗条件を最低限 2 週間に 1 回報告するための会議体を設定すること。会議体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。

6.2. 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。

6.2.1. 設計に関するドキュメント

6.2.1.1. 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
- ケーブル接続表
- L3 ベースのシステム論理構成図
- 仮想基盤システム及び共有ストレージのリソース
- 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、回線サービスをすべて含む。)

6.2.1.2. 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。

6.2.1.3. 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
- 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
- ハードウェアの設置場所に応じたハードウェア障害時の保守対応手順
- データセンタの入館申請手順
- データセンタに入館可能な人物の変更手順
- 共有ストレージのディスク交換手順

6.2.1.4. 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利用者影響、運用管理影響、システム構成変動の要素から段階化し、各段階におけるシステムの状態、周囲のシステムとの接続、運用状態を時系列で図示すること。既存システムからの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 週間以上前に PMDA に影響範囲を報告し合意すること。

6.2.1.5. 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。テスト設計時には、使用する全機能の正常動作の確認、冗長構成における部分障害時の動作、セキュリティ装置の機能動作に特に留意すること。

6.3. 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、システムが正常に動作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実施計画書に定めた設計変更管理方針、ドキュメント管理方針に基づきドキュメントの修正を行うこと。

6.3.1. 導入に関するドキュメント

6.3.1.1. 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たテスト結果報告書を作成すること。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。

6.4. 引継ぎ

6.4.1. 運用に関するドキュメント

6.4.1.1. 運用手順書

運用手順書には以下の内容を記載すること。

- 運用設計書に基づき具体的な製品操作方法を記載すること。
- ハードウェア及びソフトウェア保守体制、保守依頼を行うための手順

7. システム構築・移行全体の要件

7.1. システム構築スケジュールの詳細

7.1.1. 基盤システム納品

別紙 2 概略スケジュールの基盤システムの納品では、本システム上に業務システムを構築するための必要となる要素を対象とした納品を行うこと。対象は以下に記す通り。

- 業務仮想基盤システムに含まれる全てのシステム
- リモート接続仮想基盤システム
- バックアップシステム全て
- IP ネットワークシステム全て
- 業務認証基盤システム
- DNS
- メールシステム
- ファイル共有システム (システム資源ファイルサーバのみ)
- 印刷管理システム
- 運用管理システム (ファイアウォールサーバログ管理サーバ、ファイアウォール管理サーバのみ)
- 外部専門委員リモート接続システム
- メンテナンスシステム
- その他の納入品

また、上記以外にもデータセンタ等、上記を稼働させるために必要なファシリティ、部材を含む。

7.1.2. 既存システムの移行

本システムの構成要素には既存システムのデータ移行が必要になるものがある。既存システムの移行は、必ずしも基盤システムの納品タイミングまでに完了させる必要はない。ただし、2024 年 5 月以降に想定している本システムの利用した業務システム構築において、旧環境に存在する移行対象システムと通信が必要になるケースでは通信の整合性をとれるようにネットワークを調整すること。

7.1.3. PMDA によるシステム構築

本システムの構成要素のうち、PMDA が構築を行うものはこの期間で構築する。基盤システム構築の進捗にあわせて構築開始を前倒しする可能性がある。製品を使用するためにライセンス等が必要な場合は 2024 年 1 月 1 日以降使用可能となるように準備すること。

7.2. 既存システムの資源利用

本システムの構築時、必要に応じて既存システムの一部資源を使用しても良い。例えば DNS キャッシュサーバやメール配送機能の利用を想定している。既存システムを利用する場合、移行スケジュールにそれらの利用や切替方法を検討に含めること。

7.3. ネットワーク移行

現行システムでは現行データセンタ、新霞が関ビル、関西支部間の接続に閉域 WAN 回線を使用しており、以下に記す接続を行っている。

拠点間	説明
現行データセンタ - 新霞が関ビル間	広域イーサネットにより接続している。
現行データセンタ - 関西支部	広域イーサネットにより接続している。

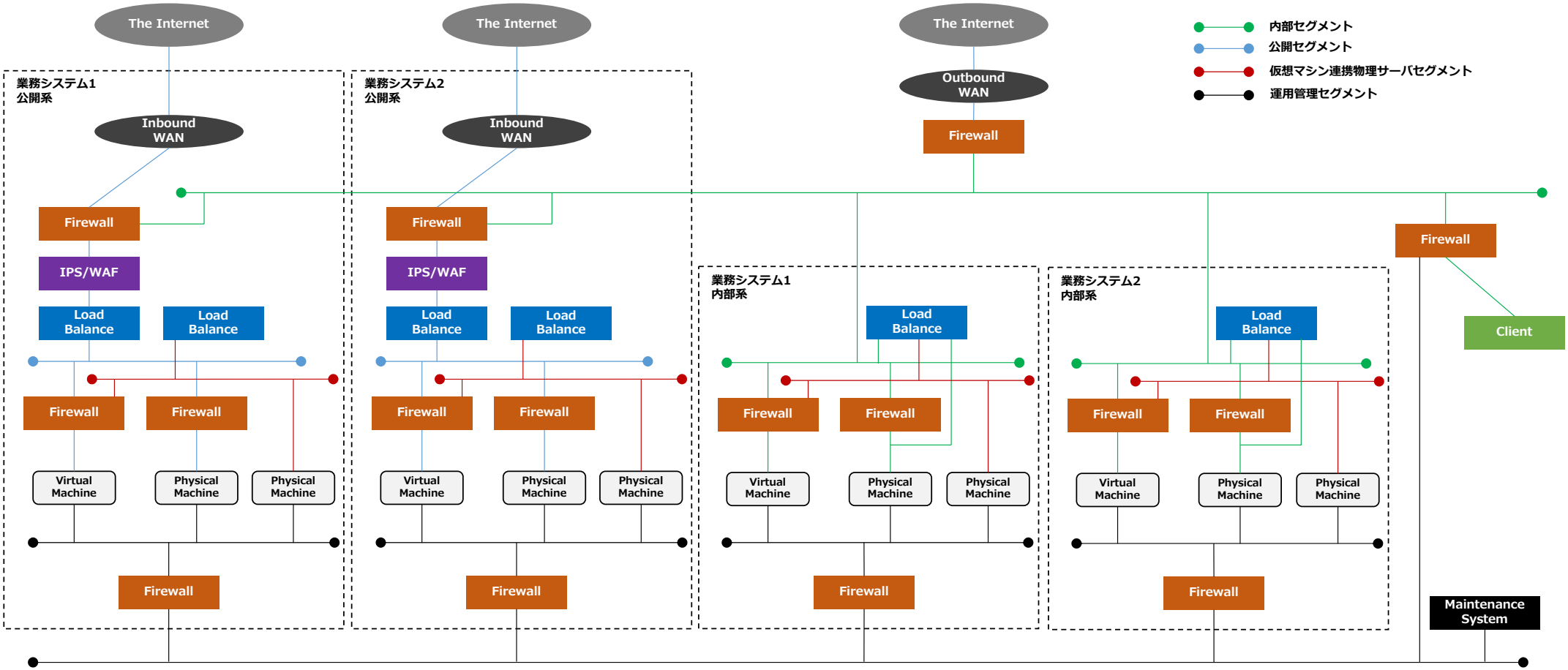
新霞が関ビル、関西支部から現行データセンタで稼働している業務システムにアクセスするにあたり、本調達で構成する閉域 WAN 回線を使用する構成に変更する場合にはネットワーク接続性を十分に検討し、通信断時間が極力短くなるように移行作業を行うこと。

7.4. インターネット通信の制限

既存システムではインターネット接続を行えるノードはホワイトリスト方式で制限している。本システムでもこの制限は継続するため、それを前提にシステム設計を行うこと。インターネット接続するためには極力 HTTP プロキシを使用するが、やむを得ない場合は直接のアクセスも許可することがある。

業務システム統合基盤の構築及び保守

調達仕様書

別紙4 業務システムネットワークアーキテクチャ

ネットワークアーキテクチャイメージ