仮想基盤システム更改に向けた情報提供依頼書

別紙 1 システム要件書

1. 概要

1.1. 依頼事項

1.1.1. 情報提供依頼内容

本システムは PMDA の業務に使用するシステムを稼働させ、ユーザが使用するためのインフラという位置づけで検討しています。本システムは以下に記すサブシステムで構成します。

- 物理・仮想サーバを稼働させる仮想基盤システム
- 通信制御を行うネットワークシステム
- システム動作状況を可視化するためのシステム監視システム
- インフラが提供する機能を実現するアプリケーション
- 各ハードウェアを配置する物理ロケーション

各サブシステムにおける構成品の要件、数量を本資料に記載しますので、各構成品の費用、ハードウェア・ソフトウェア保守費用、以下に記載する技術情報のご提供をお願い致します。

- 具体的な製品名、メーカ名
- 本書に示す各要件の対応可否
- ハードウェアの場合、質量、寸法、電源仕様、他要素との近傍(同一ラックや隣接ラック)設置制限の有無
- 製品のカタログ(インターネットリソースの URL や PDF)
- 製品のマニュアル(インターネットリソースの URL や PDF)

尚、現時点では本書に記す全ての要件を満たしていなくても問題ありません。ご提供頂いた情報に基づいて今後の検討を行います。特に記載がない限り、1700 ユーザにて 5 年間の運用を想定して下さい。

1.1.2. 特記事項

一部の構成品では情報提供特記事項として特定の情報提供を求めているものがあります。情報をご提供頂く際はその内容について特に情報のご提供をお願い致します。

構成品に付随する必要のある部材に関してはある程度 PMDA で前提を記載しており、見積の前提条

件として記載をしています。こちらの条件を元に費用算出をお願い致します。

1.1.3. 期限

2021 年 12 月 23 日中までのご提供をお願い致します。

1.1.4. 提出方法

「cm-kyoyolan●pmda.go.jp」宛の電子メールまたはオンラインストレージ等にてご提出をお願い致します。一部のオンラインストレージは PMDA からアクセスできない可能性があります。尚、宛先メールアドレスは「●」を「@」に変更して下さい。紙面でのご提出は原則不要です。

1.2. 留意事項

本情報提供依頼は将来の調達、システム構成を確約するものではありません。

2. 情報提供依頼対象のシステム構成

システム構成の概略図は「別紙 システム構成概略図」に示す通りです。また、情報をご提供頂きたい要素を次の表に書き出しています。数量は構成品をある程度の単位に集約したものを記載しています。一部の構成品では構成品の各要件に詳細情報を記載していますので、そちらも併せて参照をお願い致します。

サブシステム名	構成品	数量
仮想基盤システム	仮想基盤物理ホスト A	10
	仮想基盤物理ホスト B	4
	仮想基盤物理ホスト C	3
	仮想基盤物理ホスト D	4
	共有ストレージ A	2
	共有ストレージ B	2
	共有ストレージ C	2
	共有ストレージ D	1
	共有ストレージ E	1
	バックアップストレージ A	2
	バックアップストレージ B	1
	FC スイッチ A	8
	FC スイッチ B	2
	FC スイッチ C	2
	マルウェア対策機能	-

ネットワークシステム	外部ファイアウォール A	2
	外部ファイアウォール B	2
	外部ファイアウォール C	2
	内部ファイアウォール A	2
	内部ファイアウォール B	2
	機関接続用 VPN 装置	2
	ハードウェアロードバランサ	4
	L3 スイッチ A	2
	L2 スイッチ B	4
	L2 スイッチ C	4
	L2 スイッチ D	2
システム管理システム	システム状態管理	-
	sFlow コレクタ	1
	RedHat ソフトウェア管理	1
	構成管理	-
	リモートパケット収集	-
	コンソールインターフェース管理	-
	ファイアウォール管理	-
アプリケーション	SAML 認証基盤	-
	HTTP プロキシ	2
	Windows 共有ファイルアクセスログ管理	-
物理ロケーション	データセンタ	-

3. 各構成要素の技術要件

3.1. 仮想基盤システム

3.1.1. 仮想基盤物理ホスト

3.1.1.1. 仮想基盤物理ホスト A

1. 合計 80 コア以上を利用可能な CPU を搭載できること。物理プロセッサ複数搭載時の合計で良いが、Hyper Threading による計算は含めない。
2. 物理メモリを 768GB 以上搭載可能なこと。
3. 500GB 以上のディスク実効量を備えること。
4. RAID5 相当のディスク障害耐性を持ち、ディスク障害時は自動的にアクティブ状態に遷移する

スペアディスクを搭載可能なこと。

5. ディスクは物理ホストのサービスを損なわずに交換可能なこと。
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。インターフェースを 4 ポート以上備えておりマルチパス構成が可能なこと。インターフェースを備えたインターフェースカードは冗長可能なこと。
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. 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。
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. ハードウェア異常を SNMP Trap で通知する仕組みを備えていること。
11. 外部 Syslog サーバに装置内イベントを送信可能なこと。
12. REST API に対応しており、スクリプトベースの HTTPS アクセスでハードウェアの状態を取得可能なこと。
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。

3.1.1.2. 仮想基盤物理ホスト B

1. 合計 80 コア以上を利用可能な CPU を搭載できること。物理プロセッサ複数搭載時の合計で良いが、Hyper Threading による計算は含めない。
2. 物理メモリを 768GB 以上搭載可能なこと。
3. 500GB 以上のディスク実効量を備えること。
4. RAID5 相当のディスク障害耐性を持ち、ディスク障害時は自動的にアクティブ状態に遷移するスペアディスクを搭載可能なこと。
5. ディスクは物理ホストのサービスを損なわずに交換可能なこと。
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。インターフェースを 4 ポート以上備えておりマルチパス構成が可能なこと。インターフェースを備えたインターフェースカードは冗長可能なこと。
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. 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。
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. ハードウェア異常を SNMP Trap で通知する仕組みを備えていること。
11. 外部 Syslog サーバに装置内イベントを送信可能なこと。
12. REST API に対応しており、スクリプトベースの HTTPS アクセスでハードウェアの状態を取

得可能なこと。

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。

3.1.1.3. 仮想基盤物理ホスト C

1. 合計 32 コア以上を利用可能な CPU を搭載できること。物理プロセッサ複数搭載時の合計で良いが、Hyper Threading による計算は含めない。
2. 物理メモリを 512GB 以上搭載可能なこと。
3. 500GB 以上のディスク実効量を備えること。
4. RAID5 相当のディスク障害耐性を持ち、ディスク障害時は自動的にアクティブ状態に遷移するスペアディスクを搭載可能なこと。
5. ディスクは物理ホストのサービスを損なわずに交換可能なこと。
6. iSCSI 接続用途として 10GBase-R 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。このインターフェースはユーザ向けサービス提供用のネットワークインターフェースとは別に用意すること。
7. 10Gbase-R に対応したネットワークインターフェースを 2 ポート以上備えていること。
8. 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。
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. ハードウェア異常を SNMP Trap で通知する仕組みを備えていること。
11. 外部 Syslog サーバに装置内イベントを送信可能なこと。
12. REST API に対応しており、スクリプトベースの HTTPS アクセスでハードウェアの状態を取得可能なこと。
13. 19 インチラックに搭載可能なこと。
14. 100V 電源で動作し、電源冗長が可能なこと。

3.1.1.4. 仮想基盤物理ホスト D

1. 合計 48 コア以上を利用可能な CPU を搭載できること。物理プロセッサ複数搭載時の合計で良いが、Hyper Threading による計算は含めない。
2. 物理メモリを 512GB 以上搭載可能なこと。
3. 500GB 以上のディスク実効量を備えること。
4. RAID5 相当のディスク障害耐性を持ち、ディスク障害時は自動的にアクティブ状態に遷移するスペアディスクを搭載可能なこと。
5. ディスクは物理ホストのサービスを損なわずに交換可能なこと。
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。インターフェースを 4 ポート以上備えており、各ポートを同時に使用可能なこと。

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. 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。
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. ハードウェア異常を SNMP Trap で通知する仕組みを備えていること。
11. 外部 Syslog サーバに装置内イベントを送信可能なこと。
12. REST API に対応しており、スクリプトベースの HTTPS アクセスでハードウェアの状態を取得可能なこと。
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。

3.1.2. ハイパーバイザ A

1. 仮想マシンの OS として少なくとも Windows Server2016 及び 2019、RedHat Enterprise Linux8、Ubuntu19 及び 20 に対応していること。
2. 仮想マシンが動作する物理ホストを動的に変更する機能を備えていること。
3. 仮想マシンが動作する物理ホストに障害が発生した際、他の物理ホストで当該仮想マシンを自動的に起動させる機能を備えていること。
4. 仮想マシンが IP 接続する仮想ネットワークの設定はハイパーバイザ A の管理対象の物理ホスト間で共有され、1 回の設定作業で全体に適用が可能なこと。
5. ハイパーバイザ内で L3 通信が可能なルータを仮想アプライアンスとして作成可能なこと。ルータはルーティングプロトコルとして OSPF が使用可能なこと。
6. 物理ネットワークで動作している OSPF と連携してルーティングテーブルを動的に更新可能なこと。
7. ハイパーバイザ内で L4 ロードバランスが可能なロードバランサを仮想アプライアンスとして作成可能なこと。ロードバランサ機能は任意の宛先 TCP ポートでバランス設定が可能なこと。
8. ハイパーバイザにより制御される各要素を管理可能な GUI を備えていること。

3.1.3. ハイパーバイザ B

1. 仮想マシンの OS として少なくとも Windows Server2016 及び 2019、RedHat Enterprise Linux8、Ubuntu19 及び 20 に対応していること。
2. 仮想マシンが動作する物理ホストを動的に変更する機能を備えていること。
3. 仮想マシンが動作する物理ホストに障害が発生した際、他の物理ホストで当該仮想マシンを自動的に起動させる機能を備えていること。

4. 仮想マシンが IP 接続する仮想ネットワークの設定はハイパーバイザ A の管理対象の物理ホスト間で共有され、1 回の設定作業で全体に適用が可能なこと。
5. ハイパーバイザ A と同一のメーカの製品であること。
6. ハイパーバイザにより制御される各要素を管理可能な GUI を備えていること。

3.1.4. 共有ストレージ

3.1.4.1. 共有ストレージ A

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. 記憶媒体は全て SSD で構成すること。
5. 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。
6. 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。
7. 実効容量として 300TB 以上の容量を有すること。
8. 特定の仮想マシンが使用する物理ディスクを限定可能なこと。この用途で使用する領域は 20TB 程度とする。
9. ストレージ論理ボリュームごとに IOPS 性能の制限を行えること。
10. 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。
11. 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。
12. 19 インチラックに搭載可能なこと。
13. 200V 電源に対応しており、電源冗長が可能なこと。

3.1.4.2. 共有ストレージ B

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。

6. 実効容量として 200TB 以上の容量を有すること。
7. ストレージ論理ボリュームごとに IOPS 性能の制限を行えること。
8. 19 インチラックに搭載可能なこと。
9. 200V 電源に対応しており、電源冗長が可能なこと。

3.1.4.3. 共有ストレージ C

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. 実効容量として 100TB 以上の容量を有すること。
6. ストレージ論理ボリュームごとに IOPS 性能の制限を行えること。
7. 19 インチラックに搭載可能なこと。
8. 200V 電源に対応しており、電源冗長が可能なこと。

3.1.4.4. 共有ストレージ D

共有ストレージ A と同等製品であること。ただしディスク実効容量は 50TB 以上あれば良い。

3.1.4.5. 共有ストレージ E

共有ストレージ B と同等製品であること。ただしディスク実行容量は 30TB 以上あれば良い。

3.1.4.6. バックアップストレージ A

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. RAID5 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。
3. ディスク暗号化が可能なこと。
4. 実効容量として 350TB 以上の容量を有すること。
5. 19 インチラックに搭載可能なこと。
6. 200V 電源に対応しており、電源冗長が可能なこと。

3.1.4.7. バックアップストレージ B

バックアップストレージ A と同等製品、同等構成であること。

3.1.4.8. リモートバックアップストレージ

バックアップストレージA、Bをストレージボリュームレベルでレプリケーション可能なこと。可能なら本装置は1台構成として良い。装置構成はバックアップストレージAと同程度とすること。ただし100V電源で動作可能であることが望ましい。

3.1.5. FCスイッチ

3.1.5.1. FCスイッチA

1. 32Gbpsでリンク可能なFCインターフェースを32ポート以上備えていること。

3.1.5.2. FCスイッチB

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。

3.1.6. マルウェア対策機能

1. 仮想基盤システムで動作させるWindows Server2016 / 2019、RetHat Enterprise Linux7 / 8のOS上のマルウェアを検出し、ファイルの駆除が可能なこと。物理サーバも保護対象に含められることが望ましい。
2. 保護対象の仮想マシンに対してエージェントのインストール有無に関する情報を提供すること。
3. Webブラウザから管理対象ノードの状態確認、本機能の設定が可能なWebインターフェースを備えていること。物理サーバも同一の管理インターフェースで一元管理可能なことが望ましい。
4. 監視対象除外ファイルパス、ディレクトリを指定可能なこと。除外指定は監視対象ノード個別に設定することなく同一の設定を使いまわすことが可能なこと。同一の設定を使わない監視対象ノードも併存可能なこと。
5. 監視対象除外パスを追加で監視対象ノード個別に設定可能なこと。
6. 検出した被疑ファイルをクラウドサービスなどのインターネット上のリソースにアップロードしないこと。管理者が任意のファイルを手動でアップロードする場合は可とする。
7. マルウェアを検出した際、そのイベント発生をWebインターフェース、Syslog、Webhookを通して管理者に通知可能なこと。これらの通知は全て同時利用可能なこと。
8. マルウェアを検出した際、検出したマルウェアのハッシュ値を取得可能なこと。Webインターフェース、Syslog、Webhookを通してハッシュ値を通知可能であることが望ましい。

3.1.7. バックアップ

1. Windows Server2016 / 2019、RedHat Enterprise Linux7 / 8で稼働している仮想サーバ、物理サーバのバックアップをフルバックアップ、増分バックアップで取得可能なこと。
2. バックアップの粒度はOSレベル、ディスクレベルで対応可能なこと。
3. ファイルベースのレプリケーションが可能なこと。レプリケーションデータは他サーバがマウントしている領域に格納可能なこと。

4. Microsoft 社 SQL Server2016 / 2019 のバックアップをオンラインで取得可能なこと。

3.1.8. バックアップ用物理サーバ A

1. 16 コア以上を利用可能な CPU を搭載可能なこと。
2. 物理メモリを 96GB 以上搭載可能なこと。
3. 500GB 以上のディスク実効量を備えること。
4. RAID5 相当のディスク障害耐性を持ち、ディスク障害時は自動的にアクティブ状態に遷移するスペアディスクを搭載可能なこと。
5. 物理サーバが活性状態でディスク交換を行えること。
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 2 ポート以上備えており同時利用が可能なこと。
7. 1000Base-X 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。
8. 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。
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. ハードウェア異常を SNMP Trap で通知する仕組みを備えていること。
11. 外部 Syslog サーバに装置内イベントを送信可能なこと。
12. REST API に対応しており、スクリプトベースの HTTPS アクセスでハードウェアの状態を取得可能なこと。
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。

3.1.9. バックアップ用物理サーバ B

1. 16 コア以上を利用可能な CPU を搭載可能なこと。
2. 物理メモリを 48GB 以上搭載可能なこと。
3. 500GB 以上のディスク実効量を備えること。
4. RAID5 相当のディスク障害耐性を持ち、ディスク障害時は自動的にアクティブ状態に遷移するスペアディスクを搭載可能なこと。
5. 物理サーバが活性状態でディスク交換を行えること。
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 2 ポート以上備えており同時利用が可能なこと。
7. 1000Base-X 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。
8. 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。
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. ハードウェア異常を SNMP Trap で通知する仕組みを備えていること。
11. 外部 Syslog サーバに装置内イベントを送信可能なこと。
12. REST API に対応しており、スクリプトベースの HTTPS アクセスでハードウェアの状態を取得可能なこと。
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。

3.1.10. 見積の前提

3.1.10.1. 仮想基盤物理ホスト A、B、D の基本構成

1. 仮想基盤物理ホスト A は 10 台、仮想基盤物理ホスト B は 4 台で構成すること。
2. 仮想基盤物理ホスト D は 3 台で構成すること。
3. 仮想基盤物理ホストではネットワークインターフェース用トランシーバとして筐体 1 台あたり SR-SFP を 4 個搭載すること。
4. 装置管理用のインターフェースを含め、1000Base-T 接続インターフェースの接続は考慮しなくて良い。
5. 仮想基盤物理ホストと共有ストレージの接続は「別紙 システム構成概要図」を参考にすること。
6. 仮想基盤物理ホスト A、B では FC インターフェースにマルチモード光ファイバを接続可能なトランシーバを筐体 1 台あたり 4 個搭載すること。
7. 仮想基盤物理ホスト A、D で数量に制限なく Windows Server2019、Windows Server2016 を利用可能なライセンスを含めること。CAL は構成に含めなくて良い。
8. 仮想基盤物理ホスト B、D で数量に制限なく RedHat Enterprise Linux を利用可能なライセンスを含めること。サポートは平日 9 時～17 時の対応のみで良い。
9. 仮想基盤物理ホスト C で Windows Server2016 / 2019 を両方使用可能なライセンスを仮想マシン 20 個分、RedHat Enterprise Linux を利用可能なライセンスを仮想マシン 10 個分含めること。サポートは平日 9 時～17 時の対応のみで良い。
10. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
11. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
12. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.1.10.2. ハイパーバイザ

1. ハイパーバイザ A を仮想基盤物理ホスト A、B、D に搭載すること。
2. ハイパーバイザ B を仮想基盤物理ホスト C､バックアップ用物理ホスト A に搭載すること｡尚、仮想基盤物理ホスト C とバックアップ用物理ホストの仮想基盤は別管理にて行う。
3. ハイパーバイザ A に関しては各要素を管理する GUI を二重化すること。

3.1.10.3. 共有ストレージ

1. 「別紙 システム構成概要図」の SAN 構成案を参考にすること。
2. 共有ストレージ A-1 と A-2 は同一の用途で動作させ、使用するストレージは設計、運用の中で選択を行う。これはストレージ筐体障害の影響範囲を限定することを意図している。ストレージ機能によるレプリケーションは想定していない。
3. バックアップストレージ A と B も共有ストレージ A-1 と A-2 同様の想定をしている。
4. リモートバックアップストレージではバックアップストレージ A と B に格納されているバックアップデータをストレージによるレプリケーションを行うことを想定している。

3.1.10.4. マルウェア対策機能

1. 仮想基盤物理ホスト A、B、C、D 上で動作する仮想マシンを無制限にマルウェアから保護可能なライセンスを含めること。
2. 物理サーバ 50 台をマルウェアから保護可能なライセンスを含めること。

3.1.10.5. バックアップ

1. 仮想基盤システム上の仮想マシンを全てバックアップ対象とできるライセンスを含めること。
2. 物理サーバを 30 台バックアップ可能なライセンスを含めること。
3. 仮想基盤システム上の仮想マシンのバックアップ処理を行う時のトラフィックは原則 SAN をするように構成可能なこと。
4. バックアップイメージはバックアップストレージ A、B に保存し、バックアップストレージ A、B のボリュームをリモートバックアップストレージにボリュームレベルでレプリケーションすることを想定している。
5. Microsoft 社 SQL Server2016 / 2019 を 10 台分バックアップ可能なライセンスを含めること。
6. バックアップ用物理ホスト A 上で動作する仮想マシンとバックアップ用物理ホスト B 上で動作させること。

3.1.10.6. バックアップ用物理ホスト A

1. 同一の筐体を 2 台構成に含めること。
2. 仮想マシン、仮想マシン上のファイル、データベースのバックアップは基本的に夜間に行うことを想定している。仮想マシンの数が多い場合バックアップ処理が夜間中に完了しない可能性があるためバックアップ処理の多重化を行う。多重化を行うため、バックアップ処理を行う実態を複数作成することを想定している。

3.1.10.7. 検証環境

本仮想基盤システム上の仮想マシンの動作確認を行うための検証環境を構築する。仮想基盤物理ホスト D、FC スイッチ B、共有ストレージ D、共有ストレージ E、バックアップ用物理ホスト

B は検証用の設備とし、本番環境とは物理的、論理的にある程度切り離すことを想定している。
設備自体のソフトウェアアップデートや冗長構成の切替テストを行うことも想定しているため、
基本的には本番環境と同等の機能を搭載する。

3.1.11. 情報提供依頼特記事項

3.1.11.1. 仮想基盤物理ホスト

1. 物理ホストの障害発生等のイベントを Syslog 送信する場合のログフォーマットに関する情報をご提供下さい。
2. 物理ホストの状態を取得するための HTTP API リファレンスをご提供下さい。

3.1.11.2. 共有ストレージ

1. コントローラ、コントローラが接続する FC スイッチ 1 台に障害が発生した時のストレージのデータアクセスの挙動に関して、I/O 性能、データアクセス停止時間の情報提供をお願い致します。
2. ストレージのソフトウェアアップデートを行う場合のデータアクセスの挙動に情報提供をお願い致します。共有ストレージ A に関しては可能な限りデータアクセス停止時間がないことが望ましいです。
3. ボリュームレベルのレプリケーションを行っている場合のリストアの流れについて情報提供をお願い致します。
4. ストレージの状態を HTTP API リファレンスの情報提供をお願い致します。
5. バックアップストレージのストレージレプリケーションに関する機能の情報提供をお願い致します。

3.1.11.3. マルウェア対策機能

1. 製品のライセンス体系に関して情報提供をお願い致します。
2. 検出したマルウェアのハッシュ値に関して、対応しているハッシュアルゴリズムの情報提供をお願い致します。

3.1.11.4. バックアップ

1. バックアップ用のエージェントの有無による機能差分に関する情報提供をお願い致します。
2. バックアップジョブのログ出力方式に関する情報提供をお願い致します。
3. ファイルベースのレプリケーションを行う際、設定可能なレプリケーション周期、実績に関する情報提供をお願い致します。
4. バックアップ処理時に発生する実際の IP 通信、SAN 通信に関する情報提供をお願い致します。
5. バックアップ処理時間を短縮させるための方法に関する情報提供をお願い致します。
6. 製品のライセンス体系の情報提供をお願い致します。

3.2. ネットワークシステム

3.2.1. ファイアウォール

3.2.1.1. 外部ファイアウォール A

3.2.1.1.1. 機能

1. 10GBase-R に対応した物理インターフェースを 2 ポート以上有すること。
2. 1000Base-T に対応した物理インターフェースを 12 ポート以上有すること。
3. 筐体内で複数の仮想的なファイアウォール装置を動作可能なこと。仮想的なファイアウォールは 3 個以上構成可能なこと。仮想的なファイアウォールを使用することで物理ポートの使用量が増加する場合、さらに 10Gbase-R を 4 ポート、1000Base-T を 8 ポート収容可能なモデルとすること。
4. 仮想ファイアウォールごとにルーティングテーブルを保持可能なこと。
5. 仮想ファイアウォールごとに OSPF を動作可能なこと。
6. 2 台の筐体を使用した HA 機能を有し、Active-Standby で動作すること。Active 機で通信経路障害やハードウェア障害が発生した場合、自動的に Standby 機が Active 機に遷移すること。
7. 仮想的なファイアウォールごとに HA 機能においてアクティブとする機器を指定可能なこと。
8. IPS 機能を有し、インバウンド通信に対して OS インジェクション、DDoS、TCP アノマリー、L4 フラッド通信、主要な Web サーバ・メールリレー・データベース等のミドルウェアや Java、PHP、Python、.NET 等のソフトウェアライブラリの脆弱性を標的とした通信を遮断可能なこと。
9. IPS に使用されるシグネチャは自動的に最新状態に更新可能なこと。
10. IPS の有効・無効はファイアウォールポリシ単位に設定が可能なこと。
11. TLS 通信に対しても復号化した上で IPS による通信の遮断が可能なこと。IPS による通信の確認後、正常と判断された通信を再暗号化して IP 転送が可能なこと。指定したトラフィックは再暗号化を行わない動作が可能なこと。
12. TLS 通信を復号化し、IPS による検査を行った上で 1.2Gbps 以上のファイアウォールスループットを備えていること。
13. 2021 年 10 月 1 日時点の CRYPTREC 暗号リストで規定される暗号方式に対応し、復号化、再暗号化が可能なこと。
14. 指定したファイアウォールポリシにマッチしたトラフィックをロギング可能なこと。

3.2.1.1.2. 見積の前提

1. 筐体 2 台により HA 構成とすること。
2. ミラーポートの出力ポート用に 10GBase-R ポートを筐体ごとに 1 ポート想定し、10GBase-LR 接続が可能になるようにモジュールを搭載すること。
3. 通信用 10GBase ポートには 10GBase-SR を搭載すること。

4. 電源冗長構成とすること。
5. 機能要件を満たす IPS 機能が使用可能なライセンスを搭載すること。
6. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
7. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
8. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.1.2. 外部ファイアウォール B

3.2.1.2.1. 機能

1. 10GBase-R に対応した物理インターフェースを 2 ポート以上有すること。
2. 1000Base-T に対応した物理インターフェースを 12 ポート以上有すること。
3. 筐体内で複数の仮想的なファイアウォール装置を動作可能なこと。仮想的なファイアウォールは 4 個以上構成可能なこと。仮想的なファイアウォールを使用することで物理ポートの使用量が増加する場合、さらに 10Gbase-R を 6 ポート、1000Base-T を 12 ポート収容可能なモデルとすること。
4. 仮想ファイアウォールごとにルーティングテーブルを保持可能なこと。
5. 仮想ファイアウォールごとに OSPF を動作可能なこと。
6. 2 台の筐体を使用した HA 機能を有し、Active-Standby で動作すること。Active 機で通信経路障害やハードウェア障害が発生した場合、自動的に Standby 機が Active 機に遷移すること。
7. 仮想的なファイアウォールごとに HA 機能においてアクティブとする機器を指定可能なこと。
8. IPS 機能を有し、インバウンド通信に対して OS インジェクション、DDoS、TCP アノマリー、L4 フラッド通信、主要な Web サーバ・メールリレー・データベース等のミドルウェアや Java、PHP、Python、.NET 等のソフトウェアライブラリの脆弱性を標的とした通信を遮断可能なこと。
9. IPS に使用されるシグネチャは自動的に最新状態に更新可能なこと。
10. IPS の有効・無効はファイアウォールポリシ単位に設定が可能なこと。
11. TLS 通信に対しても復号化した上で IPS による通信の遮断が可能なこと。IPS による通信の確認後、正常と判断された通信を再暗号化して IP 転送が可能なこと。指定したトラフィックは再暗号化を行わない動作が可能なこと。
12. 2021 年 10 月 1 日時点の CRYPTREC 暗号リストで規定される暗号方式に対応し、復号化、再暗号化が可能なこと。
13. TLS 通信を復号化し、IPS による検査を行った上で 1.2Gbps 以上のファイアウォールスループットを備えていること。
14. 指定したファイアウォールポリシにマッチしたトラフィックをロギング可能なこと。

3.2.1.2.2. 見積の前提

1. 筐体 2 台により HA 構成とすること。

2. ミラーポートの出力ポート用に 10GBase-R ポートを筐体ごとに 1 ポート想定し、10GBase-LR 接続が可能になるようにモジュールを搭載すること。
3. 通信用 10GBase ポートには 10GBase-SR を搭載すること。
4. 電源冗長構成とすること。
5. 機能要件を満たす IPS 機能が使用可能なライセンスを搭載すること。
6. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
7. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
8. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.1.3. 外部ファイアウォール C

3.2.1.3.1. 機能

1. 10GBase-R に対応した物理インターフェースを 2 ポート以上有すること。
2. 1000Base-T に対応した物理インターフェースを 12 ポート以上有すること。
3. 筐体内で複数の仮想的なファイアウォール装置を動作可能なこと。仮想的なファイアウォールは 3 個以上構成可能なこと。仮想的なファイアウォールを使用することで物理ポートの使用量が増加する場合、さらに 10Gbase-R を 4 ポート、1000Base-T を 8 ポート収容可能なモデルとすること。
4. 仮想ファイアウォールごとにルーティングテーブルを保持可能なこと。
5. 仮想ファイアウォールごとに OSPF を動作可能なこと。
6. 8Gbps 以上のファイアウォールスループットを備えていること。
7. C2C サーバ等の悪意ある IP アドレスのデータベースを有し、DNS による名前解決が行われる際に悪意ある IP アドレスが返された場合に、実際のアプリケーション通信が行われないように通信遮断が可能なこと。
8. 2 台の筐体を使用した HA 機能を有し、Active-Standby で動作すること。Active 機で通信経路障害やハードウェア障害が発生した場合、自動的に Standby 機が Active 機に遷移すること。
9. 仮想的なファイアウォールごとに HA 機能においてアクティブとする機器を指定可能なこと。
10. 指定したファイアウォールポリシにマッチしたトラフィックをロギング可能なこと。

3.2.1.3.2. 見積の前提

1. 筐体 2 台により HA 構成とすること。
2. ミラーポートの出力ポート用に 10GBase-R ポートを筐体ごとに 1 ポート想定し、10GBase-LR 接続が可能になるようにモジュールを搭載すること。
3. 通信用 10GBase ポートには 10GBase-SR を搭載すること。
4. 電源冗長構成とすること。
5. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
6. 最新のファームウェアやアプリケーションソフトウェアを提供すること。

7. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.1.4. 内部ファイアウォール A

3.2.1.4.1. 機能

1. 10GBase-R に対応した物理インターフェースを 2 ポート以上有すること。
2. 1000Base-T に対応した物理インターフェースを 12 ポート以上有すること。
3. 筐体内で複数の仮想的なファイアウォール装置を動作可能なこと。仮想的なファイアウォールは 3 個以上構成可能なこと。仮想的なファイアウォールを使用することで物理ポートの使用量が増加する場合、さらに 10Gbase-R を 4 ポート、1000Base-T を 8 ポート収容可能なモデルとすること。
4. 仮想ファイアウォールごとにルーティングテーブルを保持可能なこと。
5. 仮想ファイアウォールごとに OSPF を動作可能なこと。
6. 4Gbps 以上のファイアウォールスループットを有すること。
7. 2 台の筐体を使用した HA 機能を有し、Active-Standby で動作すること。Active 機で通信経路障害やハードウェア障害が発生した場合、自動的に Standby 機が Active 機に遷移すること。
8. 仮想的なファイアウォールごとに HA 機能においてアクティブとする機器を指定可能なこと。
9. 指定したファイアウォールポリシにマッチしたトラフィックをロギング可能なこと。

3.2.1.4.2. 見積の前提

1. 筐体 2 台により HA 構成とすること。
2. ミラーポートの出力ポート用に 10GBase-R ポートを筐体ごとに 1 ポート想定し、10GBase-LR 接続が可能になるようにモジュールを搭載すること。
3. 通信用 10GBase ポートには 10GBase-SR を搭載すること。
4. 電源冗長構成とすること。
5. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
6. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
7. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.1.5. 内部ファイアウォール B

3.2.1.5.1. 機能

1. 10GBase-R に対応した物理インターフェースを 2 ポート以上有すること。
2. 1000Base-T に対応した物理インターフェースを 12 ポート以上有すること。
3. 筐体内で複数の仮想的なファイアウォール装置を動作可能なこと。仮想的なファイアウォールは 3 個以上構成可能なこと。仮想的なファイアウォールを使用することで物理ポートの使用量が増加する場合、さらに 10Gbase-R を 2 ポート、1000Base-T を 8 ポート収容可能なモデルとすること。

4. 仮想ファイアウォールごとにルーティングテーブルを保持可能なこと。
5. 仮想ファイアウォールごとに OSPF を動作可能なこと。
6. 8Gbps 以上のファイアウォールスループットを有すること。
7. 2 台の筐体を使用した HA 機能を有し、Active-Standby で動作すること。Active 機で通信経路障害やハードウェア障害が発生した場合、自動的に Standby 機が Active 機に遷移すること。
8. 仮想的なファイアウォールごとに HA 機能においてアクティブとする機器を指定可能なこと。
9. 指定したファイアウォールポリシにマッチしたトラフィックをロギング可能なこと。
10. 高さは 2RU 以下であること。

3.2.1.5.2. 見積の前提

1. 筐体 2 台により HA 構成とすること。
2. 通信用 10GBase ポートには 10GBase-SR を搭載すること。
3. 電源冗長構成とすること。
4. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
5. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
6. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.1.6. 情報提供依頼特記事項

1. 「3.3.7 ファイアウォール管理システム」に記す管理システムとあわせ、ファイアウォールトラフィックログ、IPS による遮断ログを別サーバにテキストファイルとして格納可能であればその方法とテキストファイルのローテーションについて情報提供をお願い致します。
2. 外部ファイアウォール C が Cloud Access Security Broker に関連する機能を有している場合、機能の情報提供をお願い致します。

3.2.2. イーサネットスイッチ

3.2.2.1. L3 スイッチ A

3.2.2.1.1. 機能

1. 10GBase-R に対応した物理インターフェースを 24 ポート以上有すること。
2. 25GBase-R に対応した物理インターフェースを 8 ポート以上有すること。
3. 1000Base-X に対応した物理インターフェースを 8 ポート以上有すること。10GBase-R インターフェースを 1000Base-X インターフェースとして使用できる場合、このインターフェースを専用に用意する必要はない。
4. 1000Baest-T に対応した物理インターフェースを 24 ポート以上有すること。
5. CPU 処理により動作する機能を制御するモジュールは二重化されており、片系のモジュールに障害が発生した場合でも通信影響が軽微なこと。
6. 通信ポートとは別に IP 通信可能な管理用インターフェースを備えていること。

7. RJ-45 または RS232C で接続可能な管理用コンソールインターフェースを備えていること。
8. 装置全体で 1Tbps 以上のスループットを備えていること。
9. スタックに対応していること。スタック接続を行うインターフェースは 360Gbps 以上の帯域幅を有すること。
10. IPv4、IPv6 デュアルスタックで動作可能なこと。
11. IPv4、IPv6 インターフェースをそれぞれ 1024 個以上設定可能なこと。
12. ルーティングプロトコルとして OSPF、OSPFv3 に対応していること。
13. グレースフルリスタートに相当する機能に対応しており、自身のルーティングプロトコル動作に異常が発生した場合、ヘルパー機能を持つ周囲の L3 通信機器に OSPF の制御指示を発行可能なこと。
14. スタックマスタとして動作している筐体に障害があった場合でもルーティングテーブルを消失しないこと。
15. L2～L4 を制御対象とする ACL を設定可能なこと。ACL はハードウェア処理であること。
16. ACL は 1 個の VLAN インターフェースに対して 50 個以上指定可能なこと。装置総数として 2000 個以上指定可能なこと。
17. sFlow または NetFlow に対応していること。
18. ポートミラーリングが可能で、ミラーリング対象ポートとして 8 ポート以上指定可能なこと。
19. 電源冗長が可能なこと。
20. 200V 電源で動作可能なこと。

3.2.2.1.2. 見積の前提

1. 筐体 2 台でスタック構成とすること。
1. 筐体 1 台あたり SR-SFP28 を 4 個、SR-SFP+を 12 個搭載すること。
2. ミラーポートの出力ポート用に 10GBase-R ポートをスタック全体で 1 ポート想定し、10GBase-LR 接続が可能になるようにモジュールを搭載すること。
3. 電源冗長構成とすること。
4. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
5. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
6. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.2.2. L2 スイッチ A

3.2.2.2.1. 機能

1. 10GBase-R に対応した物理インターフェースを 32 ポート以上有すること。
2. 25GBase-R に対応した物理インターフェースを 2 ポート以上有すること。
3. ワイヤーレートで通信が可能なこと。
4. スタック機能を有すること。

5. sFlow または NetFlow に対応していること。
6. ポートミラーリングが可能で、ミラーリング対象ポートとして 8 ポート以上指定可能なこと。
7. 電源冗長が可能なこと。電源ユニットの交換は活性状態で実施可能なこと。

3.2.2.2.2. 見積の前提

1. 筐体 2 台でスタック構成とし、同様の構成を 2 セット用意すること。
2. 筐体 1 台あたり SR-SFP28 を 1 個、SR-SFP+を 16 個搭載すること。
3. ミラーポートの出力ポート用に 10GBase-R ポートをスタック全体で 1 ポート想定し、10GBase-LR 接続が可能になるようにモジュールを搭載すること。
4. 電源冗長構成とすること。
5. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
6. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
7. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.2.3. L2 スイッチ B

3.2.2.3.1. 機能

1. 10GBase-R に対応した物理インターフェースを 2 ポート以上有すること。
2. 1000Base-T に対応した物理インターフェースを 48 ポート以上有すること。
3. ワイヤーレートで通信が可能なこと。
4. スタック機能を有すること。
5. sFlow または NetFlow に対応していること。
6. ポートミラーリングが可能で、ミラーリング対象ポートとして 8 ポート以上指定可能なこと。

3.2.2.3.2. 見積の前提

1. 筐体 2 台でスタック構成とし、同様の構成を 2 セット用意すること。
2. 筐体 1 台あたり SR-SFP+を 1 個搭載すること。
3. ミラーポートの出力ポート用を 1 ポート想定すること。
4. 電源冗長構成とすること。
5. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
6. 最新のファームウェアやアプリケーションソフトウェアを提供すること。
7. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.2.4. 情報提供依頼特記事項

1. L3 スイッチ A について、装置にトラフィックが着信して発信される間における装置内モジュールやモジュール間接続のスループットに関する情報提供をお願い致します。
2. 装置の設定情報とソフトウェアのバックアップ方法について情報提供をお願い致します。

3. 運用管理目的で装置にログインする際に使用するアカウント保持、対応している認証方式について情報提供をお願い致します。

3.2.3. ハードウェアロードバランサ

3.2.3.1. 機能

1. 10GBase-R に対応した物理インターフェースを 4 ポート以上有すること。
2. 1000Base-T に対応した物理インターフェースを 4 ポート以上有すること。
3. ルーティングプロトコルとして OSPF に対応していること。
4. 16Gbps 以上の L4/L7 ロードバランススループットを有すること。
5. ECDH 暗号に対して 2500CPS 以上の TLS 復号化性能を有すること。
6. L3 Direct Server Return に対応していること。
7. セッション ID を記した Cookie をベースとしたロードバランスが可能なこと。装置に備わったスクリプト機能を使用して良い。
8. 特定のロードバランス用仮想 IP アドレスにアクセス可能な送信元 IP アドレスを制御可能なこと。
9. REST API に対応しており、スクリプトベースの HTTP アクセスでロードバランス設定、設置値、負荷状況の取得が可能なこと。
10. 装置 2 台で冗長構成が可能なこと。
11. 装置内で複数の仮想的なロードバランサを構成可能なこと。仮想ロードバランサはそれぞれルーティングテーブル、ロードバランス、管理用 WebGUI、管理用 CLI を有すること。
12. 仮想ロードバランサごとにアクティブとする物理筐体を指定可能なこと。物理筐体に障害が発生した場合は自動的に待機系の筐体で動作をするように構成可能なこと。
13. 装置にログインするアカウントに権限を割り当て、権限に応じた仮想ロードバランサのみ設定、状態参照が可能なこと。ログインアカウントは装置内アカウントの他に LDAP(S)認証、Radius 認証が可能なこと。SAML 認証に対応していることが望ましい。
14. VLAN や IP インターフェース、その他基本的な装置のシステム設定は全体管理者のみ可能なように権限設定が可能なこと。
15. 冗長構成としている装置の設定は同期可能なこと。同期動作の開始は WebUI・CLI からの手動実行、スクリプトベースの HTTP アクセスで実行が可能なこと。
16. 19 インチラックに搭載可能なこと。
17. 電源冗長が可能なこと。

3.2.3.2. 見積の前提

1. 装置を 2 台で HA 構成とし、同様の構成を 2 セット用意すること。
2. 10GBase-R インターフェースに 10GBase-SR で接続可能なモジュールを搭載すること。
3. 電源冗長構成とすること。

4. ハードウェア保守は平日日中帯オンサイト対応とし、障害検出翌営業日までに対応すること。
5. 細心のファームウェアやアプリケーションソフトウェアを提供すること。
6. 製品の技術仕様に関するメール、電話による問い合わせに対応すること。

3.2.3.3. 情報提供依頼特記事項

1. 対応しているロードバランスアルゴリズムの情報提供をお願い致します。
2. IPv4/IPv6 デュアルスタック及びルーティングプロトコルの対応状況、実績について情報提供をお願い致します。
3. 複数の管理者で装置を管理する場合の権限付与、認証の仕組みに関する情報提供をお願い致します。

3.3. システム管理システム

3.3.1. システム状態管理

稼働するシステムの状態管理を行うための製品として Zabbix 社 Zabbix を使用することを想定している。Zabbix は仮想基盤システム上に構築する。Zabbix 用の OS 構築、必要なソフトウェアインストール、監視設定は PMDA が行う。

用途に応じて 4 台の Zabbix サーバを構築する場合のソフトウェアサポートを 2 年間提供すること。そのうち 1 台の Zabbix プロキシをあわせて構築する。

ソフトウェアサポートの要件は以下の通り。

1. 1 年間に 5 件以上のソフトウェアトラブルの解決に必要な情報を提供すること。
2. Zabbix で使用可能な関数等の一覧を記したドキュメントを閲覧可能なこと。
3. 操作方法に問い合わせに対応可能なこと。
4. 平日日中帯に対応可能な体制を維持すること。問い合わせに対する一次回答を翌営業日までに行うこと。

3.3.2. sFlow コレクタ

ネットワーク機器からネットワークフローを採取し、sFlow コレクタで統計を取る。以下の要件を満たす sFlow コレクタの製品、サポートを提供すること。尚、OS、ソフトウェアインストール、監視設定は PMDA が行うことを想定している。

1. 仮想基盤システム上の仮想マシンにて、Windows Server2016、Windows Server2019、RedhatEnterpriseLinux8 のいずれかで動作可能なこと。
2. Web ブラウザでアクセス可能な GUI を備えていること。
3. SAML 認証の SP として登録可能であることが望ましい。
4. sFlow、NetFlow に対応していること。
5. 1000 物理インターフェース以上の監視対象からフロー情報を取得可能なこと。
6. 1 秒あたり 70000 フロー以上を処理可能なこと。

7. REST API に対応しており、スクリプトベースの HTTPS アクセスで本製品に保存されたフロー情報を取得可能なこと。

3.3.3. RedHat Enterprise Linux 向けソフトウェア管理

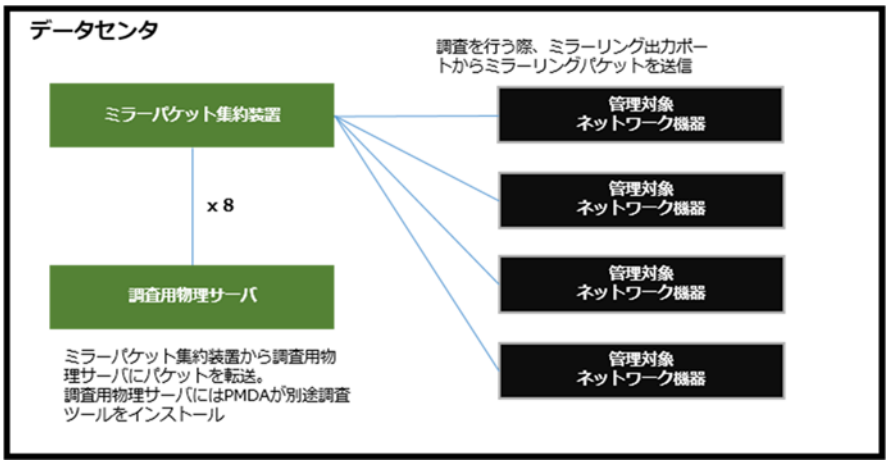
本システムで稼働させる RedHat Enterprise Linux のソフトウェアを集中管理するための製品として Satellite を仮想基盤システム上に構築する。OS 設定、ソフトウェアインストール、設定は PMDA が行うので、必要なライセンスを含めること。

3.3.4. 構成管理

本システムで稼働させるサーバ等の各ノードの構成管理を行うための製品として Ansible 及び Ansible Tower を仮想基盤システム上に構築する。OS 設定、ソフトウェアインストール、設定は PMDA が行うので、必要なライセンスを含めること。管理対象ノード数は 500 台とすること。

3.3.5. リモートパケット収集システム

トラブルシュートを目的として、データセンタ内のネットワーク機器の任意の物理インターフェースを通過するパケットを現地に行かなくても取得できるような仕組みを導入する。システム構成のイメージは図の通り。本システムの冗長化は基本的に不要とする。



パケットミラーリングを行い、ミラーパケット集約装置に接続することを想定している機器種別は以下の通り。

- イーサネットスイッチ
- ファイアウォール

ミラーパケット集約装置は以下のような機能、性能を有していることが望ましい。

1. ミラーパケットの受信、受信したミラーパケットの送出を行える物理ポートを 16 ポート以上備

えていること。

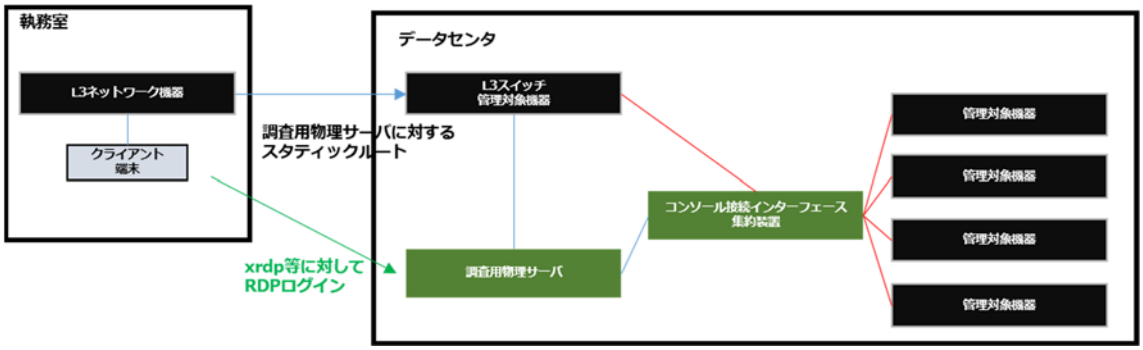
2. 管理対象のネットワーク機器のミラーパケットを受信するポート、調査用物理サーバと接続するポートは 10Gbps 以上のスループットを有すること。
3. ミラーパケットの受信ポートが違っていても同時に調査用物理サーバに送信可能なこと。
4. 指定した受信ポートからのミラーパケットのみ調査用物理サーバに送信可能なこと。
5. ミラーパケットを調査用物理サーバに送信する際、L2、L3、L4 フィルタリングが可能なこと。
6. IP 通信による装置の死活監視が可能なこと。
7. 19 インチラックに搭載可能なこと。

調査用物理サーバは以下のような機能、性能を有していることが望ましい。

1. RedHat Enterprise Linux が動作可能な汎用サーバであること。
2. OS ライセンスも含めること。
3. ミラーパケット受信用インターフェースとして 10Gbps のスループットを持つネットワークインターフェースを 8 個以上有すること。
4. サーバが通信するためのインターフェースとして、1000Base-T または 1000Base-X のネットワークインターフェースを 2 個有すること。
5. L2 スイッチ(運用管理)に 1000Base-T でチーミングにより冗長接続可能なこと。
6. 8 コア以上を備えたプロセッサを 2 個以上搭載可能なこと。
7. 物理メモリを 96GB 以上搭載していること。
8. RAID5 相当のディスク障害耐性を持ち、オンラインでディスク交換可能なこと。ディスク障害時に自動的にオンライン状態に遷移するスタンバイディスクを備えていること。
9. 実効ディスク容量として 1 TB 以上を備えていること。
10. 装置管理用の IP 通信可能なネットワークインターフェースを備えていること。

3.3.6. コンソールインターフェース管理システム

データセンタ内のネットワーク機器に搭載されているローカルコンソールインターフェース経由で、ネットワーク機器をリモート操作可能な環境を構築する。設定変更や障害によりネットワーク機器のルーティングテーブルが意図しない状態になり、各ノードの通信が不安定になった時でもローカルコンソールからネットワーク機器のメンテナンス作業を行えるようにすることを想定している。システム構成のイメージは下図の通り。本システムの冗長化は基本的に不要とする。



赤い線はコンソールインターフェース、青い線は IP 通信インターフェースを意図している。

リモート操作対象として想定している機器種別は以下の通り。

- イーサネットスイッチ
- ファイアウォール
- ハードウェアロードバランサ

コンソール接続インターフェース集約装置の要件は以下の通り。

1. 操作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 40 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. 調査用物理サーバと IP 通信可能な 1000Base-T インターフェースを 1 ポート以上備えていること。ネットワーク接続はイーサネットスイッチを経由する可能性がある。

調査用物理サーバは「3.3.5 リモートパケット収集システム」のものと兼用で良い。

3.3.7. ファイアウォール管理システム

「3.2.1 ファイアウォール」に記した各ファイアウォールの設定、装置状態、ログを集中管理する。このシステムの要件は以下の通り。尚、必ずしも単一製品で全機能を提供する必要はない。

1. 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。
2. 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。
3. 管理対象のファイアウォールにファイアウォール管理システムからファイアウォールポリシを設定可能なこと。
4. 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。
5. 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。

6. 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。トラフィックログとして 1 日あたり 20GB 以上のログを取得可能かつ、合計 5TB 以上のログを保持可能なこと。
7. 管理対象のファイアウォール及びファイアウォール管理システムの操作ログ、システムログを集約して記録可能なこと。
8. ファイアウォール管理システムをハードウェアベースで実現する場合、少なくともディスク 1 個の障害によりシステム停止しないようにディスク冗長化を行うこと。
9. システム管理機能へのログインは SAML 認証に対応していることが望ましい。

3.4. アプリケーション

3.4.1. SAML 認証基盤

3.4.1.1. 概要

現行システムでは Microsoft 社 Active Directory を使用したドメイン認証、LDAP 認証と Microsoft 社 Azure Active Directory を使用した認証を行っている。この基本構成は変更しないが、本システムではオンプレミスで SAML 認証が可能となる認証基盤を新しく構築する。現時点で業務システムをまたいだ SAML 認証によるシングルサインオン認証は行わないが、今後のシステム拡張を踏まえて基本的な認証基盤を構築することを目的としている。下記の要件を満たす製品を構成に含めること。

3.4.1.2. IdP サーバ

クライアント端末の Web ブラウザから IdP サーバにより既存 Active Directrory 上のユーザアカウント情報を利用して認証が行えるような形を想定している。

クライアント端末へのログオンと IdP サーバでの認証をシングルサインオン構成とはせず、手起動による Web ブラウザから認証実施とする。IdP サーバはオンプレミスで動作する製品とすること。

3.4.1.3. SP

PMDA が構築する Zabbix 社 Zabbix(バージョン 5 系)を現時点での必須対象とするが、他に本システムの運用管理に使用される各アプリケーションが SP として登録可能であることが望ましい。PMDA の既存業務システムを SP として準備することは想定していない。

3.4.1.4. 要件

1. 多要素認証に対応していること。
2. IdP サーバが Active Directory に対して行うアカウント情報の照合は LDAD(S)、Kerberos が使用可能なこと。

3. 認証とあわせて認可によるアクセス制御が可能なこと。
4. 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。
5. 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。
6. フロントエンドになる IdP サーバの冗長化が可能なこと。
7. Web アプリケーション以外のアプリケーションに対するシングルサインオンが実現可能なこと。

3.4.1.5. 見積の前提

1. IdP サーバは冗長構成とすること。

3.4.1.6. 情報提供依頼特記事項

1. 対応している多要素認証に関する情報提供をお願い致します。
2. 対応している認証バックエンド方式(LDAP 認証等)に関する情報提供をお願い致します。
3. Web アプリケーション以外のアプリケーションに対する認証の仕組みに関する情報提供をお願い致します。

3.4.2. HTTP プロキシ

3.4.2.1. 機能

1. 1 台あたり 500 名の同時利用が可能なこと。実績では 1 分あたりの HTTP リクエスト数は 9000 程度。
2. 2 台で両アクティブの冗長構成が可能なこと。冗長には別途ロードバランサを使用しても良い。
3. カテゴリベースの URL フィルタが可能なこと。
4. URL フィルタのカテゴリには少なくともギャンブル、犯罪、薬物、思想、暴力、ソーシャルメディア、P2P サービス、オンラインファイル共有サービス、Web メールサービスを指定可能なこと。
5. ブロック対象のカテゴリであっても指定した宛先に対する通信は許可可能なこと。
6. プロキシサーバ利用時のユーザベースの認証に対応し、Kerberos、NTLM、LDAP(S)が使用可能なこと。
7. URL フィルタの適用単位として送信元 IP、ユーザベース認証のユーザ名を指定可能なこと。
8. HTTP アクセスログを HTTP プロキシサーバ内と外部 Syslog サーバ両方に出力可能なこと。
9. SSL/TLS を復号化し、HTTPS 通信の内容をロギング可能なこと。
10. SSL/TLS 対象外の宛先を指定可能なこと。
11. 管理者が任意に遮断対象の URL を設定可能なこと。URL にはドメインのみの指定、FQDN での指定、ワイルドカードが使用可能なこと。
12. 任意に設定する遮断対象の宛先は 25000 件以上登録可能なこと。
13. 遮断対象をグルーピング可能なこと。遮断対象にマッチした通信は HTTP アクセスログに記録可能なこと。そのログからどのグループにマッチしたか確認が可能なこと。

14. スクリプトベースの HTTP アクセスにより遮断登録、解除が可能な API を備えていること。スクリプトベースの処理ができない場合、少なくとも CLI ベースでこれらの操作が可能なこと。
15. API はトークンベースの認証に対応していること。
16. 全体の設定を確認可能な WebUI を備えていること。

3.4.2.2. 見積の前提

1. 2 台構成とすること。
2. 既存 Active Directory 上のユーザアカウントをプロキシ認証に使用可能な構成とすること。

3.4.2.3. 情報提供依頼特記事項

1. プロキシ認証を行った場合にユーザ単位に制御可能な設定項目に関する情報提供をお願い致します。
2. 対応しているプロキシ認証の認証方式に関する情報提供をお願い致します。
3. プロキシ認証使用時、VDI やターミナルサーバ等、利用者と端末が固定されない環境での動作実績、構成、課題について情報提供をお願い致します。
4. URL フィルタのカテゴリに関して、設定可能なカテゴリ一覧の情報提供をお願い致します。

3.4.3. Windows Server によるファイル共有サーバアクセスログ出力

本システムには Windows Server の機能を使用したファイル共有サーバを別途数台構築する。このファイルサーバ上で共有されているファイル、フォルダに対するアクセスログを Windows イベントログより分かりやすい形で保存する。

3.4.3.1. 機能

1. ファイルの読み取り、書き込み(新規作成、削除を含む)について、時刻、クライアントの Windows ドメインユーザ、接続元 IP アドレス、対象のファイル名、ファイル操作種別を記録可能なこと。
2. フォルダの書き込み(新規作成、削除、名称変更)について、時刻、クライアントの Windows ドメインユーザ、接続元 IP アドレス、対象のフォルダ名、フォルダ操作種別を記録可能なこと。
3. 記録したログをテキストファイルに自動出力可能なこと。ログはファイル、フォルダに対する 1 アクセスあたり 1 行で構成されること。テキストデータであればテキスト、CSV 等ファイル形式は問わない。
4. ログのテキストファイル出力は 3 時間より短い周期で実施可能なこと。31 日分のログを本機能内に保持可能なこと。指定した日数経過後に自動的にテキストファイルがローテーションされることが望ましい。現行システムでもこうしたログを取得しており、1 時間あたりのログファイルのサイズは 50MB 程度であることが分かっている。

3.4.3.2. 情報提供依頼特記事項

1. ライセンス体系に関して情報提供をお願い致します。
2. 導入に際する具体的なネットワーク構成、サーバ構成、必要であればエージェントソフトウェアに関する情報提供をお願い致します。ログ取得対象のファイル共有サーバは仮想マシン、物理サーバ両方の可能性があります。

3.5. 物理ロケーション

本システムの構成要素を設置するデータセンタを指す。

3.5.1. 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. 全ての開口部は地面より高いこと。
8. 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。
9. 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。
10. 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。
11. 耐震性能は耐震安全性とグレードが特級以上であり免震であること。
12. 不正侵入及び平井物による損傷を防止するため、データセンタの外壁に防護柵等の対策が施されていること。
13. 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。
14. 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 48 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。
15. 燃料業者との間で優先供給契約を締結していること。
16. 自家発電装置が稼働するまでの装置の電源供給として並列冗長動作可能な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。
17. 自家発電装置は免震設備の建屋に設置されていること。
18. 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。

19. 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。
20. 内装材は不燃材または難燃材であること。
21. 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。
22. 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。
23. 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。
24. 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。
25. 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。
26. 塩害を受ける恐れの少ない場所であること。
27. 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。
28. 什器・備品は転倒、移動防止措置が施されていること。
29. データセンタの出入り口に施錠機能を有すること。
30. 24 時間 365日警備員による入退館者の管理・監視を実施していること。
31. 搬入設備は搬入専用の設備があること。
32. データセンタ内で作業に必要な媒体を保管するための保管庫を有していること。
33. 機器設置室内はフリーアクセス床であること。天井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。
34. フリーアクセス床や天井は許可なく開閉ができないような対策を行っていること。

3.5.2. 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。

3.5.3. 運用要件

1. ラックごとの電力消費量を可視化可能なこと。
2. ラックに搭載している機器の LED を確認し、事前に定めた正常ルールに合致しない場合、メール、電話にてアラート発報が可能なこと。LED の確認は 1 日に 1 回以上行われること。

3.5.4. 見積の前提

1. ラック要件を満たす 19 インチラック 1 台あたりのコストを算出すること。

3.5.5. 情報提供依頼特記事項

1. ラック 1 本あたりの最大消費可能電力に関する情報提供をお願い致します。
2. ラック 1 本あたりの耐荷重に関する情報提供をお願い致します。
3. PMDA がラックを搬入し設置可能な場合、前提となる条件に関する情報提供をお願い致します。