共用 LAN システム
情報インフラセキュリティログ管理システム及び
EDR の更新に係る賃貸借
調達仕様書

令和 6 年 4 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）　調達件名

共用 LAN システム 情報インフラセキュリティログ管理システム及び EDR の更新に係る賃貸借

（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、業務に使用する IT システムを複数保有しており、業務システムを構成するサーバ及びその情報セキュリティ対策の一環としてネットワークセキュリティ装置、エンドポイントセキュリティ装置を導入している。現在、サーバの監査ログ、各セキュリティ装置の各機能の動作ログを格納し可視化するログ管理システムを運用しているが、このシステムの運用終了に伴い、機能を再設計した上で新しいログ管理システムを構築する。また、クライアント端末やサーバを対象とした EDR ツールの更新も同時に行う。(以下本件に関する調達内容を指して「本調達」という。)

（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	業務システム統合基盤システムの構築及び保守	

（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 業務システム統合基盤システムの構築及び保守

本調達で導入する製品を稼働させるためのファシリティ、リソースの一部を本件の導入品から充当する。仮想マシンを稼働させるための仮想基盤システム、ハードウェアを設置するためのデータセンタ及びラック、電源設備が該当する。詳細な技術要件は別紙 3 システム詳細要件に記載している。以後、この仮想基盤システムを以後「既存仮想基盤システム」、ラック及び電源設備のことを「既存ラック」という。

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。

① ログ管理システムの構築

受注者は業務サーバ、ネットワークセキュリティ装置、エンドポイントセキュリティ装置の各ログを受信し、各機能の動作状況、監査ログの検索、可視化を分かりやすいグラフィカルインターフェースで提供するログ管理システムを導入すること。既存仮想基盤システム以外にハードウェアが必要な場合はそれを含めること。ハードウェアは既存ラックに搭載すること。

② EDR 環境の更新

受注者は現在運用している EDR のための環境である Tanium 社 Tanium を利用できる環境を構築すること。クライアント端末を管理するためのソフトウェアをインストールするサーバは既存仮想基盤システム上に構成する。また、現環境の Tanium クライ

アントソフトウェアのバージョンアップ作業の計画、実施支援も含む。実際のクライアントソフトウェアのバージョンアップ作業は PMDA が行う。

③　ハードウェアの設置、配線作業

受注者は本調達で導入するハードウェアを既存ラックに搭載し、そのハードウェアが既存仮想基盤システムのネットワークや共有ストレージを使用できるようにネットワークケーブルを敷設すること。ケーブル敷設作業は既存ラックが設置されているデータセンタの指定業者が行う必要がある。受注者はそれらの作業、費用を構成に含めること。

④　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。

⑤　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。具体的な保守内容は別紙 3 システム詳細要件に記載している。

（２）　成果物の期日等

納入成果物は以下のそれぞれの期限までに提出し、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	ログ管理システムの画面設計書	2024 年 8 月 31 日
2	別紙 3 システム詳細要件に記す全てのドキュメント (※データ消去証明書を除く)	2024 年 12 月 20 日
3	データ消去証明書	2029 年 12 月 26 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５年度版）」に準拠しているので、必要に応じ参照すること。セキュリティポリシーの開示については、契約締結後、受注者が担当職員に「秘密保持等に関する誓約書」を提出した際に開示する。

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

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

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

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

６　成果物の取扱いに関する事項

（１）　知的財産権の帰属

知的財産の帰属は、以下のとおり。

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

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

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

④ 本件に係り作成・変更・修正されるドキュメント類及びプログラム等に第三者が権利を有する著作物が含まれる場合、受注者は当該著作物の使用に必要な費用負担や使

用許諾契約に係る一切の手続きを行うこと。この場合は事前に PMDA に報告し、承認を得ること。

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

（２） 契約不適合責任

① 本業務の最終検収後 1 年以内の期間において、委託業務の納入成果物に関して本システムの安定稼動等に関わる契約不適合の疑いが生じた場合であって、PMDA が必要と認めた場合は、受注者は速やかに契約不適合の疑いに関して調査し回答すること。調査の結果、納入成果物に関して契約不適合等が認められた場合には、受注者の責任及び負担において速やかに修正を行うこと。なお、修正を実施する場合においては、修正方法等について、事前に PMDA の承認を得てから着手すると共に、修正結果等について、PMDA の承認を受けること。

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

（３） 検収

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

なお、以下についても遵守すること。

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

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

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

7　入札参加資格に関する事項

（1）　入札参加要件

応札希望者は、以下の条件を満たしていること。

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

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

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

（2）　入札制限

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

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

② 各工程の調達仕様書の作成に直接関与した事業者等

③ 設計・開発等の工程管理支援業者等

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

⑤ ①～③と同一の親会社を持つ事業者

⑥ ①～③から委託を請ける等緊密な利害関係を有する事業者

8　情報セキュリティの履行状況の確認に関する事項

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

① 情報セキュリティ履行状況の報告

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

② 情報セキュリティ監査の実施

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

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

受注者は自ら実施した外部監査についても PMDA へ報告すること。

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

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

9 再委託に関する事項

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

② ①における「主要部分」とは、以下に掲げるものをいう。

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

- 2.3.1 プロセス開始の準備
- 2.3.2 システム要件定義プロセス
- 2.3.3 システム方式設計プロセス
- 2.4.2 ソフトウェア要件定義プロセス
- 2.4.3 ソフトウェア方式設計プロセス

ただし、以下の場合には再委託を可能とする。

- 補足説明資料作成支援等の補助的業務
- 機能毎の工数見積において、工数が比較的小規模であった機能に係るソフトウェア要件定義等業務

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

④ 再委託先が、更に再委託を行う場合も同様とする。

⑤ 再委託における情報セキュリティ要件については以下のとおり。

- 受注者は再委託先における情報セキュリティ対策の実施内容を管理し PMDA に報告すること。
- 受注者は業務の一部を委託する場合、本業務にて扱うデータ等について、再委託先またはその従業員、若しくはその他の者により意図せざる変更が加えられないための管理体制を整備し、PMDA に報告すること。
- 受注者は再委託先の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関して、PMDA から求めがあった場合には情報提供を行うこと。
- 受注者は再委託先にて情報セキュリティインシデントが発生した場合の再委託先における対処方法を確認し、PMDA に報告すること。
- 受注者は、再委託先における情報セキュリティ対策、及びその他の契約の履行状況の確認方法を整備し、PMDA へ報告すること。
- 受注者は再委託先における情報セキュリティ対策の履行状況を定期的に確認すること。また、情報セキュリティ対策の履行が不十分な場合の対処方法を検討し、PMDA へ報告すること。
- 受注者は、情報セキュリティ監査を実施する場合、再委託先も対象とするものとする。
- 受注者は、再委託先が自ら実施した外部監査についても PMDA へ報告すること。
- 受注者は、委託した業務の終了時に、再委託先において取り扱われた情報が確実に返却、又は抹消されたことを確認すること。

１０ その他特記事項

（１） 環境への配慮

環境への負荷を低減するため、以下に準拠すること。

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

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

（２） その他

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

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 概略スケジュール案

別紙 3 システム詳細要件

別紙 4 データセンタの配線作業の費用算出依頼の連絡先 (本資料は参加要項に記載の秘密保持誓約書を提出した応札者にのみ開示する)

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

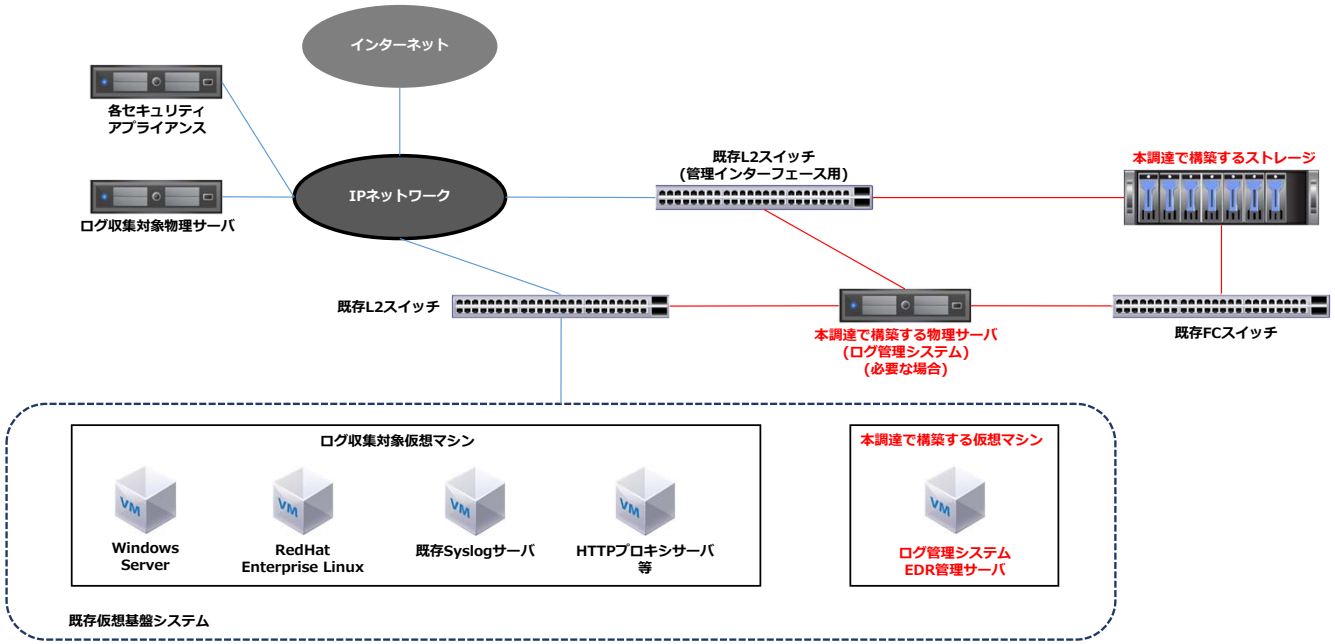
※迷惑メール防止対策をしているため、●を半角のアットマークに置き換えること。

共用LANシステム
情報インフラセキュリティログ管理システム及び
EDRの更新に係る賃貸借

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
各セキュリティ
アプライアンス
IPネットワーク
ログ収集対象物理サーバ
既存L2スイッチ
(管理インターフェース用)
本調達で構築するストレージ
既存L2スイッチ
本調達で構築する物理サーバ
(ログ管理システム)
(必要な場合)
既存FCスイッチ
ログ収集対象仮想マシン
Windows
Server
RedHat
Enterprise Linux
既存Syslogサーバ
HTTPプロキシサーバ
等
本調達で構築する仮想マシン
ログ管理システム
EDR管理サーバ
既存仮想基盤システム

共用LANシステム 情報インフラセキュリティログ管理システム及びEDRの更新に係る賃貸借 調達仕様書

別紙2 概略スケジュール案

項番	項目	日程																			
		2024年									2025年				2026年	2027年	2028年	2029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	-	-			-	10月	11月	12月
1	現行システム運用期間																				
2	設計・構築・テスト																				
3	運用テスト・フィードバックによる構成変更																				
4	システムカットオーバ																				
5	システム保守の提供期間																				
6	データ消去作業																				

共用 LAN システム 情報インフラセキュリティログ管理システム及び

EDR 基盤の更新に係る賃貸借 調達仕様書

別紙 3 システム詳細要件

1. システム構成

1.1. システム構成概要

本調達で導入するシステムは下記の要素で構成される。

- 情報インフラセキュリティログ管理システム
- EDR 基盤
- 検証環境

1.2. システムの利用者

本システムは下記に記す立場のユーザが利用する。

- 全体管理者
- 業務システム管理者
- 保守作業者

立場	説明
全体管理者	本システム全体の管理を行う。システム設定、監査ログ閲覧、機能設定及び閲覧、ユーザ管理ができる。
業務システム管理者	保護対象ノードに限定してシステム設定、監査ログ閲覧、機能設定及び閲覧ができる。 業務システムは複数あるため、業務システムに応じて異なる立場の業務システム管理者が存在する。
保守作業者	本調達の受注者で、本調達仕様書に定めるシステム保守作業を行う。

2. 各システム構成要素の詳細

2.1. 情報インフラセキュリティログ管理システム

情報インフラセキュリティログ管理システム(以後、ログ管理システムと呼ぶ。)では、ログ管理対象ノードのログを集約し、ログの検索、集約レポート、アラート発報、ログ分析が可能なログ管理システムを構築する。ログ管理システムは Web ブラウザからアクセス及び操作可能な WebUI を提供し、WebUI にログインするユーザに応じてログの開示範囲を変動させられるように構成する。これは、例えば同一のセキュリティ装置が生成した同種のログであっても保護対象のノードの管理者が異なる場合があり、管理者自身の責任範囲のログのみ閲覧可能な構成とすることを意図している。

2.1.1. ログの種別

ログ基盤への入力対象となるログは下記の通り。

1. PMDA の Syslog サーバに格納されたログ
2. Windows イベントログ
3. ログ収集対象サーバのローカルディスク上のログファイル
4. ログ収集対象サーバのリレーショナルデータベース内のレコード(必要な場合)

2.1.1.1. PMDA の Syslog サーバに格納されたログ

ログ収集対象の製品のうち、本システムでの監視対象ログを外部の Syslog サーバに送信可能なものは PMDA の Syslog サーバにログを送信する。この Syslog サーバでは送信されたログは送信ノードのホスト名によりディレクトリ分類され、ログの受信年月日ごとにファイル分類される構成を想定している。格納されたログは 60 日程度でアーカイブされる。これらのログファイルの内容を本調達で導入するログ管理システムに送信する。

2.1.1.2. Windows イベントログ

ログ取得対象には Windows のイベントログにのみ出力可能なものがある。これらのイベントログを本件で導入するログ管理システムに送信する。

2.1.1.3. ローカルディスク上のログファイル

ログ取得対象には Syslog 送信や Windows イベントログではなく、ローカルディスクにファイルとしてログを書き出すものがある。ログファイルのファイルパスは対象ノードによって異なる。これらのログを本件で導入するログ管理システムに送信する。

2.1.1.4. リレーショナルデータベース内のレコード

ログ取得対象には製品のデータベース内に機能の動作状況を保持しているものがある。ログの

可視化を行うにあたり、より適切な処理が可能な場合はこの情報をログ管理システムに送信する。

2.1.2. ログ管理システムへのログ送信

ログ管理システムにログを送信するためのエージェントソフトウェアを必要に応じて Syslog サーバ、ログ監視対象ノードに送信する。エージェントソフトウェアには以下の機能を期待する。

- Windows Server2019/2022、RedHat Enterprise Linux8/9(以後、RedHat Enterprise Linux は RHEL と呼ぶ。)で動作可能なこと。
- ログ基盤に送信するログファイルを正規表現などで特定可能で、複数のログファイルパスを指定可能なこと。
- 監視対象のログファイルやイベントログが追記されたことを検知して自動的にログ基盤に送信可能なこと。
- エージェントソフトウェアの設定を中央の管理装置から集約管理可能なこと。
- UTF-8(BOM 無し及び BOM 有り)、Shift-JIS の文字コードを処理可能なこと。

2.1.3. ログ管理対象ノード

取得を想定しているログは以下の通り。

対象ログ	ログ種別	備考
Paloalto Networks 社 Paloalto の IPS ログ	Syslog	2 台 2 セット
Paloalto Networks 社 Paloalto の URL フィルタログ	Syslog	2 台 1 セット
Imperva 社ハードウェアアプライアンスの WAF ログ	Syslog	2 台 2 セット
A10 Networks 社 Thunder CFW の TLS 復号化・再暗号化ログ、ロードバランスログ(複数の Partition を使用している)	Syslog	2 台 3 セット
Squid の HTTP プロキシログ	ローカル	2 台
nginx の HTTP ログ	ローカル	4 台
Windows Server の RDP 接続ログ	イベントログ	150 台程度
IIJ 社 Secure MX のメール配送ログ、スパムフィルタ等のフィルタ検知ログ	ローカル	-
Postfix のメール配送ログ	ローカル	12 台
Trendmicro 社 DeepSecurity のマルウェア検出ログ	Syslog	管理サーバ 1 台
Trendmicro 社 DeepSecurity の変更監視検出ログ	Syslog	管理サーバ 1 台
Trendmicro 社 ApexOne のマルウェア検出ログ	イベントログ	管理サーバ 1 台
Red Hat Enterprise Linux の SSH アクセスログ	ローカル	50 台程度

ログ総量は 1 日 60GB 程度を想定している。ログは当日から過去 397 日間分を保存する。

2.1.4. 機能要件

2.1.4.1. 管理用の WebUI

ログ管理システムの管理や各機能を利用するための WebUI を備えていることを要件とする。この WebUI には各利用者が Web ブラウザ(Edge、Chrome、Firefox)からアクセスする。WebUI にはセキュリティ運用状況を表示することから、WebUI と Web ブラウザ間の通信は TLS により暗号化されていることを前提とする。

2.1.4.2. ログインとロール

ログ管理システムの WebUI には異なる立場の管理者がログインする。ログインユーザに対してログ管理システムがアクセス制御ロールを割り当てることでログ管理システムの利用者の立場に応じてログの可視化範囲を適切に制御する。

PMDA では Microsoft 社 Active Directory にユーザアカウントを格納しており、ログ管理システムへのログインにこれらのアカウントを使用することを想定している。ユーザアカウントはアクセス制御用に作成しているセキュリティグループに所属している。ログ管理システムではユーザアカウントではなくセキュリティグループを対象にロールを制御できることが望ましい。また、1 個のユーザアカウントは複数のセキュリティグループに所属することがある。

ロール制御に関しては以下のような機能を要件とする。

1. ログインに使用するアカウントソースとして既存の Active Directory が使用可能なこと。認証プロトコルとして LDAPS が使用なこと。
2. ログ管理システム自体の設定を変更・参照できる全体管理者、自身の管理対象のノードに関するログのみ参照可能な業務システム管理者のようなロールを定義可能なこと。ログインしたユーザに対して自動的にこれらのロールを付与可能なこと。
3. 同じ装置のログであっても、業務システム管理者は自身の管理対象のログのみ参照可能な制御が可能なこと。例えば IPS のログフォーマットが「yyyy/mm/dd hh:mm:ss srcip=x dstip=y」というようなものだった場合、dstip には保護対象ノードの IP アドレスが記載される。この IP アドレスに応じてログ検索範囲を制限可能なアクセス制御が可能なことを想定している。

2.1.4.3. ダッシュボード

全体管理者、業務システム管理者が管理対象ノードの稼働状態を俯瞰するため、指定した期間の各ログの集計結果をログ管理システムの WebUI に一覧表示するダッシュボードを定義する。ダッシュボードの生成のために集計するログは WebUI にログインしたユーザのロールによって自動的に変動し、同種のダッシュボードのであっても表示内容が変わるように構成する。ダッシュボードに表示する保護対象ノードのリストなど、事前に定義可能な情報は CSV 等の形式でログ管理システムにインポートしておくことを想定している。

ダッシュボードのレイアウトやページ分割については詳細な指定は行わないが、受注者はPMDA と協議の上で実運用を考慮し画面設計を行うこと。

2.1.4.3.1. 全体管理者向けのダッシュボード

全体管理者向けには以下のダッシュボードを想定している。

大分類	内容
IPS	保護対象ノードの IP アドレスごとに以下の情報を表示する。 ・ 総検知件数。 ・ 縦軸を検出件数、横軸を時間としたグラフ。 ・ シグネチャレベルごとの攻撃件数。 ・ シグネチャごとの攻撃件数。(表示数を制限する) ・ 検知除外対象のシグネチャリスト。 ・ 送信元 IP アドレスベースの攻撃件数。(表示数を制限する) ・ 送信元 IP アドレスベースの検知シグネチャ。(表示件数を制限する)
URL フィルタ	フィルタされた対象 URL の IP アドレスごとに以下の情報を表示する。 ・ フィルタ対象の URL ベースのフィルタ件数。 ・ 縦軸を検出件数、横軸を時間としたグラフ。(グラフの種類は別途検討) ・ フィルタ対象の URL ベースの送信元 IP アドレス。ただし、L3 ヘッダの送信元 IP アドレスには Squid の IP アドレスが格納されている可能性があるため、Squid の HTTP ログと照合しタイムスタンプ、宛先から推測される送信元 IP アドレスのリストを表示する。 ・ フィルタ対象 URL の情報。(ログから判明する情報に限る)
WAF	保護対象ノードの IP アドレスごとに以下の情報を表示する。 ・ 総検知件数。 ・ 縦軸を検出件数、横軸を時間としたグラフ。 ・ シグネチャレベルごとの攻撃件数。 ・ シグネチャごとの攻撃件数。(表示数を制限する) ・ 検知除外対象のシグネチャリスト。 ・ 送信元 IP アドレスベースの攻撃件数。(表示数を制限する) ・ 送信元 IP アドレスベースの検知シグネチャ。(表示件数を制限する)
ロードバランス時の TLS 処理	クライアントからの接続を受け付けるロードバランサのバーチャル IP ごとに以下の情報を表示する。

	・ TLS 処理エラー総件数。(エラーの定義は設計時に行う) ・ 頻出エラーログの件数とログ内容。 ・ 検出した全てのエラーログの種類のリスト。 ・ 縦軸をログ件数、横軸を時間としたグラフ。
ロードバランスログ	クライアントから接続を受け付けるロードバランサのバーチャル IP ごとに以下の情報を表示する。 ・ ロードバランスログ総件数。 ・ ロードバランスログの種類ごとの件数。 ・ 縦軸をログ件数、横軸を時間としたグラフ。
HTTP プロキシログ	以下の情報を表示する。 ・ プロキシログ総件数。 ・ 送信元 IP アドレスベースのログ件数。 ・ 宛先 FQDN トップ N 数のリスト。(N は設計時に検討する) ・ 縦軸をログ件数、横軸を時間としたグラフ。
RDP 接続ログ	RDP 接続対象の IP アドレスもしくはホスト名ごとに以下の情報を表示する。 ・ ユーザごとの RDP 接続件数。 ・ ユーザごとの RDP 切断件数。 ・ 特定ユーザの RDP 接続、切断ログ。 ・ 縦軸を接続件数及び切断件数、横軸を時間としたグラフ。
メール配送	以下の情報を表示する。 ・ アウトバウンドメール配送件数。 ・ インバウンドメール配送件数。 ・ 受信数の多い宛先メールアドレスのトップ N 数。 ・ 縦軸をアウトバウンドメール配送件数及びインバウンドメール配送件数、横軸を時間としたグラフ。
メールフィルタ	以下の情報を表示する。 ・ フィルタ総件数。 ・ フィルタ理由別の件数。 ・ フィルタ数の多い配送元メールリレーサーバの IP アドレスのトップ N 数 ・ 縦軸をフィルタ件数、横軸を時間としたグラフ。
マルウェア検出 変更監視検出	以下の情報を表示する。 ・ マルウェア検出総数。 ・ 変更監視検出総数。 ・ マルウェア検出ログから分かるマルウェア種別。

	・　変更監視が検出されたファイルパス。
SSH 接続ログ	対象の IP アドレスもしくはホスト名ごとに以下の情報を表示する。 ・　ユーザごとの SSH 接続件数。 ・　ユーザごとの SSH 切断件数 ・　特定ユーザの RDP 接続、切断ログ。 縦軸を接続件数及び切断件数、横軸を時間としたグラフ。(グラフの種類は別途検討)

ダッシュボード中のグラフは基本的に 1 日のうちどの時間帯に該当イベントが発生しているかを把握することを意図している。

2.1.4.3.2.　業務システム管理者向けのダッシュボード

以下のダッシュボードを想定している。全体管理者向けのダッシュボードと異なり、業務システム管理対象のノードのみが表示対象となるようにする。

大分類	内容
IPS	保護対象ノードの IP アドレスごとに以下の情報を表示する。 ・　総検知件数。 ・　縦軸を検出件数、横軸を時間としたグラフ。 ・　シグネチャレベルごとの攻撃件数。 ・　シグネチャごとの攻撃件数。(表示数を制限する) ・　検知除外対象のシグネチャリスト。 ・　送信元 IP アドレスベースの攻撃件数。(表示数を制限する) ・　送信元 IP アドレスベースの検知シグネチャ。(表示件数を制限する)
WAF	保護対象ノードの IP アドレスごとに以下の情報を表示する。 ・　総検知件数。 ・　縦軸を検出件数、横軸を時間としたグラフ。 ・　シグネチャレベルごとの攻撃件数。 ・　シグネチャごとの攻撃件数。(表示数を制限する) ・　検知除外対象のシグネチャリスト。 ・　送信元 IP アドレスベースの攻撃件数。(表示数を制限する) ・　送信元 IP アドレスベースの検知シグネチャ。(表示件数を制限する)
ロードバランス時の TLS 処理	クライアントからの接続を受け付けるロードバランサのバーチャル IP ごとに以下の情報を表示する。

	・ TLS 処理エラー総件数。(エラーの定義は設計時に行う) ・ 頻出エラーログの件数とログ内容。 ・ 検出した全てのエラーログの種類のリスト。 ・ 縦軸をログ件数、横軸を時間としたグラフ。
ロードバランスログ	クライアントから接続を受け付けるロードバランサのバーチャル IP ごとに以下の情報を表示する。 ・ ロードバランスログ総件数。 ・ ロードバランスログの種類ごとの件数。 ・ 縦軸をログ件数、横軸を時間としたグラフ。
RDP 接続ログ	RDP 接続対象の IP アドレスもしくはホスト名ごとに以下の情報を表示する。 ・ ユーザごとの RDP 接続件数。 ・ ユーザごとの RDP 切断件数。 ・ 特定ユーザの RDP 接続、切断ログ。 ・ 縦軸を接続件数及び切断件数、横軸を時間としたグラフ。
マルウェア検出 変更監視検出	以下の情報を表示する。 ・ マルウェア検出総数。 ・ 変更監視検出総数。 ・ マルウェア検出ログから分かるマルウェア種別。 変更監視が検出されたファイルパス。
SSH 接続ログ	対象の IP アドレスもしくはホスト名ごとに以下の情報を表示する。 ・ ユーザごとの SSH 接続件数。 ・ ユーザごとの SSH 切断件数。 ・ 特定ユーザの SSH 接続、切断ログ。 縦軸を接続件数及び切断件数、横軸を時間としたグラフ。

2.1.4.4. ログの検索

ダッシュボードとは別に、詳細なログ調査を行うために実際のログを確認することがある。効率的なログ確認、運用中の監視ログ追加に効率的に対応するため、ログ管理システムのログ検索では以下の機能を要件とする。

1. ログを高速検索するため、ログのタイムスタンプをベースとしたインデクシングが可能なこと。
2. 異なるノードの同種のログを画一的に処理するためログフォーマットに応じた各項目の意味付け、ログ送信ノードに応じた分類ができることが可能なこと。
3. 年、月、日、時間をキーに指定した期間の各装置のログ検索が可能なこと。
4. ログ検索を行うための検索クエリを作成可能なこと。検索クエリにはログフォーマットに対し

て施したログの意味付けを使用可能なこと。

5. ログ検索用のクエリを保存可能なこと。
6. 一定期間を経過したログに対してディスク消費量を低減させることを目的としたサイズ圧縮機能を有すること。圧縮されたログの検索パフォーマンスが低下することは許容する。
7. 固定的なデータを記載した CSV ファイルや TSV ファイルを登録し、そのデータを検索クエリに利用可能なこと。
8. 検索結果を特定のキーでソート可能なこと。

2.1.4.5. 定期レポート

2.1.4.5.1. 月次レポート

全体管理者向け、業務システム管理者向けのダッシュボードと同等の内容で前月 1 か月間を期間としたダッシュボードの描画結果を月次レポートとして自動生成し、ファイルとしてネットワーク上の共有領域に書き出した上で書き出したことを通知するメールを送信する。宛先メールアドレスは事前に定義しておく。

2.1.4.5.2. 通年レポート

各年で 1 か月ごとの各検出項目の件数をグラフ表示する。全体管理者向けの通年レポートの表示内容は以下の通り。

分類	内容
IPS	・ 総検出数 ・ 保護対象ノードごとの総検出数 ・ マッチ数の多いシグネチャ名(数量は設計時に検討)
URL フィルタ	・ フィルタマッチ総件数
WAF	・ 総検出数 ・ 保護対象ノードごとの総検出数 ・ マッチ数の多いシグネチャ名(数量は設計時に検討)
ロードバランス時の TLS 処理	・ TLS 処理エラー総件数 ・ バーチャル IP ごとの TLS 処理エラー総件数
ロードバランスログ	・ ロードバランスログ総件数 ・ バーチャル IP ごとのロードバランスログ総件数
HTTP`プロキシログ	・ HTTP プロキシログ総件数
RDP 接続ログ	・ RDP 接続ログ総件数 ・ RDP 切断ログ総件数 ・ 特定ユーザごとの RDP 接続、切断ログ総件数
メール配送	・ アウトバウンドメール配送件数 ・ インバウンドメール配送件数

メールフィルタ	・	フィルタマッチ総件数
マルウェア検出	・	マルウェア検出総件数
変更監視検出	・	変更監視検出総件数
SSH 接続ログ	・	SSH 接続ログ総件数
	・	SSH 切断ログ総件数
	・	特定ユーザごとの SSH 接続、切断ログ件数

業務システム管理者向けの通年レポートの表示内容は以下の通り。

分類		内容
IPS	・	総検出数
	・	保護対象ノードごとの総検出数
	・	マッチ数の多いシグネチャ名(数量は設計時に検討)
URL フィルタ	・	フィルタマッチ総件数
WAF	・	総検出数
	・	保護対象ノードごとの総検出数
	・	マッチ数の多いシグネチャ名(数量は設計時に検討)
ロードバランス時の TLS 処理	・	TLS 処理エラー総件数
	・	バーチャル IP ごとの TLS 処理エラー総件数
ロードバランスログ	・	ロードバランスログ総件数
	・	バーチャル IP ごとのロードバランスログ総件数
マルウェア検出	・	マルウェア検出総件数
変更監視検出	・	変更監視検出総件数

2.1.4.6. アラート

下記を条件にログ基盤システムからアラートを発報するように構成する。

- IPS、WAF に関して 10 分程度の間に規定件数以上のログを受信した場合。
- Linux の root 等、普段は使用しない特権アカウントをはじめとした指定アカウント利用時

2.1.5. 既存機能の移行

既存システムのダッシュボードに相当するものやアラート、既存ログの移行は不要とする。

2.2. EDR 環境

現在 Tanium 社 Tanium を EDR 用途、ノード情報収集のために使用している。Tanium を使用し

た運用が PMDA 内である程度定着しているため、同製品を継続して利用する。Tanium の機能としてベースの機能、Connect、Threat Response を使用している。これらに加えて以下の機能ライセンスを追加する。

- Asset
- Comply
- Discover
- SBOM

Tanium の管理対象とするノードは Windows10/11 Enterprise が動作するクライアント端末及び VDI、Windows Server2019/2022 が動作する Windows Server、RHEL8/9 が動作する Linux サーバとする。

2.2.1. 利用を想定する機能

2.2.1.1. 端末の状態静止点の取得

Asset の機能を使用して管理対象ノードの状態が事前に定めた「正しい状態」であることを確認する。また、管理対象ノードの状態を取得後にそれをファイルとしてエクスポートし履歴管理を行う。

2.2.1.2. CVE 番号ベースの脆弱性該当状況の取得

Comply の機能を使用して管理対象ノードの CVE 番号ベースの脆弱性該当状況を可視化する。

2.2.1.3. Tanium 管理対象外ノードの一覧化

Discover の機能を使用して Tanium が検出されないノードを一覧化し、インストールができないノードや管理対象外としたノードをホワイトリストノードとして管理する。

2.2.1.4. 侵害状況の調査と対応

Threat Response の機能を使用し、IoC を基に管理対象ノードが危険と判断される状況に該当するか確認できるようにする。管理対象ノードが特定の状況に該当する場合、そのタイミングでの端末の TCP 接続状態、ファイルシステム状況を取得し、リモートからそれらの情報にアクセスできるようにする。また、管理対象ノードが通信可能な宛先を Tanium サーバなど必要最低限のものに限定するような仕組みを導入する。

2.2.1.5. ユーザロール

Tanium の管理対象ノードには業務システム管理者が管理するノードが含まれている。Tanium の管理用 WebUI には業務システム管理者のログインも想定しており、Comply により可視化された CVE 番号ベースの脆弱性該当状況を確認できるようにする。この時、自身の管理対象外ノードの状態は表示されないように権限設定を行う。また、Tanium サーバ自体の設定変更が行えないようにする。尚、WebUI のログインに使用する ID ソースにはログ管理システムと同様に既存の Active

Directory を使用する。

2.2.1.6. ワンライナー実行用センサの作成

管理対象の Windows10/11、Windows Server、RHEL で任意のコマンドをワンライナーで実行するためのセンサを作成すること。

2.2.2. 既存機能の移行

既存の IoC、監視設定の移行は不要とする。

2.3. 検証環境

情報インフラセキュリティログ管理システムは運用中にダッシュボードやアラートの変更、追加を行う可能性がある。これらの変更を行うために事前の検証を行うことを想定している。これを実現するために本番環境として運用する情報インフラセキュリティログ管理システムのサイズを小さくした検証環境を構成する。

3. インフラ構成

本調達で構築するログ管理システム、EDR 環境及び付随するハードウェア等は原則としてオンプレミス環境に構築する。ハードウェアは既存ラックに搭載する。製品の正常性監視等の目的のための一部の機能はクラウドサービスとしても良い。

3.1. ハードウェアの設置

本システムを構成するにあたり導入が必要なハードウェアは PMDA が指定するデータセンタ内の既存ラックに搭載する。このラックは 42RU のサーバ・ネットワークラック 1 架で構成される。

3.2. サーバリソースと共有ストレージ

ログ管理システム、EDR 環境を稼働させるために必要なサーバが仮想マシンの場合、特段の制限がなければ PMDA が既に運用している既存仮想基盤システム上に仮想マシンを構成する。仮想マシンの OS に Windows Server2019/2022、RHEL8/9 を利用できる。仮想マシンのリソースとして CPU、メモリはこの環境を利用できるが、ディスク領域として使用する共有ストレージは本件での導入になる。共有ストレージは PMDA が運用する 2 台の既存 FC スイッチに接続する。接続には 32Gbps、マルチモード光ファイバ(LC コネクタ)を使用する。

3.3. 物理サーバ

製品の仕様や性能確保のために物理サーバが必要な場合は構成に含め、既存ラックに搭載すること。

3.4. ネットワーク接続

3.4.1. 共有ストレージ

装置を管理するためのインターフェースを既存ラック内の L2 スイッチと UTP で接続する。

本件で導入するハードウェアのネットワーク接続は PMDA の既存ネットワーク機器に接続する。ハードウェアを設置するラックの近傍に既存ネットワーク機器を搭載したラックがある。このネットワーク機器では 10GBase-SR または 1GBase-SX 接続のみ提供している。

3.4.2. 物理サーバ

物理サーバを導入する場合、以下のネットワーク接続を行う。

- サービス系のトラフィックを送受信するため、10GBase-SR 2 本で PMDA の既存ネットワーク機器に接続する。

- 運用管理系のトラフィックを送受信するため、10GBase-SR 2 本で PMDA の既存ネットワーク機器に接続する。
- 装置管理用のインターフェースを 1000Base-T または 100Base-TX で PMDA の既存ネットワーク機器に接続する。
- 光ケーブルによる接続を行う場合は PMDA の既存ネットワーク機器側を含めて SFP+または SFP を受注者が用意すること。

3.5. バックアップ

3.5.1. 汎用 OS のノード

PMDA が運用するバックアップシステムをベースにバックアップを取得する。

3.5.2. コンフィグファイル等

構成の復元に必要なコンフィグファイルなどを保全する。

3.6. エンドポイントセキュリティ

PMDA が運用している Trendmicro 社 DeepSecurity(エージェントベース)による保護を行う。

4. システム運用

4.1. 監視対象の追加対応

運用状況に応じてログ基盤に新規のログを送信するように PMDA が設定することがある。ログ送信対象に対するエージェントインストール、ログ基盤側の設定を PMDA が行う。この作業は本件の範囲では受注者の役務範囲外とする。ただし、Windows Server の RDP 接続ログのように、サーバが別でも同じ構成で取得可能なログの場合は対象サーバが追加になっても機械的な処理でログ収集対象を追加できるようにあらかじめ設計すること。

4.2. ダッシュボードの表示変更

運用状況に応じてダッシュボードの内容を変更することがある。変更内容は表示位置の変更や表示テキストの変更など外観に関する微調整を想定している。この作業は本件の範囲では受注者の役務範囲外とする。

5. 構成要件

5.1. 情報インフラセキュリティログ管理システム

5.1.1. ログの可視化

1. 本書の「2.1.4 機能要件」に記載している各要件を満たすようなダッシュボード、ログ検索機能、ロールによるログの表示制御を行うこと。
2. 全体管理者のみが EDR 環境の監査ログを検索できるように構成すること。このログについてはダッシュボードの作成は本調達の対象外とする。
3. ダッシュボードの画面構成は PMDA と協議の上で設計すること。設計時には少なくとも画面のワイヤフレームを作成し、PMDA との認識差異を最小化すること。ワイヤフレームの作成にあたり、設計時に PMDA と十分に打合せを行うこと。尚、今回想定しているダッシュボードでは細かいレベルでのレイアウト構成や画像作成などを含む見栄えの充実性を求めるものではない。
4. ダッシュボードに表示するログの集計ロジックを PMDA と合意した上で実装すること。
5. 本調達でログの収集対象としている各装置の一般的な位置づけを理解し、ダッシュボード表示やログ検索を高速化するために必要なログフィールドの定義、インデクシングを適切に行い、その内容を PMDA と合意した上で実装すること。
6. ダッシュボードの最終的な構成を決定する際はプロトタイプを作成し、各機能の動作イメージや画面表示、画面遷移が想定通り使用できるか PMDA が確認できるようにすること。
7. プロトタイプの動作が設計通りでない場合は設計に合わせてプロトタイプを修正すること。
8. ワイヤフレームやプロトタイプの作成、評価、修正は構築スケジュールに組み込み、適切な日程を確保すること。

5.1.2. 管理機能

1. PMDA が運用している既存の Active Directory のアカウント情報を利用してログイン可能な WebUI を構成すること。
2. ログ管理システムの管理機能を使用して、ログ取得管理対象ノードにインストールしたエージェントにログ収集のルールを配信可能となるように構成すること。
3. 収集対象とするログファイル、ディレクトリ、ログ内容を指定するための設定をまとめた操作手順書を作成すること。
4. ログ管理に関する機能要件を満たすために作成する必要のある静的なデータ(例えば氏名とアカウント名の対応表)について整理し、運用中に更新のしやすいフォーマット、形式となるように設計すること。それらの変更方法、インポート方法を操作手順書として作成すること。
5. ログ管理システム全体の基本設定は全体管理者のみ行えるように構成し、業務システム管理者が全体に影響が波及するような操作が行えないように抑止すること。
6. WebUI にログインするユーザが変更になった場合、ログイン可能なユーザの変更や割り当てる

ロールを変更するための操作手順を作成すること。

7. 1 日に 60GB のログを受信可能なこと。

5.1.3. OS の構築

1. 既存仮想基盤システムを使用して仮想マシンを構成する場合、受注者は必要な OS、システムリソースを PMDA に提示すること。OS がインストールされた仮想マシンのデプロイは PMDA が行う。その後の OS のパラメータ設定は受注者が行うこと。
2. 追加でインストールが必要なソフトウェアがある場合、受注者がインストール作業を行うこと。一部の特権アカウントが必要になる場合、特権アカウントの認証は受注者の作業とせず、PMDA が行うことがある。
3. ビルトインで搭載されている特権アカウントは無効化し、新たに特権アカウントを作成すること。
4. 特段課題がなければ PMDA が運用する Active Directory にドメイン参加させること。
5. PMDA が運用している Trend Micro 社 DeepSecurity のエージェントのインストールすること。インストール手順は PMDA が提供する。

5.1.4. 物理サーバ

ログ管理システムを構成するために物理サーバが必要な場合、物理サーバの構築を行い既存ラックへの搭載、ネットワーク接続などの物理作業を行うこと。ケーブルや部材なども構成に含めること。

1. ログ管理システムを構成するソフトウェアが正常に動作する構成とすること。
2. 物理サーバは複数台で構成し、物理サーバ 1 台に障害が発生した際でもログの収集、検索、保全機能が確保できるように構成すること。ログの検索性能の縮退は許容するが、速やかにハードウェア交換を行うための保守体制とすること。
3. ディスクは全て 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。ディスク障害時には自動的にリビルドが行われるようなホットスペアディスクを 1 本以上搭載すること。
5. 10GBase-SR で接続可能な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。インターフェースを 2 個ずつそれぞれ業務系トラフィックの転送、バックアップトラフィックの転送用に構成し、それぞれの用途に PMDA が保持している L2 スイッチと接続すること。L2 スイッチは同一データセンタの別ラックに搭載されている。
6. バックアップトラフィックを転送するために必要なスタティックルーティングの設定を行うこと。
7. 物理サーバのハードウェア稼働状況を管理するための IPMI インターフェースを PMDA が保持している L2 スイッチに接続すること。L2 スイッチは同一データセンタの同一ラックに搭載されている。接続は UTP による 1000Base-T もしくは 100Base-TX を想定している。

8. IPMI インターフェースから稼働状況を Syslog 送信するように構成すること。
9. IPMI インターフェースに Web ブラウザからアクセスできるような UI を利用できるように構成すること。WebUI は認証機能を有効にし、PMDA の既存 Active Directory 上のアカウントを使用してログインできるように構成すること。
10. 電源は冗長構成とすること。
11. 保守や構築を考慮し、必要であれば KVM コンソールを構成すること。

5.1.5. 共有ストレージ

1. ログ管理システムのログがこの共有ストレージに格納されるように構成すること。
2. 必要なストレージボリューム設計を行うこと。
3. ストレージコントローラは 2 台以上での冗長構成とすること。
4. 既存の 2 台の FC スイッチと冗長構成となるように光ケーブルを接続すること。FC 接続の帯域は 32Gbps でリンクするように構成すること。既存 FC スイッチはマルチモード光ファイバ(LC コネクタ)での接続を想定している。
5. 既存 FC スイッチの設定変更は PMDA が行う。物理サーバを含めてソフトゾーニングを行うことを想定している。受注者は FC スイッチの設定に必要な情報を PMDA に提供すること。
6. 装置を管理するためのネットワークインターフェースを PMDA が保持している L2 スイッチに接続すること。L2 スイッチは同一データセンタの同一ラックに搭載されている。接続は UTP による 1000Base-T もしくは 100Baes-TX を想定している。
7. ディスクは全て SSD で構成すること。
8. ディスク 2 本が同時に故障してもデータの欠損がないように構成すること。
9. ストレージのハードウェア稼働状態をネットワーク経由で監視できるように構成すること。インターネット回線が必要な場合、PMDA が保持する既存インターネット回線を使用して良い。可能であれば PMDA が保持する既存の HTTP プロキシを使用すること。
10. ディスク交換作業は PMDA の担当者がストレージの設置場所に赴かなくても保守員のみで実施可能なこと。データセンタへの入館手続きは PMDA が行い、設置場所へのアテンドはデータセンタのスタッフが行うことを想定している。
11. 電源は冗長構成とすること。
12. ストレージスナップショットを取得する機能を有すること。
13. 重複排除機能を有し、有効化した場合でも十分なデータアクセススループットを確保できること。
14. ディスク暗号化機能を有し、有効化した場合でも十分なデータアクセススループットを確保できること。
15. ログ管理システムが使用する実効容量に対して 20%の余剰領域を備えていること。
16. 基本的なボリューム作成手順を操作手順として作成すること。

5.1.6. エージェントソフトウェアのインストール

1. ログ取得対象ノードにエージェントのインストールが必要な場合、インストール作業は PMDA が行う。受注者は OS ごとのインストール手順を PMDA に提供すること。

5.2. EDR 環境

5.2.1. EDR 機能構築

1. 各機能を実装する上で、考慮が必要になる Tanium の機能について PMDA に説明し、実装内容を PMDA と合意した上で導入作業を行うこと。
2. 管理対象ノード数は 2100 とする。この中には Windows10/11、Windows Server、RHEL が含まれる。
3. EDR 環境では仮想マシンを冗長構成とする必要はない。

5.2.1.1. 監視対象の状態の定期採取

1. 監視対象の状態を定期的に採取し、EDR 環境からネットワーク接続可能な共有領域に出力できるように構成すること。採取する情報として Windows10/11、Windows Server、RHEL の OS アーキテクチャを基に一般的に監視すべき重点項目を検討し、PMDA と内容を合意すること。
2. 共有領域に出力された情報を数世代程度保存しておくことを検討している。データのローテーションの実装は PMDA が行うが、実装しやすいようにタイムスタンプなど世代を識別しやすい情報を付加するなど工夫を行うこと。
3. システム運用中に採取すべき情報が追加、削除、変更される場合に追従できるように操作手順書を作成すること。

5.2.1.2. CVE 番号ベースの脆弱性診断

1. 使用する脆弱性情報の定義リストとその更新方法を明確にし、実装方法や更新方法を PMDA と合意した上で実装すること。
2. 定期的な評価レポートを出力できるように構成すること。評価レポート内には SBOM の観点からの報告を含めること。SBOM における情報取得ソースとして少なくとも Java、Python、Go、Windows DLL、Linux の共有オブジェクトを使用可能なこと。
3. WebUI にログインした時、業務システム管理者は自身が管理するノードのみ状態確認ができるように構成すること。
4. 脆弱性情報の定義リストを更新する方法を操作手順として作成すること。
5. 脆弱性に該当した場合でもレポート対象外として設定する方法を操作手順として作成すること。設計内容にあわせてノード単位別、CVE 単位別での設定方法を検討すること。

5.2.1.3. Tanium 管理対象外のノードの一覧化

1. Tanium がインストールされていないノードの IP アドレスを一覧化すること。
2. 専用 OS の装置などの Tanium がインストール出来ないノードや何らかの理由でインストールしないノードをホワイトリスト化するための操作手順を作成すること。

5.2.1.4. 侵害状況の調査と対応

1. Tanium で利用可能な異常挙動の定義を使用し、管理対象ノードの不正な操作を検出、アラート通知が可能なように構成すること。
2. 異常挙動の定義方法を操作手順として作成すること。詳細な定義自体の方法の説明は不要とするが、作成に必要なリファレンスや外部の情報を提供すること。
3. 異常挙動をホワイトリストとして登録する方法を操作手順として作成すること。
4. 一定の挙動を示した端末をネットワークから切り離し、許可された IP アドレスとしか通信ができないように構成すること。ただし、この動作の条件や納品時の状態については PMDA と協議の上で決定すること。

5.2.2. 管理機能

1. EDR 環境を管理するための WebUI を構成すること。
2. WebUI にログインするための ID ソースとして PMDA の既存 Active Directory のアカウントを利用可能なこと。
3. 管理対象ノードを業務システム管理者が管理するにあたり、WebUI へのログインに使用したアカウントに応じて表示する管理対象ノードを変更できるように構成すること。
4. EDR 環境全体の基本設定は全体管理者のみ行えるように構成し、業務システム管理者が全体に影響が波及するような操作が行えないように抑止すること。
5. EDR 環境に対する監査ログをログ管理システムに送信すること。対象ログは Tanium アプリケーションサーバの操作ログを想定しているが、モジュールサーバやデータベースサーバの動作ログについても、EDR 環境自体のセキュリティレベルを確保するために有用であれば設計の上で送信すること。
6. モジュールサーバ、データベースサーバにアクセス可能な IP ノードを最小限になるように通信設計を行うこと。制御ポイントとして PMDA が保持するファイアウォールもしくは EDR 環境のサーバ自体のファイアウォール機能を想定しているが、セキュリティ、保守性のバランスを考慮した設計を行うこと。
7. データベースに接続可能なユーザが最小限となるように使用する DBMS にあわせてアクセス設計を行うこと。必要に応じてアクセスログをログ管理システムに送信すること。

5.2.3. OS の構築

1. 既存仮想基盤システムを使用してサーバを構築すること。受注者は必要な OS、システムリソー

スを PMDA に提示すること。OS がインストールされた仮想マシンのデプロイは PMDA が行う。その後の OS のパラメータ設定は受注者が行うこと。仮想マシンのディスクは PMDA が保持する既存のストレージを使用する。ボリューム作成や付随する作業は PMDA が行う。

2. 追加でインストールが必要なソフトウェアがある場合、受注者がインストール作業を行うこと。一部の特権アカウントが必要になる場合、特権アカウントの認証は受注者の作業とせず、PMDA が行うことがある。
3. root アカウントによる SSH 接続は無効化すること。
4. SSH 接続時は公開鍵認証方式によるものとすること。
5. SSSD を構成し、SSH アクセスに Active Directory のアカウントを使用できるように構成すること。PMDA が使用している SSSD の基本的な構成情報は提供するが、必要に応じてパラメータの調整を行うこと。
6. PMDA が運用している Trend Micro 社 DeepSecurity のエージェントのインストールすること。インストール手順は PMDA が提供する。

5.2.4. クライアントソフトウェアの展開

1. 管理対象ノードの一部(主に Windows10 クライアント端末)では既存の Tanium クライアントソフトウェアが動作している。このクライアントソフトウェアを本調達で導入する Tanium のバージンにあわせて更新すること。
2. Tanium クライアントソフトウェアの配布には Microsoft 社 MECM、Sky 社 Skysea ClientView Light Edition を使用できる。これらのソフトウェアの操作は PMDA が行うが、受注者はクライアントソフトウェアの配布設定に必要な情報を PMDA に提供すること。
3. クライアントソフトウェアの配布作業時に問題が生じた場合、正常にクライアントソフトウェアを配布できるように Tanium クライアントソフトウェアの挙動に関する原因調査、対処方法の検討を行い、PMDA に情報提供すること。
4. 全体に展開する前にクライアントソフトウェア配布のテストを行うこと。現行のバージョンの Tanium クライアントソフトウェアがインストールされたテスト用の端末は PMDA が用意する。

5.3. その他の要件

5.3.1. システム監視

本システムの一般的なシステム監視は Zabbix 社 Zabbix で行うことを想定している。Zabbix エージェントのインストールは本件の受注者が行うこと。インストールの手順は PMDA が提供する。Zabbix サーバ側の監視設定は PMDA が行うが、本件で導入するシステムが正常に動作していることを示す監視基準は本件受注者が PMDA に提供すること。Zabbix エージェントをインストールできないノードの監視は SNMP など代替手段を検討する。

5.3.2. バックアップ・リストア

構築するサーバをリストアできるようにバックアップを構成すること。必ずしも OS レベルのバックアップを取得する必要はなく、構築するシステムの特性に応じてバックアップ・リストア設計を行い PMDA と合意すること。

5.3.2.1. 既存仮想基盤システム上の仮想マシンのシステムバックアップ

既存仮想基盤システム上の仮想マシンを対象としたエージェントレスバックアップを行う。バックアップ、リストアの設定は PMDA が行う。ただし、リストアを行った後の仮想マシンの動作確認は受注者が行うこと。

RDM が必要とする場合、RDM 領域のバックアップを行うにはエージェントのインストールが必要になる。エージェントのインストール手順は PMDA が提供する。

5.3.2.2. 物理サーバのシステムバックアップ

バックアップ及びリストアは PMDA が保持するバックアップ、リストアシステムを使用する。バックアップの取得にエージェントのインストールを行うこと。起動メディアの作成など、リストアに必要な事前準備を PMDA と協議の上で行い動作テストを行うこと。

5.3.2.3. コンフィグファイルなどのファイルバックアップ

PMDA が保持している Windows Server によるファイル共有システムに定期的にファイルを保存する構成を設計、実装すること。このファイル共有システムには Active Directory のアカウントを使用した SMB アクセス、SSH アクセスができる。

5.3.3. ログフォーマットの情報提供

ログ取得対象ノードの多くが PMDA の既設設備であることから、原則としてログフォーマットの提供は PMDA が行う。ただし、本システムを正常に構成する上でログフォーマットやログ内容に確認が必要な場合、PMDA が既設設備の導入者に確認を行うための確認事項や質問内容を受注者が準備すること。

5.3.4. ネットワーク設計

本調達で構築するサーバ等のノードの IP アドレス割り当てや基本的なネットワーク設計は PMDA が行う。受注者は PMDA がネットワーク設計を行う上で必要になる本調達の構成品のネットワーク制約や推奨構成に関する情報提供を行い、PMDA のネットワーク構成を支援すること。

5.3.5. サプライチェーンマネジメント

情報セキュリティの確保を目的とし、サプライチェーンを十分に行った上で導入製品の選定を行うこと。

5.4. 検証環境

情報インフラセキュリティログ管理システムの検証環境として以下のような構成で導入すること。

1. 1 日 5GB のログを受信可能なこと。
2. 既存仮想基盤システム上の仮想マシンで構成可能なこと。OS は RHEL8 または 9 とする。仮想マシンのデプロイは PMDA が行う。
3. ログデータを保持するサーバは 2 台の冗長構成となるように構成すること。その他の機能のサーバが必要な場合、どのような構成とするかを PMDA と協議の上で決定し構成すること。
4. ログ管理システムのアプリケーションのインストールを行うこと。
5. PMDA が保持する既存 Active Directory のアカウントを使用してアプリケーションにログインできるように設定すること。
6. OS 設定は本番環境に準じて構成すること。
7. ログの受信と検索のための事前処理をテストすること。テストには nginx の HTTP アクセスログを使用すること。テスト用の nginx をインストールしたサーバは PMDA が用意する。

6. 受注者の作業

6.1. プロジェクト管理

6.1.1. 工程の内容

受注者は本調達における各作業を履行するための計画、作業体制、情報管理方針、重点事項を整理し、各工程の作業を遅滞なく進めるためのプロジェクト管理を行うこと。必要に応じて PMDA との会議を行い、進捗状況及び課題対応状況、予定作業の報告を行うこと。

本調達の導入物を使用して PMDA が運用を行うにあたり、プロトタイプ作成時点で画面構成や使い勝手、出力形式に関してチューニングを依頼する可能性がある。PMDA から無制限のチューニング依頼を行う想定はないが、受注者はこの工程にかかる作業量を減らすためプロジェクトの進行方法を検討し PMDA と合意すること。

6.1.2. 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。

6.1.3. プロジェクト管理に関するドキュメント

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

- プロジェクトスコープ
- プロジェクト体制表
- WBS (受注者と PMDA の作業分担を含めること)
- 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、PMDA との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としても良い。

6.2. システム設計・構築

6.2.1. 工程の内容

本調達仕様書に示す各要件を満たすように各構成要素を設計し導入作業を行うこと。PMDA が作業を行うことを明記しているもの以外は原則として受注者の作業範囲とする。

6.2.2. システム設計・概要に関するドキュメント

6.2.2.1. 基本設計書

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

- システムの各構成要素の役割と設計の意図及び実装概略
- システム全体の概要及び他システムとの接続点が分かるシステム全体構成図
- 物理装置間の接続情報を記したシステム物理構成図
- 仮想基盤システム及び共有ストレージのリソース
- 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
- 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。)

6.2.2.2. 詳細設計書

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

6.2.2.3. 運用手順書

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
- 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
- 共有ストレージのディスク交換手順

6.2.2.4. 導入設計書

本調達で導入するシステムの導入計画を WBS にあわせて具体的に記述すること。特にプロトタイプの評価、チューニングの期間や対応方針の整備は詳細に行うこと。

6.3. テスト

6.3.1. 機能テスト

各機能が設計の通り動作することを確認すること。

6.3.2. 障害テスト

冗長構成となる部分については想定した障害発生時の動作継続性、切り替わり発生時の動作をテストすること。

6.3.3. 性能テスト

ログ管理システムについては以下に示す観点で性能のテストを行い、報告書を作成の上、PMDA に報告すること。性能テストのテスト条件の決定にあたっては性能に影響する主要因を洗い出し PMDA と協議し決定すること。運用上支障のある性能の場合、ボトルネックの調査、チューニングを求めることがある。

- ログ検索時に指定する期間に応じたログ検索完了までの時間
- 検索対象ログ数及び検索条件に応じたログ検索完了までの時間
- ダッシュボードの生成、表示にかかる所要時間

6.3.4. バックアップ・リストアテスト

構築した仮想マシンのバックアップ取得、バックアップイメージからのリストアを行った結果、システムが正常に復旧することを確認すること。実際の挙動を確認した上で、システムが正常に復旧するまでの基本的な手順を確立させること。

6.3.5. テストに関するドキュメント

6.3.5.1. 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、ログ検索性能に特に留意すること。

6.3.5.2. 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. 受入テスト及び実装の修正

各機能が正常に動作することを PMDA が主体となり確認する。受注者は PMDA が確認作業を行うにあたり、PMDA が求めた場合は設計や実装の詳細に関する情報を提供すること。この確認作業で調達仕様書の要件を満たしていないと判断される場合や、実運用に求められる性能を大きく下回っている場合は設定や設計の修正を依頼する場合がある。確認作業は必ずしも全ての設計・構築作業が完了した後の実施とすることはないので、効率的に確認作業と実装の修正を行えるようにプロジェクト実施計画の時点で本工程を十分に考慮すること。

6.5. 運用引継ぎ

本調達で導入するシステムを PMDA が運用するにあたり要点となる部分を説明し、運用のための引継ぎを行うこと。引継ぎには各操作手順の作成を求める。操作手順書の記載粒度は PMDA と協議の上で決定するものとするが、Windows、RHEL、データベースを使用した一般的なシステム設計の経験がある者を対象とし、過度に丁寧な記載とする必要はない。

6.5.1. 本番環境に関する操作手順

受入テストが完了し本調達の構成品が最終的な構成になった後、受注者は下記の内容に関する操作手順書を作成し説明会を行うこと。受入テストで十分にテストできた項目や操作手順書から内容が十分に読み取れる項目については説明対象外とする場合がある。

- 本書で求めている具体的な製品操作手順
- システムの冗長構成状態の確認方法
- ログ管理システム上で作成したダッシュボードの集計ロジックと簡易的な変更方法
- ログ管理システム上で作成したアラート発報の閾値変更方法
- ログ管理システムのダッシュボード新規作成方法
- ログ管理システムのエージェントの設定変更方法
- ログ管理システムの WebUI にログインするためのユーザアカウント改廃手順
- ログ管理システムにおけるログ監視ノードの追加(ログフォーマットの意味付け方法を含む)
- Tanium の WebUI にログインするためのユーザアカウント改廃手順
- Tanium で作成するワンライナー実行用センサの使用方法

6.5.2. 検証環境に関する操作手順

検証環境を使用して下記の内容に関する操作手順書を作成し説明会を行うこと。操作手順書か

ら内容が十分に読み取れる項目については説明対象外とする場合がある。

- ログ管理システムアプリケーションのインストール方法
- 管理機能に Active Directory のアカウントを使用するための設定手順
- ログフィールドの意味付け定義の方法
- 格納しているログの消去手順
- ログのアーカイブ手順
- 導入バージョンにおける製品のログ検索で使用できるフィルタや関数のリファレンス (外部リソースの参照として良い)

6.6. データ消去作業

本調達で導入する共有ストレージのデータの消去作業を行うこと。消去作業は本システムの運用終了日から 3 週間前以降に実施可能とする。作業は設置場所からディスクを移動させずに行うこと。

6.6.1. データ消去作業に関するドキュメント

データ作業を行った後、対象ディスクの固有識別番号ごとに、データ消去方式、消去結果、消去日時を記した作業報告書を作成し消去証跡を添付すること。

6.7. システム保守

1. ハードウェア保守については平日 9 時～17 時オンサイトで対応可能な体制とすること。
2. ハードウェア保守の結果、システムが正常構成となるまで受注者の対応内容として作業計画を想定すること。
3. 導入ソフトウェア、設計内容に関する問い合わせに対応可能な体制とすること。問い合わせはメール、電話にて日本語対応が可能なこと。問い合わせに対する応答は平日 9 時～17 時での対応が可能なこと。