共用LANシステム
マネージドセキュリティサービス調達一式
調達仕様書

平成30年9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）　契約期間・賃貸借期間 1
（5）　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 2
（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 2
（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）　作業の概要 4
（2）　作業の内容 6
（3）　成果物の範囲、納品期日等 9
4　満たすべき要件に関する事項 13
5　作業の実施体制・方法に関する事項 13
（1）　作業実施体制 13
（2）　プロジェクトマネージャに求める資格等の要件 13
（3）　作業場所 13
6　作業の実施に当たっての遵守事項 13
（1）　基本事項 13
（2）　機密保持、資料の取扱い 14
（3）　遵守する法令等 15
7　成果物の取扱いに関する事項 15
（1）　知的財産権の帰属 15
（2）　瑕疵担保責任 16
（3）　検収 16
8　入札参加資格に関する事項 17
（1）　入札参加要件 17
（2）　入札制限 17
9　再委託に関する事項 18
１０ その他特記事項 20
（1）　環境への配慮 20
（2）　その他 20
１１ 附属文書 20
（1）　要件定義書 (入札説明会で配布) 20
１２ 窓口連絡先 20

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 マネージドセキュリティサービスの調達一式

（2）　用語の定義

表 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、その情報セキュリティ対策の一環としてマネージドセキュリティサービス(以下「MSS」という。)を導入している。現行の MSS では PMDA で導入されているセキュリティ製品やシステムの動作状況に基づいて、不正通信や不正プログラム、不正ファイル検知を行い遮断や防御またはこれらを実施するための助言を行っている。現行の MSS の契約は平成 30 年 12 月 31 日に満了予定であることから、昨今の PMDA や一般的な情報セキュリティ情勢を考慮した上で、今後必要な情報セキュリティ監視に必要な機材の賃貸借と当該機材を用いた監視サービスを調達する。(以下「本調達」という。)

本調達では PMDA 内で情報セキュリティ対策を効率的に行うことを目的として、PMDA による自主運用が可能な情報セキュリティ解析基盤を構築するものである。現行の情報セキュリティ対策運用体制から段階的に自主運用体制への移行を行うため、移行中の各フェーズにおいては次フェーズ以降の運用を見据えた運用設計も本調達に含む。

（4）　契約期間・賃貸借期間

契約期間は契約締結日から平成 36 年 12 月 31 日までとする。

機材の賃貸借期間は平成 31 年 1 月 1 日から平成 36 年 12 月 31 日までとする。

監視サービスの提供期間は平成 31 年 1 月 1 日から平成 32 年 12 月 31 日までとする。

（5）　スケジュール

本調達に係る想定スケジュールの概要を表 １.２　想定スケジュールに示す。最終的はフェーズ 5 に示すような受注者による SOC 機能を含まない自主運用に切り替えることを目標とする。

表 1.2　想定スケジュール

フェーズ	時期	実施内容
1	契約開始時 ～ 平成 30 年 12 月	導入作業
2	平成 31 年 1 月 ～ 平成 31 年 3 月	導入作業 仮運用期間
3	平成 31 年 4 月 ～ 平成 32 年 9 月	正運用期間 受注者による SOC 機能有り 運用状況に応じて随時チューニング
4	平成 32 年 10 月 ～ 平成 32 年 12 月	正運用期間 受注者による SOC 機能有り フェーズ 5 に向けた運用設計のチューニング
5	平成 33 年 1 月 ～ 平成 36 年 12 月	正運用期間 受注者による SOC 機能無し

2　調達案件及び関連調達案件の調達単位、調達の方式等に関する事項

（1）　調達案件及び関連する調達案件の調達単位、調達の方式、実施時期

関連する調達案件の調達単位、調達の方式、実施時期は次の表のとおりである。

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	調達の方式	更改予定時期	補足
1	共用 LAN システムサーバリプレイス調達一式	一般競争入札(総合評価方式)	平成 30 年 12 月	-
2	共用 LAN システム クライアントパソコン等リプレイス作業一式	一般競争入札(最低価格)	平成 30 年度中を予定	-
3	無線 LAN 環境構築一式	一般競争入札(最低価格)	平成 30 年度中を予定	
4	共用 LAN システム等に係る運用管理支援業務(仮)	未定	-	-

（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で導入予定のセキュリティ機器やネットワーク機器等からセキュリティログ及び動作状況を示すログを本調達の業務用に提供する。本調達の受注者は、本調達の業務を実施するにあたり必要となる情報や提供形式を PMDA 及び関連する調達案件の実施業者に伝えること。エージェントソフトウェアのインストールが必要な場合、原則として本調達の受注者が実施すること。

関連する調達案件に示した業務を円滑に行うために PMDA の指示の下、各業務を行う業者に構成情報や導入スケジュールの情報提供を行うこと。本調達における機器等が起因となる問題が発生した場合は問題解決のために速やかに調査及び解決のための作業を実施すること。これらの調達案件と本調達の導入スケジュールは同時期に行われることが想定される。

遅延なく各調達案件の導入作業を行うために、必要な情報の提供、作業依頼等の業者間の調整が必要となる事項は判明次第速やかに申告すること。

本調達の受注者は、PMDA が許可した者からの製品仕様や設計等の各種問い合わせにも対応すること。

① 共用 LAN システムサーバリプレイス調達一式

共用 LAN システムで使用する仮想基盤システム、仮想サーバ、データセンタや WAN 回線の更新を行う案件。本調達に求める要件を実現するためのセキュリティ製品としてこの案件での導入物の一部を使用することを想定している。本案件で導入するハードウェアを、この案件で使用するデータセンタに設置する場合、この案件の受注者と調整を行い必要な費用や作業を含めること。この案件の受注者の連絡先は入札説明会参加者に電子データで通知する。

また、この案件で導入した仮想基盤システム上で共用 LAN システム以外の一部の業務システムが動作する。この業務システムで使用するサーバも監視対象に含まれる。業務システムの一部には運用支援業者がいる。共用 LAN システムの運用支援業者とは異なる業者になる可能性があるため、監視対象サーバと運用支援業者の違いを意識した導入および運用体制をとること。

② 共用 LAN システム クライアントパソコン等リプレイス作業一式

共用 LAN システムで使用する業務端末の更新を行う。新しい業務端末の配布は平成 30 年 12 月を跨いで実施される可能性がある。本調達で業務端末に影響のあるソフトウェア等を導入する場合、本調達のフェーズ 1 以降は業務端末の配布前後いずれの環境にも本調達のサービスを提供できるように対応すること。

③ 無線 LAN 環境構築一式

共用 LAN システム クライアントパソコン等リプレイス作業一式で業務端末を更新した後は原則として無線 LAN 接続主体とするため、必要となる無線 LAN インフラを導入する案件。共用 LAN システム クライアントパソコン等リプレイス作業一式と並行または先んじて実施する。本調達のフェーズ 1 以降は業務端末のネットワーク接続が有線・無線いずれの環境にも本調達のサービスを提供できるように対応すること。

④ 共用 LAN システム等に係る運用管理支援業務(仮)

この案件の受注者は共用 LAN システムの運用支援を行うヘルプデスク業務を行う。本調達の運用設計と直接関係するため、本調達の受注者はこの案件の受注者とも運用設計情報を共有可能かつ問い合わせを受け付け可能な体制とすること。

３　作業の実施内容に関する事項

（１）　作業の概要

本調達で受注者が実施する作業の概要は下記のとおり。

①　セキュリティログ解析システムの導入・構築

受注者は、PMDA が運用しているセキュリティ製品、サーバ、端末の動作状況を可視化、調査するためのセキュリティログ解析システムを導入すること。セキュリティログ解析システムは、セキュリティ製品、サーバ、端末の状況を一元的に管理できるように統一的な GUI を提供できるように構成すること。別紙 1 サービス要件にセキュリティログ解析システムが備えるべき機能及び検知、遮断すべき内容が記載されているが、PMDA が運用する製品では解析、検知、遮断が困難な場合は、製品の追加や代替により対応することも可とする。製品の代替を行う場合は代替前の機器と同等以上の正常及び機能を有することを条件とする。代替に伴う作業も行うこと。PMDA が運用しているセキュリティ製品及びシステム構成、利用者人数については別紙 2 共用 LAN システム構成を参照すること。構成品の具体的な製品名は別紙 3 共用 LAN システム構成製品を参照すること。

②　セキュリティ対策ソフトウェアの導入・構築

受注者は、セキュリティログ対策ソフトウェアを導入し利用可能となるように導入作業を行うこと。このソフトウェアについてもセキュリティログ解析システムで一元的に管理ができるように構成すること。これらのソフトウェアを使用して別紙 1 サービス要件に記載する内容を実現すること。ソフトウェア単体に求める要件は別紙 1 サービス要件に記載する。本ソフトウェアは表　１.２　想定スケジュールに示したフェーズ 2、3、4、5 の期間において使用する。

③　運用設計

受注者は、表　１.２　想定スケジュールに示したフェーズ 2、3、4、5 の期間において、本調達で導入する製品及び既に PMDA に導入されているセキュリティ機器やネットワーク機器、サーバ等を用いてセキュリティインシデントの調査、分析、結果報告が行えるように運用設計を行うこと。

フェーズ 4 では、フェーズ 5 にて PMDA が運用を行うための運用設計を行うこと。運用設計はフェーズ 4 時点のセキュリティ情勢を鑑みて行うこと。

各フェーズの運用設計に即した運用手順書、製品の操作手順書を作成すること。

④　MSS

受注者は、表　1.2　想定スケジュールに示したフェーズ 2、3、4 の期間において、リモートによる情報システムの監視、本調達で導入する製品の運用、セキュリティインシデント発生時の対応支援を実施すること。詳細な要件は別紙 1 サービス要件に記載する。

⑤　報告

受注者は、表　1.2　想定スケジュールに示したフェーズ 2、3、4 の期間においてインシデント発生時もしくはインシデント発生の疑いがある場合、運用設計に定められた方法で PMDA に連絡を行った上で MSS 対応を開始すること。

フェーズ 2、3、4 においては監視対象の機器の動作状況について集計し、定期的に報告を行うこと。

⑥　ハードウェア保守

受注者は、表　1.2　想定スケジュールに示したフェーズ 2、3、4、5 の期間において、本調達で導入した製品のハードウェア保守を行うこと。ハードウェア障害時はオンサイト対応を行いシステムが正常に復旧するまでの対応を行うこと。

⑦　ソフトウェア保守・技術サポート

受注者は、表　1.2　想定スケジュールに示したフェーズ 2、3、4、5 の期間において、本調達で導入した製品のソフトウェア保守及び技術サポートを行うこと。

⑧　既存システムからのログ移行

受注者は、現行 MSS のセキュリティログサーバのログを本調達で導入するセキュリティログ解析システムで検索可能な状態にすること。現行のログはテキストデータで PMDA が用意するが、セキュリティログ解析システムでログを参照するために必要なログデータ加工やログのインポートは本調達にて行うこと。

⑨　セキュリティログ解析システム利用状況のアセスメント

受注者は、表　1.2　想定スケジュールに示したフェーズ 2、3、4 の期間において、最大で 1 年あたり 2 回の頻度でセキュリティログ解析システムの利用状況のアセスメントを行い、PMDA と協議の上、利用方法の改善について提案及び改善作業を行うこと。

フェーズ 5 の期間においても同等のアセスメントを行い、利用方法の改善について提案を行うこと。

⑩　運用終了時の処理

受注者は、表 １.２　想定スケジュールに示した各フェーズの終了時、導入製品において運用上不要なデータがある場合、不要なデータを完全に消去すること。データ消去作業が完了した後、消去が完了したことを明記した証明書を作業ログとともに PMDA に提出すること。データ消去作業に必要な機器等は受注者が用意すること。

フェーズ 5 完了時はセキュリティログ解析システム上のログ及びデータを PMDA の指定する機器に移動すること。フォーマットや移動方法については PMDA と協議の上受注者が実施すること。

本仕様書及び別紙に示す性能・機能等については、主要な事項のみを示したものであり、本仕様に明記していない事項についても当該システムとして備えるべき事項については完備されるものとする。

また、導入作業状況により既存機器等の賃貸借期限を延長する必要が生じた場合には延長賃貸借の費用等について受注者が負担すること。

（２）　作業の内容

①　設計・導入

ア　プロジェクト計画

アー1　受注者は、PMDA の指示に基づき、プロジェクト実施計画書を作成し、PMDA の承認を受けること。

イ　物品

イー1　受注者は、本調達仕様書に記述する要件を全て満たすために必要な製品を納品すること。詳細は、別紙 1 サービス要件に示す。なお、導入役務に必要な部材を含むものとする。

ウ　設計

ウー1　受注者は、本調達で導入するハードウェア、ソフトウェア及びサービスの設計を行うこと。

ウー2　受注者は、セキュリティを考慮して以下の点を留意し設計すること。

・導入製品に対する必要十分なアクセス権設定

・ログインアカウントの整理

ウー3　受注者は、以下の点を留意しシステム設計すること。

・単一障害点の排除
・システム稼働状況の視認性
・システム異常時の通知の視認性

ウ－4　受注者は、以下の点を留意しテスト設計すること。
・全使用機能の動作確認の実施
・冗長構成時の片系障害時の動作確認の実施(縮退動作を含む)
・実際の利用環境からの動作確認の実施
・リソース負荷を考慮した性能試験

ウ－5　受注者は、円滑な保守対応のためハードウェア及びソフトウェア障害発生時の対応方法を PMDA(または PMDA の委託業者)に受注者が作成した成果物をもとに説明すること。

エ　導入・移行・テスト

エ－1　受注者は、導入に当たり、情報セキュリティ確保のためのルール遵守や成果物の確認方法（例えば、導入場所での調査等についての実施主体、手順、方法等）を定めた導入計画書を作成し、PMDA の承認を受けること。

エ－2　受注者は、移行にあたり機器等の詳細な移行スケジュールを作成し、移行順序や移行時の影響範囲を明確にした移行計画書を作成し PMDA の確認を受けること。

エ－3　受注者は、機器等の導入に係るテストについて、テスト体制、テスト環境、作業内容、作業スケジュール、テストシナリオ、合否判定基準等を記載したテスト計画書を作成し、PMDA の承認を受けること。

エ－4　受注者は、テスト計画書に基づき、機器等の導入に係るテストを行うこと。

エ－5　受注者は、テスト計画書に基づき、各テストの実施状況を PMDA に報告すること。

オ　検収支援

オ－1　受注者は、PMDA が導入・構築された情報セキュリティ監視基盤の検収を実施するに当たり、環境整備、必要な情報の提供等の協力を行うこと。

カ　引継ぎ(フェーズ 2、3 開始前)

カ－1　受注者は、設計・導入の設計書、作業経緯、残存課題等を文書化し、PMDA 及び共用 LAN 運用支援業務受注者に対して確実な引継ぎを行うこと。必要に応じて設計書や運用手順書の説明会を実施すること。

カ－2　受注者は、別紙 1 サービス要件に示す監視要件について、運用設計に基づいたインシデント発生時の対応手順書を作成すること。

キ　引継ぎ(フェーズ 5 開始前)

キ－1　受注者は、本引継ぎ時のセキュリティ情勢や PMDA での運用状況を考慮し、最適な運用設計を行うこと。

キ－2　受注者は、本引継ぎ時の運用設計に基づいて設計書、残存課題、運用手順書等の関連する文書の改訂を行うこと。

キ－3　受注者は、改訂した文書を基に PMDA 及び共用 LAN 運用支援業務受注者に対して確実な引継ぎを行うこと。必要に応じて改訂した文書の説明会を実施すること。

② 保守・運用

ア　保守計画の支援

ア－1　受注者は、PMDA が保守計画を確定するに当たり、情報システムの構成やライフサイクルを通じた共用 LAN の運用業務及び保守作業の内容について情報提供等の支援を行うこと。

イ　保守期間

イ－1　受注者は、各機器等の保守を本調達の運用期間中を対象として実施すること。

イ－2　受注者は、PMDA が運用期間中に導入製品及び MSS を確実に利用できるようにサポートすること。

ウ　保守対応

ウ－1　別紙 1 サービス要件に詳細を記載する。

③ 作業報告

ア　会議・報告

ア－1　受注者は、プロジェクト管理要領にもとづき、本調達の進捗状況を 2 週間に 1 回 PMDA で報告する会議体を設定すること。特に以下の内容を報告すること。また、当該会議後 3 営業日以内に議事録を作成し PMDA の承認を受けること。本会議体はフェーズ 1、2 にて実施すること。

・WBS で定義した計画と実績

・課題等の対応状況

・翌 2 週間以内の作業内容予定の報告

ア－2　受注者は、本調達の各工程における設計内容や成果物などに関する PMDA との協議を随時行い、PMDA と受注者間で認識違いのないように業務を行うこと。

ア－3　受注者は、PMDA の既存システムに対する変更及び既存システムに影響のある作業を行う場合は、原則として作業を行う 7 日以上前に当該作業内容と影響内容・範囲を提示すること。また、当該作業が終了した後は速やかに作業結果の報告を行うこと。

（３）　成果物の範囲、納品期日等

① 成果物

作業工程別の納入成果物を表３．１に示す。ただし、納入成果物の構成、詳細については、受注後、PMDA と協議し取り決めること。

表 3.1　工程と成果物

項番	工程	納入成果物	提出期限
1	計画	・プロジェクト実施計画書	契約締結日から 2 週間以内
2	設計	・環境設計書 ・環境定義書 ・導入物品一覧	導入工程着手まで
3	導入	・導入・移行手順書	導入・移行作業着手まで
		・導入・移行作業結果報告書	テスト工程着手まで
4	テスト	・テスト計画書	テスト作業着手まで
		・テスト結果報告書	各テスト作業実施後 1 週間以内
6	引継	・引継計画書 ・引継実施報告書	平成 31 年 3 月 22 日
7	運用・保守	・運用手順書 ・保守計画書 ・保守手順書	平成 31 年 3 月 22 日
8	その他	・課題管理表 ・打合せ資料 ・議事録 ・機密情報受理管理簿 ・データ消去証明書 ・瑕疵担保責任対応に係る保有情報の一覧	資料作成、更新時都度

② 納品方法

納入成果物については以下の条件を満たすこと。

ア　文書を磁気媒体等（CD-R 又は CD-RW 等）により日本語で提供すること。

イ　磁気媒体等に保存する形式は、PDF 形式及び Microsoft Office2013 以上で扱える形式とする。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。

ウ　一部のドキュメントについては PMDA からフォーマットを提供し、そのフォーマットに記入を依頼することがある。提供フォーマットのファイル形式は Office2013 ファイル(Excel、Powerpoint、Word、Visio)、PDF 形式とする。

エ　磁気媒体は二部用意すること。

オ　一般に市販されているツール、パッケージ類の使用は PMDA と協議の上、必要であれば使用を認めることとするが、特定ベンダーに依存する（著作権、著作者人格権を有する）ツール等は極力使用しないこと。

カ　本調達で使用した開発ツール等のライセンス及びメディアを納入すること。

キ　本業務を実施する上で必要となる一切の機器物品等は、受注者の責任で手配するとともに、費用を負担すること。

ク　表３．１に記載のある成果物を期日までに提出すること。設計や作業手順、運用手順の共有にあたり PMDA が随時成果物の提供を求めることがあるので、受注者はこれに対応すること。

③　納入成果物に記載すべき内容

納入成果物に記載すべき内容を以下に記す。ただし、導入作業や運用を行うにあたり追記もしくは他に作成すべきものがあれば PMDA と協議の上作成すること。

ア　プロジェクト実施計画書

- プロジェクトスコープ
- 体制表
- 受注者と PMDA の作業分担表
- スケジュール
- プロジェクト管理要領(文書管理要領、セキュリティ管理要領、品質管理要領、変更管理要領)
- WBS

イ　環境設計書(※1)

- システム全体の設計方針
- MSS サービス定義

・　システム構成図(物理・論理)
・　ネットワーク及び IP アドレス一覧
・　システムアカウント及びアクセス方法、用途の一覧
・　運用設計

ウ　環境定義書

・　導入製品のパラメータ一覧
・　動作アプリケーション及びサービス、ジョブ一覧

エ　導入物品一覧

・　導入物品の一覧(動作するサブシステム、構成、シリアル、ライセンス、バージョン情報が分かるようにすること)

オ　導入・移行手順書

・　各サブシステムの移行における具体的な手順 (システム影響がある作業は特に影響範囲を明示すること)

カ　導入・移行作業結果報告書

・　移行作業後の結果及び課題

キ　テスト計画書

・　テストの実施方針
・　単体テスト、複合テスト、移行作業における正常及び異常テストの内容

ク　テスト結果報告書

・　テスト計画書に従い実施したテスト結果
・　テストデータ
・　テスト証跡

ケ　引継計画書

・　本調達機器等の運用にあたり必要となる手順の説明スケジュール

コ　引継実施報告書

・　教育計画書に記した説明を実施したことを示す報告書。報告日・報告内容・報告者・報告対象者を記載すること。

サ　運用手順書

・　環境設計書に記した運用設計に基づいた導入製品の運用手順 (危険度に応じた対応手順を明記すること)
・　各機器等の全マニュアル

シ　保守計画書

・　機器等のライフサイクル(導入時に判明しているもの)
・　保守体制図

ス　保守手順書

・　機器等のハードウェア、ソフトウェア保守を行うにあたり必要な内容

セ　課題管理表

・　各工程で発生する課題の一覧
・　課題発生日、起票者、回答者、解決期限、対応履歴を記載

ソ　議事録

・　各会議での議論概要
・　日時及び場所
・　出席者

タ　機密情報受理管理台帳

・　PMDA から受領した機密情報の開示範囲及び日時
・　PMDA が破棄を指示した機密情報の破棄日時
・　PMDA が返却を指示した機密情報の返却日時

チ　データ消去証明書

・　本調達の運用終了後に機器等のデータ消去が確実に行われたとわかるもの

ツ　瑕疵担保責任対応に係る保有情報の一覧

・　瑕疵担保責任対応に必要となる資料(導入作業時に言及のなかった資料がある場合)

(※1)システム全体の設計方針には、導入製品のシステム構成、役割、構成の意図を明示すること。MSS サービス定義書には、導入製品を使用して MSS が提供するサービスの内容について詳細を記載すること。

フェーズ 5 に向けて、フェーズ 4 で行った運用設計に基づいて成果物の改訂を行うこと。改訂した成果物はフェーズ 5 開始日までに提出すること。

④　納品場所

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

４　満たすべき要件に関する事項

本業務の実施にあたっては、別紙１ サービス要件を参照し、本業務に求められる各要件を満たすこと。

５　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いてはその他の業務を兼務することがないように体制を整えること。

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）　プロジェクトマネージャに求める資格等の要件

① プロジェクトマネージャは原則として本調達に関わる PMDA との会議に全て参加できる体制を取ること。やむを得ず欠席する場合は PMDA の承認を得ること。

② プロジェクトマネージャは過去に同規模、同様内容のマネージドセキュリティサービス導入業務においてプロジェクトマネージャとして参画した経験が 2 件以上あること。

（３）　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 なお、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。

６　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、情報セキュリティ対策の履行状況の確認等の指示に応じること。PMDA が必要と判断した場合は PMDA が情報セキュリティ監査を行うことがある。この場合、PMDA の事前通知に従い受入に必要な対応を行うこと。また、修正及び改善要求があった場合には、別途協議の場を設けて対応すること。

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

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

（２）　機密保持、資料の取扱い

本業務を実施する上で必要とされる機密保持に係る条件は、以下のとおり。

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

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

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

③　応札希望者についても上記①及び②に準ずること。

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

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

⑥　機密保持の期間は、当該情報が公知の情報になるまでの期間とする。

（３）　遵守する法令等

本業務を実施するにあたっての遵守事項は、以下のとおり。

① 受注者は、最新の「政府機関の情報セキュリティ対策のための統一基準」、「府省庁対策基準策定のためのガイドライン」、「医療情報システムの安全管理に関するガイドライン」及び「独立行政法人　医薬品医療機器総合機構情報セキュリティポリシー」（以下、「セキュリティポリシー」という。）に遵守すること。セキュリティポリシーは非公表であるが、「政府機関の情報セキュリティ対策のための統一基準群（平成 28 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。

7　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） 瑕疵担保責任

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瑕疵の疑いが生じた場合であって、PMDA が必要と認めた場合は、受注者は速やかに瑕疵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瑕疵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、瑕疵担保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。瑕疵担保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（日本工業標準）に従い、また個人情報を取り扱う場合には JISQ15001（日本工業標準）に従い、厳重に管理をすること。また、瑕疵担保責任の期間が終了した後は、保守業務を行うにあたり必要のないデータを速やかに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、「3（3）①成果物」に記載のすべて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。

8 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 作業責任部署は 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（日本工業標準）のいずれかを取得していること。

③ セキュリティオペレーションセンター（SOC）専門部門を日本国内に設置していること。また、総合機構のセキュリティオペレーションセンター（SOC）の見学が可能であること。

④ サイバーセキュリティに関する専門部門を設置しており、 Certified Information Systems Security Professional (CISSP)CISSP 認定資格または Certified Ethical Hacker (CEH)認定資格を有している社員が 15 名以上在籍すること。

⑤ 導入する OS、ミドルウェア等の製品に関する資格を有するなど、仕様に精通している担当者が作業体制に含まれること。

⑥ 応札時には、詳細な見積内訳及び作業ごとに細分化された工数、ハードウェア・ソフトウェア構成、概略スケジュールを含む見積根拠資料の即時提出が可能であること。なお、応札後に総合機構が上記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。

⑦ 1000 人以上のユーザを有する官公庁において、同種の導入作業及びセキュリティ運用案件を 3 件以上対応した実績があること。

（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から委託を受ける等緊密な利害関係を有する事業者

９ 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。

ア 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。

イ 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。

ウ 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。

１０ 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。

ア　総合的企画、業務遂行管理、手法の決定及び技術的判断等。

イ　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。

１１ 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、「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）」（平成 15 年 7 月 16 日法律第 119 号）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。

１２ 附属文書

（１） 調達仕様書別紙

別紙 1 サービス要件
別紙 2 共用 LAN システム構成
別紙 3 共用 LAN システム構成製品

別紙 2 共用 LAN システム構成、別紙 3 共用 LAN システム構成製品は本調達仕様書と同時に公示される秘密保持誓約に記載及び紙面による提出を行った応札希望者に電子データで配布する。

１３ 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 サーバリプレイス調達担当者

電話：03-3506-9485

Email：ml-c-mssrep-a@pmda.go.jp

マネージドセキュリティサービスの更新調達一式

別紙 1 サービス要件

1 セキュリティログ解析システム及び MSS に求める要件

本項目に記載する内容は断りがない限り調達仕様書の想定スケジュールに示すフェーズ 2、3、4、5 で提供を求めるものとする。

1.1 監視対象

1.1.1 業務端末

1. 1720 台を想定すること。
2. OS は Windows7 Enterprise、Windows10 Enterprise を想定すること。

1.1.2 リモート接続 VDI 端末

1. 300 台を想定すること。仮想デスクトップは VMware 社 Horizon View で管理されている。
2. OS は Windows10 Enterprise を想定すること。

1.1.3 インターネット閲覧 VDI 端末

1. PMDA ではインターネット接続に VMware 社の仮想デスクトップクラウドサービスを使用している。この仮想デスクトップを監視対象とすること。
2. 仮想デスクトップは 400 台を想定すること。
3. OS は Windows7 Enterprise、Windows10 Enterprise を想定すること。
4. 本仮想デスクトップの用途を考慮し、1.2.3 に示す監視項目は既知のマルウェアのダウンロードやアップロードのみ満たせば良い。

1.1.4 共用 LAN サーバ

1. 共用 LAN システムで運用している物理サーバ、仮想サーバを監視対象とし、100 台を想定すること。共用 LAN システムで運用している仮想基盤システム上で動作している業務システムサーバも含む。
2. OS は Windows Server2016、Windows Server2012(R2 含む)、Redhat Linux Enterprise7、CentOS7 を想定すること。

1.1.5 業務システムサーバ

1. 業務システムサーバの IP アドレスやホスト名、URL 等を監視対象として業務システムサーバへの通信を監視すること。
2. 業務システムサーバ内の OS、アプリケーションは監視外として良い。
3. PMDA が指定した業務システムサーバについては 1.1.4 と同様の監視を行うこと。台数、や OS は 1.1.4 の範囲内での対応とする。

1.2 監視機能要件

本調達で導入するセキュリティログ解析システムと PMDA で運用しているセキュリティ装置を使用して本項目に示す挙動を検知すること。PMDA で運用しているセキュリティ装置では対応ができない場合、受注者にて製品の追加や代替により対応すること。

1.2.1 以下の不正通信の発生を検知すること。

1. 不正な URL へのアクセス
2. 不正な User-Agent による Web アクセス
3. 各種インジェクション攻撃、クロスサイト攻撃、プロトコルアノマリ、バッファオーバーフロー、その他 OS やアプリケーション脆弱性に対する攻撃性のある通信
4. 暗号化された不正な通信
5. 疑わしい拡張子のついた実行ファイルの転送に用いる各種通信プロトコル
6. ダウンローダを使用したマルウェアの段階的ダウンロード
7. C&C サーバへのアクセス
8. 既知の C&C サーバの名前解決
9. 標準的に利用される通信ポート以外の IRC 通信
10. Windows ドメインログオンの過剰な失敗を示す通信
11. Instant Messaging アプリケーションの通信
12. P2P アプリケーションの通信
13. ストリーミング通信
14. ファイルサーバへの不正アクセス

1.2.2 以下の不正メールの受信を検知すること。

1. 不正 URL を本文に含むメール
2. スパムメール
3. 既知のメール中継サーバから中継される不正メール
4. フィッシングメール

1.2.3 以下の不正ファイルの存在、挙動を検知すること。

1. 既知マルウェアのダウンロードやアップロード
2. Windows の管理共有フォルダへ実行ファイルを転送する通信
3. 業務端末のプロセスやメモリ、ファイル I/O の挙動
4. ファイルレス、インメモリマルウェアの挙動
5. ランサムウェアによるファイル暗号化の挙動
6. ファイル暗号化が行われないランサムウェアの挙動

7. 任意の IOC ファイルを契機とした監視対象の挙動

1.2.4 以下のログを格納し、内容を調査可能な状態とすること。

1. 監視対象サーバへの特権 ID によるログイン記録
2. 監視に使用しているセキュリティ装置の動作ログ
3. VDI 端末の利用履歴(利用者と VDI 端末の紐づけ)

1.3 監視業務要件

調達仕様書の想定スケジュールに示すフェーズ 2,3,4 の期間を対象として、受注者はセキュリティログ解析システムを活用した監視業務を行うこと。監視業務に求める要件以下に示す。

1.3.1 不正通信の検知及び通知

1. PMDA と外部、PMDA 内同士の双方向通信において、セキュリティアナリストが監視、分析を行うこと。
2. 危険度が高いと判断されるセキュリティインシデントを検知し、その内容から攻撃元の IP アドレスを特定できる場合は対象の IP アドレスを PMDA に通知し、遮断措置を行うべきセキュリティ装置の助言を行うこと。
3. マルウェア感染後のコールバック通信発生時や、未知のマルウェア感染の可能性が極めて高いと判断される通信が発生した場合、PMDA に対して電話及びメールで 15 分以内に通知を行うこと。
4. 検知ポリシは日常的なセキュリティ監視業務において能動的に見直し、PMDA にその内容を報告すること。
5. 検知結果に対してセキュリティアナリストにより解釈を行った上で報告を行うこと。
6. 監視業務の中でベンダの提供するシグネチャで防御ができない攻撃が検知された場合、IPS 装置のカスタムシグネチャ作成を行うこと。カスタムシグネチャの適用は PMDA との協議の上実施すること。

1.3.2 運用改善の提案

1. 監視、分析を行った結果、追加で対策を行った方が良いと判断される内容があれば PMDA に助言を行うこと。
2. 検知及び防御するべきと判断される脅威情報のカスタム IOC ファイルを作成すること。セキュリティ装置ベンダが提供する IOC 以外にも対応すること。
3. PMDA 内外問わず、新たに発見された攻撃手法や脅威情報について、概要や対処法そのタイミングでのセキュリティ体制を考慮した場合にどの程度脅威となるか助言を行うこと。

1.3.3 セキュリティ装置の正常動作確認

1. 監視に使用する各セキュリティ装置が適切に動作していることを確認するための仕組みを導入すること。この仕組みはフェーズ 5 でも PMDA が利用可能なように構成すること。
2. 本調達で新たにセキュリティ製品の導入を行った場合、シグネチャ等のセキュリティコンテンツは自動的にアップデートされる構成とし、常に最新の状態に保つこと。アップデート状況は受注者が 1 日 1 回確認を行い、失敗している場合は PMDA に報告を行うとともに手動でアップデートを実施すること。また、アップデートに失敗した原因を PMDA に報告すること。

1.3.4 体制

1. 24 時間 365 日の有人監視が可能な設備、人数規模を持つ受注者専用の環境にて監視業務を行うこと。
2. PMDA からの電話及びメールによる連絡を 24 時間 365 日受け付けられる体制を整えること。
3. PMDA をサポートする担当者を設け、サポート担当者が PMDA とのサポート窓口となること。
4. セキュリティインシデントが発生した際、PMDA 内でないと対応できないようなケースの場合はオンサイトでの対応を行うこと。
5. 必要に応じてサポート担当者が PMDA に訪問し、問題解決のための打ち合わせが可能なこと。本打ち合わせは定期的に行うものではない。

1.4 通信遮断に関する操作

調達仕様書の想定スケジュールに示すフェーズ 2,3,4 の期間を対象として、監視により脅威が検知された場合、本項目に記載するケースに該当する場合は受注者が不正通信の遮断を行う。尚、遮断を行った際の監視対象やセキュリティ機器の状態に関する情報取得は受注者がリモートで行うこと。

1.4.1 24 時間 365 日での対応を求める項目

1. 事前に定めた基準(台数)を超えたマルウェア検知時の通信遮断、ファイル削除、プロセス停止
2. ランサムウェア等による、攻撃者が定めた任意のファイルに対する暗号化の阻止

1.4.2 平日 9～18 時での対応を求める項目

1. IPS 装置のシグネチャ適用(カスタムシグネチャを含む)
2. IPS 装置のホワイトリスト設定

1.5 システム構成要件

セキュリティログ解析システムの構成要件を示す。システム構成はオンプレミス、クラウド環境は問わないが、それぞれの環境に応じた要件を満たすこと。

1.5.1 ハードウェア要件

オンプレミス環境にハードウェアを設置する場合、以下の要件を満たすこと。

1. ハードウェアは共用 LAN 仮想基盤システムが設置されているデータセンタ内に設置すること。必要なデータセンタ費用も本調達に含む。
2. 各要件に対応可能なハードウェア構成とすること。
3. ハードウェアの冗長化を行い、単一障害点を極力なくすこと。
4. ハードウェア障害時は自動的に予備機等への切り替わりが行われること。
5. 1 日あたり 50GB 程度のログ受信を想定すること。
6. 過去 13 か月分のログを検索可能なこと。
7. ログを保管するノードはクラスタ構成とし、検索を高速化する構成とすること。
8. クラスタ構成されたログ保管ノードの容量を増加する際はシステムの停止を伴わない構成とすること。

1.5.2 ネットワーク構成

1. 受注者のネットワークと接続する場合、PMDA ネットワークと論理的に分離された構成とし、PMDA の業務トラフィックと受注者の監視トラフィックが混在しないようにすること。
2. セキュリティログ解析システムが WAN 回線を経由して受注者のネットワークと接続される場合、WAN 回線上ではトラフィックの暗号化を行うこと。
3. オンプレミス環境にハードウェアを設置する場合、共用 LAN システムで使用しているネットワーク機器と接続しても良い。物理ポートが不足する場合、必要となるネットワーク機器を構成に含めること。接続作業に伴う既存機器の設定変更も受注者の作業範囲とする。
4. クラウド環境にセキュリティログ解析システムを構成する場合、ログを送信するためのインターネット回線を構成に含めること。この時、PMDA とクラウド環境間の通信は暗号化を行うこと。共用 LAN システムのネットワーク機器と接続しても良いが、インターネット回線との接続機器や通信の暗号化を行う装置は本調達に含めること。インターネット回線との接続ポイントの前にはファイアウォールを設置し、必要最低限の通信のみ許可すること。接続作業に伴う既存機器の設定変更も受注者の作業範囲とする。
5. クラウド環境にセキュリティログ解析システムを構成する場合、パブリッククラウドのような他テナントとの共用スペースを使用しないこと。国外にデータを配置する構成は不可とする。
6. 監視対象から情報を収集する際のネットワークトラフィックに留意すること。各 WAN 回

線の業務利用に影響を与える場合は専用の WAN 回線を本調達に含めること。

1.5.3 セキュリティ機能要件

1. 不正な URL、IP アドレス、メール中継サーバ等の脅威情報を格納した脅威情報データベースを搭載すること。脅威情報データベースはセキュリティ製品ベンダの情報ではなく受注者により提供しているものを使用すること。
2. 脅威情報データベースを使用した不正通信の検知は本調達の全フェーズを通して受注者及び PMDA が利用可能なこと。
3. 脅威情報データベースの情報更新は毎時間以内で行われること。
4. 業務端末、VDI 端末上でランサムウェアを検知する等、事前に定めた条件を満たした場合に自動的に当該端末をネットワークから遮断可能なこと。遮断時でもセキュリティログ解析システムの最小限の構成要素と通信を継続し、当該端末の稼働ログを取得可能なこと。

1.5.4 レポート要件

収集したログ情報を集約し、下記の情報を Web ブラウザから閲覧可能な GUI をセキュリティログ解析システムにて提供すること。期間を指定することで一度に 60 日間分の統計情報を表示可能なこと。各セキュリティ製品の管理画面を閲覧するのではなく、セキュリティログ解析システム上で表示及び確認が可能なこと。詳細な表示方法は PMDA と協議の上決定するものとする。

1. IPS 装置の脅威度中以上の攻撃検知件数
2. IPS 装置に適用したカスタムシグネチャによる遮断件数
3. 業務端末、VDI 端末にインストールされたマルウェア対策製品による検知状況
4. 共用 LAN サーバにインストールされたマルウェア対策製品による検知状況
5. インターネット接続用 VDI 端末にインストールされたマルウェア対策製品による検知状況
6. HTTP プロキシサーバの通信成立件数(HTTP プロキシサーバの機能を使用してカテゴリ単位での件数分類を行うこと)
7. HTTP プロキシサーバの通信遮断件数(HTTP プロキシサーバの機能を使用してカテゴリ単位、ブラックリストごとの件数分類を行うこと)
8. 入力した URL、IP アドレスに対するアクセスの有無
9. Gmail 等のフリーメール宛のメール送信件数(宛先ドメインごとに表示し、添付ファイルの有無ごとに件数表示すること)
10. PMDA から外部へのメール送信件数、外部からのメール受信件数
11. ファイル管理サーバに発生したアクセス数(アクセス元端末、読み取り、書き込みごとに表示すること)
12. ファイル管理サーバ内の指定したファイルへのアクセス有無(ファイルパスを指定し、アク

セス元端末を表示できるようにすること)

13. 業務端末、VDI 端末、共用 LAN サーバを対象とした任意のセキュリティパッチの適用状況
14. 業務端末、VDI 端末、共用 LAN サーバを対象とした任意のファイルの有無
15. 業務端末、VDI 端末、共用 LAN サーバを対象とした動作ミドルウェア、アプリケーション、プロセスの一覧
16. ランサムウェアの検出件数
17. 共用 LAN サーバへの特権 ID を用いたログイン、ログアウト履歴(サーバ単位で表示が可能なこと)
18. 監視対象のローカルディスク残量の監視

1.5.5 ログ機能要件

1. 複数のログフォーマットを対象として横断的な検索が可能なこと。
2. ログ検索文字列として正規表現が利用可能なこと。
3. ログ検索条件として論理演算子が利用可能なこと。
4. 任意の周期で事前定義した検索を自動的に実行可能なこと。
5. 検索条件を保存可能なこと。
6. 検索結果として表示された文字列を REST API により外部システムに受け渡し可能なこと。
7. ログは Syslog、CEF、LEEF での受信が可能なこと。
8. テキストファイルに出力されたログをリアルタイムに取得可能なこと。テキストファイルに追記が行われた場合、追記した部分のみ取得が可能なこと。
9. アーカイブされたログファイルを自動的に解凍して取得可能なこと。
10. 非対応ログフォーマットのログを取得するためのアドオン追加が可能なこと。
11. RDBMS に発行されたクエリ情報を取得可能なこと。
12. 取得したログは圧縮して管理可能なこと。
13. 取得したログをハッシュ化する等の改ざんを防止する機能を有すること。改ざんが発生した場合、検知が可能なこと。

1.5.6 レポート機能要件

1. ログ検索結果や統計処理により抽出された数値や項目を棒グラフや線グラフで表示可能なこと。
2. グラフは PDF 形式で出力可能なこと。
3. 任意のダッシュボード画面を作成し、表示項目のカスタマイズが可能なこと。
4. 作成したレポートはメールによる自動送信が可能なこと。

1.6 保守要件

1.6.1 ハードウェアオンサイト保守

1. 本調達で導入したハードウェアのオンサイト保守を行うこと。対応時間は 24 時間 365 日とすること。PMDA からの連絡を受け、オンサイト保守対象製品の調査及び交換を行うこと。
2. オンサイト保守は 4 時間以内の駆け付けが可能な体制とすること。
3. オンサイト保守作業の実施日程は PMDA と協議の上決定すること。
4. ハードウェアの交換だけでなく、システムが正常稼働状態に復旧するまで対応を行うこと。
5. オンサイト作業後は作業時間及び結果を記した作業報告書を提出すること。
6. セキュリティログ解析システムのバージョンアップやアップデートパッチを適用しても導入時と同様に保守対象としてハードウェア保守を行うこと。

1.6.2 ソフトウェア保守要件

1. 本調達で導入したソフトウェア保守を行うこと。ソフトウェアバグや新たに発見された脆弱性、サポート期間の終了等の理由によりソフトウェアバージョンアップの必要が生じた場合は、受注者によりバージョンアップ作業を行うこと。バージョンアップ作業は PMDA に作業内容及び影響範囲の報告を行い、承認を得て実施すること。この対応はフェーズ 2、3、4 を対象とする。
2. 本調達で導入したソフトウェアの技術サポートを行うこと。技術サポートは平日 9 時～17 時を対象とすること。
3. 本調達で導入したソフトウェアのサポート期限が判明した時点で PMDA にサポート期限の連絡を行うこと。
4. PMDA が保持するセキュリティ装置のバージョンアップ等によりセキュリティログ解析システムの設定変更が必要となる場合、PMDA と協議の上、受注者が設定変更を行うこと。尚、PMDA が保持するセキュリティ装置のバージョンアップ作業は本調達受注者の作業範囲外とする。
5. セキュリティログ解析システムのバージョンアップやアップデートパッチを適用しても導入時と同様に保守対象として情報提供及びソフトウェア保守を行うこと。

2 セキュリティ対策ソフトウェアに求める要件

セキュリティログ解析システムに求める要件を満たすように構成すること。他にソフトウェアとして本項目に記す機能を有すること。複数のソフトウェアで構成しても良い。これらのソフトウェアがネットワークに業務影響を及ぼすほどのトラフィックを発生させる場合は専用の回線を用意する等の対応を行うこと。

2.1 基本構成

1. 監視対象にインストールするエージェント型であること。インストール対象は業務端末、リモート接続 VDI 端末、共用 LAN サーバとする。
2. 監視対象を一元管理するための管理サーバを有すること。
3. 管理サーバはセキュリティログ解析システムと連携可能であり、セキュリティログ解析システムから本ソフトウェアの操作が可能なこと。
4. 監視対象の機密情報が含まれたデータをクラウド等の外部に送信しないこと。
5. システム負荷やスケジューリングを考慮し、監視対象の操作を一斉操作だけでなく任意のグループに対して実行可能なこと。

2.2 ファイル操作

1. ファイルの配布や削除が可能なこと。
2. マルウェアのハッシュ値を基に該当マルウェアに感染した端末を検知できること。
3. 監視対象に保存されているデータをネットワーク経由でセキュリティ対策ソフトウェアの管理サーバにインポート可能なこと。
4. 監視対象のローカルディスク内のファイルハッシュ地を SHA-256、MD5 で取得可能なこと。

2.3 プロセス監視

1. 任意のプロセス停止が可能なこと。
2. 実行中アプリケーションや動作プロセスの情報を表示できること。
3. 確立している通信のポート番号、通信しているプロセスを表示できること。
4. プロセスは親子関係を表示可能なこと。

2.4 ネットワーク制御

1. 端末監視ソフトウェア用の監視サーバや任意の宛先以外との通信を停止できること。通信制御は L3、L4 での制御が可能なこと。
2. 有線 LAN と無線 LAN のように同一端末で異なる NIC(IP アドレス)によるアクセスが発生した場合でも同一端末として認識可能なこと。

2.5 ランサムウェア検知

1. ランサムウェアの検知が可能なこと。検知はシグネチャによるもののみではなく、ランサムウェアの振る舞いまたはファイル暗号化に伴うファイルの挙動により行えること。

2.6 その他

1. セキュリティログ解析システムで発行する監視対象向けのコマンドを監視対象で実行しそ

の結果をセキュリティログ解析システムに送信可能なこと。

2. 任意の IOC ファイルを取り込み、取り込んだ IOC に基づいたスキャンが可能なこと。
3. 本ソフトウェアで検出した状況により IOC ファイルを作成可能なこと。

3 運用設計に求める要件

フェーズ 1 時点ではフェーズ 2、3、4 を対象とした運用設計を行うこと。フェーズ 4 ではフェーズ 5 を対象とした運用設計を行うこと。本項目に記載する内容を基本として、運用設計を行うタイミングでのセキュリティ情勢や PMDA のシステム構成を考慮した運用設計を行うこと。

3.1 定常的な正常性確認

3.1.1 正常稼動の確認

1. セキュリティログ解析システムが正常に動作していることを確認するための方法を明確化し、PMDA に情報提供を行うこと。
2. 正常稼動を示す情報の生成、管理者への情報共有はセキュリティログ解析システムの機能により極力自動化すること。

3.1.2 セキュリティ装置の稼働状況確認

1. 1.5.4 に示す要件を集約したダッシュボードを作成し、その表示を PDF 化して PMDA に自動的にメール送信すること。詳細な表示内容は PMDA と協議の上決定すること。

3.2 セキュリティインシデント発生時

3.2.1 危険度の定義

1. セキュリティインシデントの危険度を定義し、セキュリティインシデントの危険度に応じて適切な連絡手段を用いて PMDA に連絡を行うこと。
2. 危険度はセキュリティ装置が出力するものではなく、監視対象の重要性、システム全体への影響度、不正アクセスの成否によって 4 段階以上で定義すること。以下に例を示す。

危険度	インシデントの定義	連絡手段
3	不正アクセスの成功 (システムに損害を与える可能性がある場合)	電話及びメール (5 分以内)
2	不正アクセスの成功可能性が高い (システムに影響を与える可能性が高い場合)	メール (60 分以内)
1	不正アクセスの成功可能性が低い (ただちにシステムに影響を与えるわけではないが、注意	メール (24 時間以内)

	が必要な場合)	
0	不正アクセスの成功可能性なしまたは極めて低い (リスクがないと考えられる場合)	月次報告

3.2.2 連絡体制・対応手順

1. PMDA とのメール、電話等での連絡体制及び対応手順を明確にすること。連絡体制や対応手順は危険度に応じて明確にすること。

3.2.3 セキュリティインシデント発生端末のフォレンジック対応

1. セキュリティインシデントが発生した際に、対象の端末(仮想、物理を問わない)のフォレンジック対応を行うこと。
2. フォレンジック対応は年 1 回 1 端末 1 インシデントの対応を想定すること。
3. セキュリティインシデントの発生原因や侵入経路、インシデントの詳細、対応内容の詳細、影響範囲について詳細に報告すること。
4. フォレンジック対応時は証拠保全のためインシデントが発生した端末及び関連するサーバやネットワーク機器の証拠データを複製し、ハッシュ値により正常性を確認すること。
5. 国内での検体解析に対応可能なこと。
6. インシデントからの復旧及び再発防止策の提案及び対策実施の技術支援を行うこと。

3.3 定例報告

3.3.1 月次報告書

1. 前月分の月次報告書を月初から 7 営業日以内までに PMDA に提供すること。
2. 月次報告書には前月の動作実績をもとに以下の情報を含めること。
    - システムに影響を与える可能性の高いインシデントの詳細情報と対応履歴
    - セキュリティ情勢及び PMDA にもたらす影響に対する見解
    - 不正メールの受信傾向の推移
    - 不正メールの種類の統計情報
    - PMDA ドメイン宛の存在しないメールアドレス宛のメール送信数
    - 不正メールの受信件数の多いメールアドレスリスト
    - IPS 装置の遮断傾向 (IPS 装置ベンダが提供する脅威度分類において上位 2 位の分類に当てはまる攻撃の種類と遮断件数を記載すること)
    - IPS 装置のカスタムシグネチャによる遮断件数
    - インターネットへの HTTP 通信量の統計
    - HTTP プロキシ及びファイアウォールにブラックリスト登録済みの宛先に対する通信の統計
    - 業務端末、VDI 端末を対象として、Microsoft 社が提供する OS 及び Office の緊

急度の高いセキュリティパッチの未適用端末の数

- 監視対象で動作しているマルウェア対策製品で検知されたマルウェアの数

3.3.2 月次定例会

1. 月次報告書の内容について説明を行うこと。
2. 新しい攻撃手法や脅威情報、対策、セキュリティトレンドの情報があれば提供すること。

3.4 利用状況のアセスメント

3.4.1 セキュリティログ解析システムのアセスメント

1. 1 年に最大 2 回の頻度でセキュリティログ解析システムの活用方法の改善を目的とした会議を実施するので、受注者はこれに参加すること。1 回あたりの実施時間は最大 3 時間程度とする。
2. ダッシュボードのカスタマイズ、ログ送信機器の増減等の要件に対して、システムに与える影響や推奨される監視内容について PMDA に対して助言を行うこと。
3. セキュリティログ解析システムにサードパーティ製品を活用する場合、サードパーティ製品のメーカも本会議に参加可能な体制とすること。