令和５年度 情報システム監査業務

調達仕様書

独立行政法人 医薬品医療機器総合機構
令和６年１月

目次

1　事業名

令和５年度情報システム監査業務

2　目的

サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、独立行政法人医薬品医療機器総合機構（以下「総合機構」という。）のサイバーセキュリティ対策に関する現状を適切に把握した上で、総合機構において対策強化のための自律的かつ継続的な改善活動の実施、及び必要なサイバーセキュリティ対策の実施を支援するとともに、当該業務が継続的かつ有効に機能するよう助言することによって、総合機構におけるサイバーセキュリティ対策の効果的な強化を図ることを目的とする。

また、標的型メール訓練を行い、総合機構のサイバー攻撃に対する知見を深めることを目的とする。

3　業務内容

（１）情報セキュリティ対策の整備・運用状況の監査

総合機構のシステム管理者に対し、聴取形式による運用面・管理面における脆弱性監査を実施し、管理対象システムごとに脆弱性・問題点の一覧及び改善項目・優先度・推奨する運用管理手法等を監査報告書に記載すること。

なお、検出された改善に関する改修等作業については本業務に含まれない。

① 監査の基準

本業務における基準は、以下によるものとする。

・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 【※】
・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
・政府機関等のサイバーセキュリティ対策のための統一規範（最新版）
・政府機関等のサイバーセキュリティ対策の運用等に関する指針（最新版）
・政府機関等のサイバーセキュリティ対策のための統一基準（最新版）

※「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」は非公開であるが、「政府機関等のサイバーセキュリティ対策のための統一基準」に準拠している。

また、参考の位置づけで以下の基準を参照する。

・ NISC 高度サイバー攻撃対処のためのリスク評価等のガイドライン（平成 28 年 10 月 7 日）
・ NISC 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（2016 年 10 月 25 日）
・ 総務省　地方公共団体における情報セキュリティポリシーに関するガイドライン（令和 4 年 3 月）

・　厚生労働省　医療情報システムの安全管理に関するガイドライン第 6 版（令和 5 年 5 月）

② 監査範囲、監査要点

総合機構における重要な情報資産を選定し、その重要な情報資産を扱う情報システムを総合機構と協議のうえ、２システムを選定し監査範囲とする。ただし、２システムのうち、「共用ＬＡＮシステム」は、必ず含むものとする。

a　マネジメント

主な監査要点	監査手続（予定）
• 組織・体制、対策基準・対策推進計画の策定に関する整備･運用 • 情報セキュリティ関係規定の整備･運用 • 総合機構事務従事者への教育 • 情報セキュリティインシデントへの対処に関する整備･運用 • 情報セキュリティ対策の自己点検(R4 年度実施済)及び過去の情報セキュリティ監査改善指摘事項への対応状況･対応内容 • 情報セキュリティ対策の見直しに関する整備･運用 • 情報の取扱い、情報を取扱う区域の管理に関する整備･運用 • 外部委託（約款による外部サービス及びクラウドサービスを含む）に関する整備･運用 • 情報システムに係る台帳等の整備･運用 • 機器等の調達に係る規程の整備･運用	• 関係者へのインタビュー • 資料の閲覧 （規程・手順書・マニュアルおよび実運用に係る証跡）

b　情報システム

主な監査要点	監査手続（予定）
• 重要な情報の取扱いに関する運用 • 情報システムのセキュリティ機能に関する整備･運用（ユーザ管理･ログ管理等） • 情報セキュリティの脅威への対策に関する整備･運用 • 情報システム構成要素に関する整備･運用（データベース、通信回線、ネットワークセグメントの隔離等） • 機器の物理的な管理 • 情報システムの利用に関する運用（総合機構外の利用者を含む） • アプリケーション・コンテンツの作成･提供に関する運用	• 関係者へのインタビュー • 資料の閲覧 （規程・手順書・マニュアルおよび実運用に係る証跡） • 必要に応じて執務室、サーバー室、データセンター【注１】の視察

【注１】　視察するデータセンターの所在地は、関東に限定する

c　外部委託先

主な監査要点	監査手続（予定）
• 重要な情報の取扱いに関する整備･運用 • 委託先において実施させる情報セキュリティ対策の履行状況 • 再委託先に関する情報セキュリティ対策の措置状況・履行状況	• 必要に応じて関係者へのインタビュー • 資料の閲覧（規程・手順書・マニュアルおよび実運用に係る証跡） • 必要に応じて委託先【注２】の視察

【注２】視察する委託先の所在地は、関東に限定する

（２）標的型メール訓練

標的型メール攻撃に対する総合機構職員の対応力および意識の向上をはかるため、標的型メールに相当するなりすましメールを作成し、総合機構が示すスケジュールに従い令和 6 年 3 月までに訓練メールの送信を行なうこと。訓練メールは最大 1,500 人へ送付する。また、Web サイトへのアクセス状況の集計等、業務を行うためのシステム環境を準備し、訓練結果の分析を行い監査報告書に記載すること。

（３）監査報告

６．（１）③･④に定める「監査報告書」に基づき、必要に応じて監査報告を実施する。
監査報告が必要な場合とは、監査の結果が標準的な結果よりも悪く、理事者らに詳細な報告が必要な場合等とする。

- 監査報告には、統括責任者・監査人等が出席すること。
- 総合機構側は、情報セキュリティに関する責任者等が出席する。
- 監査報告の実施如何及び実施の場合の報告内容・報告時間等は別途協議する。

なお、監査報告の実施如何に関わらず、監査室及び情報化統括推進室の役職員等の主な監査関係者等が出席する監査評価会を実施し、監査報告書記載内容に関する認識合わせ等を実施すること。

・監査評価会における出席者・報告内容・報告時間等は別途協議する。

４　システム監査対象

監査対象となる総合機構の情報システムは、別紙１に記す。

5　実施期間

契約日から令和6年3月29日までとし、受託者が派遣する監査員が実施スケジュールに基づいて業務を行う。

受託者は6.(1)①に定める「実施計画書」の体制図に基づき監査員を派遣すること。

6　納入成果物及び納入期日

（1）　納入成果物

納入成果物を表　6.1に示す。ただし、納入成果物の構成、詳細については、受注後、総合機構と協議し取り決めること。

表　6.1　工程と成果物

項番	区分	納入成果物	納入期日
1	計画書	①実施計画書 ②情報セキュリティ管理計画書	契約締結日から 2 週間以内
2	監査報告書	③監査報告書（情報セキュリティ対策の整備・運用状況の監査） ④監査報告書（標的型メール訓練） ⑤各種証跡	令和6年3月１９日

①　実施計画書

実施計画書は以下の項目を含むこと。

a. 監査対象システム

情報セキュリティ対策の整備・運用状況の監査に関しては、総合機構担当者と協議の上、対象となる情報システムの一覧を業務内容単位で記載すること。

b. 使用ツール、機器一覧

本業務を遂行するために使用するツール及び機器があれば、明記すること。

c. システム監査全体スケジュール

総合機構担当者と協議の上、監査業務全体のスケジュールを作成すること。

d. 体制図

本業務を遂行するための体制を記載すること。

e. 実施工程

情報セキュリティ対策の整備・運用状況の監査、標的型メール訓練の実施要領を記載すること。

②　情報セキュリティ管理計画書

「１１ 情報セキュリティ対策の実施」に記載している要件を満足すること。

③　監査報告書（情報セキュリティ対策の整備・運用状況の監査）

a. 監査結果報告

マネジメント及び監査対象システムごとの考察と推奨される対策をまとめたもの。

b. 監査概要

監査概要として、以下の事項を記載すること

- 監査の目的
- 監査の基準
- 監査の実施内容
- 監査範囲・監査対象
- 監査基準日・監査実施期間
- 主な実施内容及び総合機構担当
- 監査人

c. 監査所見

監査の結果を元に、監査対象ごとに検出された改善推奨事項等を記載し、その改善推奨事項に対する一般的な対応方法、総合機構の IT 環境を踏まえた対応方法、優先度を記載すること。

d. 聴取結果レポート（担当者ごと）

担当者ごとの聴取結果の一覧と監査員のコメントを一覧で記載すること。

一覧には、問題点、対応優先度、改善項目、推奨する運用管理方法を含めること。

④　監査報告書（標的型メール訓練）

a. 監査結果報告

標的型メールの開封率・開封者などの傾向が視覚的に分かるレポートをまとめたもの。

b. 監査概要

監査概要として、以下の事項を記載すること

- 監査の目的
- 監査の基準
- 監査の実施内容
- 監査範囲・監査対象
- 監査基準日・監査実施期間
- 監査人

c. 監査所見

監査の結果を元に評価を行い、改善推奨事項等があれば記載し、その改善推奨事項に対する一般的な対応方法、総合機構の IT 環境を踏まえた対応方法、優先度を記載すること。

⑤　各種証跡

監査を行った証跡となるデータはすべて納品すること。

（２） 納入品目

納入品目は以下のとおりとする。

a. 計画書　　外部電磁的記録媒体　2 個（紙媒体は別途協議）
b. 監査報告書　　外部電磁的記録媒体　2 個（紙媒体は別途協議）
c. 各種証跡　　外部電磁的記録媒体等　2 個
※資料は電子ファイルとして加工可能なものを含む

納入品目については、以下の条件を満たすこと。

- 文書を紙及び磁気媒体等（CD-R 又は CD-RW 等）により日本語で提供すること。
- 紙のサイズは、日本産業規格 A 列 4 番を原則とする。図表については、必要に応じて A 列 3 番縦書き、横書きを使用することができる。
- 成果物は、すべて日本語で作成すること。ただし、日本国においても、英字で表記されることが一般的な文言については、そのまま記載しても構わないものとする。
- 用字・用語・記述符号の表記については、「公用文作成の要領」に準拠すること。
- 情報処理に関する用語の表記については、日本産業規格（ＪＩＳ）の規定に準拠すること。
- 受託者は、指定のドキュメントを外部電磁的記録媒体（ＣＤ‐Ｒ等)により納品すること。また、総合機構が要求する場合は紙媒体でも納品すること。紙媒体の納品部数については、総合機構と協議すること。
- 紙媒体のサイズは、日本産業規格Ａ列４番を原則とする。図表については、必要に応じてＡ列３番を使用することができる。
- 外部電磁的記録媒体に保存する形式は MicrosoftWord２０１６、同 Excel２０１６、同 PowerPoint２０１６で読み込み可能な形式及びＰＤＦ形式とすること。ただし、総合機構が他の形式による提出を求めた場合は、これに応じること。なお、受託者側で他の形式を用いて提出したいファイルがある場合は、協議に応じるものとする。
- 納品したドキュメントに修正等があった場合は、紙については、それまでの変更内容を表示するとともに変更履歴と修正ページ、外部電磁的記録媒体については、それまでの変更内容及び修正後の全編を速やかに提出すること。
- 外部電磁的記録媒体は、２部納品すること。
- 納品後、総合機構において改変が可能となるよう、図表等の元データも併せて納品すること。
- 成果物の作成に当たって、ＣＡＤ等の上記以外の特別なツールを使用する場合は、総合機構の承認を得ること。

- 成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
- 外部電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行う等して、成果物に不正プログラムが混入することのないよう、適切に対処すること。
- 成果物の作成及び納品に当たり、内容、構成等について総合機構が指摘した場合には、指摘事項に対応すること。
- 報告書、計画書等の成果物の記載様式については、記載様式案を総合機構に提示すること。総合機構は、案について受託者と協議の上、決定する。

（３） 納品場所

独立行政法人　医薬品医療機器総合機構　監査室
ただし、総合機構が納品場所を別途指示する場合はこの限りではない。

7　作業の実施体制・方法に関する事項

（１） 作業実施体制

受託者は、本業務に係る要員の役割分担、責任分担、体制図等を実施計画書の一部として作成し、総合機構に報告するとともに、承認を得ること。また、受託者は、必要な要員の調達を遅滞なく実施し、要員を確定すること。

①本業務の実施に当たり、総合機構の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

②本業務に関連する資料等に総合機構の意図しない変更が行われるなどの不正が見つかった時（不正が行われていると疑わしい時も含む）に、追跡調査や立入検査等、総合機構と受託者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

③当該管理体制を確認する際の参照情報として、資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。具体的な情報提供内容については総合機構と協議の上、決定するものとする。

④受託者は、総合機構側やその他関連事業者を含めた全体の体制・役割を示した上で、プロジェクトの推進体制及び本件受託者に求める作業実施体制を総合機構と協議の上定めること。また、受託者の情報セキュリティ対策の管理体制については、作業実施体制とは別に作成すること。

⑤受託者は、インシデント発生時などの連絡体制図を総合機構と協議の上定めること。

（２）　作業要員に求める資格等の要件

受託者は、統括責任者（業務全体を統括する責任者)、監査人（業務完了まで継続して事業の実施を行える者であって、業務の実施にあたっての責任者)、監査補助者（監査人の配下に属する者であって、個々の業務を行う者)、アドバイザー（業務の品質を管理する者）からなる、監査チームを編成すること。

監査チームには、監査に関する知識・技能（監査理論全般、監査実務)、情報セキュリティ技術に関する知識・技能を有する専門家、すなわち「別紙２　監査人の資格要件」に記載された資格を有する専門家が 2 人以上含まれていること、並びに、監査の効率と品質の保持のため次のいずれかの実績（実務経験）を有する専門家が 1 人以上含まれていること。

a. 情報セキュリティ監査

b. 情報セキュリティに関するコンサルティング

監査チーム各者の氏名、所属部署及び連絡先とともに、各者の経歴、専門分野、各種保有資格等について、契約締結後 5 日以内に総合機構に提出し、了承を得ること。

本監査業務の開始後、適切な業務が実施できないと総合機構が判断した場合には、受託者は、監査チーム体制を変更すること。

なお、受託者は、体制を変更する際は、監査業務の遂行に影響がでないようにするとともに、変更に要した費用については、自らが負担すること。

（３）　作業方法

①　実施計画書

契約締結後、実施計画書（6. 納入成果物及び納入期日（１）納入成果物 ① 実施計画書　参照）を提示し、作業体制や役割分担について総合機構に対して報告し、承認を得て業務を進めること。また、契約締結以降に変更が発生した場合には、そのつど速やかに変更後の実施計画書を提出すること。

② 会議について

月次会議を開催し、総合機構に対し、進捗状況や障害、課題の状況等の報告を行うとともに、必要に応じて状況を説明するための資料等の作成及び会議での説明を行うこと。

業務の進め方について改善事項がある場合は月次会議の場で総合機構に提案し、総合機構の了承を得た上で変更する事とする。

本件の受託者が出席する会議においては、会議が開催される都度、本件の受託者が議事録の作成を行い、全出席者に内容の確認行った上で、3 営業日以内に総合機構に議事録を提出すること。

（４）　作業の管理に関する要領

総合機構が管理するエリアからの情報の持ち出しは原則許可しない。持ち出しが必要な場合は事前に総合機構に対し、持ち出し目的、対象情報の範囲、情報利用端末、情

報の利用者等に関し申請を行うこと。また受託者は、持ち出した情報を台帳等により管理すること。さらに受託者は、持ち出した情報は使用後に確実に消去し、そのエビデンスを提出すること。

（５） 作業場所

総合機構にて作業を実施する必要がある場合、総合機構の承認した総合機構内所定の場所で作業すること。総合機構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。

ただし、問合わせ対応業務等総合機構内での作業を必ずしも必要としない業務を実施する場所は、総合機構の承認した、受託者の用意した施設内（日本国内に限る。）とする。必要に応じて総合機構担当者は現地確認を実施できることとする。

作業場所やその他必要となる環境については、受託者の責任において確保すること。またこれらの環境に対しても十分な情報セキュリティ対策を実施すること。

８ 作業の実施に当たっての遵守事項

（１） 基本事項

受託者は、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、総合機構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 受託者は、本業務の履行に際し、総合機構からの質問、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 総合機構が依頼する技術的支援に対する回答、助言を行うこと。

（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 受託者は、受注業務の実施の過程で総合機構が開示した情報（公知の情報を除く。以下同じ。）、他の受託者が提示した情報及び受託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 受託者は、本受注業務を実施するにあたり、総合機構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、速やかに総合機構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、受託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総合機構に提出すること。

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。「秘密保持等に関する誓約書」には、受託業務に従事する者を列挙し、従事者以外に秘密情報を閲覧してはならない。また、本受託業務実施中に従事者に変更が生じた場合は、速やかに「秘密保持契約等に関する誓約書」を訂正し、提出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 受託者は、民法、刑法、著作権法、不正アクセス行為の禁止等に関する法律、行政機関の保有する個人情報の保護に関する法律等の関連法規及び労働関係法令を遵守すること。

② 受託者は、次の文書に記載された事項を遵守すること。遵守すべき文書が変更された場合は変更後の文書を遵守すること。

ア 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
イ 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
ウ 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
エ 政府機関等のサイバーセキュリティ対策のための統一規範（最新版）
オ 政府機関等のサイバーセキュリティ対策の運用等に関する指針（最新版）
カ 政府機関等のサイバーセキュリティ対策のための統一基準（最新版）

なお、「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」は非公開であるが、「政府機関等のサイバーセキュリティ対策のための統一基準（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。「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」の開示については、入札に参加した事業者のうち、事業者が総合機構に「秘密保持等に関する誓約書」を提出した際に開示する。

③ 総合機構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

④　受託者は、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、総合機構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、事前に総合機構に提出すること。また、そのような事態が発生した場合は、総合機構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。

9　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、受託者が本件のシステム開発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、総合機構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総合機構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、受託者は著作者人格権（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、受託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、受託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。この場合は事前に総合機構に報告し、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総合機構の責めに帰す場合を除き、受託者の責任、負担において一切を処理すること。この場合、総合機構は係る紛争の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者にゆだねる等の協力措置を講ずる。なお、受託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、受託者の責任において著作者等の承認を得るものとし、総合機構に提出する際は、その旨併せて報告するものとする。

（２）　検収

納入成果物については、適宜、総合機構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、「６．（１）納入成果物」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、総合機構が確認し、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 レビューの結果、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、受託者は直ちに引き取り、必要な修復を行った後、総合機構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 総合機構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、担当者の指示に従い対応を行うこと。

１０　　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 経済産業省が定める、情報セキュリティサービスに関する審査登録機関の審査をうけ、本調達時点情報セキュリティサービス基準適合サービスリストに登録されている者であること。

② 国、独立行政法人、政府系特殊法人、都道府県等地方自治体、自社以外の企業、海外の医薬品・医療機器の規制当局において、情報システム監査業務を過去 3 年以内に請け負った実績を有し、かつ、本業務を履行できること。また、これら実績を証明できること。

③ 信頼性を確保するため、1000 人以上の標的型メール訓練を 5 組織以上で行った実績があること。

④ 情報セキュリティを確保する観点から、（財）日本情報経済社会推進協会または海外の認定機関により認定された審査機関による情報セキュリティマネジメントシステム（ISMS）の認証を受けていること。

⑤ 応札業者の社内に情報セキュリティ対策等に関する役務提供を専門とする部門を有していること。

⑥ 取り扱う情報がセキュリティに関するものとなるため、応札者の事務所では個人ごとに配布された ID カード等による入退室管理が行われていること。

⑦ 総合機構にて現行関連システムの設計書等を閲覧し、内容を十分理解できる能力と意思を有していること。

⑧ 応札時には、機能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、応札後に総合機構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

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 総合機構の 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 本業務の調達仕様書の作成に直接関与した事業者等

③　①～②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　①～②と同一の親会社を持つ事業者

⑥　①～②から委託を請ける等緊密な利害関係を有する事業者

１１　情報セキュリティ対策の実施

受託者は、以下を含む情報セキュリティ対策を実施すること。また、その実施内容及び管理体制についてまとめた情報セキュリティ管理計画書を実施計画書に添付して提出すること。

ア　総合機構から提供する情報の目的外利用を禁止すること。

イ　本業務の実施に当たり、受託者又はその従業員、本調達の役務内容の一部を再委託する先、若しくはその他の者による意図せざる変更が加えられないための管理体制が整備されていること。

ウ　受託者の資本関係・役員等の情報、本業務の実施場所、本業務従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供を行うこと。具体的な情報提供内容については総合機構と協議の上、決定するものとする。

エ　情報セキュリティインシデントへの対処方法が確立されていること。

オ　情報セキュリティ対策その他の契約の履行状況を定期的に確認し、総合機構へ報告すること。

カ　情報セキュリティ対策の履行が不十分である場合、速やかに改善策を提出し、総合機構の承認を受けた上で実施すること。

キ　総合機構が求めた場合に、速やかに総合機構が実施する情報セキュリティ監査を受入れること。

ク　本調達の役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるように情報セキュリティ管理計画書に記載された措置の実施を担保すること。

ケ　総合機構から要保護情報を受領する場合は、情報セキュリティに配慮した受領及び管理方法にて行うこと。

コ　総合機構から受領した要保護情報が不要になった場合は、これを確実に返却、又は抹消し、書面にて報告すること。

サ　本業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合は、速やかに総合機構に報告すること。

１２　再委託に関する事項

①　受託者は、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　受託者は、再委託する場合、事前に再委託する業務、再委託先等を総合機構に申請し、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、受託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総合機構に提出すること。受託者は、機密保持、知的財産権等に関して本仕様書が定める受託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、総合機構に報告し、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託者が負うこと。

③ 再委託先が「１０（２）入札制限」の要件を満たすこと。

④ 受託者の責任において、サプライチェーンリスクの発生を未然に防止するための体制を確立すること。

⑤ 再委託先において、本調達仕様書に定める事項に関する義務違反、義務を怠った場合には、受託者が一切の責任を負うとともに、総合機構は当該再委託先への再委託の中止を請求することができる。

⑥ 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。

- 再委託先が「１１情報セキュリティ対策の実施」の要件を満たすこと
- 総合機構から提供する情報の目的外利用を禁止すること。
- 受託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総合機構に報告すること。
- 受託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、総合機構に報告すること。
- 受託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、総合機構から求めがあった場合には情報提供を行うこと。
- 受託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、総合機構に報告すること。
- 受託者は、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、総合機構へ報告すること。
- 受託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、総合機構へ報告すること。
- 受託者自らが情報セキュリティ監査を実施する場合には、再委託先も対象とするものとする。
- 受託者は、再委託先が自ら実施した外部監査についても総合機構へ報告すること。
- 受託者は、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。

⑦ 上記①～⑥について再委託先が、さらに再委託を行う場合も同様とする。

１３　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

① 本業務を遂行するために総合機構に対する資料要求、要望等がある場合は、原則文書にて行うこと。
② 本業務における提出物等の公表にあたっては、事業者名も併せて公表することとする。応札にあたっては、最低限、以下の書類の内容を熟知しておくこととする。

A) 総合機構パンフレット
B) 独立行政法人医薬品医療機器総合機構法
C) 独立行政法人医薬品医療機器総合機構平成 31～令和 4 事業年度業務報告
D) 独立行政法人医薬品医療機器総合機構業務システム・最適化計画
E) 独立行政法人医薬品医療機器総合機構職員就業規則、同嘱託等就業規則、同事務補助員就業規則、同継続雇用職員就業規則、同任期付職員就業規則、同特任職員就業規則

※上記 A)から E)については総合機構ホームページよりダウンロードすること。

③ 総合機構全体管理組織（PMO）が担当課に対して指導、助言等を行った場合には、受託者もその方針に従うこと。
④ 総合機構全体管理組織（PMO）が担当課に対して指導、助言等を行った場合には、受託者もその方針に従うこと。

（３） 各業者との役割分担

本業務を複数業者が連携（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。

１４ 応札希望者が閲覧できる資料一覧

令和 4 年度情報システム監査業務に係る関連資料

✧ 閲覧資料 1 令和４年度情報システム監査結果報告書一式

✧ 閲覧資料 2 Web アプリケーション脆弱性診断結果報告書（令和５年３月）一式

資料閲覧については別紙３を参照すること。

１５ 窓口連絡先

独立行政法人 医薬品医療機器総合機構 監査室

鳥海 兼市、安達　義晃
電話：03-3506-9488
E-mail: toriumi-kenichi●pmda.go.jp、adachi-yoshiaki●pmda.go.jp
迷惑メール防止対策をしているため●を半角のアットマークに置き換えること。

【別紙 1】　監査対象となる総合機構の情報システム

ｼｽﾃﾑｺｰﾄﾞ システム名	システム概要	サーバー 設置場所	ｲﾝﾀｰﾈｯﾄ 有無
SA-001 共用ＬＡＮシステム	総合機構の共通的基盤システム。メールサーバーやグループウェアサーバー等で構成され、全職員に PC を貸与している。	ＤＣ	○
SO-001 人事給与システム	職員の役職・所属情報の管理及び給与や各種手当等の計算に関する業務に使用	ＤＣ	×
ZA-001 会計システム	収支、出納管理、物品購入請求書、旅費請求書等作成支援、予算支出簿等各種帳簿作成、帳票出力等	ＤＣ	×
KI-003 PMDA ウェブサイト	PMDA ウェブサイト（www.pmda.go.jp）の運用支援、及び保守業務。コンテンツ管理システム（ALAYA）の利用に関するヘルプデスク業務、導入済みの各種ミドルウェアの保守、クラウドにてサイト構築しているサーバー機器群の保守管理業務。	Cloud	○
HIAN-001 拠出金徴収管理システム	副作用拠出金、感染拠出金及び安全対策等拠出金の徴収業務に係る申告書類の送付、収納、債権管理等の業務支援を行うもの。なお、債権発生決議書の作成については、会計システムを利用している。	サーバー室	×
HI-001 救済給付業務システム	副作用等被害の救済に係る給付金について、請求受理から支払までの情報の管理等業務を支援する。	サーバー室	×
SI-004 医療機器 WEB 申請プラットホーム	総合機構における医療機器の WEB 申請・受付等業務	ＤＣ	○
SI-006 医薬品等申請・審査等システム	改正薬事法に基づく医薬品、医薬部外品、化粧品及び医療機器の審査の迅速化等により、ドラッグ・ラグ、デバイス・ラグの解消等を目的とし、申請系・審査系・調査系の業務を統合したシステム	ＤＣ	×
SI-007 申請電子データシステム	新医療用医薬品承認申請において、申請者が申請等の予告、臨床試験データ・eCTD 等大容量データの転送、照会への回答をインターネット経由で可能とする Web システム	ＤＣ	○
AN-001 医薬品医療機器情報提供システム	添付文書・副作用情報・不具合情報等に係る諸情報を、ホームページを介して一般国民や医療関係者及び製薬会社・医療機器メーカーに提供を行う	ＤＣ	○
AN-006 医療情報データベース	申請に基づいて複数の協力医療機関から匿名化した医療情報を入手し統合解析を行う。	ＤＣ及び拠点	×
AN-008 医薬品副作用・安全対策支援統合システム	医薬品・医療機器等安全性情報報告制度に基づき、製造販売業者及び医療機関等から報告があった症例について、本システムを用いて入力・管理を行う。また、副作用報告の解析結果、データマイニング手法による統計学的評価、企業面談時の情報を統合し、安全対策業務の支援を行う。さらに、関係機関との情報共有を行っている。	ＤＣ	○

【別紙２】　監査人の資格要件

監査人は、監査に関する知識・技能（監査理論全般、監査実務)、情報セキュリティ技術に関する知識・技能を有すること。

その知識・技能に関する資格の例として、以下のような資格を有していることが必要となる。

- ✧ 公認会計士
- ✧ 公認内部監査人(CIA):内部監査人協会(The Institute of Internal Auditors,Inc.(IIA))が認定する内部監査人の資格。
- ✧ 公認システム監査人：特定非営利活動法人日本システム監査人協会が認定するシステム監査人の資格
- ✧ システム監査技術者:独立行政法人情報処理推進機構により行われている、システム監査技術を有していることを認定するための国家試験
- ✧ 公認情報システム監査人(CISA)：ISACA（Information Systems Audit and Control Association 情報システムコントロール協会）により認定されるシステム監査人の資格。
- ✧ ISMS 主任審査員
- ✧ ISMS 審査員
- ✧ 公認情報セキュリティ監査人(CAIS)：特定非営利活動法人日本セキュリティ監査協会により認定される情報セキュリティ監査人の資格
- ✧ 情報セキュリティスペシャリスト：独立行政法人情報処理推進機構により行われている、情報セキュリティ機能の企画、開発、運用などについての一定の専門的知識・能力を有していることを検定するための国家試験
- ✧ 公認情報セキュリティ管理者(CISM)：情報システムコントロール協会（Information Systems Audit and Control Association）により認定されるセキュリティ管理者としての専門的能力を有していることを証明する資格
- ✧ 公認情報システムセキュリティ専門家(CISSP)：International Information Systems Security Certification Consortium）により認定される情報セキュリティについての専門的能力を有していることを保証する資格
- ✧ 公認システムセキュリティ熟練者(SSCP)：International Information Systems Security Certification Consortium）により認定される情報セキュリティについての専門的能力を有していることを保証する資格
- ✧ 情報処理安全確保支援士:独立行政法人情報処理推進機構により行われている、情報セキュリティに関する知識・技能を有していることを認定するための国家試験

【別紙３】資料閲覧について

1. 閲覧対象物

令和５年度情報システム監査業務に係る関連資料

2. 閲覧場所

独立行政法人 医薬品医療機器総合機構内

3. 閲覧期間

令和６年１月２２日（月）から令和６年１月２９日（月）までの平日（11:00～16:00）

4. 閲覧上の注意

(1) 閲覧に際しては、5.閲覧連絡先に連絡し、社名・連絡先・人数等を登録すること。なお、3.閲覧期間の後半は閲覧場所を確保できなくなる場合があるので、早めに閲覧希望日時を登録すること。

(2) 閲覧前に総合機構の提示する様式にて秘密保持誓約書を作成し、総合機構に提出すること。

(3) 一回あたりの閲覧時間は1時間程度とする。閲覧回数は原則制限しない。

(4) 閲覧時に個々の内容に関する質問に応じることはできない。

5. 閲覧連絡先

独立行政法人　医薬品医療機器総合機構　監査室
鳥海 兼市、安達　義晃
電話：03-3506-9488
E-mail: toriumi-kenichi●pmda.go.jp、adachi-yoshiaki●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。