令和８年度脆弱性診断及び
ペネトレーションテスト業務

仕様書

日本年金機構情報管理対策室

令和８年９月

本紙余白

目　次

１　委託業務の概要

（１）目的

平成２７年１２月に策定された日本年金機構（以下「機構」という。）の業務改善計画において、独立した外部の専門家による脆弱性診断により情報セキュリティの問題点を把握することとしている。

このため、以下の診断対象システムに、安全性が維持されていることを確認することを目的とした脆弱性診断及びペネトレーションテスト業務を調達するものである。

①　脆弱性診断対象システム

・インターネット環境
・日本年金機構ホームページ
・オンライン事業所年金情報サービス
・電子入札システム
・チャットボット

②　ペネトレーションテスト対象システム

脆弱性診断の結果等を踏まえ、脆弱性診断対象のシステムから２システムを選定

（２）定義

本仕様書で用いる用語について、「表１．（２）．１用語の定義」に示す。

表１．（２）．１用語の定義

項番	用語	説明
1	本部	日本年金機構の本部。
2	稼働維持環境	本番運用を行う上で必要な維持作業を実施する環境及び機器。 各種セキュリティパッチ、ウイルス定義ファイル等の配布、アプリケーションプログラムの保守・改修及び各種環境のバージョンアップ等の本番環境へのリリースに際し、事前の動作検証を実施する環境及び機器。
3	統合ネットワーク	厚生労働省内の各組織が共通して利用する回線等のネットワーク設備。

２　システム概要

（１）インターネット環境

機構職員が業務を実施する上で必要な情報をインターネットより取得するための環境。

（２）日本年金機構ホームページ

国民向けのサービスとして、年金に関する申請・手続き、年金に関する情報をはじめ、機構に関する情報等について、幅広くご案内しているインターネットサービス。

AWS を利用したクラウド環境上に構築されている。

（３）オンライン事業所年金情報サービス

事業所向けのサービスとして、通知書等のデータを受け取れるサービス。

（４）電子入札システム

入札情報の入手や、審査書類の提出から開札結果確認までの一連の入札手続きをインターネット上で実施可能なシステム。

AWS を利用したクラウド環境上に構築されている。

（５）チャットボット

お客様からの一般的な問い合わせに対して、対話形式により自動で 24 時間回答するシステム。

３　作業内容・納入成果物等

（１）作業内容

本調達における作業は、以下のとおりである。

①　脆弱性診断

ア　実施計画作成、対象であるシステムに関する情報提供依頼及びその対応

イ　診断対象システムとの事前打ち合わせ・調整対応

ウ　診断作業

エ　診断結果報告書

オ　エや成果物についての機構からの問合せに対する対応

②　ペネトレーションテスト

ア　実施計画作成、対象であるシステムに関する情報提供依頼及びその対応

イ　攻撃シナリオ作成

ウ　診断対象システムとの事前打ち合わせ・調整対応

エ　ペネトレーションテスト実施

オ　診断結果報告書

カ　オや成果物についての機構からの問合せに対する対応

役務内容の詳細は、「９　作業要件」に記述されている項目とする。

また、作業スケジュールは、「表３．（１）．１ 主要マイルストン一覧」のとおりである。

表３．（１）．１ 主要マイルストン一覧

項番	主要マイルストン	スケジュール
1	契約締結	令和 8 年 10 月 9 日
2	脆弱性診断及びペネトレーションテスト役務開始	令和 8 年 10 月 13 日
3	診断結果報告書	令和 9 年 3 月 12 日
4	契約終了	令和 9 年 3 月 31 日

（２）作業場所等

本業務の作業場所は、受託者の事業所内又は事業所と別に受託者が用意する場所（いずれも日本国内に限る）及び機構本部内とする。機構本部内での作業はリモートアクセス環境でも実施可能とする。

ただし、診断作業等のため機構が必要と判断した場合は、必要と判断される範囲においてオンサイト等機構の指示する場所で作業すること。

機構本部内での作業については、所定の手続に従って事前に承諾を得ること。

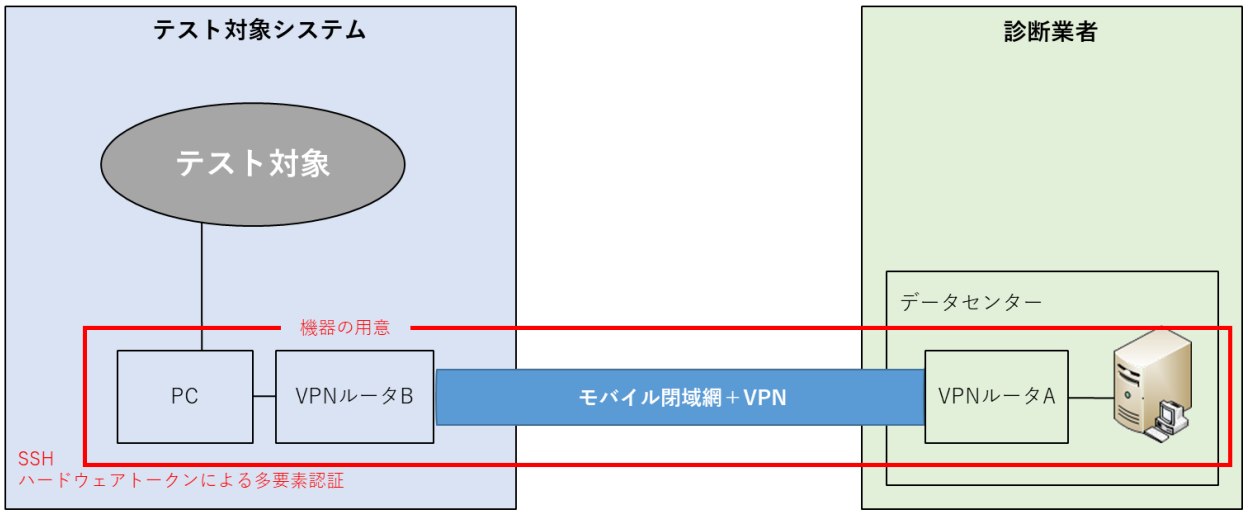
情報システムへのリモートアクセス環境を構築する場合は VPN 回線を整備するなどして、通信経路及びアクセス先の情報システムのセキュリティを確保すること。その VPN 回線等のアクセス認証には多要素認証等※の措置を講ずること。

なお、VPN 回線はモバイル閉域網に整備し、インターネットを経由しないセキュアな閉域網とすること。（日本年金機構ホームページなどインターネットからリモート診断可能なシステムは除く。）

また、本業務で必要となる機材類及び媒体等について、受託者の負担と責任において準備し、適切な管理を行うこと。

※当該情報システムの主体認証機能の設定において、知識（パスワード等、業務従事者本人のみが知り得る情報）による認証、所有（電子証明書を格納する IC カード、ワンタイムパスワード生成器、業務従事者本人のみが所有する機器等）による認証、生体（指紋や静脈等、本人の生体的な特徴）などの主体認証方式を２つ以上の組み合わせた多要素主体認証方式を用いること。

リモート接続イメージ



・VPNルータ B から通信できるのは、VPN ルータ A のみ
・VPNルータ A には、事業所が用意した端末からしかアクセスできないようにすること。

（３）報告会

診断等により発見された個々の脆弱性に対し、詳細な分析と対策方法を明らかにした診断結果報告書を作成し、診断又は分析を実施した者を含めて報告会を行うものとする。

予定している報告会については、「表３．（３）．１ 報告会」のとおりとする。

なお、報告会は機構が指定した日時、機構が指定した機構内の場所で実施するものとする。

また、緊急性の高い脆弱性が発見された場合は、報告会を待たず、速やかに報告すること。

表３．（３）．１ 報告会

項番	報告会名称	内容等	実施タイミング	開催頻度

1	担当部署向け報告会	診断結果報告書について、担当部署向けの報告会を実施する。	各システムの診断報告書作成時	6回
2	経営層向け報告会	診断結果報告書について、経営層向けの報告会を実施する。	担当部署向け報告会の完了後に、脆弱性診断として1回、ペネトレーションテストとして1回	2回

（４）成果物の範囲、納品期日等

本調達における成果物の内容及び納品期日は、「表３．（４）．１ 成果物及び納品期日一覧表」のとおりである。

各成果物に係るレビューや会議等で使用した説明資料や関連資料などについても、併せて納品すること。また、「表３．（４）．１ 成果物及び納品期日一覧表」に示した成果物以外に必要あるいは有益と考える成果物があれば、積極的に提案し、納品するとともに、納品後の成果物に対する照会に対応すること。

なお、各成果物の納品期日については、双方協議の上、プロジェクトの進捗に影響を及ぼさないことを機構が認めた場合に限り、変更することができることとする。

表３．（４）．１ 成果物及び納品期日一覧表

項番	成果物	記載内容等	納品期日
1	業務実施計画書	本調達に係る業務の全体計画書であり、「９ 作業要件」に示した項目に係る具体的な診断内容、方法（使用する機材、脆弱性診断のテスト仕様書のサンプル（実施される観点や想定される脆弱性等を一覧化したもの）やツール等の内容を含む。）、機構への依頼事項及び実施スケジュールを記入するものとする。	契約締結後 8 営業日まで 見直し・修正時は随時

2	診断結果報告書	診断結果報告書は、以下の事項を記述することとする。なお、脆弱性診断結果の記述については、各情報システム別に「９作業要件」の表９.（２）.①.１、表９.（２）.①.２及び表９.（３）.①のとおりに整理することとし、ペネトレーションテストの結果の記述については、シナリオ別に整理することとする。 ・診断結果全体の総評 ・情報システムごとの評価 ・検出された脆弱性とその危険度を示す以下の２つの観点からのリスクレベル ☞診断対象システムの環境における当該脆弱性のリスクレベル ☞参考として、共通脆弱性評価システム(CVSSv3)における基本評価基準によるリスクレベル ・検出された脆弱性を用いた攻撃シナリオと機構の情報システム環境を考慮した攻撃の実現性 ・検出された脆弱性の解説と影響 ・検出された脆弱性の対策方法及びパッチ適用以外による改善案 ・脆弱性を検出した画面、パラメータ名 ・検査の実施範囲（入力文字列の例、レスポンスの例等の脆弱性を検出した際の情報検査対象サイトにおける検査範囲と範囲外を明示すること） ・検出した脆弱性の存在を確認できる証跡（検出時の画面イメージ等）及び脆弱性の検出を再現できる手順 ・実施時期、実施体制、前提条件、診断方法、使用した診断ツール、診断環境、診断対象（診断範囲）、用語説明及び問合せ先 ・上記の任意様式の他に、様式１検出事項一覧へ検出事項（対象システム、対象 IP アドレス、検出事項、内容、CVSS 値）を記載して提出すること。	令和９年３月12日 見直し・修正時は随時
3	フォローアップ関連資料	報告会、診断結果報告書等に関する機構からの問合せ対応について整理、記述するものとする。	令和９年３月末日まで 見直し・修正時は随時

（５）納品方法

① 受託者は、指定のドキュメントを日本語で作成し、電子ファイルを保存した記録媒体（媒体種類は機構の指定による。）により納品すること。ただし、電子ファイルにて納品できないものについては、機構は協議に応じるものとする。

② 電子ファイルは、原則として、「Microsoft Word 2024」、「Microsoft Excel 2024」、又は、「Microsoft PowerPoint 2024」（以下「Word 等」という。）のうちいずれかで編集が可能な形式及び PDF 形式とすること。機構が他の形式による提出を求める場合は、協議の上、これに応じること。

③ ②にいう「Word 等で編集が可能な形式」につき、次の点に留意すること。

ア 特殊なソフトウェアを用いて作成した文書等であって、Word 等によって閲覧及び編集ができないものがある場合は、機構は納品の形式について協議に応じるものとする。

イ Word 等に他のソフトウェアで作成した図表等を図として貼付する場合は、編集可能な図表も併せて納品すること。

④ PDF 形式は、「表３．（４）．１ 成果物及び納品期日一覧表」に示す項番ごとに一括にて閲覧・印刷が可能となるように成果物を結合したものとすること。

⑤ 電子ファイルを保存した記録媒体については、事前に最新のウイルスパターンによる検疫を実施し、パスワードによる暗号化を実施した上で正副各１式を納品すること。また、当該記録媒体に格納された成果物の一覧を、紙媒体で添付すること。

⑥ 納入したドキュメント（既存ドキュメントも含む）に修正等があった場合には、更新履歴と修正後の全編を速やかに機構に提出すること。

⑦ 「表３．（４）．１ 成果物及び納品期日一覧表」に則って成果物を提出すること。その際、機構の指示により、別途品質の保証状況を確認できる資料を作成し、成果物と併せて提出すること。

また、「表３．（４）．１ 成果物及び納品期日一覧表」に記載した成果物については、成果物一覧表を作成し、成果物と併せて提出すること。

⑧ 「表３．（４）．１ 成果物及び納品期日一覧表」による以外にも、必要に応じて成果物の提出を求める場合があるので、作成資料は常に管理し、最新状態に保っておくこと。

（６）納品場所

６に示す調達担当部署とする。

（７）検査

① 成果物の検査は、「表３．（４）．１ 成果物及び納品期日一覧表」に示す納品期日までに納品された後に行う。

② 検査の結果、成果物の全部又は一部に不合格品が生じた場合には、受託者は直ちに引き取り、必要な修復を行った後、指定した日時までに修正が反映されたすべての成果物を納品すること。

③ 本調達の役務は、受託者が納入する完了報告書に対する機構の検収、承認をもって完了するものとする。

４ 関連業者

本業務の実施にあたり、関連する業者を「表４．１ 関連業者一覧」に示す。

表４．１ 関連業者一覧

項番	関連業者	説明

1	ハードウェア保守業者	診断対象システムに係るハードウェアの保守業者。診断対象システムで使用している基盤環境に係る調整も行う。
2	アプリケーションプログラム保守業者	診断対象システムのアプリケーションプログラムの保守業者。診断対象システムで使用しているアプリケーションプログラムに係る調整も行う。
3	運用管理業者	診断対象システムの運用管理業務を行う業者。システムのリソース使用状況監視、障害監視等も行う。
4	IPS 監視業者	侵入検知・防御システム（IPS）を使用して診断対象システムへの不正アクセスの監視及び防御を行う業者。侵入検知・防御システム（IPS）に係る調整も行う。
5	共通基盤保守業者	機構内を接続するネットワークの運用・保守を行う業者。
6	インターネット回線供給業者	診断対象システムとインターネットを接続する回線及び接続サービスを提供する業者。
7	統合ネットワーク保守業者	統合ネットワークの運用・保守を行う業者。拠点間を繋ぐネットワークに係る調整も行う。

５　契約期間、履行期限

契約締結日から令和 9 年 3 月 31 日までを契約期間とする。

受託者は、本業務開始前に、受託者の負担により本業務の準備作業を済ませておくこと。

６　調達担当部署

東京都杉並区高井戸西 3 丁目 5 番 24 号

日本年金機構 情報管理対策室 情報リスク分析グループ

担当者：渡邊、三野島

電話： 03（5344）1100（内線：6404）

７　情報セキュリティ要件

（１）基本事項

受託者は、以下の情報セキュリティに関する規程等を遵守した上で、市場で認知されているセキュリティ対策全般を考慮して、情報セキュリティの向上に資する施策を講じること。

① 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

② 日本年金機構個人情報保護管理規程

③ 日本年金機構情報セキュリティポリシー

④ 情報セキュリティインシデント対処手順書

上記の③及び④は非公表であるが、③は①に準拠しているため、必要に応じて参照すること。

なお、上記③及び④は、契約締結後、受託者が機構の担当職員に守秘義務の誓約書を提出した際に開示する。

上記の②～④について改正が行われた場合は、改正点に関する対応についての協議に応じること。

また、「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」及び「『高度標的型攻撃』対策に向けたシステム設計ガイド」を参照の上、必要に応じてその内容を取り込むこと。

（２）遵守事項

① 受託者は、本調達に係る業務を実施するに当たり、関連する法規（民法、刑法、日本年金機構法、著作権法、不正アクセス行為の禁止等に関する法律、独立行政法人等の保有する個人情報の保護に関する法律等）を遵守すること。

② 機構へ提示する電子ファイルは事前にウィ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 受託者は、本業務の実施のために機構から提供する情報その他該当業務の実施において知り得た情報（本業務の診断結果及び診断結果報告書等の診断により知り得た情報など）については、その秘密を保持し、漏えい・紛失・盗難等が起こらぬように必要な処置を講じ、当該業務の目的以外に利用しないこと。

④ 受託者は、本業務に必要な範囲を超えて、システム内の情報の閲覧・取得や調査対象外のシステムへの侵入等を行わないこと。また、本業務において機構から貸与された診断対象システム等のアカウントが目的外に使用されないよう適切に管理するとともに、本業務におけるシステムの操作ログや作業履歴等を記録すること。

なお、記録すべき具体的なログ・情報については機構と協議し、機構が要求した場合は速やかに提出できるようにすること。

⑤ 万一、情報の漏えい、改ざん、消失等が発生した場合、「７（１）基本事項」における④の手順書に基づき機構へ報告し迅速に対応すること。

⑥ 受託者は、本部及びその他機構の施設で作業するにあたり、常に身分証明書を他者に見えやすい位置に着用すること。

⑦ 業務情報へのアクセスが許可される主体が、当該業務情報を扱うことが認められる正当な業務従事者のみに確実に制限されるように、アクセス制御機能を設けること。

⑧ 診断に使用する機器（端末等）には、最新のソフトウェアアップデート及びセキュリティパッチを適用すること。

⑨ 作業用端末は診断中インターネットに接続しない。（日本年金機構ホームページなどインターネットからリモート診断可能なシステムは除く。）

⑩ 受託者は、本業務で取得又は作成した情報をクラウドサービスに保存する場合、国内リージョンを利用し、保存先及び実施するセキュリティ対策について事前に機構の承認を得ること。

（３）情報セキュリティ対策

① 情報セキュリティが侵害された場合の対策

本調達に係る業務の遂行において情報セキュリティが侵害され又はその恐れがある場合には、速やかに機構に報告すること。これに該当する場合には以下の事象を含む。

ア 受託者に提供し、又は受託者によるアクセスを認める機構の情報の外部への漏えい及び目的外利用

イ 受託者による機構のその他の情報へのアクセス

ウ　各システムへの不正アクセス、又は不正プログラムの感染による情報漏えい、サービス停止、情報の改ざん

エ　委託者が作成した情報の漏えい及び目的外利用

② 情報セキュリティ対策の履行状況の報告

本調達に係る業務の遂行におけるセキュリティ対策の履行状況について、機構が報告を求めた場合には速やかに提出すること。

③ 情報セキュリティ監査への対応

本契約期間中において、機構が第三者機関等による情報セキュリティ監査を受ける場合には、業務実施計画書、診断内容及び診断結果に関する監査機関への説明について支援すること。情報セキュリティ監査の結果、対策が必要な場合は、機構と協議を行い、合意した対策を実施すること。

④ 情報セキュリティ対策の履行が不十分な場合の対処

本調達に係る業務の遂行において、受託者における情報セキュリティ対策の履行が不十分であると認められる場合には、受託者は、機構の求めに応じ、機構と協議を行い、合意した対応を実施すること。

⑤ 管理体制の整備

委託事業の実施に当たり、委託先企業又はその従業員、再委託先、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を整備すること。

また、本調達の履行期間において、不正が見つかったときに、追跡調査や立入検査等により原因を調査・排除できる体制を整備すること。

⑥ 受託者に関する情報提供

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）・実績に関する情報提供を行うこと。

８　情報システム稼働環境

各情報システムに関する閲覧資料は「別紙１　閲覧資料一覧」に記載したとおり。

資料閲覧を希望する場合は「１１（９）資料等の閲覧」により手続きを行うこと。

９　作業要件

（１）共通事項

① 受託期間中、確実に診断を行える体制を整えること。

② 業務実施計画の策定に当たっては、システム（サービス）停止の回避等、業務に支障をきたさないよう十分に配慮すること。

なお、診断実施中に機構のシステムの停止・異常動作の発生を認識した場合は、診断に起因するか否かを問わず、速やかに機構に連絡すること。

③ 原則として、運用中システムを停止することなく診断を実施することを想定しているが、システムや回線に影響を与える可能性がある診断項目については、計画停止期間に実施する、あるいは稼働維持環境を使用するなど、機構と診断方法や診断日時について調整すること。

④ 脆弱性診断及びペネトレーションテスト業務の実施においては、運用管理業者及びその他関連する業者と協力し、システムの安定稼働に努めること。

なお、本調達の契約期間中に「４　関連業者」に示す業者に変更が発生する可能性にも留意すること。

⑤　使用する診断ツールは最新の攻撃手法を反映した実績ある商用ツールを活用すること。フリーツールや自社製ツールのみによる診断は行わないこと。診断に用いる診断ツールの例を表９.（１）.⑤に記載する。なお、診断ツールによる機械的診断のみでなく、手作業による疑似攻撃や侵入検査等を実施すること。

なお、診断ツールによる診断結果については、手作業による検証等により、偽陽性（False Positive）を排除すること。

表９.（１）.⑤ 脆弱性診断ツール（例）

項番	脆弱性診断	診断ツール
1	Web アプリケーション診断	・Vulnerability Explorer(VEX) ・HCL AppScan ・Burp Suite Professional
2	インフラ診断	・QualysGuard ・Tripwire IP360 ・Nessus ・Metasploit ・OpenVAS

⑥　機構本部内での診断について、診断用機器を持ち込む場合は事前に機構の承諾を得ること。

⑦　診断の実施時期については、令和９年３月１２日までの実施を予定している。
また、診断を実施する時間帯については、原則平日の１０：００～１７：００とする。

⑧　診断範囲と診断拠点を表９.（１）.２に示す。

表９.（１）.２　診断範囲

項番	情報システム	脆弱性診断		ペネトレーションテスト	診断拠点
		Web アプリ診断	インフラ診断		
1	インターネット環境	－	○	※対象システムから２システムをテスト予定	A
2	日本年金機構ホームページ	○	○		B
3	オンライン事業所年金情報サービス	○	○		A
4	電子入札システム	○	○		B
5	チャットボット	○	－		B

⑨　診断拠点（Ａ）は、東京都内に存在する。

⑩　診断拠点（Ｂ）は、インターネット経由で診断する。

⑪　脆弱性診断及びペネトレーションテストの対象となるシステムは、本業務開始までに他のシステムと変更を行う場合がある。

なお、その場合においては表９．（２）.②に記載の診断対象画面数、表９．（３）.②に記載の診断対象 IP アドレス数の総数には変更がないよう調整を行う。

（２）Web アプリケーションの脆弱性診断の作業要件

①　脆弱性診断の観点

Web アプリケーションの脆弱性診断の指標として、デジタル庁が示している「政府情報システムにおける脆弱性診断導入ガイドライン」に準拠するものとする。

診断事項については表９．（２）.①.１に、「政府情報システムにおける脆弱性診断導入ガイドライン」に記載以外の診断事項については表９．（２）．①．２に示す。

表９．（２）.①.１　診断事項（Web アプリケーション）

項番	脆弱性の種類	診断内容
1	SQL インジェクション	SQL コマンドによる不正なデータベース操作等の脆弱性の有無を診断
2	OS コマンド・インジェクション	OS コマンドを実行する不正な文字列入力に係る脆弱性の有無を診断
3	ディレクトリ・トラバーサル	リクエストのパスに不正な内容を指定することで、公開していないディレクトリにアクセスできる等の脆弱性の有無の診断
4	セッション管理の不備	セッション ID の保持方法・有効期限、セッション破棄、Cookie の扱い等セッション管理に係る脆弱性の有無を診断
5	クロスサイト・スクリプティング（XSS）	不正なスクリプト文字列や HTML タグなどが埋め込まれ、利用者が意図しないアクセスをしてしまう等の脆弱性の有無を診断
6	クロスサイト・リクエスト・フォージェリ(CSRF)	外部サイトを経由した悪意のあるリクエストが、利用者が予期せずに実行される等の脆弱性の有無を診断
7	HTTP ヘッダ・インジェクション（CRLF インジェクション）	不正な HTTP レスポンスヘッダにより、意図しないレスポンスが実行される等の脆弱性の有無を診断
8	メールヘッダインジェクション	不正なメールヘッダにより、意図しないメールアドレスへ送信される等の脆弱性の有無を診断
9	クリックジャッキング	細工された外部サイトにより、意図しない機能を実行させられる等の脆弱性の有無を診断
10	バッファオーバーフロー	プログラムが確保したメモリ領域を超えて領域外のメモリを上書きされ、意図しないコードを実行してしまう等の脆弱性の有無を診断 ※稼働維持環境で実施

11	アクセス制御（認証制御）と認可処理の不備	不適切な設計によるアクセス制御や認証機能により、ほかの人になりすましてアクセスしてしまう、利用者本人以外のデータを変更できてしまう等の脆弱性の有無を診断
12	eval インジェクション	文字列をプログラムとして実行する機能を持つ言語を利用して、任意のプログラムが実行される等の脆弱性の有無を診断
13	レースコンディション	ウェブアプリケーションの機能を複数の利用者が全く同時に利用したときに、利用者の処理を取り違える脆弱性の有無を診断
14	ファイルアップロードに関する不備	展開すると数 GB になる圧縮ファイル（ZIP BOMB）の有無などの圧縮ファイルの不備等の脆弱性の有無を診断
15	オープンリダイレクト	適切な検証がされていないリダイレクトが実行されてしまう脆弱性の有無を診断
16	安全でないデシリアライゼーション	外部から与えられるデータをデシリアライズする際に意図しないオブジェクトを操作され不正な動作を引き起こす脆弱性の有無を診断
17	サーバサイドリクエストフォージェリ（SSRF）	インターネット等の外部に公開しているウェブアプリケーションから、本来は外部から到達できない領域にある任意の送信先に対して、リクエストを送ることが可能な脆弱性の有無を診断
18	クロスサイトウェブソケットハイジャッキング（CSWSH）	WebSocket 通信を経由してアプリケーションを操作できる機能の有無を診断
19	XML 外部エンティティ参照（XXE）	リクエストに XML が含まれている箇所や、アップロードされた DOCX や PPTX などの XML が含まれるファイルを処理する機能の有無を診断
20	その他の情報漏えいにつながる脆弱性	クエリストリング情報の漏えい、キャッシュからの情報漏えい、パスワードの管理不備や暗号化強度の弱いアルゴリズムの使用等の脆弱性の有無を診断

表９.（２）.①.２　「政府情報システムにおける脆弱性診断導入ガイドライン」以外の診断事項

項番	脆弱性の種類	診断内容
1	LDAP インジェクション	LDAP クエリに不正な文字列を挿入し、想定外の動作をさせる等の脆弱性の有無を診断
2	SSI インジェクション	ブラウザの入力をもとに Web ページを生成する機能により、利用者が意図しないアクセスをしてしまう等の脆弱性の有無を診断

3	安全でないオブジェクトの直接参照	ファイルやディレクトリ、データベースキーなどの実装オブジェクトが、直接参照可能になっている等の脆弱性の有無を診断
4	未検証のフォーワード	適切な検証がされていないフォーワードが実行されてしまう脆弱性の有無を診断

② 脆弱性診断の対象画面

脆弱性診断を実施する画面については、対象ドメイン内で、Ｗｅｂアプリケーションによる動的な画面遷移を対象として診断を行う。

診断対象の画面数の内訳については、表９.（２）.②に示す。

表９.（２）.② 診断対象画面数

項番	情報システム	区分	
		インターネット公開画面	内部限定画面
1	インターネット環境	－	－
2	日本年金機構ホームページ	１４画面	－
3	オンライン事業所年金情報サービス	－	９５画面
4	電子入札システム	３２画面	５４画面
5	チャットボット	－	２画面

（３）インフラの脆弱性診断の作業要件

① 脆弱性診断の観点

インフラの脆弱性診断では、システムの外側（インターネット）からのリモート診断及び内部からの診断を行う。

また、診断対象としては「別紙１　閲覧資料一覧」の各閲覧資料に記載している、サーバ及びネットワーク機器とする。

インフラの脆弱性診断の指標として、デジタル庁が示している「政府情報システムにおける脆弱性診断導入ガイドライン」に準拠するものとする。

診断事項については表９.（３）.①に示す。

表９.（３）.① 診断事項（インフラ）

項番	診断事項	診断内容
1	脆弱なソフトウェアの利用	ポートスキャンにより検知したオープンポートに接続を試み、サーバから取得したバナー情報に基づき、ポートを待ち受けている OS やミドルウェアの情報を推定し、既知の脆弱性を含むバージョンのソフトウェアの利用等を検出する。

2	不要なポート、サービスの存在	ポートスキャンにより通信可能なポートを確認し、外部からの接続を意図していないオープンポートや、第三者に仕掛けられたバックドア等の不審なサービスを検出する。
3	公開ディレクトリ、ストレージの非公開情報の保存	公開不要なファイルの存在等を確認する。
4	DNS やメールの設定不備	オープンリゾルバ、ゾーン転送の設定不備やメールの不正中継等の脆弱性の有無を確認する。
5	暗号化されていない、または脆弱な暗号による通信	ネットワーク盗聴される通信がないか等を確認する。
6	サーバ証明書の不備	サーバ証明書の設定の不備等を確認する。
7	サーバソフトウェアの設定不備	初期パスワードの利用、ディレクトリリスティング等を確認する。

② 脆弱性診断の実施対象

サーバ及びネットワーク機器を対象として診断を実施する。

診断対象のＩＰアドレス数の内訳については、表９.（３）.②に示す。

表９.（３）.② 診断対象ＩＰアドレス数

項番	情報システム	区分	
		インターネット公開機器	内部限定機器
1	インターネット環境	－	８４IP ｱﾄﾞﾚｽ
2	日本年金機構ホームページ	－	４１IP ｱﾄﾞﾚｽ
3	オンライン事業所年金情報サービス	－	１８IP ｱﾄﾞﾚｽ
4	電子入札システム	２ IP ｱﾄﾞﾚｽ	５ IP ｱﾄﾞﾚｽ
5	チャットボット	－	－

（４）ペネトレーションテストの作業要件

ペネトレーションテストの実施に当たっては、以下を踏まえ、実施すること。ただし、これに加え、望ましいテスト手法があれば提案すること。

なお、本調達仕様書において、「ペネトレーションテスト」を「テスト」と表記する場合がある。

① 侵入（ペネトレーション）の定義

ア 管理者権限を持つアカウントによるOS 又はミドルウェア等へのログイン

イ 一般ユーザ権限を持つアカウントによるOS 又はミドルウェア等へのログイン

ウ 認証を回避してのOS に対するコマンドの実行
エ 上記ア～ウ以外での対象ホスト内の情報の操作

② 本業務におけるペネトレーションテストの内容

いわゆる脆弱性診断は、システムが悪用された場合に侵害可能性のある脆弱性を検出・優先付けして報告するものであるが、本業務におけるペネトレーションテストは、攻撃者の視点に立ち、検出された複数の脆弱性や設定不備などを単独又は組み合わせにより擬似攻撃を行い、前段階の擬似攻撃で得られた情報をさらに次の擬似攻撃に利用したりすることで、システムのセキュリティを実際に迂回・突破した結果を報告することを意味する。

本業務におけるペネトレーションテストは、システム情報及び脆弱性情報等の収集、対象ホストへの侵入可否の業務及び分析、侵入可能な攻撃の実行、侵入後の攻撃活動（情報収集や攻撃の結果により判明した対象機器の脆弱性等を利用し、他の更に重要なホストへの侵入を試行すること等）を網羅するものとする。

なお、ソーシャルエンジニアリングやテスト対象への物理的な攻撃は、原則として実施しない。

一般的なペネトレーションテストのための方法論や疑似攻撃の手法には、NISTSP800-115 や Penetration Testing Execution Standard (PTES)などに示されたものがあるが、受託者は、近年のサイバー攻撃の動向や最新の攻撃手法を勘案し、攻撃者の視点に立ったより実践的なテストとなるよう攻撃手法や使用するツールを採用し、本業務を遂行すること。

③ ペネトレーションテストの実施完了条件

対象となる各種サーバ等に対し、上記①に示す侵入を達成できる可能性のある攻撃手法を全て実施する。ただし、多数の攻撃手法が存在するなど、実施期間内に全ての攻撃手法を実施することが困難であると想定される場合には、機構と協議の上、実施する攻撃手法数を調整する。

④ ペネトレーションテスト実施期間

１システム当たりのペネトレーションテスト実施期間は、４日間程度とする（２システムで計８日間程度）。

なお、「ペネトレーションテスト実施期間」は、テスト対象システムに対して侵入を試みる作業を行う期間であり、ペネトレーションテストの実施結果に関する分析及び評価を行う期間は含まない。

また、侵入シナリオ作成のための事前ポートスキャン等の実施に要する期間も、ペネトレーションテスト実施期間には含めないものとする。

さらに、テスト当日にテスト対象システムとの通信の疎通が取れないなどの不測の事態が発生した場合も、ペネトレーションテスト実施期間を縮めず、４日間程度の作業を行うこと。４日間程度の作業が困難であると想定される場合には、機構と協議の上、調整すること。

⑤ ペネトレーションテストの攻撃手法

業務において使用する攻撃手法は、稼働中のサービスに支障を与える可能性がある場合、その影響について事前に説明し、承認を得てから業務を実施すること。

⑥　テスト対象システム及び対象機器

ア 脆弱性診断対象システムに記載した６システムのうち、２システムを対象とする。

イ　対象システムの本番環境または稼働維持環境でテストを実施する。ただし、原則として稼働維持環境での実施とする。

ウ　IPアドレス数は全体で48以内（１システム当たり平均24IPアドレスを想定。ただし、システムの規模により増減する。）とする。詳細については、契約締結後、別途指示する。

エ ペネトレーションテストの対象は、各種サーバ、端末、通信回線装置とする。なお、IPv6アドレスも対象となる場合があることに留意すること。

１０　作業の体制及び方法

（１）作業体制

①　基本方針

受託者は、本業務を円滑に遂行するため、プロジェクトの統括責任者、作業責任者を配置することとし、その他必要な役割を定義し、適切な人員を配置すること。受託者は、プロジェクトの体制図とそれぞれの役割の詳細について、書面にて機構へ連絡し承認を得ること。

②　統括責任者の条件

プロジェクトの統括責任者に求める要件は、次に掲げる項目のとおりである。

ア　過去３年間において、日本の政府機関の情報システムに係るプロジェクトの統括責任者としての経験を有すること。

イ　統括責任者は、原則として機構との会議及び機構への報告会に出席すること。なお、機構との会議等に出席できない場合は事前に機構の了解を得ること。また、病気等により当該者が本業務を遂行できない状況が生じた場合は、当該者と同等の能力及び資格を有する要員を配置すること。

③　作業責任者の条件

作業責任者に求める要件は、次に掲げる項目のとおりである。

ア　情報セキュリティに係る業務の経験年数を５年以上有し、かつセキュリティ診断業務及びペネトレーションテストの責任者としての経験を有すること。

イ　「情報処理の促進に関する法律」（昭和 45 年法律第 90 号）に基づいて行われる情報技術者試験に基づく情報処理安全確保支援士、ほかの民間団体が認定するセキュリティ資格のうち、以下のいずれかの資格を有しているか又は、資格を有する者と同等以上の技術を保持していること。

・情報処理安全確保支援士（情報処理安全確保支援士として登録する資格を有する者は、これと同等とみなす。）
・CISSP（Certified Information Systems Security Professional）
・CEH（Certified Ethical Hacker）
・CISM（Certified Information Security Manager）
・GWAPT（GIAC Web Application Penetration Tester）またはその上位資格
・GPEN（GIAC Penetration Tester）またはその上位資格

④　作業従事者の条件

作業従事者に求める要件は、次に掲げる項目のとおりである。

ア　脆弱性診断における作業従事者は２名以上（うち少なくとも２名は、３年以上のセキュリティ診断業務の経験を有すること。）であること。

イ　ペネトレーションテストにおける作業従事者は３名以上（うち少なくとも２名は、３年以上のペネトレーションテストの経験を有すること。）であること。なお、上記アの作業従事者と同一の作業従事者であることを可能とする。

ウ　ア、イの作業従事者のうち２名以上は、以下のいずれかの資格を有しているか又は、資格を有する者と同等以上の技術を保持していること。

・情報処理安全確保支援士（情報処理安全確保支援士として登録する資格を有する者は、これと同等とみなす。）
・CISSP（Certified Information Systems Security Professional）
・CEH（Certified Ethical Hacker）
・CISM（Certified Information Security Manager）
・GWAPT（GIAC Web Application Penetration Tester）またはその上位資格
・GPEN（GIAC Penetration Tester）またはその上位資格
・OSCP（Offensive Security Certification Professional）またはその上位資格

（２）作業方法等

①　進捗管理

脆弱性診断及びペネトレーションテスト業務について、受託者は、「業務実施計画書」に基づき、「９　作業要件」に係る作業について、以下の要件を満たす進捗管理を実施すること。

ア　作業項目の順序関係及び依存関係を明確にした上で、必要作業量を踏まえてスケジュールを作成すること。

イ　作業実績を把握し、計画との差異分析、傾向分析などに基づく対応措置をとること。

ウ　定期的な報告会（定例報告会議など）を原則隔週で開催し、作業状況の報告を行うこと。なお、報告会が実施されない週においては、報告書を機構へ送付すること。

エ　報告会での報告時に、対象とする作業期間に予定していた全作業について計画からの乖離を報告すること。

オ　計画からの遅れが 10 日以上となった場合（複数作業において遅れが発生している場合には、予定作業完了までに要する日数が最も大きい作業を基準とする。）には、機構と協議の上要員の追加又は担当者の変更といった体制の見直しを含む改善策を提示し、機構の承認を得ること。

②　リスク管理

受託者は、以下の要件を満たすリスク管理を実施すること。

ア　プロジェクトの遂行に影響を与えるリスクを識別し、その発生要因、発生確率、影響度を整理すること。

イ　リスクを顕在化させないための対応策、リスクが顕在化した後の対応策を識別し、緊急時対応計画（コンティンジェンシープラン）として具体化すること。

③　セキュリティ管理

受託者は、契約締結後に開示する「日本年金機構情報セキュリティポリシー」を踏まえ、以下の要件を満たすセキュリティ管理を実施すること。

ア　受託者内における情報セキュリティ対策に関する事務を統括する、情報セキュリティ管理責任者を上記１０（１）②、③及び④の者とは別に設けること。

イ　本業務を適用範囲とする情報セキュリティポリシーを策定し、機構の承認を得ること。また、策定した情報セキュリティポリシーを遵守すること。

特に以下の事項について、その徹底を図ること。

・情報管理（守秘義務の遵守／データ輸送時の対応／データ暗号化など）

・文書管理（開示情報、機密情報、秘扱文書の管理など）

ウ　受託者内の品質管理部門等の第三者を主体として、内部的なセキュリティ監査を実施した上で、機構にセキュリティ対策状況を報告すること。

④　品質管理

受託者は、以下の要件を満たす品質管理を実施すること。

ア　品質改善のための各種取組が、しかるべき手続に則って実施されていることを確認すること。

イ　受託者内のプロジェクト参画メンバー以外の第三者による品質レビューを、定期的に実施すること。

⑤　要員管理

受託者は、以下の要件を満たす要員管理を実施すること。

ア　各作業工程の過程又は必要な時期において、プロジェクトを円滑に進捗するための組織計画の策定及び組織の編成を行い、作業体制を確立させること。

イ　組織計画に基づく要員の調達及び配置を確実に実施すること。

ウ　すべての要員について、参画時に保有スキル及び実務経験等の情報を提示することとし、事前に機構の承認を得ること。

エ　本調達では、本書で提示する要件を満たしている限りにおいて、作業担当者の常駐化を求めるものではないことから、受託者の内部体制管理上、最も効率的な対応を計画すること。

ただし、機構が提供する環境で業務を行う場合は、本プロジェクトの業務のみ行うこと。

オ　各種調整等は、受託者の責任で実施し、機構との共同作業において、当該調整等に起因する工程管理に係る機構側の負荷が生じないようにすること。

⑥　コミュニケーション管理

受託者は、以下の要件を満たすコミュニケーション管理を実施すること。

ア　プロジェクトの参加者の誰が誰に対し、どのような情報やメッセージをどのようなサイクルやタイミングで、何を使って伝えるのか、フィードバックはどのように実施するのか、等に関するコミュニケーション計画を作成し、コミュニケーション管理のための仕組みを構築すること。

イ　報告フォームは、プロジェクトの現状、計画との差異、今後の予測及び対応策などの記載を必須とし、機構がプロジェクトの状況・進捗の把握、各種判断を行うことができるものとすること。

ウ　プロジェクトで実施すべきすべての会議・報告会等について、内容、出席者、開催頻度、提示情報及びこれらに必要なフォーム等を定義し、会議・報告会等を開催すること。

⑦　課題・問題管理

受託者は、以下の要件を満たす課題・問題管理を実施すること。

ア　課題の内容、発生日、担当者、検討状況、検討結果及び解決日などの必要情報を、一元管理すること。

イ　機構とのインタフェース機能として、起票、検討、確認及び承認といった一連のワークフローを意識した仕組みを整備すること。

ウ　定期的に課題対応状況を監視し、解決を促す仕組みを確立すること。

エ　課題発生時には、速やかに機構に報告し、対応を検討すること。

オ　課題が発生する可能性がある場合には、未然に防止するための対応を行うこと。

カ　仕様の追加又は変更に関しても、課題・問題管理の対象として同様に管理を実施すること。

（３）契約不適合責任

受託者は、診断実施時点において公知であり、かつ診断において容易に発見し得たと判断できる脆弱性（表９．（２）．①．１、表９．（２）．①．２に記載の脆弱性、表９．（３）．①に関する脆弱性）が検収後に発見された場合は、作業の再実施を行うこと。

１１　特記事項

（１）入札制限

本件調達の公平性を確保するため、参加者は、以下に挙げる事業者並びにこの事業者の「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、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者でないこと。

ア「日本年金機構におけるシステム支援等業務」（平成 28 年度以降）の受託者

イ「社会保険オンラインシステム監査に係る外部委託」（平成 28 年度以降）の受託者

ウ「日本年金機構におけるシステム監査に係る支援業務」（平成 28 年度以降）の受託者

エ「年金個人情報提供システム」に係る開発、運用及び保守業務のいずれかの受託者

オ「インターネット環境」に係る開発、運用及び保守業務のいずれかの受託者

カ「日本年金機構ホームページ」に係る開発、運用及び保守業務のいずれかの受託者

キ「個人番号管理情報連携サブシステム」に係る開発、運用及び保守業務のいずれかの受託者

ク「電子入札システム」に係る開発、運用及び保守業務のいずれかの受託者

ケ「オンライン事業所年金情報サービス」に係る開発、運用及び保守業務のいずれかの受託者

コ 「チャットボットを利用したサービス提供業務」に係る開発、運用及び保守業務のいずれかの受託者

サ 「日本年金機構における情報セキュリティリスクの評価・分析業務」（平成 28 年度以降）の受託者

シ 「日本年金機構における最高情報セキュリティアドバイザー及び情報セキュリティ対策等支援業務」の受託者

ス 「日本年金機構における情報セキュリティ監査に係る業務」の受託者

（２）応札条件

応札者は、次に掲げる条件を満たすこと。

・経済産業省が定める「情報セキュリティサービス基準」に適合する企業を掲載した「情報セキュリティサービス基準適合サービスリスト」における脆弱性診断サービスのリストに登録されており、登録を示せること。

（３）知的財産等

① 本業務遂行上作成された成果物（電子媒体を含む）又その他類似の派生物（提案等の構想等も含む）については、それらに関する一切の著作権及び所有権が機構に帰属するものとする。

② 本件に関して発生した権利については、受託者は著作者人格権を行使しないものとする。

③ 本件に関して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 本件に関して作成・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、事前に機構へ報告し、承認を得ること。

⑤ 本件に関して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、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委ねる等の協力措置を講ずる。

（４）再委託

① 再委託の制限及び再委託を認める場合の条件

ア 受託者は、受託業務の全部又は受託業務における総合的な企画及び判断並びに業務遂行管理部分を第三者に再委託することはできない。原則として、再委託を認める部分は「表１１.（４）.① 再委託区分」に示す作業区分とする。

表１１.（４）.① 再委託区分

項番	作業概要	受託業務内容	分類	再委託の可

				否
1	総合的な企画・判断・業務遂行上の管理部分及び実作業	・プロジェクト管理 ・アプリケーションの脆弱性診断 ・インフラの脆弱性診断 ・ペネトレーションテスト ・診断結果報告 ・問合せ・立会い対応	主体的部分	再委託不可
2	上記を除く作業	・アプリケーションの脆弱性診断の準備 ・インフラの脆弱性診断の準備 ・ペネトレーションテストの準備 ・診断結果報告に係る一部作業	上記以外の部分	再委託可

イ　受託者は、再委託先の資本関係・役員等の情報、業務の実施場所、作業要員の所属、専門性（情報セキュリティに係る資格・研修実績等）及び実績に関する情報の提供を行うとともに、再委託事業に対して意図せざる変更が加えられないための十分な管理体制がとられることを報告し、係る業務体制について機構の確認（立入調査）を随時受け入れること。

ウ　受託者は、知的財産権、情報セキュリティ（機密保持及び遵守事項）、ガバナンス等に関して本仕様書が定める受託者の責務を再委託先事業者も負うよう、必要な処置を実施し、機構に報告し、承認を受けること。

エ　受託者が再委託する事業者は、「１１（１）入札制限」に定める事業者及びその関連会社でないこと。

オ　受託者は、再委託先による当該業務の更なる第三者への委託（再々委託）をさせてはならない。

② 承認手続

受託者は、委託業務の一部を再委託する場合は、あらかじめ再委託の相手方の商号又は名称及び住所、再委託を行う業務の範囲、再委託の必要性（合理的理由）、業務を遂行する能力、契約金額、再委託業務実施場所、役員等の情報・資本関係、再委託先における責任者（統括管理補助者、情報セキュリティ管理補助者）の氏名、再委託事業従事者の所属・専門性及びガバナンスの確立方法及び情報セキュリティの確保方法について記載した「再委託に係る承認申請書」を機構に提出し、承認を受けること。

再委託先の相手方の変更を行う必要が生じた場合は、「再委託に係る変更承認申請書」を機構に提出し、承認を受けること。

③ 再委託先等の契約違反等

再委託先が本調達仕様書に定める事項に関する義務違反があった場合又は義務を怠った場合には、受託者が一切の責務を負うとともに、機構は、受託者に対し、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。

（５）機密保持

① 受託者は、本受託業務の実施の過程で機構が開示した情報（公知の情報を除く。以下同じ）、関連業者が提示した情報及び受託者が作成した情報を、本受託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、本受託業務を実施するに当たり、機構から入手した資料、受託者が作成した情報等については管理台帳等により適切に管理し、かつ、以下の事項に従うこと。

ア 受託者における提供情報等の複製は原則禁止する。ただし、受託者において複製が必要であると判断した場合には、あらかじめ機構と協議を行い、その承認を得ること。

イ 受託業務に必要がなくなった日から７日以内に機構に返却すること。

ウ 受託業務完了後、上記ア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機構へ提出すること。

③ 機密保持及び資料の取扱いについて、適切な管理が講じられていることを確認するため、機構が遵守状況の報告や実地調査を求めた場合には応じること。

④ 応札希望者についても、上記①から③に準じること。

（６）その他遵守事項

本調達仕様書は、診断対象システムの脆弱性診断及びペネトレーションテスト業務について最低限必要な要件を示したものであり、一般的に脆弱性診断及びペネトレーションテスト業務において必ず求められる事項については、本調達仕様書に明記されていなくても考慮すること。

（７）立入監査

本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に、機構が情報セキュリティ監査の実施を必要と判断した場合は、情報セキュリティ監査を受け入れること。

なお、その実施内容については、「１１（５）機密保持」に記載した内容、実施計画書に基づく履行状況、受託者の作業環境等について行う。

（８）環境への配慮

本受託業務に係る納入物については、「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）」に基づいた製品を可能な限り納品すること。

（９）資料等の閲覧

資料閲覧については、下記①から⑤に従い、申請先より事前の許可と日程調整を行った上で、閲覧を行うこと。

なお、閲覧対象の資料は「別紙１　閲覧資料一覧」に示す。

① 申請方法

ア 申請先（申請書提出先）は「６　調達担当部署」のとおり。

イ 「別紙２　資料閲覧申請書兼秘密保持誓約書」を提出すること。※当日提出可

② 閲覧条件

ア 「１１（２）応札条件」を満たしていること。

イ 閲覧希望日の２営業日前までに閲覧の許可を得ていること。

③ 閲覧場所

東京都杉並区高井戸西 3 丁目 5 番 24 号

日本年金機構 情報管理対策室 情報リスク分析グループ

④ 閲覧日時

ア 閲覧可能期間： 入札日の３営業日前まで（土、日、祝祭日を除く）

イ 閲覧可能時間： 10:00～12:00、13:00～17:00

⑤ 留意事項

ア 閲覧希望５営業日前までに希望日時を申請窓口に連絡する。希望日が複数社で重複した場合は、機構において調整を行うのでその指示に従うこと。

イ 指定された日時に閲覧場所で、「別紙２ 資料閲覧申請書兼秘密保持誓約書」の確認及び閲覧者の身分確認を行う。「別紙２ 資料閲覧申請書兼秘密保持誓約書」については閲覧期間中、一度提出すれば閲覧日毎に提出する必要はない。

ウ 閲覧者の身分確認は、社員証など応札希望業者の社員であることが確認できるもので行う。

エ 閲覧には機構の職員が立ち会うので、閲覧者はその指示等に従うこと。

オ 閲覧場所にはカメラ等の撮影機器及びパソコン等記録媒体は持ち込めない。また、閲覧時に複写又は写真撮影等を禁止する。違反行為があった場合は、機構は閲覧の中止、退去を求める場合がある。

カ 閲覧資料の内容に関する質問については、後日回答する。

閲覧資料一覧

No	情報システム	閲覧資料の内訳
1	インターネット環境	NW構成図
2	日本年金機構ホームページ	NW構成図
3	オンライン事業所年金情報サービス	NW構成図
4	電子入札システム	NW構成図
5	チャットボット	NW構成図

別紙２

日本年金機構　御中

資料閲覧申請書　兼　秘密保持誓約書

申請日　　令和　　年　　月　　日（　）
会社名　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　社印
担当者　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
所在地　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
電話番号＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
E-mail　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

件名「令和８年度脆弱性診断及びペネトレーションテスト業務　仕様書」に関し、以下のとおり資料を閲覧させて頂きたく申請書を提出致します。

また、閲覧にて知り得た情報は、本件以外の目的に使用すること並びに第三者に開示及び漏洩をしないことを誓約します。

■閲覧希望日時

①　令和　　年　　月　　日（　）　　午前　・　午後
②　令和　　年　　月　　日（　）　　午前　・　午後
③　令和　　年　　月　　日（　）　　午前　・　午後

■閲覧希望資料

項番	資料名
1	
2	
3	

■閲覧者

項番	氏　名	ふりがな	TEL
1			
2			
3			

※　注意事項

① 閲覧時間は原則として３時間以内とする。
② 閲覧する資料の複写等は原則として禁止する。
③ 希望する日時を第３希望まで記載し、後日、日本年金機構本部が指定する。
④ 閲覧する資料の閲覧場所からの持ち出しは禁止する。
⑤ 閲覧にて知り得た情報は、本件以外の目的に使用すること並びに第三者に開示並及び漏洩をしてはならない。
⑥ 閲覧時に日本年金機構職員が立ち会うものとする。
⑦ 本件に関して日本年金機構又は第三者に損害を与えた場合は、日本年金機構又は当該損害を被った者に対し、一切の損害を閲覧業者にて賠償するものとする。なお、損害には、日本年金機構又は当該損害を被った者が要する一切の費用、訴訟に関する弁護士費用の相当額が含まれるものとする。