年金業務システム（個人番号管理サブシステム（情報連携））の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
Japan Pension Service

基幹システム開発部
令和8年5月

目次

○別紙一覧

別紙１　用語の定義
別紙２　守秘義務に関する誓約書
別紙３　再委託承認申請書
別紙４　技術資料閲覧に係る実施要領

○技術資料一覧（以下に示す資料は、希望する者へ開示予定）

技術資料１　年金業務システム要件定義書
技術資料２　年金業務システム非機能要件定義書
技術資料３　年金業務システム基本設計書
技術資料４　年金業務システム詳細設計書
技術資料５　共通基盤システムに関する資料
技術資料６　個人番号管理サブシステム（情報連携）各サーバリソース使用状況
技術資料７　本部ネットワークに関する資料
技術資料８　NW 構成図（概要）

1　委託業務の概要

（1）　目的

令和9年1月に更改する年金業務システム（個人番号管理サブシステム（情報連携））（以下、「本システム」という。）について、更改（構築）中のシステムに対し、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における安全性及び信頼性を確保することを目的とし、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。

■対象システム

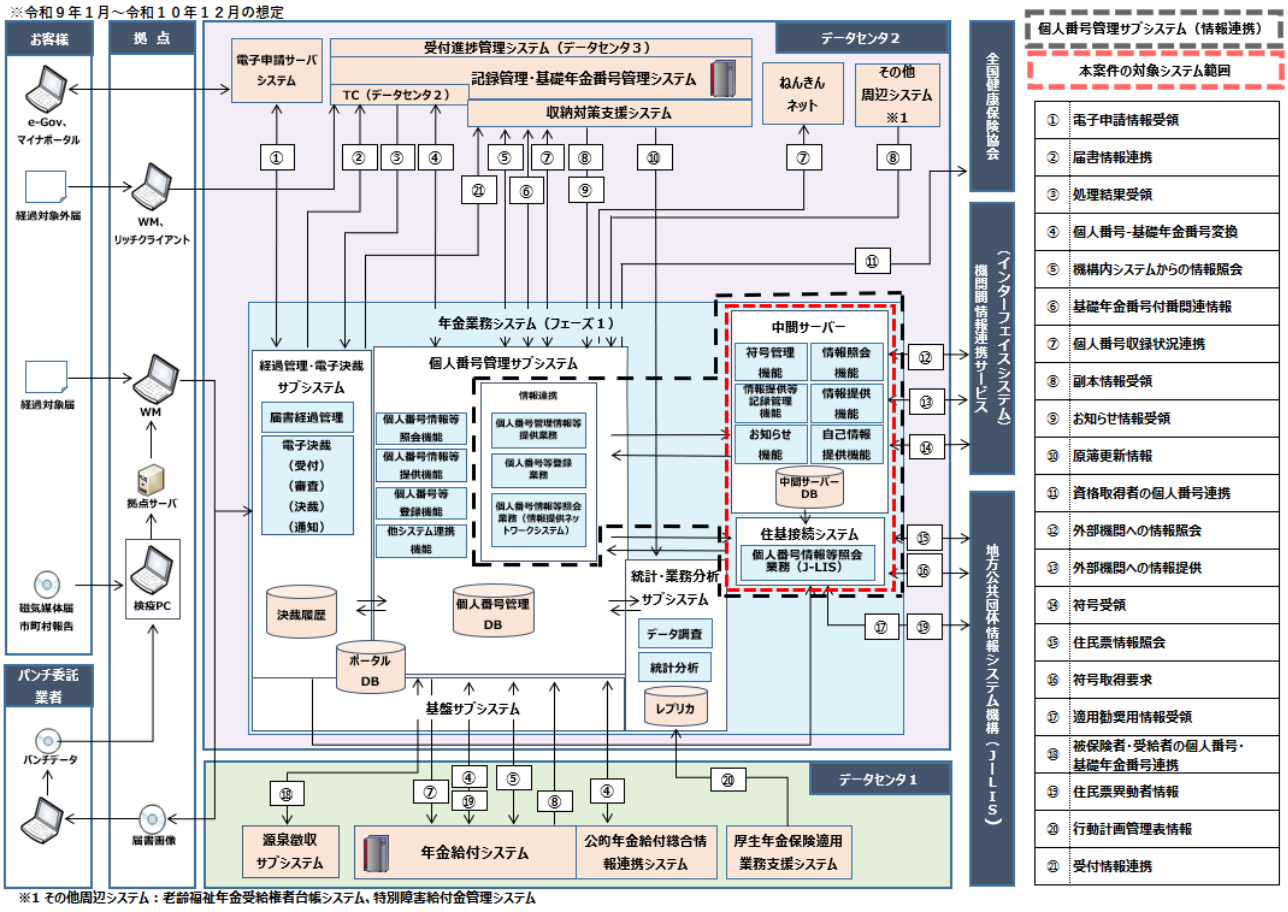
本システムの概要は「図1.（1） 年金業務システムの各サブシステムが有する主要機能を示した概要図」のとおりである。

・個人番号管理サブシステム（情報連携）

中間サーバー、住基接続システム及び個人番号管理サブシステムから構成されるシステムの総称であり、以下の機能を保有する。本案件の対象システムは、中間サーバー及び住基接続システムのみとする。

・情報提供ネットワークシステムへの符号取得依頼と取得した符号の管理
・適用・徴収業務における外部機関保有情報の活用
・給付業務における外部機関保有情報の活用
・届書等の経過管理・電子決裁による外部機関保有情報の活用
・届出受理・審査業務における外部機関保有情報の活用
・外部機関からの照会に対する情報提供の実施
・お知らせ情報表示機能に係る業務
・自己情報表示機能に係る業務
・情報提供等記録の追記等業務
・情報開示請求及び監査機関からの監査に備えた情報連携等に係る証跡管理
・情報連携の対象となる特定個人情報の副本の保存・管理
・住基即時照会
・異動者情報照会及び生存状況照会等の一括照会
・住基ネットへの接続と符号の取得依頼

図1.（1） 年金業務システムの各サブシステムが有する主要機能を示した概要図



（２） 定義

本仕様書で用いる用語については、「別紙 １ 用語の定義」を参照すること。

2　作業内容・納品成果物等

（1）　業務概要

本調達における作業内容（以下、「本業務」という。）は、「表2.（1） 作業概要一覧」のとおりである。

なお、契約締結後、本システムの更改（構築）状況によりスケジュールが変更される場合は、適宜日本年金機構（以下、「機構」という。）及び「表3　関連事業者一覧」に示す事業者と協議の上、決定すること。

表2.（1） 作業概要一覧

項番	項目	実施スケジュール（予定）	作業概要
1	契約締結	令和8年6月中旬	－
2	事前準備 ※各種調整含む	令和8年6月中旬から	・診断項目及び診断方式の検討 ・更改事業者とスケジュール、診断環境等の調整 ・業務実施計画書の作成 ・対象システムに関する情報提供依頼 ・各種診断準備（データ、端末） ・月次定例報告会資料の作成
3	業務実施計画書報告	令和8年8月上旬	業務実施計画書を提示
4	脆弱性診断（インフラ診断）及びペネトレーションテスト(*1)	令和8年8月24日から 9月11日	本番環境(*2)での診断を予定 詳細は「6 診断要件」を参照
5	診断結果報告（脆弱性診断（インフラ診断）及びペネトレーションテスト）	令和8年9月28日	診断結果報告書を提示 結果報告後は問合せ対応（*3）を実施
6	脆弱性診断（Web アプリ診断）(*1)	令和8年10月13日から 11月20日	検証環境(*4)での診断を予定 （同環境で更改事業者による総合テストが並走される予定） 詳細は「6 診断要件」を参照
7	診断結果報告（脆弱性診断（Web アプリ診断））	令和8年11月27日	診断結果報告書を提示 結果報告後は問合せ対応（*3）を実施
8	契約終了	令和9年1月29日	－
以下、再診断が必要な場合のみ実施			
9	再診断（脆弱性診断（インフラ診断）及びペネトレーションテスト）(*1)	令和8年10月5日から 11月13日のうち1週間	本番環境(*2)での診断を予定
10	再診断結果報告（脆弱性診断（インフラ診断）及びペネトレーションテスト）	令和8年11月20日	再診断結果報告書を提示 結果報告後は問合せ対応（*3）を実施
11	再診断（脆弱性診断（Web アプリ診断））(*1)	令和8年12月7日から 12月11日	検証環境(*4)での診断を予定

項番	項目	実施スケジュール(予定)	作業概要
12	再診断結果報告(脆弱性診断(Web アプリ診断))	令和8年12月18日	再診断結果報告書を提示 結果報告後は問合せ対応(*3)を実施

(*1) 実施日数に懸念がある場合は、期間内での作業が可能となる方法を機構へ提案し、協議すること。
(*2) 本番環境:本システムの本番サービスが稼働する環境。診断時は更改中の環境。
(*3) 問合せ対応:機構からの質問及び依頼を受付け、速やかに回答すること。また、質問及び依頼内容は管理簿による管理を行い、追跡できるようにしておくこと。管理簿には質問管理 No、質問者、質問年月日、質問の内容、回答期限及び回答を記載すること。
(*4) 検証環境:本番環境へのリリースに際し、各種テスト(事前検証)の実施、セキュリティパッチ適用やウイルス定義ファイルの更新、ソフトウェアバージョンアップに伴う影響調査等で使用する環境。

(2) 作業場所等

本業務の作業場所は、受託者の履行場所(日本国内に限る)又は機構が指定する場所(東京都内)とする。
なお、機構の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。
また、本業務で必要となる診断用の端末、機材類及び媒体について、受託者の負担と責任において準備すること。なお、ペネトレーションテストの侵入シナリオにおいて、受託者で準備できないものについては、別途協議の上、貸し出すものとする。

(3) 成果物の内容等

本業務における成果物の内容は、「表2.(3) 成果物一覧表」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、併せて納品するとともに、納品後の成果物に対する照会に対応すること。
また、「表2.(3) 成果物一覧表」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、積極的に提案すること。

表2.（3）成果物一覧表

項番	成果物	記載内容等
1	業務実施計画書	本業務の全体計画書であり、以下を含むものとする。 ・「表6.（2）.①.1 「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」の診断事項（Web アプリ診断）」、「表6.（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（Web アプリ診断）」、「表6.（3）.① 「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」の診断事項（インフラ診断）」、「6 （4） ① 侵入（ペネトレーション）の定義」及び「6 （4） ② 本業務におけるペネトレーションテストの内容」を踏まえた具体的な診断内容 ・診断方法（使用する機材・環境、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の一覧）や利用するツール等の内容を含む。） ・スケジュール ・実施上の留意事項や準備事項（機構への依頼事項を含む。）
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、「表6.（2）.①.1 「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」の診断事項（Web アプリ診断）」、「表6.（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（Web アプリ診断）」及び「表6.（3）.① 「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」の診断事項（インフラ診断）」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 ・検出された脆弱性とその危険度を示す以下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(CVSSv4．0)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
3	月次定例報告会資料	月次定例報告会用の資料一式（スケジュール及び進捗状況、課題・問題・リスク・ToDo 等を報告すること。（報告内容詳細は別途機構と協議の上、決定する。））

4	フォローアップ関連資料	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。

（4） 納品

① 納品方法

ア. 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。

イ. 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。

ウ. 上記イの「Word 等のうちいずれかで編集が可能な形式」において、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。

エ. PDF 形式は、「表2.（3） 成果物一覧表」に示す項番ごとに一括で閲覧・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。

オ. 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、正副各一式を納品すること。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。

カ. 納品したドキュメント（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。

キ. 「表2.（3） 成果物一覧表」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2.（3） 成果物一覧表」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。

ク. 「表2.（3） 成果物一覧表」に記載した成果物以外にも、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。

② 納品場所

東京都杉並区高井戸西3丁目5番24号
日本年金機構 基幹システム開発部 年金業務システム開発第2G
担当者：藤野、本城
電話：03（6861）8143（内線：4867）

3　関連事業者

関連する事業者を「表3　関連事業者一覧」に示す。

表3　関連事業者一覧

項番	関連事業者	説明
1	更改ハードウェア等納入保守事業者	本システムに係るハードウェアの更改及び保守事業者。本システムの基盤環境に係る調整も行う。
2	更改アプリケーションプログラム設計開発事業者	本システムのアプリケーションプログラムの開発事業者。本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	共通運用管理事業者	本システムの運用管理業務を行う事業者。システムのリソース使用状況監視、障害監視等も行う。
4	共通基盤システム保守事業者	統合認証 ID 管理、監査、端末管理、運行監視、ウイルス対策、ログ管理等の機能を提供する共通基盤システムの保守事業者。

※関連事業者は追加となる可能性あり。

4　契約期間

契約締結日から令和9年1月29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準備作業を済ませておくこと。

5　情報システム稼働環境

環境（NW 構成図（概要））の閲覧を希望する場合は「15　資料等の閲覧」により手続を行うこと。

6　診断要件

（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、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、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、必要に応じて関連する事業者と協力すること。なお、契約期間中に「表3　関連事業者一覧」に示す事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6.（1）.⑤　脆弱性診断ツール（例）」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。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6．（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 アプリ診断	・Vulnerability Explorer(VEX) ・HCL AppScan ・Burp Suite Professional
2	インフラ診断	・QualysGuard ・Tripwire IP360 ・Nessus ・Metasploit ・OpenVAS

⑥ 検出された脆弱性の改修後、改修した脆弱性に対する再診断を行うこと。

⑦ 診断は機構の指示場所（東京都内）で実施すること。
なお、持ち込む診断用機器は事前に機構の承諾を得ること。

⑧ 診断の実施時期については、「表2．（1） 作業概要一覧」を参照すること。また、診断を実施する時間帯については、原則平日の10：00～18：00を予定しているが、診断状況及び令和9年1月に更改する本システムの構築状況により調整を行うこととする。

⑨ 有益と考える診断事項及び診断手法があれば、積極的に提案すること。

⑩ 診断範囲を「表6．（1）．⑩ 診断範囲」に示す。

表6．（1）．⑩ 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	
		Web アプリ診断		インフラ診断			
		本番環境	検証環境	本番環境	検証環境	本番環境	検証環境
1	中間サーバー	－	○	○	－	○	－
2	住基接続システム	－	－	○	－	－	－

（２） 脆弱性診断（Web アプリ診断）の診断要件

① 脆弱性診断（Web アプリ診断）

脆弱性診断（Web アプリ診断）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。

「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」に記載の診断事項については「表6．（2）．①．1「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」の診断事項（Web アプリ診断）」に示す。それ以外の

診断事項については「表6．(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（Web アプリ診断）」に示す。

表6．(2)．①．1 「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」の診断事項（Web アプリ診断）

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を診断
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
11	整数オーバーフロー	プログラムで扱える整数の範囲を超えることで、予期しない数値に変化してしまう不具合や脆弱性の有無を診断
12	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
13	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
14	レースコンディション	Web 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
15	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）など、ファイルアップロードにおける脆弱性の有無を診断
16	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

項番	脆弱性の種類	診断内容
17	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
18	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Web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
19	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
20	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
21	セキュリティの設定ミス	セキュリティの設定ミスに伴う脆弱性の有無を診断
22	その他の情報漏えいにつながる脆弱性	上記以外のインジェクション（サーバサイドテンプレートインジェクション（SSTI）、相対パスによる上書き等を含む）、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、エラー処理からの情報取得等の脆弱性の有無を診断

表6．（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（Webアプリ診断）

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（Webアプリ診断）の対象画面

脆弱性診断（Webアプリ診断）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6．（2）．② 診断対象画面数」に示す。

表6．(2)．② 診断対象画面数

項番	情報システム	画面数
1	中間サーバー	120画面

（3） 脆弱性診断（インフラ診断）の診断要件

① 脆弱性診断（インフラ診断）

診断対象は NW 構成図（概要）に記載のサーバ及びネットワーク機器とする。

脆弱性診断（インフラ診断）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。

「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」に記載の診断事項については「表6．(3)．①「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」の診断事項（インフラ診断）」に示す。

表6．(3)．① 「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」の診断事項（インフラ診断）

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
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
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
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
5	暗号化されていない、又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
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
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

② 脆弱性診断（インフラ診断）の実施対象

本番環境の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 アドレス数は、「表6．(3)．② 診断対象 IP アドレス数」に示す。

表6.（3）.② 診断対象 IP アドレス数

項番	情報システム	IP アドレス数
1	中間サーバー	計36 IP アドレス
2	住基接続システム	

（4） ペネトレーションテストの診断要件

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。

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し、優先度を付け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合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更に次の擬似攻撃に利用することで、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、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ペネトレーション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ペネトレーション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完了条件

対象となる各種サーバ及びネットワーク機器に対し、上記①侵入（ペネトレーション）の定義に示す侵入を達成できる可能性のある攻撃手法を機構へ提示し、実施内容を協議の上、本業務を実施する。

④ ペネトレーションテストの実施対象

本番環境のサーバ及びネットワーク機器を対象としてペネトレーションテストを実施する。

対象の IP アドレス数は、「表6.（4）.④ ペネトレーションテスト対象 IP アドレス数」に示す。

表6.（4）.④ ペネトレーションテスト対象 IP アドレス数

項番	情報システム	IP アドレス数
1	中間サーバー	計6IP アドレス

⑤ ペネトレーションテスト実施期間

実施期間は、「表2.（1） 作業概要一覧」に示す期間程度とし、該当期間には以下の作業を含まない。

ア. 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

イ. 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

また、ペネトレーションテスト当日に対象システムとの通信の疎通が取れないなど、不測の事態が発生した場合は、ペネトレーションテストの実施日数を短縮せずに対応すること。実施日数に懸念がある場合は、機構と協議の上、調整すること。

7 会議体

本業務で予定している会議体については、「表7 会議体」のとおり。

なお、会議は機構が指定した日時で実施するものとし、機構と協議の上、リモートアクセス環境においても実施可能とする。

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7 会議体

項番	会議名称	内容等	実施タイミング	出席者(*1) (受託者)
1	月次定例報告会	進捗状況、課題、リスク等をとりまとめて月次で報告する。	月次(月末を予定)(*2)	統括責任者 作業責任者 作業従事者
2	診断結果報告会	診断等により検出した個々の脆弱性に対し、詳細な分析と対策方法をとりまとめた診断結果報告書を作成した上、担当部署向けに報告する。	以下の診断結果報告書作成後、合計2回 ・脆弱性診断(インフラ診断)及びペネトレーションテスト ・脆弱性診断(Web アプリ診断)	統括責任者 作業責任者 作業従事者
3	マルチベンダ会議	更改事業者との調整及び受託者のみで対応できない課題・問題の対応方針を決定する。	随時	統括責任者 作業責任者 作業従事者

(*1)出席者の詳細については、「8 （1） ② 作業要員に求める資格等の要件」を参照すること。

(*2)各月において、機構が実施不要と判断した場合は当該報告会を省略するものとする。

8　体制

（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、書面にて機構へ提示し承認を得ること。

② 作業要員に求める資格等の要件

ア．統括責任者

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、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、「表7　会議体」に記載の会議に出席できない場合、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。

イ．作業責任者

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5月22日法律第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）又はその上位資格
- GPEN（GIAC Penetration Tester）又はその上位資格
- OSWA（Offensive Security Web Assessor）
- OSWE（Offensive Security Web Expert）
- BSCP（Burp Suite Certified Practitioner）

ウ．作業従事者

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） 上記(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）又はその上位資格
・GPEN（GIAC Penetration Tester）又はその上位資格
・OSCP（Offensive Security Certified Professional）又はその上位資格
・OSWA（Offensive Security Web Assessor）
・OSWE（Offensive Security Web Expert）
・BSCP（Burp Suite Certified Practitioner）

エ. 情報セキュリティ管理責任者

情報セキュリティ管理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） 上記ア、イ及びウの者とは別に設け、公正に情報セキュリティ管理ができるよう専任で配置することとし、他の役割との兼務を禁止する。

（２） 管理体制

① 本業務の実施に当たり、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り、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 本システムに機構の意図しない変更が行われる等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、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。なお、国籍に関する情報の確認は、「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）」の規定により実施するものであり、主に委託事業者に対して外国政府からの影響を受けるおそれが十分排除されていることを確認することを目的とする。

④ 受託者は、本業務で知り得た情報を適切に管理するため、次に掲げる体制を確保し、当該体制を確保していることを証明するため、担当部署に対し「情報取扱者名簿」（当該業務に従事する者のうち、保護を要する情報を取り扱う可能性のある者の名簿をいう。業務の一部を再委託する場合は再委託先も含む。）、「情報セキュリティを確保するための体制を定めた書面（情報管理体制図、情報管理に関する社内規則等）」（業務の一部を再委託する場合は再委託先も含む。）及び「業務従事者名簿」（当該業務に従事する者の名簿をいう。）を提出すること。

（確保すべき体制）

ア. 情報取扱者は、本業務の遂行のために必要最低限な範囲の者とすること。

イ. 本業務で知り得た情報について、担当部署が承認した場合を除き、受託者の役員等を含め、「情報取扱者名簿」に記載のある者以外の者に伝達又は漏えいされないことを保証する履行体制を有していること。

ウ. 本業務で知り得た情報について、担当部署が承認した場合を除き、受託者の親会社、地域統括会社、ブランド・ライセンサー、フランチャイザー、コンサルタントその他の受託者に対して指導、監督、業務支援、助言、監査等を行う者を含め、受託者以外の者に伝達又は漏えいされないことを保証する履行体制を有していること。

※ 「情報取扱者名簿」には、情報管理責任者（当該業務の情報取扱の全てに責任を有する者）、情報取扱管理者（当該業務の進捗管理等を行い、保護を要する情報を取り扱う可能性のある者）、その他保護を要する情報を取り扱う可能性のある者について、氏名、住所、生年月日、所属部署、役職等を、業務の一部を再委託する場合は再委託先も含めて、記載すること。なお、情報管理責任者は、情報の取扱いに関して、情報セキュリティが侵害される、そのおそれがある場合等の非常時における対策を定めるとともに、その内容を従事者に徹底すること。また、情報取扱管理者を指定すること。

※ 「業務従事者名簿」には、当該業務に従事する者について、氏名、所属部署、役職、学歴、職歴、業務経験、研修実績その他の経歴、専門的知識その他の知見、母語及び外国語能力、国籍等を記載すること。

⑤ 受託者は、上記④の「情報取扱者名簿」、「情報セキュリティを確保するための体制を定めた書面（情報管理体制図、情報管理に関する社内規則等）」及び「業務従事者名簿」に変更がある場合は、あらかじめ担当部署に申請を行い、承認を得なければならないこと。

⑥ 上記①～④で求める内容や体制（情報セキュリティ管理体制を含む）等に変更等がある場合は、直ちに機構へ連絡し指示を受けるとともに、定例会議等でその内容を報告すること。

9 プロジェクト管理関連業務

（1） 進捗管理

受託者は、以下の要件を満たす進捗管理を実施すること。

① プロジェクトの状況を正しく把握し、所定の期日までに納品成果物を作成することを目的として、進捗を管理すること。なお、スケジュールは、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作成すること。

② 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。

③ 進捗状況は月次定例報告会で報告すること。ただし、プロジェクトの進捗に大きく関わる遅れが発生する場合は、速やかに機構に報告すること。

④ 月次定例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と実績との間で生じた乖離とその理由を報告すること。

⑤ 計画からの遅れが1週間以上となった場合（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。

① 受託者は、事前にリスクを洗い出し適切に管理することにより、リスクの発現を防ぐとともに、リスク発現後の手戻りを最小化することを目的として、リスクを管理すること。
② リスクについては、リスク管理台帳を作成し、それを更新し保持することにより管理すること。なお、リスク管理台帳には、洗い出したリスクにおける緊急度、発生要因、発生確率、影響度、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、緊急時対応計画（コンティンジェンシープラン）を具体化すること。
③ リスク管理台帳に記載されたリスクの顕在化に係る状況に変化がないか、チェックする期日を設定し、その当否を確認する。また、その際に、新たに管理すべきリスクの有無についても併せて確認する。
④ リスク管理台帳に記載したリスクについて、リスクが発生する可能性がなくなった場合や、リスク対策に基づき対応等を実施したことによりリスクそのものがなくなった場合は、リスクは消滅したとみなし、リスク管理を完了する。
⑤ リスクの管理状況、対応状況については、月次定例報告会で機構に報告すること。

（３） 情報セキュリティ管理

受託者は、以下の要件を満たすセキュリティ管理を実施すること。

①「10 （3） 情報セキュリティ管理」に示す内容を踏まえ、情報セキュリティにおける実施内容及び管理体制に基づき、情報セキュリティ管理を行うこと。
② 本調達案件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適切な措置の実施を担保すること。
③ 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）

④ 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。
⑤ 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） 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。

① 納品成果物の品質が目標とする基準を達成することを目的として、納品成果物の達成基準への合否の確認、不合格の原因の除去及びその結果の監視を行うこと。
② 品質管理プロセスにおいて決定した改善策に係る事項を踏まえて、品質管理の手法を適宜見直すこと。
③ 品質管理部門以外の第三者を主体として、内部的な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。

① 納品成果物の品質を確保すること、及び本業務を円滑に推進することを目的として、要員計画を作成し、要員の調達及び配置を確実に実施すること。

② 全ての要員について、履行開始前まで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。
③ 本業務では、本仕様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、本業務のみ行うこと。
④ 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。

① 各種情報を効率的に取得、共有、通知及び伝達することを目的として、5W1H の観点に基づき、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を実施すること。
②「表7 会議体」に示す会議体を含めて、プロジェクトで実施すべき全ての会議・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た上で、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。

① 課題・問題の早期解決・再発防止に役立てることを目的として、課題・問題を管理すること。
② 課題・問題については、課題管理台帳を作成し、それを更新し保持することにより管理すること。
③ 課題・問題発生時には、速やかに機構に報告し、対応を検討すること。
④ 課題・問題の対応状況については、課題管理台帳を用いて月次定例報告会で報告すること。ただし、緊急性が高い場合は、速やかに機構に報告すること。
⑤ 受託者のみで対応できない課題・問題については、機構へ報告後、機構の指示のもと更改事業者とのマルチベンダ会議に出席し、対応方針を決定すること。
⑥ 作業範囲に係る課題・問題については、月次定例報告会において報告し、機構と協議すること。

１０ 作業の実施に当たっての遵守事項

（１） 機密保持、情報・資料の取扱い

① 受託者は、受託業務の実施の過程で機構が提供した情報（公知の情報を除く。以下同じ。 ）、他の受託者が提示及び作成した情報・資料を、本業務の目的以外に使用又は第三者に開示若しくは漏えい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、本業務を実施するに当たり、機構が提供した情報・資料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. 機構の許可なく、情報を指定した場所から持ち出さないこと。なお、個人情報等の重要な情報が記載された情報・資料に関しては、原則として社外に持ち出さないこと。

ウ. 受託者組織内に移送する際は、暗号化や施錠等適切な方法により、情報セキュリティを確保すること。また、機構との調整等に必要な場合及び返却時以外は原則として、受託者組織外に持ち出さないこと。

エ. 受託者組織内で作業を行う場合には、作業を行う施設は、IC カード等電磁的管理による入退館管理がなされていること。

オ. 作業を行う施設内の作業実施場所は、IC カード等電磁的管理による入退室管理がなされていること。

カ. 電磁的に情報・資料を保管する場合には、当該業務に係る体制以外の者がアクセスできないようアクセス制限を行うこと。また、アクセスログにより不審なアクセスがないかの確認を行うこと。

キ. 電子計算組織及び情報へのアクセスの際に使用するパスワードは、12文字以上で、英大文字、英小文字、数字、記号のうち3種以上を組み合わせて設定をすること。なお、パスワードは文字数が多く推測困難な文字列を使用することとし、「氏名、生年月日等の個人情報」、「法人・会社名を類推できるような文字列」、「規則性のある数を含む文字列」及びこれらの組合せ等の推測可能なパスワードは設定しないこと。

ク. 情報・資料を保管する端末やサーバ装置等は、受託者の情報セキュリティポリシー等により、サイバー攻撃に備え、ウイルス対策ソフト、脆弱性対策及び検知・監視等の技術的対策が講じられ、適切に管理・運用される必要があるため、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や日本年金機構情報セキュリティポリシーに準拠し、管理等することとし、準拠した対応ができない場合は、代替のリスク軽減策を講じ、機構の承認を得ること。

ケ. 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。

コ. 受託業務完了後、機構が提供した情報・資料を削除又は返却し、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 機密保持及び情報・資料の取扱いについて、適切な措置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 受託業務の実施に当たり、履行開始の前日までに、「別紙2　守秘義務に関する誓約書」を機構に提出すること。

⑤ 応札希望者についても、上記①～④に準じること。

（2）　遵守する法令等

① 受託者は、本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、個人情報の保護に関する法律等）を遵守すること。

② 受託者は、本業務の実施のために機構から提供する情報及び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。

③ 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。

④ 万一、情報の漏えい、改ざん、消失等が発生した場合、「（3）　情報セキュリティ管理」に基づき機構へ報告し迅速に対応すること。

⑤ 受託者は、本部及びその他機構の施設で作業するに当たり、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。

（３） 情報セキュリティ管理

① 情報セキュリティ規定等の遵守

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ずること。

ア．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
イ．日本年金機構個人情報保護管理規程
ウ．日本年金機構情報セキュリティポリシー
エ．情報セキュリティインシデント対処手順書

上記ウ及びエは非公表であるが、ウはアに準拠しているため、必要に応じて参照すること。

なお、上記ウ及びエは、受託者が機構の担当職員に「別紙2 守秘義務に関する誓約書」を提出した際に開示する。上記のイ～エ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 情報セキュリティ要件が侵害された場合の対策

本業務の遂行において情報セキュリティの侵害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

③ 情報セキュリティ対策の履行状況の報告

本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。

④ 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。

⑤ 情報セキュリティ対策の履行が不十分な場合の対処

本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。

（４）　立入検査

本業務の遂行において、適切な履行を確保するため、「日本年金機構外部委託実施要領」に従って、契約締結時から履行開始前までの間、機構が必要と認める場合に、機構が受託者と検査実施方法、スケジュール、事前提出書類等を調整の上、機構が本業務の作業場所やデータ保管場所に立入検査を行うこととする。

なお、受託者及び再委託先事業者（再委託先事業者が用意した作業場所となる場合のうち、受託者等と協議の上、機構が指定する範囲に限る。）は、当該立入検査等における機構の質問及び資料提供等の指示に応じ、修正及び改善要求があった場合は、これに応じるとともに、各種作業が完了した際には、機構に対してその旨を報告し承認を得ること。

（５）　履行完了後の資料の取扱い

受託者は、担当部署から提供した資料又は担当部署が指定した資料の履行完了後の取扱い（返却・削除等）について、本仕様書の定めの他、担当部署の指示に従うこと。

（６）　その他遵守事項

本仕様書は、本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、本仕様書に明記されていなくても考慮すること。

１１　成果物の取扱いに関する事項

（１）　知的財産権の帰属

① 本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第21条から第28条までに定める全ての権利を含む。）は、受託者が本調達の実施の従前から権利を保有していた等の明確な理由により、あらかじめ知的財産権の帰属に係る表明書にて権利譲渡不可能と示されたもの以外は、全て機構に帰属するものとする。なお、当該表明書は遅くとも「表2.（3） 成果物一覧表」に定める業務実施計画書の案と併せて提出すること。

② 機構は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。
また、受託者は、成果物について、産業技術力強化法（平成12年法律第44号）に基づき、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（以下、「複製等」という。）ができるものとする。ただし、成果物に第三者の権利が帰属する時や、複製等により機構がその業務を遂行する上で、支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

③ 本件プログラムに関する権利（著作権法第21条から第28条に定める全ての権利を含む。）及び著作物の所有権は、機構から受託者に対価が完済された時受託者から機構に移転するものとする。

④ 納品される著作物に第三者が権利を有する著作物（以下、「既存著作物等」という。）が含まれる場合には、受託者は、当該既存著作物の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の受託者は当該既存著作物の内容について事前に機構の承認を得ることとし、機構は、既存著作物等について当該許諾条件の範囲で使用するものとする。

⑤ 受託者は機構に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

（２） 検査

①「表2.（3） 成果物一覧表」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、品質保証が確認できる資料を作成し、成果物と併せて提出すること。
② 検査の結果、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、指定した日時までに修正が反映された全ての成果物を納品すること。
③「表2.（3） 成果物一覧表」に記載の成果物以外にも、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。

（３） 契約不適合責任

① 納品検査に合格した成果物を受領した後において、当該成果物が契約の内容に適合していないこと（以下、「契約不適合」という。）を知った時から1年以内に（数量又は権利の不適合については期間制限なく）その旨を受託者に通知した場合は、次のア、イのいずれかを選択して請求することができ、受託者は、これに応じなければならない。なお、機構は、受託者に対して以下イを請求する場合において、事前に相当の期間を定めて本項の履行を催告することを要しないものとする。

ア. 機構の選択に従い、機構の指定した期限内に、受託者の責任と費用負担により、修正又は不足分の引渡しを行うこと。
イ. 直ちに代金の減額を行うこと。

② 機構は前項の通知をした場合は、上記①ア、イに加え、受託者に対する損害賠償請求及び本契約の解除を行うことができる。
③ 受託者が契約不適合について知り若しくは重大な過失により知らなかった場合、又は契約不適合が重大である場合は、上記①の通知期間を経過した後においてもなお上記①、②を適用するものとする。
④ 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6.（2）.①.1 「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」の診断事項（Web アプリ診断）」に記載の脆弱性、「表6.（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（Web アプリ診断）」に記載の脆弱性、「表6.（3）.① 「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」の診断事項（インフラ診断）」に記載の脆弱性）が検収後に発見された場合は、作業の再実施を行うこと。

１２　入札参加要件に関する事項

（１）　入札参加資格要件

応札者は、次に掲げる条件を満たすこと。

・経済産業省の「情報セキュリティサービスに関する審査登録機関基準」における「脆弱性診断サービス」の認定を取得しており、認定の取得を示せること。

（２）　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。

①「日本年金機構におけるシステム支援等業務一式」（令和6年度以降）の受託者
②「個人番号管理サブシステム（情報連携）」に係る開発、運用及び保守業務のいずれかの受託者

１３　再委託に関する事項

（１）　再委託の制限及び再委託を認める場合の条件

① 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（受託者の子会社（会社法第2条第3号に規定する子会社をいう。）を含む。）に再委託することはできない。また、本事業の契約金額に占める再委託金額の割合は、原則2分の1未満とすること。原則として、再委託を認める部分は「表13.（1）.①　再委託区分」に示す作業区分とする。

表13.（1）.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	・プロジェクト管理 ・脆弱性診断（Web アプリ診断） ・脆弱性診断（インフラ診断） ・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	上記を除く実作業部分	・脆弱性診断（Web アプリ診断）に係る一部作業 ・脆弱性診断（インフラ診断）に係る一部作業 ・ペネトレーションテストに係る一部作業 ・診断結果報告に係る一部作業	上記以外の部分	再委託可

② 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。なお、第三者に再委託する場合は、その最終的な責任を受託者が負うこと。
③ 再委託先が本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。
④ 受託者が再委託する事業者は、「12 (2) 入札制限」 に定める事業者及びその関連会社でないこと。
⑤ 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)及び再委託先事業者からの報告徴取方法について記載した「別紙3 再委託承認申請書」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、「再委託等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。

１４ その他特記事項

調達に係る納品物については、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)第6条に基づく環境物品等の調達の推進に関する基本方針に定める判断の基準を満たすこと。

１５ 資料等の閲覧

入札期間中に開示予定の応札希望者が閲覧できる資料は、「○技術資料一覧」を参照すること。
希望者は「別紙4 技術資料閲覧に係る実施要領」を参照し、手続きの上、閲覧すること。

別紙 1

年金業務システム（個人番号管理サブシステム（情報連携））の
脆弱性診断及びペネトレーションテスト業務

用語の定義

令和 8 年 5 月

日本年金機構 基幹システム開発部

用語		定 義 ・ 説 明
か	コアシステム	情報提供ネットワークシステムの中核的な機能を担い、情報提供に用いられる個人を特定するための符号等の付番・変換や、情報提供に係る処理の制御等を行うシステム。
	個人番号	行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）（以下「番号法」という。）第 2 条第 5 項に規定する個人番号。
	個人番号管理サブシステム	社会保障・税番号制度導入に伴う、個人番号を利用した年金記録に関する相談・照会業務等を行うため、番号紐付情報を管理する業務ソフトウェア。
	個人番号管理サブシステム（情報連携）	住基接続システム、中間サーバー、及び個人番号管理サブシステムの機能のうち、以下の機能を保有するシステムの総称。 ● 情報提供ネットワークシステムへの符号取得依頼と取得した符号の管理 ● 適用・徴収業務における外部機関保有情報の活用 ● 給付業務における外部機関保有情報の活用 ● 届書等の経過管理・電子決裁による外部機関保有情報の活用 ● 届出受理・審査業務における外部機関保有情報の活用 ● 外部機関からの照会に対する情報提供の実施 ● お知らせ情報表示機能に係る業務 ● 自己情報表示機能に係る業務 ● 情報提供等記録の追記等業務 ● 情報開示請求及び監査機関からの監査に備えた情報連携等に係る証跡管理
さ	サービスレベル合意書（SLA： Service Level Agreement）	受注者が機構との間で作業を行う際に、提供するサービスの内容と範囲、品質に対する要求（達成）水準を明確にして、それが達成できなかった場合の措置を含めて、あらかじめ合意した内容を記載した文書のこと。
	自己情報表示機能	情報提供等記録開示システムにおいて、利用者が自身の端末から情報提供ネットワークシステムを通じて自己情報の開示請求を情報保有機関に対して行い、情報保有機関からの回答を画面表示する機能。
	住基接続システム	住基ネットと接続するため、住基接続システムアプリケーションを実装し、以下の機能を保有するシステム。 ● 住基即時照会を可能とする。 ● 異動者情報照会及び生存状況照会等の一括照会を可能とする。 ● サーバーと住基ネットを接続し、住基ネットへ符号の取得依頼を可能とする。
	住基ネット	住民基本台帳法に基づき、情報システム機構が運営する住民基本台帳ネットワークシステム。

用語		定 義 ・ 説 明
	情報照会者	番号法第 19 条第 7 号に規定された情報照会者及び同条第 14 号の規定により、情報提供ネットワークシステムを使用して特定個人情報の提供を求める者。
	情報提供者	情報照会者の求めに応じて、特定個人情報を提供する者及び番号法附則第 6 条第 6 項の規定により、情報を開示又は提供する者。
	情報提供等記録	番号法 19 条第 7 号及び第 14 号の規定に基づき、情報照会者と情報提供者との間で行った、特定個人情報の提供の求め及び提供に係る記録。
	情報提供等記録開示システム	番号法附則第 5 条に基づき、情報提供ネットワークシステムに記録された利用者本人の情報に係る提供等記録の開示、情報保有機関が保有する利用者本人の情報の開示及び情報保有機関からのお知らせ情報を通知する機能を提供するシステム。
	情報提供ネットワークシステム	番号制度の導入に伴い、番号法第 2 条第 14 項に基づいて設置された、行政機関（情報照会者と情報提供者）の間を高度なセキュリティ管理とプライバシー保護の下で接続するネットワークシステム。
	情報保有機関	情報照会者及び情報提供者。
	情報連携	各情報保有機関が、情報提供ネットワークシステムを利用して行う情報の相互交換。
	処理通番	システム間における処理連携において、処理の要求時に提供した情報と処理結果として受領する情報を一意に識別するために払い出す一連の番号。
た	中間サーバー	各情報保有機関のシステムが、情報提供ネットワークシステムと接続の際に経由するシステムで、主に以下に示す機能を有するシステム。 ● 情報連携の対象となる特定個人情報の副本の保存・管理 ● インターフェイスシステムと個人番号管理サブシステムとの情報の授受の仲介 ● 情報提供等に用いる符号の管理
	特定個人情報	番号法第 2 条第 8 項に規定された、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報。
は	符号	情報保有機関が、情報提供ネットワークシステムを介して情報連携を行う際に、個人を一意に識別するために個人番号に替えて用いる識別子。 コアシステムにおいて、個人ごとかつ情報保有機関ごとに生成される。

※上記表中の「機構」は日本年金機構。

別紙２

令和　　年　　月　　日

日本年金機構　理事長代理人
基幹システム開発部長　　佐藤　利行　　殿

所　　在　　地
法人名又は商号
氏　　名　　印

守秘義務に関する誓約書

弊社は日本年金機構の下記の委託業務（以下「本業務」という。）に従事するにあたり、下記の秘密保持に関する事項を遵守することを誓約いたします。

また、本業務の全従事者について、下記の事項内容を周知しており、内容を理解し、遵守することを証明いたします。

対象業務：年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務
契約期間：令和８年６月１９日～令和９年１月２９日

記

１．本業務に従事中、本業務を通じて知り得た一切の情報（以下「秘密情報」という。）について、第三者に開示、漏えい、目的外利用、又は自ら不正に使用しないこと。
※第三者：役員等を含む情報取扱者以外の者並びに親会社・地域統括会社等を含む受託事業者以外の者（機構が承認した場合を除く）

２．本業務が終了した後においても、前項の秘密情報を第三者に開示、漏えいし、又は自ら不正に使用しないこと。

３．上記各誓約事項に違反して日本年金機構に損害を与えたときは、その損害を賠償する責任を負うこと。

４．本業務の実施にあたり、日本年金機構法（平成１９年法律第１０９号）、個人情報の保護に関する法律（平成１５年法律第５７号）及び個人情報関係諸法令を順守すること。

以上

（参考）日本年金機構法（平成１９年法律第１０９号）より抜粋
・守秘義務（第３１条第２項）：受託者等（委託を受けた者（その者が法人である場合にあっては、その役員）若しくはその職員その他の当該委託を受けた業務に従事する者）は当該業務に関して知り得た秘密を漏らしてはならない。
・罰則規定（第３１条第３項）：受託者等にも、機構役職員に対する刑法その他の罰則の適用を準用する。
・罰則（第５７条）：秘密を漏らした者は、１年以下の拘禁刑又は１００万円以下の罰金

別紙 3

令和　　年　　月　　日

日本年金機構　理事長代理人
　基幹システム開発部長　　佐藤　利行　　殿

所　在　地
法人名又は商号
代 表 者 名　　㊞

再 委 託 承 認 申 請 書

下記の年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務のうち主体的部分を除く一部について下記に記載のとおり第三者に請け負わせることを承認願います。

なお、第三者に請け負わせる業務を含む一切の業務責任は、弊社にあること、弊社は第三者に請け負わせる業務を異なる第三者に更に請け負わせないこと、また、再委託先に対しては、本契約にて弊社に課されている守秘義務等と同等以上の条件（本契約終了後の秘密保持を含む。）を遵守させるほか、日本年金機構が必要に応じ再委託先に対して調査等を実施する場合には、これに応じさせることを誓約いたします。

記

（対象案件名）　年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務

（委託部分）　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

（委託先業者名／住所／連絡先）

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

（委託する理由）　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

（委託先業者からの報告徴取方法）

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

別紙４

年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務

技術資料閲覧に係る実施要領

日本年金機構
Japan Pension Service

基幹システム開発部
令和８年５月

別紙４

令和８年５月１１日
日本年金機構
基幹システム開発部

「年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務」における技術資料閲覧に係る実施要領

「年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務」において、技術資料閲覧を希望する事業者に係る取扱いを以下のとおり定める。

１．閲覧方法

電子媒体の貸出による閲覧とする。なお、閲覧できる技術資料は、仕様書の「〇技術資料一覧」を参照すること。

２．貸出対象者

貸出対象者は、仕様書の「１２　入札参加要件に関する事項」を満たしていること。

３．使用の制限

(1) 技術資料及び技術資料から知り得た情報を仕様書に対する意思表示の検討及び見積書の算出以外に使用することは許可しない。

(2)　貸出期間中に、謄写等を行うことは許可しない。

４．法令等の遵守

「年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務」の遵守事項は、以下に示すとおりである。

(1)　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等の関連法規を遵守すること。

(2) 「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群」の内容を正しく理解し、遵守すること。

５．事前手続

貸出を希望する場合は、「７．連絡先」の担当者に対し事前に連絡すること。

６．貸出に当たっての注意事項

(1) 貸出場所

東京都杉並区高井戸西3-5-24 日本年金機構本部
基幹システム開発部　年金業務システム開発第2G

(2) 貸出期間

令和8年5月13日（水）（入札公告の2営業日後）～令和8年6月3日（水）（競争参加書類提出期限）
※営業日とは、土日祝祭日を除く平日とする。
※時間は10:00～12:00、13:00～17:00とする。

(3) 貸出及び返却手順

① 貸出を希望する営業日の2営業日前の午前10時までに、貸出希望日時、貸出対象法人等の名による「別紙4-1 技術資料の閲覧に係る同意書」の写し及び「別紙4-3 技術資料を閲覧する者の名簿」の写し、並びに「２．貸出対象者」を証明できる書類の写しを「７．連絡先」の担当者宛に電話連絡の上、別途指定するメールアドレスに送付すること。

② 貸出希望日時に、上記①の「別紙4-1 技術資料の閲覧に係る同意書」の原本及び「別紙4-3 技術資料を閲覧する者の名簿」の原本、並びに「２．貸出対象者」を証明できる書類の写しを貸出場所に持参し提出すること。

③ 技術資料一式（電子媒体）の受取の際に身分確認を行うため、社員証等、貸出対象法人等の社員等であることが確認できるものを提示すること。

④ 仕様書案に対する意思表示の検討終了後、貸出対象法人等の名による「別紙4-2 誓約書」及び技術資料一式（電子媒体）を貸出場所に持参し返却すること。

(4)　返却時期

貸出期間のうち、仕様書に対する意思表示の検討終了後、直ちに返却すること。

7．連絡先

〒168-8505　東京都杉並区高井戸西3-5-24 日本年金機構本部
基幹システム開発部　年金業務システム開発第2G
担当：藤野、本城
TEL：03-6861-8143（内線 4867）

別紙 4-1

令和　　年　　月　　日

日本年金機構　理事長代理人
　基幹システム開発部長　　佐藤　利行　　殿

住　所

法人名

代表者名

技術資料の閲覧に係る同意書

当社は、「年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務」に関する仕様書に対する意思表示の検討のため、日本年金機構（以下「貴機構」という。）から貸出を許可される技術資料について、以下に記す条項を遵守します。

なお、当社は『「年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務」における技術資料閲覧に係る実施要領』の「２．貸出対象者」に掲げる条件を全て満たしていることを保証します。

（技術資料）

第１条　当社は、本同意書でいう「技術資料」とは、技術資料一覧に定めるものと理解します。また、当該技術資料が変更される場合があることについて、同意します。

（目的外使用の禁止）

第２条　当社は、技術資料及び技術資料から知り得た情報を仕様書に対する意思表示の検討以外に使用しません。

（返却時期）

第３条　当社は、令和８年５月 13 日（水）から令和８年６月３日（水）までの間のうち、仕様書に対する意思表示の検討終了後、技術資料を直ちに返却します。

（実施場所）

第４条　当社は、技術資料を、ISO/IEC 27001 認証（国際規格）又は JIS Q 27001 認証（日本産業規格）を取得している場所（以下「実施場所」という。）にて、仕様書に対する意思表示の検討に使用します。

（技術資料の閲覧等に係る遵守条件）

第５条

１　当社は、技術資料を実施場所から持ち出し（移送時を除く。）又は複製（本件技術資料の内容に係る記述又は画像としてこれを保持する行為並びにこれらに準ずる行為等を含む。）しません。また、技術資料及び技術資料から知り得た情報を当社の従業員以外の第三者に開示、漏えい又は公開しません。

２　当社は、技術資料を閲覧する者（以下「閲覧者」という。）を定め、別紙 4-3 の様式により閲覧者の名簿を申告します。また、閲覧者に本同意書に定める条件を確実に遵守させるとともに、閲覧者の本同意書に定める条件違反について一切の責任を負います。

３　当社は、技術資料の過誤・不正確によって、当社又はこれに関して第三者に生じた損害を被ったときにも、貴機構に対し、損害賠償請求その他一切の請求を行いません。

４　当社は、貴機構への技術資料の返却に際し、確実に全ての情報を返却し、かつ、作成された二次的情報を確実に抹消し、複製を含め保持していない旨の誓約書を提出します。

５　当社は、移送責任者を決め、責任者を含めた 2 名以上で施錠可能な移送用のカバン等を使用して、技術資料を移送します。

（調査）

第６条　当社は、貴機構において本同意書が遵守されていることの確認を行う必要があると判断した場合は、貴機構が当社に報告を求めること又は貴機構担当者及び貴機構の指定する者を当社の事業所等に派遣して調査することに、同意します。

（権利付与）

第７条　当社は、技術資料が開示されたことによって、当社に何等新たな権利が付与されるものではないことについて、了解します。

（損害賠償）

第８条　当社が貴機構に損害を与えた場合は、当社は、貴機構に対し一切の損害を賠償します。また、損害には、貴機構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ことに、同意します。

（管轄裁判所）

第９条　本同意書に関する一切の紛争は、東京地方裁判所を第一審の専属の合意管轄裁判所とします。

（協議）

第１０条　本同意書に定めのない事項、その他本同意書の条項に関して疑義が生じたときは、貴機構と当社の協議により、円満に解決を図ります。

別紙 4-2

令和　　年　　月　　日

日本年金機構　理事長代理人
　基幹システム開発部長　　佐藤　利行　　殿

住　所

法人名

代表者名

誓約書

当社は、「年金業務システム（個人番号管理サブシステム（情報連携））の脆弱性診断及びペネトレーションテスト業務」に関する仕様書の意思表示の検討のため、日本年金機構から貸出を許可されていた技術資料について、「技術資料一覧」に記載されている全ての情報を返却し、かつ、二次的情報を抹消しており、複製を含め保持していないことを誓約いたします。

以上

別紙 4-3

技術資料を閲覧する者の名簿

	部署名	役職	氏名	連絡先	国籍
1					
2					
3					
4					
5					
6					
7					
8					
9					
１０					
１１					
１２					
１３					
１４					
１５					