導入時脆弱性診断業務一式

仕様書

Vulnerability Assessment at the time of Installation

1 Set

国立大学法人一橋大学

2025 年 1 月

目次

1. 委託業務の概要

1.1. 目的

昨今頻発する政府機関や重要インフラ関連企業等に対する、標的型攻撃や DDoS 攻撃等の脅威に対し、一橋大学（以下「本学」という。）では、一橋大学情報セキュリティポリシー等を定め、様々な観点から情報セキュリティ対策の強化や高度化に取り組んでいるところである。

本件は本調達と同時期に別途更新が予定されている「業務系情報基盤システム」の次期基盤（学内の各種業務系情報システムのサーバ、ストレージ、ネットワーク等のシステムリソースを集約して管理するパブリッククラウドのシステム基盤。以下「クラウド基盤」という。）、セキュリティネットワーク機器（ファイアウォール等）及びクラウド基盤上で稼働する以下のシステムを対象に、構築導入するシステム等に脆弱性がないかセキュリティの担保を目的とした脆弱性診断業務を調達するものである。

- 人事給与統合システム
- マイナンバーシステム
- 勤怠管理システム
- 財務会計システム
- 入退管理システム
- 図書館情報システム
- 構成員情報管理システム
- 統合 ID 管理システム
- グループウェア
- 学務情報システム
- 文書管理システム

2. 作業内容・納入成果物等

2.1. 作業内容

本調達における作業は、以下のとおりである。

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　診断作業

ウ　診断結果報告書

エ　ウや成果物についての本学からの問合せに対する対応

役務内容の詳細は、「４．　作業要件」に記述されている項目とする。

また、作業スケジュールの想定案としては、「表２．１．１　主要マイルストン一覧」のとおりである。

なお、スケジュールについては、契約締結後、クラウド基盤構築業者や各部局のシステム構築業者等との協議により決定するものとする。

表２．１．１ 主要マイルストン一覧

項番	主要マイルストン	想定するスケジュール案
1	契約締結	令和 ７年 4月 上旬
2	脆弱性診断役務開始	令和 ７年 4月 中旬
3	事前相談・ヒアリング・日程調整	令和 ７年 4月～5月
4	脆弱性診断の実施	令和 ７年 7月～8月
5	診断結果報告書・報告会	令和 7年 9月 10日まで
6	契約履行期限	令和 7年 9月 30日

2.2. 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）及び本学国立キャンパス内とする。

ただし、診断作業等のため本学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本学の指示する場所で作業すること。

本学国立キャンパス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。

2.3. 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２．３．１ 報告会」のとおりとする。

なお、報告会は本学が指定した日時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２．３．１ 報告会

項番	内容等	実施タイミング	開催形式	開催頻度
1	診断結果報告書について、情報推進課・各システム担当課向けの報告会を実施する。	各システムの診断報告書作成後	オンライン	1回以上

2.4. 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２．４．１ 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２．４．１ 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本学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２．４．１ 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、「４．　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。）、本学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、各システム別に「４．　作業要件」の表４．２．１及び表４．３．１のとおり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本学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	令和７年9月１０日まで 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本学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7年9月30日まで見直し・修正時は随時

2.5.　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（媒体種類は本学の指定による。）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、本学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 2021」、「Microsoft Excel 2021」、又は、「Microsoft PowerPoint 2021」（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。本学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、本学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２．４．１ 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本学に提出すること。

⑦ 「表２．４．１ 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、本学の指示により、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２．４．１ 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２．４．１ 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。

2.6.　納入期限及び納品場所

納入期限は 2025 年 9 月 30 日（火）とし、納入場所は本学国立キャンパスとする。

2.7.　検査

①　成果物の検査は、「表２．４．１　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本学の検収、承認をもって完了するものとする。

3.　情報セキュリティ要件

3.1.　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 政府機関等のサイバーセキュリティ対策のための統一基準群

② 国立大学法人一橋大学情報セキュリティ対策規程

③ 一橋大学 情報セキュリティ対策基準

④ 一橋大学 サイバーセキュリティ対策等基本計画

上記の③及び④は非公表であるが、③は②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、契約締結後に必要に応じて本学より開示するものとする。
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。

3.2.　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、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　本学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　受託者は、本業務の実施のために本学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、本業務において本学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・情報については本学と協議し、本学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、「３．１　基本事項」における④の手順書に基づき本学へ報告し迅速に対応すること。

⑥　受託者は、本部及びその他本学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。

3.3.　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、速やかに本学に報告すること。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本学の情報の外部への漏えい及び目的外利用

イ　受託者による本学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、本学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、本学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、本学と協議を行い、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、本学の求めに応じ、本学と協議を行い、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。

4. 作業要件

4.1. 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、診断実施中に本学のシステムの停止・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、速やかに本学に連絡すること。

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、本学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クラウド基盤及び各情報システムの構築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４．１．１ 脆弱性診断ツール」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、専門家による手動の診断も実施すること。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４．１．１ 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 (WEB診断)	・Vulnerability Explorer(VEX) ・HCL AppScan ・Burp Suite Professional
2	プラットフォーム診断 (PF診断)	・QualysGuard ・Tripwire IP360 ・Nessus ・Metasploit ・OpenVAS

⑥ オンサイトでの診断について、診断用機器を持ち込む場合は事前にウイルスチェック確認票を提出し本学の承諾を得ること。

⑦ 診断の実施時期については、令和７年８月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（国民の祝日に関する法律に規定する休日、１２月２９日

から１月３日及びその他本学の休業日以外の日。）の８：３０～１７：１５とする。

⑧　診断範囲を表４．１．２に示す。

表４．１．２　診断範囲

項番	システム名	脆弱性診断	
		PF診断	WEB診断
1	人事給与統合システム	○	○
2	マイナンバーシステム	○	○
3	勤怠管理システム	○	○
4	財務会計システム	○	○
5	入退管理システム	○	－
6	図書館情報システム	○	○
7	構成員情報管理システム	○	○
8	統合ID管理システム	○	○
9	グループウェア	○	○
10	学務情報システム	○	○
11	文書管理システム	○	○
12	運用系サーバ（SMTPサーバ、ファイルサーバ等）	○	－
13	物理ファイアウォール装置	○	－

⑨　オンサイトの診断拠点は本学国立キャンパスとする。

⑩　表４．２．２に記載の診断対象サイト数、表４．３．２に記載の診断対象 IP アドレス数は構築前の想定であり、実際の数は協議により決定すること。

4.2.　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（学内ネットワーク）からのオンサイト診断を行う。

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４．２．１に示す。

表４．２．１ 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	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
14	ファイルアップロードに関す	展開すると数GBになる圧縮ファイル（ZIP BOMB）の有無など

	る不備	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
18	クロスサイトWebSocket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

② 脆弱性診断の対象サイト

脆弱性診断を実施する画面については、対象サイト内で、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。

サイト数は FQDN 単位とし、診断対象のサイト数の内訳については表４．２．２に示す。

診断対象の画面数（リクエスト数）の上限は、リモートは５０画面、オンサイトは１０画面とする。なお、同じ FQDN でポート番号が異なる場合であっても、１サイトとして扱うこととする。

表４．２．２ 診断対象サイト数

項番	情報システム	診断実施場所	
		リモート	オンサイト
1	人事給与統合システム	１サイト	１サイト
2	マイナンバーシステム	－	１サイト
3	勤怠管理システム	－	１サイト
4	財務会計システム	－	２サイト
5	図書館情報システム	１サイト	２サイト
6	構成員情報管理システム	－	２サイト

7	統合ID管理システム	２サイト	３サイト
8	グループウェア	１サイト	１サイト
9	学務情報システム	２サイト	１サイト
10	文書管理システム	－	１サイト

4.3.　プラットフォームの脆弱性診断の作業要件

①　脆弱性診断の観点

プラットフォームの脆弱性診断では、システムの外側（インターネット経由）からのリモート診断及び内部（学内ネットワーク）からのオンサイト診断を行う。

また、診断対象のIPアドレスは契約締結後に本学より開示する。

プラットフォーム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４．３．１に示す。

表４．３．１ 診断事項（プラットフォーム）

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、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の設定不備	オープンリゾルバ、ゾーン転送の設定不備等を確認する。
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４．３．２に示す。

表４．３．２ 診断対象ＩＰアドレス数

項番	情報システム	診断実施場所	
		リモート	オンサイト
1	人事給与統合システム	１IPアドレス	２IPアドレス
2	マイナンバーシステム	－	２IPアドレス
3	勤怠管理システム	－	２IPアドレス
4	財務会計システム	－	４IPアドレス
5	入退管理システム	－	１IPアドレス
6	図書館情報システム	１IPアドレス	４IPアドレス
7	構成員情報管理システム	－	４IPアドレス
8	統合ID管理システム	４IPアドレス	９IPアドレス
9	グループウェア	１IPアドレス	３IPアドレス
10	学務情報システム	６IPアドレス	３IPアドレス
11	文書管理システム	－	１IPアドレス
12	運用系サーバ（SMTPサーバ、ファイルサーバ等）	－	１８IPアドレス
13	物理ファイアウォール装置	－	１IPアドレス

5. 作業の体制及び方法

5.1. 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、書面にて本学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、原則として本学との会議及び本学への報告会に出席すること。なお、本学との会議等に出席できない場合は事前に本学の了解を得ること。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１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。

5.2.　作業方法等

①　進捗管理

脆弱性診断業務について、受託者は、「業務実施計画書」に基づき、「４．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、報告書を本学へ送付すること。

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、本学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、本学の承認を得ること。

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「情報セキュリティ対策基準」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５.１.②、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、本学の承認を得ること。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、本学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、事前に本学の承認を得ること。

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、本学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、本学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本学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、本学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　本学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、速やかに本学に報告し、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。

5.3.　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４．２．１に記載の脆弱性、表４．３．１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。

6.　特記事項

6.1.　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。

6.2.　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本学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、事前に本学へ報告し、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本学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、本学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。

6.3. 再委託

受託者が本調達・役務内容の一部を外部に再委託する場合は、本学の了解を得なければならない。また、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本仕様書と同水準の措置の実施を再委託先にも担保すること。

6.4. 機密保持

① 受託者は、本受託業務の実施の過程で本学が開示した情報（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、本学から入手した資料、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、あらかじめ本学と協議を行い、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日以内に本学に返却すること。

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本学へ提出すること。

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、本学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 本学秘密情報の取扱いにおいて、再委託をする場合は、本学の了解を得なければならない。

本システムの開発及びカスタマイズに関して、業務の再委託を行う場合は、委託先企業についても本義務を遵守させること。

⑤　応札希望者についても、上記①から④に準じること。

6.5.　提案に関する留意事項

①　提案書は日本語で具体的に記述すること。

②　提案書には、本仕様書の要件（２．作業内容・納入成果物等、３．情報セキュリティ要件、４．作業要件、５．作業の体制及び方法、６．特記事項に記載の全ての要件）の各項目とそれに対する提案内容を明確かつ簡潔に示した対照表を添付すること。

③　提案書には以下の項目を明瞭に記載すること。

ア　診断業務の実施方針等

イ　本業務の前提条件（要求を満たす作業スコープの設定等）

ウ　診断の具体的な手順と確実な手順実行の仕組み

エ　品質確保のための方策（診断品質確保の具体的な手法、体制等）

オ　作業計画と体制（再委託する場合は委託先の体制も含む）

カ　本事業実施の、体制、環境及び類似事業の実績、業務ノウハウの蓄積等の実施能力

キ　業務従事者の過去の経験、業務遂行上有効な知識の有無等。

ク　ワーク・ライフ・バランス等の推進に関する指標

ケ　その他、提案内容を説明するために必要な資料

④　提案書に疑義が生じた場合、詳細な資料の提出を求めることがある。また、必要に応じ、提案物品についてサンプルの提供やデモンストレーションの実施を求めることがある。

⑤　提出要領

ア　提出先及び提出期限は入札説明書を参照すること。

イ　紙媒体で 3 部、電子媒体で 1 部提出すること。

ウ　電子データを格納する媒体の種別は CD-R 又は DVD-R とする。また、データの形式はマイクロソフト社の Office 製品で可読なこと。

エ　納入媒体及びデータについては、ウィルス等を混入させないように、納入前に受託者側で責任をもってチェックを行うこと。

オ　紙媒体でしか納入できないもの（手書き図面等）又は電子データのみで納入する方が効率的であるもの（膨大なログデータ等）の納入方法については、受託者と本学が協議して決定すること。

カ　問い合わせの受付については、入札説明書を参照すること。

6.6.　その他遵守事項

本調達仕様書は、本システムの脆弱性診断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. 総合評価基準

7.1. 脆弱性診断業務の総合評価基準

本調達に係る入札の評価に関する基準は次のとおりとする。

① 落札方式

ア 次の各要件に該当する入札者のうち、以下に示す総合評価の方法によって得られた数値の最も高い者を落札者とする。

⑴ 入札価格が、予定価格の制限の範囲内であること。

⑵ 性能等が、仕様書において明らかにした性能等の要求要件のうち、必須とされた項目の最低限の要求要件を全て満たしていること。

イ 上記アの数値の者が 2 人以上あるときは、当該者にくじを引かせて落札者を定める。

② 総合評価の方式

ア 仕様書に記載する要件を満たしているか否かの判定及び総合評価基準に基づき付与する得点の判定は、複数の本学技術審査職員が仕様書その他の入札説明書で求めた提案資料の内容を審査して行う。

イ 入札価格に対する得点配分と、性能等に対する得点配分は等しいものとする。

ウ 入札価格の評価方式については、以下のとおりとする。

入札得点は、入札価格を予定価格で除して得た値を一から減じて得た値に、入札価格に対する得点配分を乗じて得た値とする。

$$入札価格に係る評価点 = \left(1 - \frac{入札価格}{予定価格} \right) \times 入札価格に係る得点配分$$

エ 性能等の要件については、本仕様書の２．作業内容・納入成果物等、３．情報セキュリティ要件、４．作業要件、５．作業の体制及び方法、６．特記事項に記載の全ての要件に記載の全ての要件とし、これらの中で必要性を明記した（～すること。等）全ての要件を必須の要求要件とする。

オ 性能等の評価方法については、以下のとおりとする。

⑴ 評価の対象とする要件については、当該調達の目的、内容に応じて必要性等の観点から評価項目を設定し、これを必須とする項目とそれ以外の項目とに区分する。

⑵ 必須とする項目については、項目ごとに最低限の要求要件を示し、この要求要件を満たしていない者は不合格とし、要求要件以上の部分については評価に応じ得点を与える。

⑶ 必須とする項目以外の項目は、項目ごとに評価に応じ得点を与える。

⑷ 各評価項目に対する得点配分は、その必要度・重要度に応じて定める。

カ 総合評価は、入札者の入札価格の得点に当該入札者の申し込みに係る性能等の得点の合計を加えて得た数値をもって行う。

7.2.　性能等に対する評価項目と得点配分基準

①　必須項目

項目	基礎点
本仕様書の要求要件（２．作業内容・納入成果物等、３．情報セキュリティ要件、４．作業要件、５．作業の体制及び方法、６．特記事項）の全てについて、最低限の必須とする要求要件を満たしていること。必須とする要求要件を満たしていない場合は、不合格とする。	50

②　加点基準

項番	加点対象項目	加点
2.1.	本業務を品質を確保しつつ効率的・効果的に実施するための方針（診断の具体的な手順や確実な手順実行の仕組み等を含む）が示されている場合は加点とする。	6
2.1.	検出された脆弱性に対して、リモートで再診断を 1 回まで無償で実施することが示されている場合は加点とする。	6
2.3.	報告会の開催頻度が 2 回以上の場合は加点とする。	5
2.4.	診断の結果報告として、「表２．４．１ 成果物及び納品期日一覧表」に示す記載内容を含む報告書の作成が、サンプルを掲載する等して日本語で具体的に示されている場合は加点とする。	5
4.2.	Web アプリケーション診断の対象サイトに対して事前調査（クローリング）を実施し、診断が必要な画面遷移を本学と協議の上決定することが示されている場合は加点とする。	6
4.2.	Web アプリケーション診断の対象画面数について、+10%まで許容する場合は加点とする。	6
5.1.	作業責任者は過去に類似の診断業務を行った経験があり、過去 1 年以内に 10 件以上の診断業務（自社内の社内システムの診断は除く）を行った実績を持っていることが示されている場合は加点とする。	6
5.1.	作業従事者のうち１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場合は加点とする。 ・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)	5

	・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	
(下表参照)	ワーク・ライフ・バランス等の推進に関する指標（※）	5
計		50

※ワーク・ライフ・バランス等の推進に関する指標

加点対象項目　（認定等の区分 ※1）		加点
女性活躍推進法に基づく認定を受けている	プラチナえるぼし（※2）	5
	認定段階 3（※3）	4
	認定段階 2（※3）	3
	認定段階 1（※3）	2
	行動計画（※4）	1
次世代法に基づく認定を受けている	プラチナくるみん（※5）	5
	くるみん(令和 4 年 4 月以降基準)（※6）	3
	くるみん(平成 29 年 4 月-令和 4 年 3 月基準)（※7）	3
	トライくるみん（※8）	3
	くるみん(平成 29 年 3 月以前基準)（※9）	2
若者雇用促進法に基づく認定（ユースエール認定企業）		4
計		5

※1 複数の認定等に該当する場合は、最も配点が高い区分により加点を行うものとする。

※2 女性の職業生活における活躍の推進に関する法律等の一部を改正する法律(令和元年法第 24 号)による改正後の女性活躍推進法第 12 条の規定に基づく認定

※3 女性活躍推進法第 9 条に基づく認定。なお、労働時間等の働き方に係る基準は満たすことが必要。

※4 常時雇用する労働者の数が 100 人以下の事業主に限る(計画期間が満了していない行動計画を策定している場合のみ)。

※5 次世代法第 15 条の 2 の規定に基づく認定

※6 次世代法第 13 条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則の一部を改正する省令(令和 3 年厚生労働省令第 185 号。以下「令和 3 年改正省令」という。)による改正後の次世代育成支援対策推進法施行規則(以下「新施行規則」という。)第 4 条第 1 項第 1 号及び第 2 号の規定に基づく認定

※7 次世代法第 13 条の規定に基づく認定のうち、令和 3 年改正省令による改正前の次世代育成支援対策推進法施行規則第 4 条又は令和 3 年改正省令附則第 2 条第 2 項の規定に基づく認定(ただし、※9 の認定を除く。)

※8 次世代法第 13 条の規定に基づく認定のうち、新施行規則第 4 条第 1 項第 3 号及び第 4 号の規定に基づく認定

※9 次世代法第 13 条の規定に基づく認定のうち、次世代育成支援対策推進法施行規則等の一部を改正する省令(平成 29 年厚生労働省令第 31 号。以下「平成 29 年改正省令」という。)による改正前の次世代育成支援対策推進法施行規則第 4 条又は平成 29 年改正省令附則第 2 条第 3 項の規定に基づく認定

以上