大阪府立大学部局サーバ・Web サイト
セキュリティ診断業務委託仕様書

1. 業務名

大阪府立大学部局サーバ・Web サイトセキュリティ診断

2. 診断目的

大阪府立大学（以下「本学」という。）の各部局がインターネットに公開している Web サイトの多くは、情報基盤センター管理の大学標準 CMS サーバ（以下、CMS サーバという）に集約しており、公開 Web サイトのセキュリティを全体で強化している。

しかし、一部の Web サイトについては、様々な理由により、各部局で個別に運用されており、セキュリティ対策もそれぞれに委ねられている。

これら部局サーバで運用されている Web サイトについて、第三者による攻撃を想定した部局サーバ本体・Web サイトの OS・ミドルウェアの欠陥、設定不備等の脆弱性を客観的に把握し、その対策方法を明らかにすることを目的とする。

3. 委託期間

契約締結の日～2021 年 1 月 29 日（金）

4. 診断対象、診断項目及び調査方法

本学の部局サーバ及び Web サイトのセキュリティ状況の診断を実施するものとする。

(1) 部局サーバ本体（OS、ミドルウェア等）の脆弱性診断

・診断対象の部局サーバは、本学が指定するインターネットからアクセス可能なグローバル IP アドレス（以下 IP という）が付与された部局サーバ 8 IP とする。

【部局サーバ本体の脆弱性診断項目】

・ポートスキャン・サービススキャン（TCP、UDP）
・FTP の脆弱性診断
・SSH の脆弱性診断

・Telnet の脆弱性診断
・SMTP の脆弱性診断（不正中継、アカウント推測を含む）
・POP の脆弱性診断
・DNS の脆弱性診断
・Finger の脆弱性診断
・HTTP/HTTPS の脆弱性診断
・NTP の脆弱性診断
・SNMP の脆弱性診断
・R 系コマンドの脆弱性診断
・NetBIOS の脆弱性診断
・SMB/CIFS の脆弱性診断
・RPC の脆弱性診断
・不正プログラムやセキュリティホールの有無チェック（トロイの木馬、バックドア等）
・セキュリティパッチ未適用による脆弱性診断
・その他必要な項目

⑵　Web サイトの脆弱性診断
・診断対象の Web サイトは、部局サーバ上で稼働している 70～80 サイトについて、1 サイト当たり 5 画面とする。

【Web サイトの脆弱性診断項目】
・ユーザ認証の脆弱性（不備）
・SQL インジェクション
・OS コマンド・インジェクション
・バッファオーバーフロー
・パストラバーサル
・アクセス制御の脆弱性
・ディレクトリ・リスティング
・セッション管理の脆弱性
・クロスサイト・スクリプティング
・クロスサイト・リクエスト・フォージェリ
・メールヘッダ・インジェクション
・意図しないリダイレクション
・HTTP ヘッダ・インジェクション
・通信の暗号化
・その他必要な項目

⑶　調査方法
・最新の共通脆弱性評価システムに適応した診断ツール等を使用して、脆弱性診断を行うこと。

・部局サーバ・Web サイトの診断について、リモート、オンサイトを問わない。但し、診断に必要な学内手続きが発生した場合は速やかに報告・処置を行い、本学からの連絡に対して即座に回答できる体制をとること。
・診断を実施する際は、診断日程の調整、診断内容の周知、診断に伴う注意、診断に際し必要な確認事項、受託者の情報について、本学が事前に各部局サーバ管理者に連絡を行う。但し、診断開始の連絡及び診断終了の連絡は受託者が行うこと。
・診断ツール等を使用して発見した脆弱性について、誤検出かどうかをマニュアル（手動）診断で再確認し、必要に応じて Web サイト管理者へ問い合わせること。

5. 委託内容

(1) 診断実施計画書の作成

部局サーバ・Web サイトのセキュリティ診断について、診断項目、診断内容、診断方法、実施スケジュール等を具体的に記載した診断実施計画書、及び実施体制図を作成すること。また、診断スケジュールは部局サーバ・Web サイトそれぞれの実施日時が分かるように計画すること。

その際、診断を実施するうえで本学が行う作業等について明示し、その内容について本学の承認を得ること。

(2) 全体報告書の作成

実施目的、対象部局サーバ、診断内容、実施結果（実施日時、脆弱性が検知された部局サーバ数、脆弱性の危険度）、主な脆弱性対策等について、エンドユーザにも理解可能な内容で、A4 両面で 2~3 枚程度にまとめること。また、以下の資料も添付すること。なお、それらの内容について本学の承認を得ること。

○検出された脆弱性一覧（部局サーバ診断・Web 診断　※脆弱性に連番を付すこと）
○判定結果別部局サーバ一覧（部局サーバ診断・Web 診断）
○部局サーバ別・Web サイト別脆弱性検出件数一覧（部局サーバ診断・Web 診断）
○脆弱性別部局サーバ一覧（部局サーバ診断・Web 診断）

(3) 部局サーバ別の診断結果報告書の作成

部局サーバ本体に係る脆弱性診断の結果を、部局サーバ別に診断結果報告書として作成すること。また、その内容について本学の承認を得ること。

報告書には、部局サーバごとに脆弱性の有無・脆弱性の内容・その脆弱性を放置した場合のリスクについての説明、部局サーバ管理者が対策すべき（OS、Apache 等のバージョンアップ・セキュリティパッチ適用等以外）と思われる脆弱性についてはその対策方法（手順）について、具体的にエンドユーザにも分かる内容で記述すること。

(4)　Web サイト別の診断結果報告書の作成

Web サイトに係る脆弱性診断の結果を、Web サイト別に診断結果報告書として作成すること。また、その内容について本学の承認を得ること。

報告書には、Web サイトごとに脆弱性の有無・脆弱性の内容・その脆弱性を放置した場合のリスクについての説明、Web サイト管理者が対策すべきと思われる脆弱性についてはその対策方法（手順）について、具体的にエンドユーザにも分かる内容で記述すること。

(5)　情報基盤センター向け全体説明会

情報基盤センター向けに、(2)全体報告書用いて全体状況について説明すること。また、(3)部局サーバ別の診断結果報告書、(4)Web サイト別の診断結果報告書を用いて、脆弱性の内容と脆弱性を放置した場合のリスク、脆弱性ごとの対策方法（手法）について、具体的に説明すること。

なお、全体説明会は、(6)の管理者向け個別説明会を行う前に実施するものとする。また、日程調整と場所の確保は本学が行う。

(6)　部局サーバ管理者向け個別説明会

(3)部局サーバ別の診断結果報告書、(4)Web サイト別の診断結果報告書を用いて、脆弱性の有無、脆弱性の内容と脆弱性を放置した場合のリスク、脆弱性ごとの対策方法（手順）について、コンピュータの専門家ではない管理者にも理解できるよう、具体的に説明すること。

なお、個別説明会は部局サーバごとに行うものとし、日程調整と場所の確保は本学が行う。

(6)　個別質問対応

結果報告書の内容についての管理者等からの質問に対しメール及び電話での個別対応を行うこと（2021 年 1 月 22 日まで）。

また、個別説明会及び個別質問対応で対応した内容について、一覧表にまとめて提出すること。

6. スケジュールの目安

診断完了期限	2020 年 10 月 30 日（金）
全体報告書・診断結果報告書提出期限	2020 年 11 月 27 日（金）
全体説明会・個別説明会	2020 年 12 月 28 日（月）までに完了
個別質問対応期間	2021 年 1 月 22 日（金）
成果物納品期限	2021 年 1 月 29 日（金）

7. 成果物の内容、納期、納品方法等

(1) 成果物の内容

下記の成果物を、印刷物（A4 判簡易製本）及び電子媒体（CD-ROM）により、必要数提出すること。なお、電子媒体におけるデータの形式は Word、Excel、PowerPoint、PDF を基本とし、それ以外のデータ形式を用いる場合は別途相談すること。

・成果物：診断実施計画書（スケジュールを含む)、全体報告書、部局サーバ別の診断結果報告書、Web サイト別の診断結果報告書、全体説明会・個別説明会・個別質問対応期間の記録

・提出物数：印刷物は各 2 部、電子媒体は 1 枚

(2) 最終納期

2021 年 1 月 29 日（金）

(3) 納品先

大阪府堺市中区学園町 1 番 1 号（C5 棟 3 階）

公立大学法人大阪　法人事務局　法人管理部　情報推進課（大阪府立大学担当）

(4) 成果物等の取扱い

① この業務委託の成果物に関する著作権は、検査完了の時をもって受託者から委託者に移転及び帰属するものとする。また、受託者は本件業務の成果物に関する著作者人格権を一切行使しないものとする。

② 委託者は、受託者に了解を得ることなく、成果物を複製・翻案し、公益上の目的に限り、これを第三者に利用させることができる。

③ 受託者は、成果物を複製し、これを第三者に譲渡又は承継させてはならない。但し、委託者が承諾した場合はこの限りでない。

④ 上記③の場合においては、委託者と受託者において、別途協定を締結するものとする。

⑤ 受託者は、この業務委託の成果物が第三者の特許権、その他の知的財産権及びノウハウに関する権利（以下「知的財産権等」という。）を侵害していないことを保証し、紛争が生じた場合は、受託者の責任と負担において解決するものとする。

8. 実施体制

① プロジェクト管理者（本学との連絡・調整及び診断作業の進捗管理・報告会主宰)、診断作業者、営業窓口担当者等で構成されるチームを編成すること。また、契約締結後、実施体制表を速やかに提出すること。

② この業務の実施に当たり、必要十分な人員で編成すること。なお、一人が複数の役割を兼ねてはならない。

③　本学が実施体制に問題があると判断し人員交代の要請を行った場合は、速やかに対応すること。

9. 委託業務の実施方法

業務の実施にあたっては以下の方法により行うものとする。

①　契約締結後、受託者は 14 日以内に診断項目、診断内容、診断方法、実施スケジュール等を具体的に記載した診断実施計画書、及び実施体制図を提出し、本学及び受託者の協議により委託業務の詳細内容及び各作業の実施時期を決定するものとする。

②　診断等のために引用又は参照する資料については、信頼しうる配布元から受託者が自らの負担で入手すること。

③　スケジュールに基づいた業務の進捗状況について、本学の求めに応じ、随時委託作業の報告や委託内容に関する資料の提出を行うこと。

④　本学の求めに応じ、キックオフ、診断実施計画書の説明、全体報告書・診断結果報告書の説明、個別説明会の報告、その他必要に応じて随時、本学との打合せを実施すること。また、その際の議事録も含め、すべての打合せにおいて議事録を作成すること。なお、議事録については、各打合せ終了後 7 日以内に提出するものとする。

⑤　その他必要な事項については、本学及び受託者による協議の上、決定する。

10. その他

①　受託者は、この契約に関して知り得た情報及び契約履行過程で生じた納入成果物等に関する情報を、この契約の目的外に使用又は、第三者に開示もしくは漏らしてはならない。そのために必要な措置を講じなければならない。委託者の承諾を得て、再委託した場合の再委託先も同様である。このことは、この契約終了後も同様とする。

②　受託者は、この契約に基づく業務を処理するために本学から提供された資料等を、本学の承諾なく複写及び複製してはならない。また、契約終了後は、速やかに本学に返却しなければならない。なお、提供された資料のうち、個人情報保護に係るものは、施錠した保管庫等で保管する等、適切に管理しなければならない。

③　この業務に必要な機器類の調達、通信費等は、この契約に含めるものとする。

④　受託者は、この契約に関して保護すべき情報を取り扱った担当者の所属・氏名等の一覧を本学に提出すること。

⑤　この仕様書に定めのない事項及び解釈上の疑義が生じた場合は、本学及び受託者による協議の上、決定する。

以上