# ウェブアプリケーション及びプラットフォーム脆弱性診断業務
# 仕様書

## 1　委託業務名
ウェブアプリケーション及びプラットフォーム脆弱性診断業務

## 2　業務の目的
昨今、国内外においてインターネット上で公開されているサーバに対する不正アクセス等により、改ざんやサービス停止等の被害が増加している。

札幌市中央図書館公式ホームページが公開しているウェブサイトやウェブアプリケーション等（以下、「サイト」と言う。）がこのような被害に遭うことを未然に防止するため、脆弱性診断を実施し、対策が必要な事項があった場合は対応策を明らかにすることを目的とする。

## 3　対象となる業務委託範囲、内容
### （１）脆弱性診断
札幌市中央図書館が公開しているサイトのうち、新たに追加されたものや、前回の診断から一定期間を経過したサイト等に対して、ウェブアプリケーション診断及びプラットフォーム診断を実施し、改善策等を提案すること。

検出した脆弱性は共通脆弱性評価システム（CVSS）v4.0に準拠して評価すること。

診断期間中に緊急度の高い脆弱性が発見された場合は、診断途中であっても、検出後翌営業日までに、速報としてメールにて報告すること。当該報告においては、下記の内容を含むこと。

ア　脆弱性名
イ　脆弱性のリスク
ウ　検出日付
エ　URL
オ　修正方法

#### ①　ウェブアプリケーション診断
診断対象とするウェブアプリケーションに対し、インターネット側からの疑似攻撃等を実施することにより、脆弱性診断を実施すること。

診断対象は札幌市中央図書館が管理する「https://www.library.city.sapporo.jp/licsxp-opac/」のURLから始まるページで、2IP、合計30ページ以内とし、詳細については委託者との打ち合わせにおいて決定すること。

事前に合意した診断対象の全パラメータに対して、診断を行うこと。診断においては、ツール等を用いて検査を行った場合でも、診断員がサーバからの応答を確認し、脆弱性の有無を判定すること。また、診断項目には「別添１」を含めて実施すること。その他に有益な結果を得られる診断手法がある場合は提案すること。

実施日時は、受託者より提案を受けたスケジュールの範囲で個別に調整して決定するものとし、原則として業務期間中の平日日中（8時45分から17時15分まで）に実施すること。

事前の診断対象の確認作業及び本番の診断作業は、原則、受託者が指定する日本国内の任意の場所から実施すること。また診断元のグローバルIPアドレスは、事前に委託者に提示すること。

#### ②　プラットフォーム診断
ウェブサイトを構成するサーバ、ネットワーク機器等に対し、インターネット側からの探査活動（ポートスキャン、IPスキャン等）を含めた疑似攻撃等を行うことによる脆弱性診断を実施すること。

診断手法は「ツール診断」を主とすること。また、診断項目には「別添２」を含めて実施すること。その他に有益な結果を得られる診断手法がある場合は提案すること。

実施日時は、受託者より提案を受けたスケジュールの範囲で個別に調整して決定するものとし、原則として業務期間中の平日日中（8時45分から17時15分まで）に実施すること。

事前の診断対象の確認作業及び本番の診断作業は、原則、受託者が指定する日本国内の任意の場所から実施すること。また診断元のグローバルIPアドレスは、事前に委託者に提示すること。

（２）報告書

脆弱性診断の結果を分析し、報告書として取りまとめ、業務履行期限内に提出すること。報告書は最低限以下の内容を含め、部門責任者や他部局等への説明及び必要に応じて外部の監査機関等への提出があることを踏まえて、図表を用いる等可視化の工夫を行うこと。また、危険度「低」に満たない非常に低い脅威レベルであるもののセキュリティ上好ましくないと考えられる事項についても、報告に含めること。

加えて、以下の内容を必ず含むこととする。

ア　診断結果全体の評価

イ　診断対象ごとに検出された脆弱性の情報（概要）・脅威レベル・影響・対策方法

ウ　脆弱性を検出した全てのパラメータ・入力文字列・確認したログ（脆弱性別に取りまとめること）

報告書には、診断の結果概要、発見した脆弱性・問題点に関するリスク分析を含めること。またリスクの度合いを高・中・低等の段階で示すこと。また具体的な回避策や改善策等を含めること。

４　成果物の納入場所

札幌市教育委員会中央図書館調整担当課
（札幌市中央区南22条西13丁目1-1）

５　業務履行期限

契約締結の日から令和９年３月31日まで

６　納品物

納品物一式を書類、CD-R等のメディア（Word、Excel、PowerPoint、PDF又は協議のうえ委託者が認める形式のファイル）として最低1部ずつ納品すること。

納品物には、以下を含めるものとする

（１）診断結果及び結果の分析・改善策の提案等の報告書

（２）その他、本業務で作成した資料、書類等一式

７　環境に対する配慮

本業務の遂行にあたっては、札幌市役所の環境マネジメントシステムに準じ、当該業務に直接的に従事する作業員はもとより、直接的に従事しない作業員についても、常に環境負荷が最小となるよう熟慮し行動すること。

（１）電気

動作確認等においては、必要最低限の機器及び時間にて対応できるようあらかじめ対応の手順を決めておくこととし、節電を図ること。

（２）公共交通の利用

業務遂行にあたり、打ち合わせ等で移動する場合には、自動車利用を控え、公共交通機関を利用することにより、環境負荷の低減を図ること。

（３）紙の使用

機器の使用上やむを得ない場合を除き再生紙を利用するとともに、最低限の枚数で

完了するようあらかじめ手順を決めておくこと。また、委託者への業務実施報告等の事務手続きに係る文書等については再生紙を使用するとともに両面印刷や必要最低限の部数・枚数にする等、紙の使用量の削減に努めること。

（４）グリーン購入ガイドライン指定品の使用

業務に係る用品等は、札幌市グリーン購入ガイドラインに従い、極力ガイドライン指定品を使用すること。

８　その他

（１）進捗状況の報告

業務の進捗状況について、委託者から問い合わせがあった時はその都度報告すること。また、業務内容については、その都度委託者の目的に合致しているか確認すること。

（２）協議

仕様書で明記のない点、または疑義のある点が生じた場合については、必ず委託者と受託者の間で協議を行い、その決定に従うこと。

（３）データ保護に関する事項

本件業務について知り得た情報については、本契約の履行期間及び履行後においても個人情報を含むすべての情報を第三者に漏らしてはならない。データの取扱いについても同様である。また、秘密保持及びデータ取扱いについて、従業員その他関係者への徹底を行うこと。

ア　委託者の情報を目的外に使用しないこと。

イ　委託者の情報を複写、複製する場合には委託者の許可を事前に得ること。

ウ　本件業務が終了した場合は、本業務にかかる情報の消去を確実に行い、削除報告を書面で行うこと。

（４）その他

ア　検査対象は本番環境であるため、使用するツール等によりサービス不能となるなどの不具合を生じる可能性は限りなく少なくすることとし、影響については事前に委託者に十分に説明を行うこと。

イ　診断業務に必要な脆弱性診断ツールの調達・導入や、かかる通信費等一切の費用は、受託者の負担とする。

ウ　診断に際し、サイトに異常の発生又はその恐れがあると判断される場合には、その状況や対処方法等について、速やかに委託者に報告を行い、必要な対処を行うこと。また、当該事案に至る経緯や原因、対処などの考察も含め報告書を提出すること。

エ　受託者は、役務の全部若しくは一部を第三者に委託し、又は請け負わせてはならない。ただし、やむを得ず再委託する場合は委託者の承認を得ること。再委託者は、受託者と同様、本仕様に記載のデータ保護に関する事項を遵守することとし、別途提出する再委託申請書に再委託の内容（再委託者名、再委託業務等）を明記すること。

オ　受託者は報告書から1か月間は、報告書の内容に関して、電話、メールによる質疑応答に対応すること。

カ　検査対象は本番環境であるためサービス不能等の不慮の事故が発生した場合、120分以内に該当部署に訪問し現象を確認できる体制を取れること。

（別添１）

ウェブアプリケーション診断項目

| 分類 | 内容 |
|---|---|
| Webアプリケーション | XSS（反射型／格納型／DOMベース） |
| | SQLインジェクション |
| | ディレクトリ・トラバーサル |
| | Webコードインジェクション |
| | XMLインジェクション |
| | OSコマンド・インジェクション |
| | HTTPヘッダ・インジェクション |
| | クロスサイト・リクエスト・フォージェリ |
| | ファイルインクルード（ロ―カル、リモート） |
| | CRLFインジェクション |
| | バッファオーバーフロー |
| | クリックジャッキング |
| | パラメータ改ざん |
| | フォーマット文字列攻撃 |
| | SSIインジェクション |
| | オープンリダイレクトの脆弱性 |
| | テンプレート・インジェクション |
| | セッション・ハイジャック |
| | セッションの固定化 |
| | 安全でないデシリアライゼーション |
| HTTP/HTTPS調査 | SSL/TLS暗号強度調査 |
| | SSL/TLSバージョン調査 |
| | SSL/TLS証明書調査 |
| | セキュリティヘッダの有無 |
| | HTTP通信の有無 |
| Webサーバテスト | サーバ情報調査（OSバージョン等） |
| | 認証バイパスの脆弱性調査 |
| | サーバエラーの調査 |
| | Cookieのセキュア属性の有無 |
| | HTTPリクエストメソッドの調査 |
| | PHPのバージョン調査 |
| | Wordpressのバージョン調査 |

（別添２）

プラットフォーム診断項目

| 分類 | 内容 |
|---|---|
| ネットワーク調査 | TCP/UDP/サービス/ICMPスキャン |
| | OS推測 |
| | ホスト名調査 |
| 各種サービスの脆弱性調査 | 脆弱性スキャン |
| FTP調査 | バナー取得／匿名接続／簡易パスワード推測 |
| SSH調査 | バナー取得／認証方法調査／簡易パスワード推測 |
| TELNET調査 | バナー取得／簡易パスワード推測 |
| SMTP調査 | バナー取得／不正中継調査／EXPN,VRFY調査 |
| POP調査 | バナー取得／簡易パスワード推測 |
| DNS調査 | バナー取得／再帰的問合せ調査／ゾーン転送調査 |
| HTTP/HTTPS調査 | バナー取得 |
| | Webスキャン |
| | ファイルとディレクトリ調査 |
| | 簡易パスワード推測 |
| | WebDAV/FrontPage調査 |
| | アプリケーションマッピング調査 |
| | Proxy調査 |
| | SSL暗号強度調査／SSLバージョン調査 |
| | SSL証明書調査 |
| | RPC情報の取得 |
| SUNRPC調査 | アカウント情報収集 |
| SMB調査 | ファイル共有情報収集 |
| | NetBIOS情報収集 |
| | 簡易パスワード推測 |
| SNMP調査 | 簡易コミュニティ名推測 |
| | MIB情報の取得 |
| NTP調査 | バナー取得 |
| バックドア調査 | ポートスキャン |