ウェブアプリケーション及びプラットフォームぜい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ぜい弱性診断業務

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。

札幌市中央卸売市場公式ホームページ（以下、市ホームページ）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、ぜい弱性診断を実施し、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)ぜい弱性診断

市ホームページ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。

検出したぜい弱性は共通ぜい弱性評価システム（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ぜい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、「ぜい弱性名」、「ぜい弱性のリスク」、「検出日付」、「URL」、「修正方法」の5点を含むこと。

ア　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、ぜい弱性診断を実施すること。

診断対象は札幌市中央卸売市場が管理する「https://www.sapporo-market.gr.jp」の URL から始まるページで、合計 30 ページ以内とし、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、ぜい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（午前8時 45 分から午後5時 15 分）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。

イ　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ぜい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（午前8時 45 分から午後5時 15 分）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

ぜい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、部門責任者や役員等への説明およ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。

ア　診断結果全体の評価

イ　診断対象ごとの検出されたぜい弱性の情報・検出されたぜい弱性の脅威レベル・検出されたぜい弱性の概要・検出されたぜい弱性による影響・検出されたぜい弱性の対策方法・ぜい弱性を検出した全てのパラメータ・ぜい弱性を検出した際の入力文字列

ウ　ぜい弱性を検出した際に確認したログ（ぜい弱性別にとりまとめること）

報告書には、診断の結果概要、発見したぜい弱性・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

札幌市経済観光局中央卸売市場経営支援課
（札幌市中央区北 12 条西 20 丁目 2-1　水産棟 4 階）

5　業務履行期限

契約締結の日から令和7年8月 29 日（金）まで

6　納品物

納品物一式を書類、CD-R 等のメディア（WORD、EXCEL、POWER POINT、PDF 又は協議の上本市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、本市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、本市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、本市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、その都度本市の目的に合致しているか確認すること。

（2）協議

仕様書で明記の無い点、または疑義のある点が生じた場合については、必ず本市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。データの取り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　本市の情報を目的外に使用しないこと。

イ　本市の情報を複写、複製する場合には本市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　診断業務に必要なぜい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。

（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 ヘッダー・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（ローカル、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ぜい弱性
	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）
	認証バイパスのぜい弱性調査
	サーバーエラーの調査
	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
各種サービスのぜい弱性調査	ぜい弱性スキャン
FTP 調査	バナー取得/匿名接続/簡易パスワード推測
SSH 踏査	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