下水道水位情報システムセキュリティ脆弱性診断業務
仕　様　書

1　委託業務名

下水道水位情報システムセキュリティ脆弱性診断業務

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、データの改ざんやサービス停止、情報漏洩等の被害が生じている。

本市が公開している下水道水位情報システムは、地下施設管理者等への浸水に対する注意喚起や避難誘導、止水板設置等の支援を主な目的として、特定の下水管内で測定した水位情報をWebサイト上でリアルタイムに閲覧できるものであるが、本システムがこのような被害に遭うことを未然に防止するため、セキュリティ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

本市が公開している下水道水位情報システム（https://sapporo.aquasmartcloud.jp/）のうち、水位情報公開Webシステムに対して、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。

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。

診断対象は計1FQDNで、ドメイン名は業務開始後に委託者より開示する。診断対象URLは、全診断対象サイトの合計で20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、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（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。

診断対象は計 1IP で、IP アドレスは業務開始後に委託者より開示する。

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）報告書作成

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

札幌市豊平区豊平 6 条 3 丁目 2 番 1 号　札幌市下水道河川局庁舎施設管理課

５　業務履行期間

契約書に示す着手の日から令和 8 年 2 月 28 日まで

６　提出書類

（１）着手時

受託者は、契約締結後すみやかに次の書類を提出し、承諾を受けたのち着手すること。

ア　業務着手届　（様式１）　1 部（労働基準監督署印は不要）
イ　業務代理人指定通知書（様式２）　1 部
ウ　業務代理人経歴書　（様式３）　1 部
エ　業務計画書（様式は要協議）　1 部

（２）完了時

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、ウィルスチェックを実施したうえで納品すること。

ア　業務完了届・業務完了検査報告書　（様式４）　1 部
イ　診断結果及び結果の分析・改善策の提案等の報告書　1 部
ウ　その他、本業務で作成した資料、書類等一式　1 部
エ　業務データの消去作業完了証明書（様式７）　1 部

（3）適宜

ア　打合せ議事録一覧、業務打合せ議事録（様式５、６）　　１部

イ　その他（業務主任の指示により提出、様式は要協議）

7　業務代理人

受託者は、業務代理人を配置しなければならない。業務代理人は、本業務に類する業務経験を有する者とする。

8　業務従事者等の配置及び職務

（1）受託者は、委託者が別途通知する業務主任の指示及び指導に従うこと。

（2）受託者は、業務代理人を定め、その経歴を添えて書面をもって委託者に通知しなければならない。また、その内容を変更したときも同様とする。業務代理人は、委託者との連絡調整及び業務従事者に対する指示及び指導を行う者であり、常に連絡場所及び連絡方法等を明らかにしておかなければならない。

9　環境に対する配慮

本業務においては、本市の環境マネジメントシステムに準じ、環境負荷低減に努めること。

（1）電気、水道、油、ガス等の使用にあたっては、極力節約に努めること。

（2）ごみ減量及びリサイクルに努めること。

（3）両面コピーの徹底やミスコピーを減らすことで、紙の使用量を減らすよう努めること。

（4）自動車等を使用する場合は、できるだけ環境負荷の少ない車両を使用し、アイドリングストップの実施など環境に配慮した運転を心がけること。

（5）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。

（6）業務に関わる従業員に対し、札幌市環境方針の理解及び業務と環境の関連について自覚を持つような研修を行うこと。

10　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、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（様式7）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（任意様式）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。

以上

（別添１）

ウェブアプリケーション診断項目

	診断項目
1	SQL インジェクション
2	OS コマンド・インジェクション
3	ディレクトリ・トラバーサル
4	セッション管理の不備
5	クロスサイト・スクリプティング
6	クロスサイト・リクエスト・フォージェリ
7	HTTP ヘッダ・インジェクション
8	メールヘッダ・インジェクション
9	クリックジャッキング
10	バッファオーバーフロー
11	アクセス制御や認可制御の欠落

各診断項目の定義は、「安全なウェブサイトの作り方」（独立行政法人情報処理推進機構、https://www.ipa.go.jp/security/vuln/websecurity.html）に記載のものとする。

（別添２）

プラットフォーム診断項目

	診断項目	診断内容
1	ポートスキャン	対象機器で稼働している各ホストのOSや、動作しているサービスについて、ポートの稼動状態にかかる情報を確認する。
2	バナー情報取得	バナー情報を収集し、OS種別やサービスのソフトウェア名、バージョン等を確認する。
3	DNSサーバの検証	DNSサーバ関連ソフトウェアが最新であるか、コンテンツサーバの再帰問い合わせ動作が無効になっているか、DNSキャッシュポイズニング攻撃をうける恐れがないか等、脆弱性の有無を確認する。
4	既知の脆弱性検証	各ホスト上の接続可能なサービスに対し、脆弱性診断ツール等を用い、ホスト上の脆弱性（ソフトウェアの不備、設定の不備等）の情報を収集する。

様式　1

業　務　着　手　届

令和　　年　　月　　日

札幌市長　　様

受託者
（住所）
代表者
（氏名）

下記役務は、令和　　年　　月　　日着手したのでお届けします。

記

1．役務番号　　第　　号

2．役 務 名

・ 提出部数　　1部
・ 提 出 先　　業務主任
・ 提出期限　　着手日と同日
・ 業務代理人指定通知書及び業務代理人経歴書を添付すること。

様式　2

業務代理人指定通知書

令和　　年　　月　　日

札幌市長　　様

受託者
（住所）
代表者
（氏名）

役務番号	役務名
第　　号	

上記役務に係る業務代理人を次のとおり定めたので、別紙経歴書を添えて通知します。

区分	氏名	備考
業務代理人		

・「区分」欄には業務代理人と記載すること。
・業務代理人と受託者との直接的かつ恒常的な雇用関係を確認できる書類（健康保険証の写し等）を添付すること。
・健康保険証の写しを提出する際は、被保険者等記号・番号及び保険者番号（これらの情報が読み取れるQRコードを含む。）にマスキングを施した状態で提出すること。

様式　3

業務代理人経歴書

現　住　所			
氏　　名		生年月日	※ 昭和　　年　　月　　日 平成

最終学歴	卒業年月	学　校　名	専攻科目
	※昭和 平成　　年　　月		

職　歴	※昭和 平成　　年　　月	入社
	※昭和 平成　　年　　月	入社

技術資格	※昭和 平成　　年　　月		取得№.
	※昭和 平成　　年　　月		取得№.

主要業務経歴	業務名	受託金額(千円)	履行期間
			年　月 年　月
			年　月 年　月
			年　月 年　月

上記のとおり相違ありません。

令和　　年　　月　　日

氏　名　＿＿＿＿＿＿＿＿＿＿＿＿

・　※印の項目については、該当するものを○で囲むこと。
・　最終学歴は、小学校・中学校・高等学校・短期大学・大学又は高等専門学校のいずれかを記載し、専修学校・各種学校等は記載しないこと。

様式　4

令和　　年　　月　　日

業務完了届

札幌市長　　様

受託者
（住所）
代表者
（氏名）

役務番号　　第　　号
役 務 名

上記役務は、令和　　年　　月　　日完了したのでお届けします。

受付　令和　　年　　月　　日	完了を確認した職員 業務主任　技術職員　　印

決裁区分	課　長	審査担当係長	
課			この役務の検査員及び立会人に次のものを命じ、 令和　年　月　日　時　分に検査を実施してよろしいか。 検査員　　技術職員 立会人　　技術職員

決裁区分	課　長	審査担当係長
課		

令和　　年　　月　　日

業務完了検査報告書

検査員　　技術職員　　印

立会人　　技術職員　　印

上記役務の検査結果は、次のとおりであったので報告します。

役　務　名	
契約の相手方	
契 約 金 額	円
契 約 年 月 日	令和　　年　　月　　日
実 施 期 間	令和　　年　　月　　日 ～ 令和　　年　　月　　日
検 査 年 月 日	令和　　年　　月　　日
検 査 の 結 果	

様式　5

打合せ議事録　一覧

令和　　年　　月

番号	実施日	議事概要	備考

様式　6

業　務　打　合　せ　議　事　録

No.

業務名	
日時	令和　　年　　月　　日　　時　　分　～　　時　　分
手段	会議　・　電話　・　その他（　　）
場所	
出席者（委託者）	
出席者（受託者）	
配布（提出）資料	

議事内容（確認事項・決定事項・保留事項・問題点など）

様式　7

令和　年　　月　　日

札幌市長　様

（住　所）
（氏　名）

業務データの消去作業完了証明書

下水道水位情報システムセキュリティ脆弱性診断業務に係る業務データにつきまして、下記のとおりデータ消去作業を実施し、正常に完了したことを確認しましたので、ここに証明いたします。

記

１　対象データ　　下水道水位情報システムセキュリティ脆弱性診断業務に係る全業務データ

２　データ消去日　　令和　　年　　月　　日

３　消去方法

４　消去場所

５　実施責任者

以上