ウェブアプリケーションのセキュリティー対策に関する仕様書

１．趣旨

この仕様書は、「小樽市学校ホームページ管理システム」更新契約の受託者がホームページの改ざん等をはじめとしたインターネット上の脅威に対処するため、開発及び運用等において、ウェブアプリケーションに対して実施する対策について定めることを目的とする。

２．開発・改修時に実施する対策

受託者は 、独立行政法人情報処理推進機構（ＩＰＡ）が策定した「安全なウェブサイトの作り方改訂第７版」の内容を理解するとともに、別紙１「ウェブアプリケーションのセキュリティチェックシート」（以下、「チェックシート」という。）に定める対策等を実施すること。

チェックシートの各実施項目について「対応済」、「未対策」、「対応不要」のいずれかをチェックすること。

ウェブアプリケーションに脆弱性がないことが明らかである場合、当該項目に「対応不要」にすることができる。

受託者は、チェックシートに基づき、全ての脆弱性を確認した上で、運用開始までに委託者に対してチェックシートを提出するものとする。

チェックシートの選択項目

対応済	対策を実施している場合に選択。
未対策	対策の実施は必要であるが、何らかの理由により未実施の場合に選択し、その理由についても記載すること 。
対応不要	脆弱性が存在しない実装である場合や、すでに他の対策を実施し、対策自体が不要であると判断される場合に選択し、その理由についても記載すること 。

３．ウェブアプリケーション運用のためのセキュリティー対策

受託者は、ウェブサイトを安全に運用するために次のセキュリティー対策を施さなければならない。

（１）保守体制表の提出について

受託者は、本番運用開始までに、保守体制表を委託者に提出しなければならない。また、業務の途中で体制に変更があった場合は、速やかに書面により委託者に通知すること。

（２）ファイアーウォールの導入

必要なポートへの通信だけを許可するようルールを設定し、ウェブサイト内の情報の書き換え、漏洩等の攻撃を防がなければならない。

（３）ウイルス対策ソフトの導入

ウェブアプリケーションが稼働するサーバーにウイルス対策ソフトを導入し、保護しなければならない。

（４）適切なリソース管理の導入

ウェブサイトのアクセスに対し、安定してサーバーを稼働させるために適切なサーバー容量を確保すること。

（5）セキュリティパッチの適用

ウェブサーバーのアプリケーション、ＣＭＳ、ＯＳ、ミドルウェア等の構成要素の全てについて、脆弱性が発見され対応パッチが公開された際は、迅速に適応させなければならない。

（6）不必要なサービスの停止・アプリケーションの削除

不必要なサービスは停止するか、削除しなければならない。サービスを提供しているポート以外に対する要求に対して応答を返さないよう、フィルタリングを施さなければならない。

（7）アカウントの適切な管理

管理者権限のアカウントは必要最低限とし、不要なアカウントは削除しなければならない。また、パスワードは英数大文字混在で１０文字以上の良質なものを設定しなければならない。

（8）その他の対策

その他、委託者と協議し、必要なセキュリティー対策がある場合はその対策を施さなければならない。

（9）監視体制

ウェブサイトの構築後は、構築したサーバーの監視を十分に行い、異常を検知することができる体制を整えること。

（１０）報告事項

受託者は、構築したシステム内で使用しているソフトウェアの種類やバージョン等について、別紙２「ウェブサーバーの運用環境報告」にて、契約締結後１週間以内に委託者に報告すること。

また、これらのソフトウェア等に関するアップデート状況等について別紙３「ソフトウェア等の運用報告」にて翌月１０日までに報告すること。

４．障害発生時の対応

故障や障害となった事象の内容及び責任分界点については別途協議をするものとし、協議内容を書面で取り交わすものとする。

システムに発生した障害等については、事象の発生時から２４時間以内に対応するものとするが、障害の程度が重度であるときは、対応及び経費について双方が十分に協議した上で、委託者が復旧作業を再度要請するものとする。

なお、この場合の障害の程度の判断は委託者が判断する。

また、障害復旧作業の内容（設定等を含む）を記録した「作業報告書」（様式任意）を１部作成し、委託者に提出すること。

５．損害賠償

受託者は、本仕様書に違反し脆弱性等が存在した場合、当該脆弱性等により委託者に発生する損害について、その賠償の責を負うものとする。なお、賠償内容については、委託者と受託者が協議の上、決定するものとする。

６．協議事項

本仕様書に定める脆弱性項目以外に、新たに脆弱性が発見され、当該脆弱性を狙った攻撃が急増するなど被害発生が予測される場合は、委託者と受託者が協議の上、対策の実施有無を決めるものとする。

７．その他

委託者は、本仕様書に定める各様式を，小樽市公式ホームページにて公開するものとする。

以上