別紙２

# ウェブアプリケーションのセキュリティ対策に関する仕様書

１　趣旨

この仕様書は、藤沢市ホームページリニューアル業務委託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）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、その理由及び未対策であることにより発生するリスクへの対応方法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対策を施さなければならない。なお、ウェブサイトの運用にあたりレンタルサーバを利用する場合は、（２）から（５）及び（１０）に記載の対応もしくは準ずる対応が可能なレンタルサーバを選択しなければならない。

（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。また、ログの取得機能は有効にし、定期的に取得したログの保存や、解析を行わなければならない。

（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。また、ソフトウエア及びパターンファイルを最新の状態に保たなければならない。

（４）適切なリソース管理、負荷分散の導入

ウェブサイトのアクセスに対し、安定してサーバを稼働させるために適切なサーバ容量を確保するとともに、必要に応じて負荷分散装置（ロードバランサー）やキャッシュサーバの導入を行わなければならない。

（５）セキュリティパッチの適用

ウェブサーバ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、１週間以内に適応させなければならない。１週間以内に対応できない場合、受託者は、速やかに委託者と協議し、適応時期や適応までの暫定対応について決定すること。

（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、パスワードは十分な長さ（８文字以上推奨）とし、文字列は想像しにくいもの（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）設定できること。設定したパスワードについては、少なくとも１８０日程度で変更することとする。

（８）新たに発見される脆弱性への対応

受託者は、委託者が契約期間中、外部のセキュリティ診断等を実施し、新たに脆弱性が発見された場合、必要なセキュリティ対策を施さなければならない。

ただし、対応に新たな費用が発生する場合、その負担について委託者と協議の上決定すること。

（９）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対策がある場合は施さなければならない。

（１０）監視体制

ウェブサイトの構築後は、構築したサーバ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。

検知対象は、Ｄｏｓ攻撃、改ざん、サーバ負荷の急増及び外部Ｃ＆Ｃサーバ等への通信等とする。

受託者は、これらの異常を検知した際は、直ちにウェブサーバの運用を停止し、委託者に連絡するとともに、対応を協議すること。

（１１）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エアの種類やバージョン等について別紙２「ウェブサーバの運用環境報告」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、これらのソフトウエア等に関するアップデート状況等について別紙３「ソフトウエア等の運用報告」にて翌月１０日までに報告すること。

４　インシデント発生時の対応

ウェブアプリケーションに、Ｄｏｓ攻撃、不正アクセス等のサイバー攻撃や、サーバの故障、停止等のインシデントが発生した場合は、ただちに委託者へ連絡し状況を報告しなければならない。対応は委託者と協議の上行い、必要に応じて、原因究明、復旧対応、プレス発表の協力等を行わなければならない。

また、インシデント対応完了後、速やかに書面にて、報告すること。

５　監督

委託者は、提出された書類等の内容について確認が必要と認められる場合は、実地に調査を行うことができるものとし、受託者はこれに協力しなければならない。

６　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、その賠償の責に任ずるものとする。

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。

７　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。

８　その他

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

以　　上

改定 2021/7/1　改