

ウェブサイト等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（以下「発注者」という。）と事業者が締結する契約（以下「本契約」という。）において、ウェブサイト及びウェブアプリケーション（以下「ウェブサイト等」という。）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に、事業者がウェブサイト等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。

なお、この仕様書は、本契約に基づき再委託を受けた者（再委託先が事業者の子会社（会社法（平成17年法律第86号）第2条第1項第3号に規定する子会社）である場合や事業者から再委託以降の全ての段階の委託業務を受託する事業者を含む。）についても適用する。

2 開発・改修時に実施する対策

事業者は、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、様式第1号「ウェブサイト等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。

ウェブサイト等に脆弱性がないことが明らかである場合、当該項目を「対応不要」にすることができる。

事業者は、チェックシートに基づき、全ての脆弱性を確認した上で、運用開始までに発注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 ウェブサイト等運用のためのセキュリティ対策

事業者は、ウェブサイト等を安全に運用するために、利用するサービスや運用形態に関わらず、以下の項目を満たさなければならない。

なお、ウェブサイト等において個人情報を取り扱う場合の個人情報とは、個人情

報の保護に関する法律（平成15年法律第57号）第2条に定められた個人に関する情報をいう。

（1）外部サービスの利用

ウェブサイト等の構築・運用において、他の事業者が提供する外部サービス（LGWAN-ASPやインターネット環境で利用するシステム、サービス（例）クラウドサービス、SNS（ソーシャルネットワーキングサービス）、検索サービス、翻訳サービス、地図サービス、ホスティングサービス、生成AI等）を利用する場合は、利用するサービスのセキュリティ要件及び取り扱う情報を明確化するとともに、発注者の許可を得ること。

（2）保守体制表の提出

事業者は、本番運用開始までに、保守体制表を発注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発注者に通知すること。

（3）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、ウェブサイト等内の情報の書き換え、漏えい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。

（4）ウイルス対策ソフトの導入

ウェブサイト等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、ソフトウェ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。

（5）適切なリソース管理、負荷分散の導入

ウェブサイト等のアクセスに対し、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。

（6）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、日々公開される脆弱性情報を積極的に収集し、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、事業者は、速やかに発注者と協議し、適応時期や適応までの暫定対応について決定すること。なお、パッチ適用後も正常にウェブサイト等が稼働することを事前に検証したうえで実施すること。

（7）通信の暗号化

ウェブサイト等で取り扱う情報の改ざん、漏えいを防ぐための暗号化及び暗号鍵の保護並びに管理を確実に行うこと。なお、暗号化を行う場合は、原則としてデジタル庁、総務省及び経済産業省が策定した「電子政府における調達のために参考すべき暗号のリスト（CRYPTREC暗号リスト）」に記載されている方法を採用すること。

(8) 不必要なサービスの停止・アプリケーションの削除

不必要的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。

(9) アカウントの適切な管理

各種設定の不正な変更を防ぐため、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。また管理者画面については、IPアドレス制限や二段階認証等の不正アクセス対策を施さなければならない。なお、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）を設定しなければならない。設定したパスワードについては、定期的に変更すること。ただし、担当者の変更やインシデント発生時にはその都度変更しなければならない。

(10) 事業者の環境におけるセキュリティ対策

個人情報及び業務上の機微情報を取り扱うウェブサイト等において、事業者が運用・保守等のためウェブサイト等に接続する場合は、接続する端末や操作者を特定し、アクセス制御や通信の暗号化などの不正アクセス対策を実施すること。また、マルウェア対策を実施すること。

(11) 新たに発見される脆弱性への対応

事業者は、発注者が契約期間中、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、その負担について発注者と協議の上決定すること。

(12) その他の対策

その他、発注者と協議し、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。

(13) 監視体制

ウェブサイト等の構築後は、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、監視体制表を発注者に提出すること。

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サーバ等への通信のほか、発注者が必要と判断したものとする。

事業者は、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、発注者に連絡するとともに、対応を協議すること。

(14) 報告事項

事業者は、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様式第2号「ウェブサーバの運用環境報告」にて、契約締結後1週間以内に発注者に報告すること。

また、これらのソフトウェア等に関してアップデートを実施した場合は様式

第3号「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。

ただし、発注期間の最終月に実施した場合は、当該発注期間の終了日までに報告すること。

4 インシデント発生時の対応

ウェブサイト等に、D o s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、ただちに発注者へ連絡し状況を報告しなければならない。対応は発注者と協議の上を行い、必要に応じて、原因究明、復旧対応、プレス発表の協力、再発防止策の検討及び提案並びに実施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 メンテナンス等によるウェブサイト等停止時の対応

事業者は、サーバのメンテナンス等でウェブサイト等の公開を一時的に停止する場合、原則10日前までに発注者に書面にて通知すること。また、作業中は「メンテナンス中」の案内を表示すること。

6 監督

発注者は、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、事業者はこれに協力しなければならない。

7 損害賠償

事業者は、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発注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発注者と事業者が協議の上、決定するものとする。

8 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、発注者と事業者が協議の上、対策の実施有無を決めるものとする。

9 その他

発注者は、本仕様書に定める各様式を、藤沢市公式ホームページにて公開するものとする。

以 上