別添４

ウェブサイトの開設・運用における特記事項

１ 前提条件

クラウドサービスを利用する場合は、別添９「セキュリティチェックリスト」のセキュリティ要件、外部サービス提供者回答欄や受託者回答欄に記載のセキュリティ対策も満たすクラウドサービスの選定、開発（導入・構築）、運用保守、更改・廃棄を行うこと。

契約後、セキュリティチェックリストの外部サービス提供者回答欄や受託者回答欄を記入し、県に根拠資料と共に提出すること。その後は、セキュリティチェックリストのセキュリティ要件に従い、時点更新を行い、定期的に県に提出すること。

なお、専用サイト及びシステムの特性等に応じて不適合又は対策不要等を判断した場合には、根拠を示す説明資料を併せて提出すること。

クラウドサービスを利用せず、データセンター等にサービス提供基盤を構築する場合は、クラウドサービスを利用する場合に準じたセキュリティ対策が実施できること。また、実施したセキュリティ対策については、発注者の求めに応じて開示すること。

２ ウェブサイトのセキュリティ対策

サイト構築時及び納品時に、独立行政法人情報処理推進機構（ＩＰＡ）がまとめた「ウェブサイトのセキュリティ対策のチェックポイント２０ヶ条 チェックリスト」及び「IPA 安全なウェブサイトの作り方」に掲載の「セキュリティ実装 チェックリスト」により点検した結果を提出すること。また、当該チェックリストに基づき必要な対策を実施するとともに、「対応不要」とした項目があるときは、根拠を示す説明資料を併せて提出すること。なお、「対応済」とした項目についても、発注者から説明を求められたときには、必要に応じて根拠を示す資料を提出するなど適切に対応すること。

３ ドメイン

作成するウェブサイトは、県が指定するドメインを使用して作成し、事業の終了をもって廃止すること。止むを得ず独自ドメインを取得する場合は、委託業務終了時に県に円滑に引き継ぐこと。なお、事業者の公式サイト等で管理しているドメインを使用する場合は、ドメインが不正利用されないよう適切な対策及び管理を委託業務終了後も行うこと。ＳＳＬ証明書の種類は、ＯＶ（実在証明型）以上とするが、独自ドメインとする場合はＥＶ（実在証明拡張型）とすること。また、ドメインの登録、ＳＳＬ証明書発行等の費用は、受注者の負担とする。

4　セキュリティ診断・侵入検査

受注者は納品時及び定期的に以下の脆弱性診断を実施すること。また、脆弱性が発見された場合は適切な対処を行い、再診断により脆弱性がないことをサイトの運用開始前までに発注者に報告すること。

なお、当該検査は経済産業省が策定した「情報セキュリティサービスに関する審査登録機関基準」に適合している事業者に実施させること。

（参考）

・情報セキュリティサービス基準適合サービスリスト（IPA）
https://www.ipa.go.jp/security/it-service/service_list.html

・日本セキュリティ監査協会（JASA）情報セキュリティサービス基準審査登録制度
https://sss-erc.org/

（1）ネットワーク侵入検査

公開サーバに対して、最新の攻撃手法等を用いて擬似的な攻撃を行い、脆弱性の有無を確認（Web サイトを動作させるサーバ・ネットワーク機器といった環境に対する診断）するなど安全性を検査すること。

（2）Web アプリケーション検査

動的コンテンツを提供するページに対して、次に示す脆弱性の有無について、Web アプリケーション検査を実施すること。

ア　ＳＱＬインジェクション
イ　ＯＳコマンド・インジェクション
ウ　パス名パラメータの未チェック／ディレクトリ・トラバーサル
エ　セッション管理の不備
オ　クロスサイト・スクリプティング
カ　ＣＳＲＦ（クロスサイト・リクエスト・フォージェリ）
キ　ＨＴＴＰヘッダ・インジェクション
ク　メールヘッダ・インジェクション
ケ　クリックジャッキング
コ　バッファオーバーフロー
サ　アクセス制御や認可制御の欠落

5　脆弱性等への対応

脆弱性診断等により脆弱性が含まれないことを定期的に確認するほか、脆弱性に関する情報（OS、その他ソフトウェアのパッチ情報等）を常に収集し、脆弱性が発見された場合は、発注者と協議のうえ修正プログラムの適用や一部サービスの停止なども含

め、脆弱性を悪用されないよう必要な対策を実施すること。

6 監視と検知の実施

クラウドサービスを含む本委託業務により運営するウェブサイト全体を構成するシステムの稼働状況、障害、セキュリティインシデントを監視し、異常を検知できる仕組みがあること。検知後、電話やメール等で通知を受けられる仕組みもあること。

7 緊急時の対応

情報セキュリティインシデントの発生など緊急時の体制と報告等のフローを整備し、インシデント発生時には直ちに復旧見込みを県に報告すること。その後、迅速に復旧作業を行い、障害原因、影響範囲、再発防止策を含む対応方針を県に報告すること。

8 コンピュータウイルス等への対策

コンピュータウイルス等の不正プログラム対策ソフトウェアの導入などの不正プログラム対策を実施すること。また、不正プログラム対策ソフトウェアのパターンファイル等を常に最新に保つこと。