別紙１

特記仕様書

１　本特記仕様書について

本特記仕様書は、令和８年度　GREEN×EXPO 2027 神奈川県出展運営等業務委託仕様書６(3)オにおける個別の要件を示す。

２　前提条件

構築するウェブサイトでは公開を前提とした情報のみを扱うこと。

３　ウェブサイトの対策

(1) セキュリティ実装チェックリストへの対応

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。

(2) ドメイン及びSSL 証明書

作成するウェブサイトは、県が指定するドメインを使用すること。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）とし、ＳＳＬ証明書発行等の費用は、受託者の負担とする。

(3) セキュリティ診断・侵入検査

受託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うこと。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/

(4) 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。

(5) 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

(6) 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、発注者と協議の上、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。

(7) 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。

(8) 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発注者に報告すること。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

方針を発注者に報告すること。

(9) 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。

(10) クラウドサービスの利用

重要情報（※）を扱うクラウドサービスを利用する場合、次の通り実施すること。

ア　別添の「外部サービス利用に係る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。

イ　契約締結後、「外部サービス利用に係る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、「外部サービス利用に係る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。

（※）重要情報とは、個人情報又は特に機密性が求められる情報を指す。

(11) その他

上記(1)から(5)にあげた項目以外、サイトの特性に応じて必要な検査を実施すること。

４　ページの構築

(1) デザイン・閲覧環境

ア　神奈川県が運営するページであることが分かるように、神奈川県公式ウェブサイト（https://www.pref.kanagawa.jp/）へのリンクと、画像（KI デザイン又は公式バナーリンク）をトップページ内に配置すること。また、県公式ウェブサイトと共通のフッターを使用すること。

イ　PC 及びモバイル端末（スマートフォンなど）で閲覧しやすいページとすること。

(2) サイトポリシー等の表示

県が運用するページであることを示すため、発注者と協議の上、サイトポリシーのページを設け、各ページの下部に、運営主体（「神奈川県環境農政局農水産部農業振興課国際園芸博覧会推進室」）、県が指定する問い合わせ先の情報ページ、サイトポリシーページへのリンクを設けること。

５　ウェブアクセシビリティの確保

(1) ウェブアクセシビリティの対応

サイト作成に当たっては、神奈川県ウェブアクセシビリティ方針（https://www.pref.kanagawa.jp/docs/fz7/accessibility/accessibility_policy.html）に則り、JIS X8341-3：2016（高齢者・障害者等配慮設計指針－情報通信における機器，ソフトウェア及びサービス－第３部：ウェブコンテンツ）（以下、「JIS 規格」という。）の達成基準に対応させ、納品前に全ページを対象に JIS 規格に基づく試験を実施すること。

なお、試験の対象範囲は JIS 規格「JB.1.2 ウェブページ一式単位」「d) ウェブページ一式を代表するウェブページとランダムに選択したウェブページとを併せて選択する場合」とする。試験の結果、達成基準に不適合となった場合は、速やかに修正するか、代替手段を用意すること。 また、成果物として、JIS 規格に基づく試験結果報告書（達成基準チェックリスト）を提出すること。

(2) HTML、CSS の雛形作成段階において、上記(1)に記載する達成基準への対応状況の確認を実施するとともに、発注者に報告して了承を得たうえでコンテンツ制作をすること。ツールによる判定が可能な検証項目については、ツールを用いた上で、そのツール名を記録すること。

６　リンク切れへの対応

公開中のページについて、月１回、目視又は任意のリンク切れチェックツールを用いたリンク切れ検査を実施し、リンク切れを確認した場合は、発注者と協議の上、リンク切れを改善する対応を行うこと。また、検査及び対応結果を月次で報告すること。