（別紙１）

ウェブアクセシビリティ、情報セキュリティ等について

１　ウェブアクセシビリティ

(1) 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ー情報通信における機器, ソフトウェア及びサービスー第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」「a) すべてのウェブページを選択する場合」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。

２　情報セキュリティ

(1) アクセスログを契約終了まで保管し、必要に応じて発注者に提示又は提出すること。

(2) 管理者認証データを通信する場合、SSL/TSL 暗号化技術を用いること。

(3) 管理者権限での操作に関しては、前号に加え、IP アドレスによるアクセス制限を行うこと。

(4) 不正アクセス等の情報セキュリティインシデントがあった場合は、直ちに発注者に報告するとともに、被害の調査・対応、原因究明及び再発防止対策を行うこと。

(5) 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本サイトの公開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

ア　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。

イ　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

ウ　その他

ア及びイであげた項目以外、サイトの特性に応じて必要な検査を実施すること

(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。

(7) 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。

(8) 修正パッチの適用やセキュリティホール対策等の日常管理を行うこと。

(9) 本サイトでは、原則として個人情報を取り扱わないこと。

(10) 独立行政法人情報処理推進機構「安全なウェブサイトの作り方」（改訂第７版）に記載の内容に従い、適切に制作・運用すること。
（https://www.ipa.go.jp/security/vuln/websecurity.html）

(11) その他、情報セキュリティの確保については、発注者の指示に従うこと。

３　ウェブサーバ・データベースサーバ

(1) 設置場所

サーバ機器類の設置場所は日本国内であること。また、火災、浸水及び自然災害等に対する対策が行われていること。

(2) 性能

インターネットで海外においても高速（回線の影響を除き通常の操作においてストレスを感じない程度）かつ安定した提供を可能とすること。

(3) バックアップ

定期的にバックアップを取得し、世代管理を行うこと。サーバに障害が発生した場合は、バックアップの情報からデータの復旧が可能であること。

(4) サービス停止

本サイトの公開を一時停止する場合は、10 開庁日前までに発注者に連絡するとともに、本サイトにアクセスした閲覧者に対して、停止中であることがわかるよう案内すること。

(5) セキュリティ

ア　サーバの構築・運用に当たっては、独立行政法人情報処理推進機構の「安全なウェブサイトの作り方（改訂第７版）」に準じ、最新のセキュリティパッチの適用、脆弱性の排除など、適切なセキュリティ対策を実施すること。

イ　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」（https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html）及び「ＩＰＡ安全なウェブサイトの作り方」（https://www.ipa.go.jp/security/vuln/websecurity/about.html）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。

(6) クラウドサービスの利用

ア　クラウドサービスを利用する場合は、別添の「重要情報を扱う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　クラウドサービスを利用する場合は、契約締結後、「重要情報を扱う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、「重要情報を扱う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。