別添

セキュリティ仕様書

○基本事項

- 独立行政法人情報処理推進機構（IPA）「安全なウェブサイトの作り方」最新版等を参考に、脆弱性の原因を排除するとともに、攻撃の影響を低減する対策を講じること。
- システム管理及びコンテンツの編集管理を除くすべての機能について、特定のＯＳ（基本ソフト）及びブラウザソフトの環境に依存せずに利用が可能であること。
- メンテナンス作業等を除き、常時システムの利用が可能であること。
- システム管理及びコンテンツの編集管理にかかるシステムへの接続については、ＩＰアドレスによるアクセス制限を行うこと。
- サイト全体について、ＳＳＬ／ＴＳＬ暗号化技術を用いること。
- 公開用領域との間は、ネットワークセグメントを分離し、必要最小限の通信に限定すること。

○ドメイン

- 日本の国別トップレベルドメイン（.jp）を使用すること。

○トップページ

最低限、以下のことを掲載すること。

- 県公式ウェブサイト（太陽光発電設備の共同購入事業に関するページ）へのリンク
- 県が指定する問合せ先の情報
- サイトの運営ポリシー

※別の独立したページとし、トップページからリンクする方法も可。

○管理・運営

- 構築したシステムは次のとおり管理・運営すること。

－ 緊急時に備え、県との連絡が取れる緊急連絡体制を構築すること。

－ 障害を県及び支援事業者が確認した場合、支援事業者は速やかに対応すること。

－ 障害を復旧した場合、復旧後に、障害状況・発生原因・事後対策等についての報告を行うこと。

○脆弱性及び不正アクセス対策

- 公開前に、サイトの脆弱性の有無について第三者機関によるリモート侵入検査等を実施し、脆弱性が発見された場合は対策の上、再度検査を実施して問題がないことを確認すること。

また、公開後も定期的（最低年１回）に検査を実施するとともに、サー

バ上で使用しているソフトウェアの脆弱性に関する情報の収集等、サイトの脆弱性の有無を常に把握し、脆弱性が確認等できた際には、セキュリティパッチの適用やソフトウェアのバージョンアップ等の対応を速やかに行い、県へ報告すること。

検査の実施方法としては、以下のとおり。

－　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するなど安全性を検査すること（リモート侵入検査）。

－　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、ウェブアプリケーションの検査を実施すること。また、必要に応じて最新の攻撃手法等に対応する検査を追加して実施すること（ウェブアプリケーション検査）。

(a) ＳＱＬインジェクション
(b) ＯＳコマンド・インジェクション
(c) 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
(d) セッション管理の不備
(e) クロスサイト・スクリプティング
(f) ＣＳＲＦ（クロスサイト・リクエスト・フォージェリ）
(g) ＨＴＴＰヘッダ・インジェクション
(h) メールヘッダ・インジェクション
(i) アクセス制御や認可制御の欠落

－　これら検査のために使用するツールは、事前に書面で県に報告し、承諾を得ること。

・　不正アクセスがあった場合は、直ちに県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。

〇ライセンス契約及び著作権

１　ライセンス契約

・　システムの稼動に必要なソフトウェアのライセンス（使用許諾）の取得は、全て支援事業者の責任と負担において行うこと。なお、使用許諾に期限（月ごとのライセンス等）がある場合は、協定期間の満了日まで有効なライセンスを取得すること。

・　全てのライセンス契約について、必要な権利の登録作業を行うこと。

２　著作権

（１）第三者が権利を有する著作物

・　納入される成果物に第三者が権利を有する著作物（以下「既存著作物」という。）が含まれている場合は、県が特に使用を指示した場合を除き、支援事業者の責任と負担において、当該既存著作物の使用承諾契約に係る一切の手続を行うこと。

（２）第三者との紛争処理

・　協定に基づく作業及び成果物に関して、第三者との間に著作権に係る権利侵害の紛争等が生じた場合は、支援事業者の責任と負担において一切を処理すること。

〇その他の情報セキュリティ対策

・　成果物及び打合せ等の際に、県に提供するデータや記録媒体については、必ずウィルスチェックを行うこと。
・　その他、情報セキュリティの確保については、県の指示に従うこと。

〇ウェブアクセシビリティ

・　ウェブアクセシビリティの対応サイト作成にあたっては、神奈川県ウェブアクセシビリティ方針（http://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」「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、JIS 規格に基づく試験結果を報告すること。