Web アプリケーションのセキュリティに係る特記仕様書

1.　調達に関する基本事項

1.1. 本特記仕様書の目的と運用

本特記仕様書（以下「本書」という。）は、福井県が導入する情報システムのうち、Web アプリケーションを含むものについて、調達仕様書（以下「仕様書」という。）に加えて必要となるセキュリティ要求仕様を記載するものである。

なお、本書に記載のないセキュリティ要求仕様に関しては仕様書による。契約書および他の仕様書等の記載が本書と異なる場合は、本書を優先する。

1.2. 本特記仕様書の適用方針

本書は福井県が導入または利用する情報システムを構成するサーバで以下のすべての条件を満たすサーバについての仕様書に適用する。

(1) インターネットからのアクセスが可能なサーバ
(2) インターネットから実行可能な Web アプリケーションが動作するサーバ

1.3. 本特記仕様書の適用範囲

契約書および仕様書に定める契約範囲と、本書中「2. Web アプリケーションのセキュリティに関する特記仕様」の適用範囲は次のとおりとする。

(1) 契約範囲に Web アプリケーションの設計を含む場合、2.1 および 2.2 の各項を適用
(2) 契約範囲に Web アプリケーションの開発を含む場合、2.1 および 2.3 の各項を適用
(3) 契約範囲に Web アプリケーションの運用・保守を含む場合、2.1 および 2.4 の各項を適用
(4) 契約範囲に Web アプリケーションを含まない場合、本書の適用範囲外とする。

2.　Web アプリケーションのセキュリティに関する特記仕様

受託者は仕様書に加え、以下の仕様を満足すること。

2.1. 基本方針

受託者は Web アプリケーションの設計・開発において、情報システムに、『別紙１脆弱性リスト』に示す脆弱性が混入しないよう対策を講じ、委託業務を実施すること。また、Web アプリケーションの運用・保守において、設計・開発以降に発見された脆弱性について、委託業務の契約範囲に基づいて対策を実施または県と協議すること。

2.2. 契約範囲に Web アプリケーションの設計を含む場合

(1) 『別紙１　脆弱性リスト』に含まれる脆弱性および、県または受託者が対策を必要と判断する脆弱性について、対策方針を策定して提出すること。（別紙２セキュリティ実装方針（サンプル）を参考として任意の様式で作成するものとし、設計書等の成果物に含めることも可とする。）

(2) 『別紙３　Web アプリケーションのセキュリティ実装チェックリスト』の「設計時チェック」欄を記入して提出すること。「設計時チェック」において「未対策」にチェックした場合はその理由および同等のセキュリティが確保できる対策を、「対応不要」にチェックした場合はその理由を「未対応または差異の理由と対策」欄に記載し、県の承認を得ること。

2.3. 契約範囲に Web アプリケーションの開発を含む場合

(1) 2.2 で設計者が策定した対策方針に基づいて開発を実施すること。

(2) 『別紙３　Web アプリケーションのセキュリティ実装チェックリスト』の「開発時チェック」欄を記入して提出すること。ただし、「設計時チェック」欄と差異が生じる場合は、その理由および同等のセキュリティが確保できる対策を「未対応または差異の理由と対策」欄に記載し、県の承認を得ること。

(3) 総合テストまたは運用テスト中に、Web アプリケーションが動作するサーバに対し、脆弱性検査ツール（注１）等を用いて、対策が必要な脆弱性がないことを確認すること。

2.4. 契約範囲に Web アプリケーションの運用・保守を含む場合

(1) 委託業務の契約期間中に、対策が必要な脆弱性が発見された場合、以下の作業を受託者の責任において実施すること。（ただし、脆弱性対策のために改修や再開発が必要となる場合には、対応について県と協議するものとする。）

- 受託者が開発した Web アプリケーションに対するセキュリティパッチの提供および適用作業。
- 受託者が開発していない Web アプリケーションに対して開発元から無償提供されるセキュリティパッチの適用作業および脆弱性対策が有償となる場合の情報提供。

(2) 委託業務の契約期間中、Web アプリケーションが動作するサーバに対して、年に１回以上脆弱性検査ツール（注１）や脆弱性攻撃検出ツール（注２）等を用いて、対策が必要な脆弱性がないことを確認すること。なお、契約期間が１年未満の場合は、契約期間中に１回以上確認すること。

(3) 前項(2)の結果、対策が必要な脆弱性が明らかとなった場合は、対策方針や実施方法についてすみやかに報告し、県と協議を行うこと。

（注１）IPA テクニカルウォッチ「ウェブサイトにおける脆弱性検査手法」（http://www.ipa.go.jp/security/technicalwatch/20160928-2.html）で紹介されている「OWASP ZAP」等。

（注２）IPA が公開している iLogScanner（https://www.ipa.go.jp/security/vuln/iLogScanner/）等。

以上

特記仕様書　別紙１　脆弱性リスト

対処を必須とする脆弱性は次のとおり。

なお、各脆弱性の定義は、下表に示す IPA 『安全なウェブサイトの作り方 改訂第 7 版第 4 刷（2021 年 3 月 31 日改訂)』（https://www.ipa.go.jp/security/vuln/websecurity.html）のページと章番号を参照すること。

No.	脆弱性名称	安全なウェブサイトの作り方 改訂第 7 版のページと章番号	
1	SQL インジェクション	p. 6	1.1
2	OS コマンド・インジェクション	p. 10	1.2
3	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	p. 13	1.3
4	セッション管理の不備	p. 16	1.4
5	クロスサイト・スクリプティング （XSS）	p. 22	1.5
6	クロスサイト・リクエスト・フォージェリ （CSRF）	p. 30	1.6
7	HTTP ヘッダ・インジェクション	p. 34	1.7
8	メールヘッダ・インジェクション	p. 38	1.8
9	クリックジャッキング	p. 41	1.9
10	バッファオーバーフロー	p. 44	1.10
11	アクセス制御や認可制御の欠落	p. 46	1.11

特記仕様書　別紙２　セキュリティ実装方針（サンプル）

○○システムにおけるセキュリティ実装方針について

標記システムに係るセキュリティ実装方針を以下に示す。

1. セキュリティ実装方針

1.1. SQL 呼び出し

（対策概要）

SQL 呼び出し時には、SQL インジェクション対策として以下を行う。

（開発方針）

必須：以下のすべてを実施すること
1.1.1.　プレースホルダを用いて SQL を呼び出す
1.1.2.　SQL の動的組み立てをしない
1.1.3.　SQL 接続時に文字エンコーディングの指定を行う

1.2. CSRF 対策

（対策概要）

CSRF 対策として、POST メソッドのリクエストにはトークンの受け渡しと確認を行う。なお、本項はクリックジャッキング対策を兼ねる。

（開発方針）

必須：以下のすべてを実施すること
1.2.1.　秘密情報を入力する画面や、副作用のある画面は POST リクエストとする
1.2.2.　POST リクエストのフォームにはトークンを hidden パラメータで埋め込む。トークンにはセッション ID の SHA-1 ハッシュ値を用いる
1.2.3.　POST リクエストのフォーム画面では、HTTP レスポンスヘッダとして X-FRAME-OPTIONS: SAMEORIGIN を生成する（クリックジャッキング対策）
1.2.4.　POST リクエストを受けるページでは処理に先立ちトークンの値を確認し、トークンが不正な場合はエラーとして直ちに処理を中止する

1.3. メールヘッダ・インジェクション対策

（対策概要）

本システムではメール送信機能を備えないため、本対応は不要。

～以降各対策について同様に続く。省略～