付属資料 3

Web アプリケーションセキュリティに係る特記仕様書

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、山口県が導入するシステム（以下「本システム」という。）のシステム調達仕様書（以下「仕様書」という。）に加え、本システムに追加で求めるセキュリティ要件、対応指針を記載するものである。

なお、本書に記載されているセキュリティ要求仕様に関して、契約書及び仕様書の記載が本書と異なる場合は、契約書及び仕様書を優先する。

2. Web アプリケーション脆弱性対応

本システムにおける Web アプリケーションの脆弱性対応として次の要件を満たすこと。

(1)『別紙 1 脆弱性リスト』で示す脆弱性が本システムに混入しないよう Web アプリケーションを構築すること。

(2)『別紙 1 脆弱性リスト』で示す脆弱性が Web アプリケーションに混入しないように構築するための方針を山口県に提示すること。

3. セキュリティ機能

本システムにおけるセキュリティ機能について、以降に示す機能を設ける場合は、各項の要件を満たすこと。

3.1. ログイン処理

3.1.1. 利用者認証方式

利用者認証を行う場合、認証方式はパスワード認証とする。

3.1.2. アクセス制御機能

(1) 利用者の認証を行い、認証した利用者のみが本システムの「利用者認証を要する機能（画面）」を利用できるようにすること。

(2) 利用者認証を経ていない者は本システムの「利用者認証を要する機能（画面）」を利用できないようにすること。

(3) 「利用者認証を要する機能（画面）」は、セッションが終了した後は利用できないこと。

3.1.3. パスワードに利用できる文字

パスワードに利用する文字は以下を遵守すること。ただし、二要素認証の第 2 要素（ワンタイムパスワードトークンの生成するパスワードなど）はこの限りでない。

(1) パスワードに利用できる文字種は、英字（大文字、小文字を区別）、数字、記号の 3 種とし、それぞれ自由に利用できること。

(2) パスワードに利用する文字数は 8 文字未満を受け付けないようにすること。また、少なくとも 64 文字のパスワードは受け入れられること。

3.1.4. ログインフォームの実装方法

パスワードの入力欄は入力した文字を伏字にすること。又は、伏字にする・しないを選択できる機能を持つこと。

3.1.5. ログイン失敗時のメッセージ出力

パスワード認証に失敗した際に、利用者 ID の間違いか、パスワードの間違いかが区別できるメッセージを表示しないこと。

3.1.6. アカウントロック機能

特定の利用者 ID に対するパスワードの間違いが一定回数を超えた場合に、アカウントをロックする機能を実装すること。

(1) パスワードは平文で保存せず、ソルトつきハッシュの形で保存すること。

(2) ソルトは利用者毎に別々に設定すること。

3.1.7. セッション管理機能

(1) 利用者のセッション管理にはプログラミング言語や Web アプリケーション実行環境の備えるセッション管理機構を用いること。

(2) ログイン状態にある利用者のセッション識別のための情報（セッション ID）は、クッキーを用いて保持すること。

3.1.8. セッションの開始

セッションはログイン処理成功後に開始すること。

3.1.9. セッションの終了

次の場合はセッションを終了し、セッション情報を破棄すること。

(1) 利用者がログアウト機能を呼び出した場合（ログアウトボタンを押す等）

(2) 最後にページが表示された時刻を起点としてセッションの有効期間を超えた（セッションタイムアウト）場合

3.2. 認可処理

3.2.1. 認可処理の要件定義と文書化

認可処理は次のとおり文書化し、権限毎の役割をロールとして作成すること。

(1) 認可処理の必要な機能、情報を識別して、認可処理の必要な画面を、山口県に提示すること。

(2) 各ロールと権限を一覧表（権限マトリックス）に整理すること。

3.2.2. 認可処理の実装

(1) 各利用者の権限確認には、セッション変数に保存された利用者識別情報（利用者 ID 等）を基準とすること。

(2) 認可を要する情報表示や機能実行をする前に、実行中の利用者が、当該情報の表示や機能を実行するための権限を有していることを画面毎に確認すること。

(3) 認可されなかった場合は、適切なエラー表示をすること。

3.3. アカウント管理

3.3.1. 利用者登録（アカウントの作成）時における登録メールアドレスの確認

(1) ログイン処理のあるシステムで、利用者登録時にメールアドレスを登録させた場合は、登録されたメールアドレスに対してメールを送付し、登録メールアドレスが利用者に利用されているアドレスであることを確認すること。

(2) 登録メールアドレスが利用者に利用されているアドレスであると確認できた後に本システムにおける利用者登録を完了（登録の確定）とすること。

(3) 登録されたメールアドレスに対してメールを送付する際に、利用者が登録したパスワードを記載しないこと。

3.3.2. 利用者 ID の重複防止機能

利用者 ID が重複しないよう、チェック処理を含めること。

3.3.3. 登録メールアドレス変更機能

利用者が登録したメールアドレスを変更する機能を実装する場合は、メールアドレス変更機能の実行後は、利用者登録時と同様の処理を経ること。

3.3.4. パスワード変更機能

利用者がパスワードを変更する機能を実装する場合は、パスワード変更機能の実行前に、現在のパスワードの入力を利用者に求め、正しいパスワードであることを確認すること。

3.3.5. パスワードリセット機能

利用者がパスワードを失念した場合の対処機能を備える場合は、次の（1)、(2）いずれかの方式とし、(3）または（4）の要件を満たすこと。(利用者確認の手段として、予め登録したメールアドレスに宛てたメールが受信できることを用いる。)

(1) パスワードリセット機能を利用するための URL を登録メールアドレスにメール送付する方式

(2) 仮パスワードを発行し、メールで通知する方式（仮パスワードでログインした場合は、パスワード変更機能のみが利用できるものとする）

(3) （1）の機能の実装に際して、第三者がパスワードリセット機能を使えないように、URL には十分長い乱数による秘密情報（以下「トークン」という。）をつけること。

(4) （2）の機能に対する総当たり攻撃対策を施すこと。

3.3.6. 管理者によるアカウント削除・一時利用停止機能

(1) 管理者による利用者アカウントの削除機能を実装すること。

(2) 管理者による利用者アカウントの一時利用停止機能を実装すること。

3.3.7. 利用者によるアカウント削除機能

利用者による自身のアカウントを削除する機能を実装する場合は、アカウント削除機能の実行前に、パスワードの入力を利用者に求め、正しいパスワードであることを確認すること。

3.4. ログイン状態にある利用者の意図に反した機能実行の防止機能

外部リンク等により本システムの画面（機能）に遷移するだけで、本システムの機能がログイン状態にある利用者の意図に反して実行されることを防止するため、以下の対策を実施すること。

・クロスサイト・リクエスト・フォージェリ（CSRF） 対策

・クリックジャッキング対策

3.5. ログ出力

システム監査、事故調査の目的のため、本システムで取得するログの内容を検討し、山口県に提示すること。また、ログの出力・保管方法についてもあわせて協議すること。

3.5.1. ログからの情報漏えい・改ざん対策

(1) ログを取得する場合は、ログが不正に参照・変更・削除されないよう保護すること。

(2) ログから個人情報等の秘密情報が漏えいすることを防ぐため、ログの目的（監査、事故追跡）を損なわない範囲で秘密情報を含めない処理又は秘密情報の一部のみの出力（マスク処理）をすること。

3.5.2. ログの保管

(1) ログの保管年限は 1 年以上とする。

(2) ログの安全な保管方法（媒体、保管フォーマット、保管場所等）を定めること。

3.6. 暗号化

3.6.1. 利用者と本システム間における Web アプリケーション通信の暗号化

(1) システムで送受信する情報のうち、機密性・完全性の高い情報を送受する場合は、通信を暗号化すること。

(2) サーバ証明書は利用を想定するすべてのブラウザで警告の出ないものを使用し、証明書の発行先名は、運営者の名称とする。地方公共団体組織認証基盤（LGPKI）を用いる場合は、Firefox を利用想定ブラウザから外すこと。

(3) SSL2.0 及び SSL3.0 は使用しない設定にすること。

3.6.2. データベースの暗号化

(1) 機密性・完全性の高い情報をデータベース・ファイルに保存する際は暗号化を施すこと。

(2) 暗号化アルゴリズムは電子政府推奨暗号リストに記載されたアルゴリズムを用いること。

(3) 暗号鍵の管理方法を計画書に記載すること。

3.7. 出荷時

納品時における OS、ミドルウェア等ソフトウェアのバージョン及び最新パッチのリリース状況を確認すること。

以上。

別紙1 脆弱性リスト

以下に記載するWebアプリケーションの脆弱性について、本システムに混入しないよう対処すること。また、脆弱性対策の実施に際しては、独立行政法人情報処理推進機構（IPA）が示す「安全なウェブサイトの作り方」の最新版における「根本的解決」および「セキュア・プログラミング講座」を参考にすること。

なお、脆弱性項目のうち、本システムのWebアプリケーションに入力フォームがない等、脆弱性がないことが明らかである場合、該当する項目は除外してよい。

項番	脆弱性項目
1	SQLインジェクション
2	OSコマンド・インジェクション
3	ディレクトリ・トラバーサル脆弱性
4	「ログイン機能」の不備 ①推測可能なセッションID ②URL埋め込みのセッションIDの外部への漏えい ③クッキーのセキュア属性不備 ④セッションIDの固定化
5	クロスサイト・スクリプティング(XSS)
6	利用者の意図に反した実行の防止機能の不備 ①クロスサイト・リクエスト・フォージェリ（CSRF） ②クリックジャッキング
7	メールヘッダ・インジェクション脆弱性
8	「アクセス制御」と「認可処理」の不備 ①アクセス制御 ②認可処理
9	HTTPヘッダ・インジェクション
10	evalインジェクション
11	競合状態の脆弱性
12	意図しないファイル公開
13	アップロードファイルによるサーバ側スクリプト実行
14	秘密情報表示時のキャッシュ不停止（キャッシュを介して情報の暴露）
15	オープンリダイレクタ脆弱性（意図しないリダイレクト）
16	クローラへの耐性