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

1 SQLインジェクション対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	SQL文の組み立ては全てプレースホルダで実装する。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要
根本的解決	SQL文の構成を文字列連結により行う場合は、アプリケーションの変数をSQL文のリテラルとして正しく構成する。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要
根本的解決	ウェブアプリケーションに渡されるパラメータにSQL文を直接指定しない。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要
保険的対策	エラーメッセージをそのままブラウザに表示しない。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要
保険的対策	データベースアカウントに適切な権限を与える。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要

2 OSコマンド・インジェクション対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	シェルを起動できる言語機能の利用を避ける。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要
保険的対策	シェルを起動できる言語機能を利用する場合は、その引数を構成する全ての変数に対してチェックを行い、あらかじめ許可した処理のみを実行する。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要

3 パス名パラメータの未チェック／ディレクトリ・トラバーサル対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	外部からのパラメータでウェブサーバ内のファイル名を直接指定する実装を避ける。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要
根本的解決	ファイルを開く際は、固定のディレクトリを指定し、かつファイル名にディレクトリ名が含まれないようにする。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要
保険的対策	ウェブサーバ内のファイルへのアクセス権限の設定を正しく管理する。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要
保険的対策	ファイル名のチェックを行う。		
（未対応または差異の理由と対策）		□ 対応済 □ 未対策 □ 対応不要	□ 対応済 □ 未対策 □ 対応不要

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

4 セッション管理の不備への対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	セッションIDを推測が困難なものにする。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	セッションIDをURLパラメータに格納しない。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	HTTPS通信で利用するCookieにはsecure属性を加える。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	ログイン成功後に、新しくセッションを開始する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	ログイン成功後に、既存のセッションIDとは別に秘密情報を発行し、ページの遷移ごとにその値を確認する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
保険的対策	セッションIDを固定値にしない。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
保険的対策	セッションIDをCookieにセットする場合、有効期限の設定に注意する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要

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

5 クロスサイト・スクリプティング(XSS)対策

対策の性質	実施項目	設計時チェック	開発時チェック
HTMLテキストの入力を許可しない場合の対策			
根本的解決	ウェブページに出力する全ての要素に対して、エスケープ処理を施す。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
根本的解決	URLを出力するときは、「http://」や「https://」で始まるURLのみを許可する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
根本的解決	<script>…</script> 要素の内容を動的に生成しない。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
根本的解決	スタイルシートを任意のサイトから取り込めるようにしない。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
保険的対策	入力値の内容チェックを行う。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
HTMLテキストの入力を許可する場合の対策			
根本的解決	入力されたHTMLテキストから構文解析木を作成し、スクリプトを含まない必要な要素のみを抽出する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
保険的対策	入力されたHTMLテキストから、スクリプトに該当する文字列を排除する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
全てのウェブアプリケーションに共通の対策			
根本的解決	HTTPレスポンスヘッダのContent-Typeフィールドに文字コード（charset）の指定を行う。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
保険的対策	Cookie情報の漏えい対策として、発行するCookieにHttpOnly属性を加え、TRACEメソッドを無効化する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
保険的対策	クロスサイト・スクリプティングの潜在的な脆弱性対策として有効なブラウザの機能を有効にするレスポンスヘッダを返す。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			

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

6 クロスサイト・リクエスト・フォージェリ（CSRF）対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	処理を実行するページを POST メソッドでアクセスするようにし、その「hidden パラメータ」に秘密情報が挿入されるよう、前のページを自動生成して、実行ページではその値が正しい場合のみ処理を実行する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
根本的解決	処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
根本的解決	Refererが正しいリンク元かを確認し、正しい場合のみ処理を実行する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
保険的対策	重要な操作を行った際に、その旨を登録済みのメールアドレスに自動送信する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			

7 HTTPヘッダ・インジェクション対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	ヘッダの出力を直接行わず、ウェブアプリケーションの実行環境や言語に用意されているヘッダ出力用APIを使用する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
根本的解決	改行コードを適切に処理するヘッダ出力用APIを利用できない場合は、改行を許可しないよう、開発者自身で適切な処理を実装する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			
保険的対策	外部からの入力の全てについて、改行コードを削除する。	☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
（未対応または差異の理由と対策）			

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

8 メールヘッダ・インジェクション対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	メールヘッダを固定値にして、外部からの入力はすべてメール本文に出力する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	ウェブアプリケーションの実行環境や言語に用意されているメール送信用APIを使用する。 （上記項目を適用できない場合）		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	HTMLで宛先を指定しない。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
保険的対策	外部からの入力の全てについて、改行コードを削除する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要

9 クリックジャッキング対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	HTTPレスポンスヘッダに、X-Frame-Optionsヘッダフィールドを出力し、他ドメインのサイトからのframe要素やiframe要素による読み込みを制限する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	処理を実行する直前のページで再度パスワードの入力を求め、実行ページでは、再度入力されたパスワードが正しい場合のみ処理を実行する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
保険的対策	重要な処理は、一連の操作をマウスのみで実行できないようにする。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要

10 バッファオーバーフロー対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	直接メモリにアクセスできない言語で記述する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	直接メモリにアクセスできる言語で記述する部分を最小限にする。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	脆弱性が修正されたバージョンのライブラリを使用する。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要

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

11 アクセス制御や認可制御の欠落への対策

対策の性質	実施項目	設計時チェック	開発時チェック
根本的解決	アクセス制御機能による防御措置が必要とされるウェブサイトには、パスワード等の秘密情報の入力を必要とする認証機能を設ける。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要
根本的解決	認証機能に加えて認可制御の処理を実装し、ログイン中の利用者が他人になりすましてアクセスできないようにする。		
（未対応または差異の理由と対策）		☐ 対応済 ☐ 未対策 ☐ 対応不要	☐ 対応済 ☐ 未対策 ☐ 対応不要