様式第９号

## ■ウェブアプリケーションのセキュリティチェックシート

| No | 脆弱性の種類 | チェック | 実施項目 | 未対策・対応不要の場合は理由を記載 |
|---|---|---|---|---|
| 1 | SQLインジェクション | ※<br>□ 対応済<br>□ 未対策<br>□ 対応不要 | **SQL文の組み立ては全てプレースホルダで実装する。** | |
| | | | **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。** | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | **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。** | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | エラーメッセージをそのままブラウザに表示しない。 | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | データベースアカウントに適切な権限を与える。 | |
| 2 | OSコマンド・インジェクション | □ 対応済<br>□ 未対策<br>□ 対応不要 | **シェルを起動できる言語機能の利用を避ける。** | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | 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。 | |
| 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 | ※<br>□ 対応済<br>□ 未対策<br>□ 対応不要 | **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。** | |
| | | | **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。** | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | 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。 | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | ファイル名のチェックを行う。 | |
| 4 | セッション管理の不備 | □ 対応済<br>□ 未対策<br>□ 対応不要 | **セッションIDを推測が困難なものにする。** | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | **セッションIDをURLパラメータに格納しない。** | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | **HTTPS通信で利用するCookieにはsecure属性を加える。** | |
| | | ※<br>□ 対応済<br>□ 未対策<br>□ 対応不要 | **ログイン成功後に、新しくセッションを開始する。** | |
| | | | **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。** | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | セッションIDを固定値にしない。 | |
| | | □ 対応済<br>□ 未対策<br>□ 対応不要 | 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。 | |

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

# ■ウェブアプリケーションのセキュリティチェックシート

| No | 脆弱性の種類 | | チェック | 実施項目 | 未対策・対応不要の場合は理由を記載 |
|---|---|---|---|---|---|
| 5 | クロスサイト・スクリプティング | HTMLテキストの入力を許可しない場合の対策 | □ 対応済<br>□ 未対策<br>□ 対応不要 | **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<br>□ 未対策<br>□ 対応不要 | **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<br>□ 未対策<br>□ 対応不要 | **<script>…</script> 要素の内容を動的に生成しない。** | |
| | | | □ 対応済<br>□ 未対策<br>□ 対応不要 | **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<br>□ 未対策<br>□ 対応不要 | 入力値の内容チェックを行う。 | |
| | | HTMLテキストの入力を許可する場合の対策 | □ 対応済<br>□ 未対策<br>□ 対応不要 | **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<br>□ 未対策<br>□ 対応不要 | 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。 | |
| | | 全てのウェブアプリケーションに共通の対策 | □ 対応済<br>□ 未対策<br>□ 対応不要 | **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<br>□ 未対策<br>□ 対応不要 | 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<br>□ 未対策<br>□ 対応不要 | 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。 | |
| 6 | CSRF<br>（クロスサイト・リクエスト・フォージェリ） | | ※<br>□ 対応済<br>□ 未対策<br>□ 対応不要 | **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。** | |
| | | | | **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。** | |
| | | | | **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<br>□ 未対策<br>□ 対応不要 | 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。 | |
| 7 | HTTPヘッダ・インジェクション | | ※<br>□ 対応済<br>□ 未対策<br>□ 対応不要 | **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。** | |
| | | | | **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<br>□ 未対策<br>□ 対応不要 | 外部からの入力の全てについて、改行コードを削除する。 | |

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

# ■ウェブアプリケーションのセキュリティチェックシート

| No | 脆弱性の種類 | チェック | 実施項目 | 未対策・対応不要の場合は理由を記載 |
|---|---|---|---|---|
| 8 | メールヘッダ・インジェクション | ※<br>☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | **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。** | |
| | | | **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(8-(i) を採用できない場合)。** | |
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | **HTMLで宛先を指定しない。** | |
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | 外部からの入力の全てについて、改行コードを削除する。 | |
| 9 | クリックジャッキング | ※<br>☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | **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。** | |
| | | | **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<br>☐ 未対策<br>☐ 対応不要 | 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。 | |
| 10 | バッファオーバーフロー | ※<br>☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | **直接メモリにアクセスできない言語で記述する。** | |
| | | | **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。** | |
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | **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。** | |
| 11 | アクセス制御や認可制御の欠落 | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | **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。** | |
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | **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。** | |

※ このチェック項目の「対応済」のチェックは、実施項目のいずれかを実施した場合にチェックします。

上記以外の脆弱性で確認すべき内容

| No | 脆弱性の種類 | チェック | 実施内容 | 備考 |
|---|---|---|---|---|
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | | |
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | | |
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | | |
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | | |
| | | ☐ 対応済<br>☐ 未対策<br>☐ 対応不要 | | |