＜診断項目一覧＞

ver3.5

Webアプリケーション診断

No.	調査項目		具体例	手動診断	ツール診断	PCIDSS v2	IPA「安全なウェブサイトの作り方 改訂第7版」（チェックリスト）	OWASP TOP10 (2017)
1	認証	ログイン	パスワードが画面表示されているか	○	×			A2
2			総当り攻撃対策の有無	○	×			A2
3			暗号化処理が適切に実施されているか	○	×	6.5.3		A2
4			自動ログイン処理に不備がないか	○	×			A2
5			認証回避が可能か	○	×			A2
6			認証失敗を利用して存在するIDが判明しないか	○	×			A2
7			脆弱なパスワードが許容されていないか	○	×	8.5.10 8.5.11		A2
8		その他	管理者がユーザーのアカウント情報が閲覧可能か	○	×			A2
9			ログイン後のページが直接参照で表示可能か	○	×			A2,A5
10	セッション管理	Cookieの取り扱い	Secure属性の指定が適切か	○	○		No4	A2
11			HttpOnly属性の指定があるか	○	○		No5	A2
12			Pathの指定が適切か	○	×			A2
13			有効期限が長いCookieを発行しているか	○	○			A2
14			Cookieに不適切な値を保持していないか	○	×			A2
15		セッションID	推測が困難なセッションIDを使用しているか	○	×		No4	A2
16			ユーザ側でセッションIDの指定が可能か	○	×			A2
17			ログイン前、ログイン後でセッションIDを変更しているか	○	○		No4	A2
18			ログアウト機能が存在するか	○	×			A2
19			セッションIDが固定か	○	×		No4	A2
20			セッションIDの有効期限、破棄が適切か	○	×		No4	A2
21			セッションIDの偽造を不正と処理しているか	○	×			A2
22			セッションIDがURLに格納されているか	○	○		No4	A2
23		クロスサイトリクエストフォージェリ	ユーザが意図しないデータ登録、更新が実施されるか	○	△	6.5.9	No4,No6	
24	入出力処理	SQLインジェクション	SQL文字列の入力を適切に処理しているか	○	○	6.5.1	No1	A1
25		クロスサイトスクリプティング	タグ文字列の入力を適切に処理しているか	○	○	6.5.7	No5	A7
26		ディレクトリトラバーサル	ディレクトリ指定文字列の入力を適切に処理しているか	○	○	6.5.1	No3	A1
27		コマンドインジェクション	コマンド文字列の入力を適切に処理しているか	○	○	6.5.1	No2	A1
28		改行インジェクション	レスポンスヘッダーにセットされる入力を適切に処理しているか	○	○	6.5.1		A1
29		LDAPインジェクション	不正なLDAPクエリが動作しないよう入力を適切に処理しているか	○	×	6.5.1		A1
30		リンクインジェクション	任意リンクの埋め込みに利用される入力を適切に処理しているか	○	○	6.5.1		A1,A7
31		パラメータ推測	各パラメータに推測可能なものがないか	○	×	6.5.1		
32		HTTPレスポンス分割	HTTPのレスポンスに不正な改行が入らないか	○	○	6.5.1	No7	A1
33		SSIインジェクション	Webページに任意のファイルを挿入可能か	○	×	6.5.1		A1
34		XXE	XMLの入力を適切に処理しているか	○	×	6.5.1		A4
35		evalインジェクション	jsonに不正なコードを入力し、想定外の動作が発生しないか	○	×	6.5.1		A1
36		バッファオーバーフロー及び整数オーバーフロー脆弱性	メモリリーク等により想定外の動作が発生しないか	○	○	6.5.2	No.10	
37		オープンリダイレクト	任意のURLへユーザを転送可能か	○	×	6.5.1		
38		リクエスト改竄	値変更による他ユーザ情報の開示	○	×	6.5.1		A5
39		その他	特殊文字のエスケープ漏れがないか	○	○	6.5.7	No5	A1
40			クエリーデータに重要情報が存在しているか	○	×	6.5.1		
41			妥当性チェックの不備が存在しているか	○	×	6.5.1	No5	
42			内部エラー（500 インターナルサーバエラー）が発生しているか	○	○	6.5.1 6.5.5	No10	
43	画面遷移	重要情報の更新	重要情報の更新時に確認メールを送信しているか	○	×			
44			重要情報の更新前に再認証を実施しているか	○	×			
45		権限昇格	他ユーザの情報が閲覧、変更可能か	○	×		No11	A5
46	ユーザ管理	履歴	ログイン履歴表示が存在するか	○	×			
47			利用履歴の表示機能が存在するか	○	×			
48		パスワード	利用者が任意のタイミングでパスワードの変更が可能か	○	×			
49			パスワード変更処理時に現在のパスワードが必須になっているか	○	×			
50			パスワードに有効期限が存在するか	○	×			
51			パスワードの世代管理を行っているか	○	×			
52			パスワードが利用者以外に閲覧可能か	○	×			
53			複雑なパスワードを強制しているか	○	×	8.5.10 8.5.11		
54			パスワードが画面やHTMLソースで確認可能か	○	×			
55			パスワード再発行で画面、メール等にパスワードを記載しているか	○	×			
56			パスワードリマインダの不備	○	×			

＜診断項目一覧＞

ver3.5

Webアプリケーション診断

No.	調査項目		具体例	手動診断	ツール診断	PCIDSS v2	IPA「安全なウェブサイトの作り方 改訂第7版」（チェックリスト）	OWASP TOP10 (2017)
57	暗号	通信の暗号化	サーバ証明書エラーが発生しないか	○	×	4.1		A3
58			パスワードやクレジットカード番号といった重要情報を暗号化通信で送信しているか	○	×	3.3		A3
59			証明書がサービス提供者のものになっているか	○	×	4.1		A3
60			強度が低い暗号方式を許容していないか	○	×	4.1		A3
61	ロジック流出	バッグドアとデバッグオプション	開発用のデバッグ情報が表示されているか	○	×	6.5.5		A6
62			開発用のバッグドアが無効になっているか	○	×	6.5.5		A6
63		エラー処理	エラー発生時にプログラムのロジックやソースを表示しているか	○	○	6.5.5		A6
64			エラー画面にバージョン情報が表示されているか	○	×	6.5.5		A6
65			カスタムエラーページが適切に設定されているか	○	×	6.5.5		A6
66		情報公開	平文に変換可能な暗号化方式によって暗号化されている情報があるか	○	×	4.1		A6
67			データベースのレコードやカラム名を連想させる情報を公開しているか	○	×	6.5.5		A6
68			サービス提供に不要な情報が公開されていないか	○	○	6.5.5		A6
69		コメント	個人情報や開発会社、ソースコードなどの情報が記載されているか	○	○	6.5.5		A3,A6
70	メール	スパムメール	メールの送信先が固定か	○	×			
71			メールの送信は同時に1通のみ許可しているか	○	×			
72			メール本文内に任意の入力文字列が記述可能か	○	×		No8	
73			送信元の改竄が可能か	○	×			
74			処理フローを無視して送信可能か	○	×			
75	画面設計	不適切な画面設計	アドレスバーを表示しているか	○	×			
76			ステータスバーを表示しているか	○	×			
77			右クリックを禁止していないか	○	×			
78			クリックジャッキング対策が行われているか	○	○		No9	
79			クレジットカード、口座番号などを画面、HTMLに表示、記載していないか	○	×	3.3		A3
80		ユーザへの説明	プライバシーポリシー（サイトポリシー）を明示しているか	○	×			
81			個人情報の取り扱い方はあっているか	○	×			
82	一般的な脆弱性	既知のソフトウェア脆弱性	脆弱性のあるバージョンのWebアプリケーションを使用しているか	○	×			A6,A9
83		強制ブラウジング	推測が容易なディレクトリ、ファイルがあるか	○	○	6.5.5		A6
84			システム管理ツールのWebインターフェースが公開されているか	○	○	6.5.8		A6
85		ディレクトリリスティング	ファイル一覧が取得可能なディレクトリがあるか	○	○	6.5.8		A6
86		ファイルダウンロード・アップロードの問題	他ユーザがアップロードしたファイルのダウンロード	○	×			A5
87			ファイルアップロードによるインジェクション攻撃	○	×			A1
88		Robots.txt	robots.txtによる情報公開があるか	○	○	6.5.8		
89	Webサーバ設定	システム情報の開示	レスポンスヘッダにバージョン情報が記載されているか	○	○	6.5.5		A6
90		不要なメソッド	OPTIONS、TRACEなど運用上不要なメソッドが有効か	○	○	6.5.5	No5	A6
91		初期アカウント	ミドルウェアの管理サイトで初期アカウントが有効になっていないか。	○	×			A6
92		ディレクトリ存在の確認	「403」コードでディレクトリ存在の確認が可能か	○	○	6.5.8		A6
93		サーバエラーメッセージ	デフォルトのサーバエラーメッセージが表示されているか	○	○	6.5.5		A6