別紙 Web アプリケーションの脆弱性チェックリスト

本システムに混入しないよう対処を求める脆弱性は次のとおり。なお、各脆弱性の定義は「脆弱性名称の定義に関する参照先」にて確認すること。

「脆弱性名称の定義に関する参照先」の各（1）～（3）で示す参照先記載内容は次のとおり。

（1）IPA 『安全なウェブサイトの作り方 改訂第 7 版(2016 年 1 月 27 日改訂)』のページと、章番号記載
http://www.ipa.go.jp/security/vuln/websecurity.html

（2）CWE－Common Weakness Enumeration の CWE 番号[1]を記載。※同サイトにおける脆弱性名称を一部和訳。
http://cwe.mitre.org/

（3）IPA『ウェブ健康診断仕様』のページと、識別記号記載
http://www.ipa.go.jp/security/vuln/websecurity.html

No	脆弱性名称		脆弱性名称の定義に関する参照先	
1	SQL インジェクション		(1)	P.6 － 1.1
			(2)	CWE-89
			(3)	P.9 － (A)
2	OS コマンド・インジェクション		(1)	P.10 － 1.2
			(2)	CWE-78
			(3)	P.12 － (D)
3	ディレクトリ・トラバーサル脆弱性		(1)	P.13 － 1.3
			(2)	CWE-98
			(3)	P.14 － (G)
4	「ログイン機能」の不備		(①～④に該当するもの)	
	①	推測可能なセッション ID	(1)	P.18 － 4-(ⅰ)
			(2)	CWE-330
			(3)	P.18 － (K) － 2
	②	URL 埋め込みのセッション ID の外部への漏えい	(1)	P.19 － 4-(ⅱ)
			(2)	CWE-522
			(3)	P.18 － (K) － 4, 5
	③	クッキーのセキュア属性不備	(1)	P.19 － 4-(ⅲ)
			(2)	CWE-614
			(3)	P.18 (K) － 3
	④	セッション ID の固定化	(1)	P.19 － 4-(ⅳ)-a、P.20 － 4-(ⅳ)-b
			(2)	CWE-384
			(3)	P.18 (K) － 1

[1] IPA 共通脆弱性タイプ一覧 CWE 概説 http://www.ipa.go.jp/security/vuln/CWE.html

No	脆弱性名称		脆弱性名称の定義に関する参照先	
5	クロスサイト・スクリプティング(XSS)		(1)	P.22 - 1.5
			(2)	CWE-79
			(3)	P.10 - (B)
6	利用者の意図に反した実行の防止機能の不備		(①、②に該当するもの)	
	①	クロスサイト・リクエスト・フォージェリ (CSRF)	(1)	P.30 1.6
			(2)	CWE-352
			(3)	P.11 - (C)
	②	クリックジャッキング	(1)	P.41 - 1.9
			(2)	該当なし
			(3)	該当なし
7	メールヘッダ・インジェクション脆弱性		(1)	P38 - 1.8
			(2)	CWE-93
			(3)	P.13 - (F)
8	「アクセス制御」と「認可処理」の不備			(次の①、②に該当するもの)
	①	アクセス制御	(1)	P.46 - 1.11.1
			(2)	CWE-284
			(3)	P.20 - (L)
	②	認可処理	(1)	P.46 - 1.11.2
			(2)	CWE-264
			(3)	P.20 - (L)
9	HTTP ヘッダ・インジェクション		(1)	P.34 - 1.7
			(2)	CWE-113
			(3)	P.16 - (I)
10	eval インジェクション		(1)	該当なし
			(2)	CWE-95
			(3)	該当なし
11	競合状態の脆弱性		(1)	該当なし
			(2)	CWE-366
			(3)	該当なし
12	意図しないファイル公開		(1)	該当なし
			(2)	CWE-425 、CWE-548
			(3)	P.13 - (E)

No	脆弱性名称	脆弱性名称の定義に関する参照先	
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	(1)	該当なし
		(2)	CWE-434
		(3)	該当なし
14	秘密情報表示時のキャッシュ不停止	(1)	該当なし
		(2)	CWE-524
		(3)	該当なし
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)	(1)	該当なし
		(2)	CWE-601
		(3)	P.15 - (H)
16	クローラへの耐性	(1)	該当なし
		(2)	該当なし
		(3)	P.21 - (M)