

## 仕様書別添 4

### 脆弱性リスト

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。なお、一部の脆弱性定義は (1) ~ (3) に該当するものがないため、当該名称解説 URL を記載している。

- (1) IPA 『安全なウェブサイトの作り方 改訂第 5 版(2012 年 3 月 30 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<sup>1</sup>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) LASDEC 『ウェブ健康診断仕様について (平成 22 年度版・一般公開用)』のページと、識別記号記載 <https://www.lasdec.or.jp/cms/12,1284.html#siyou-h22>

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. 7 - (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. 9 - (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. 10 - (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. 13 - (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. 13 - (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. 13 (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

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

		(3)	P. 13 (K) - 1
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. 8 - (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)
	(2)		CWE-352
	(3)		P. 8 (C)
	② クリックジャッキング	(1)	該当なし
		(2)	該当なし
		(3)	該当なし
		<参考> <a href="http://en.wikipedia.org/wiki/Clickjacking">http://en.wikipedia.org/wiki/Clickjacking</a>	
7	メールヘッダ・インジェクション脆弱性	(1)	P37 - 1.8
		(2)	CWE-93
		(3)	P. 10 - (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)
	(2)		CWE-284
	(3)		P. 14 - (L)
	② 認可処理	(1)	P. 40 - 9-(ii)
		(2)	CWE-264
		(3)	P. 14 - (L)
9	HTTP ヘッダ・インジェクション	(1)	P. 44 - 1.7
		(2)	CWE-113
		(3)	P. 11 - (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. 9 - (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)	P11 - (H)
16	クローラへの耐性	(1)	該当なし
		(2)	該当なし
		(3)	P. 15 - 2.5