

令和4年度 春期 情報処理安全確保支援士試験 解答例

午後Ⅱ試験

問1

出題趣旨	
アジャイル開発を行っている企業が増えている中、短期間でリリースすることを優先した結果、システムの脆弱性^{ぜい}対応が後回しになっているケースも見られる。 本問では、Web サイトのセキュリティを題材として、Web サイトにおける脆弱性対策の理解力、開発プロセスの変化に応じたセキュリティへの対応方法を検討する能力を問う。	

設問	解答例・解答の要点		備考
設問1	(1)	ア	
	(2)	・ダウンロードするライブラリに既知の脆弱性がないかを確認する。 ・特定の Web サイトからの入手をルール化し、明文化する。	
設問2	a	利用者 ID	順不同
	b	セッションオブジェクト	
設問3	(1)	c イ	
		d ア	
		e ア	
		f ア	
		g イ	
		h イ	
	(2)	i エ	
		j イ	
設問4		topic の値を https://db-y.b-sha.co.jp/ に変更した。	
設問5	(1)	k V 氏が用意したサイト	
	(2)	returnURL の値を固定値にする。	
設問6	(1)	① ・一部のセッション管理の脆弱性	
		② ・認可・アクセス制御の脆弱性	
	(2)	改良フェーズにおける1か月の休止期間	
	(3)	・専門技術者による脆弱性診断が必要なときは、改良リリースを次回に持ち越す。 ・半年に一度、改良リリースの期間を長くする。 ・定期的に、期間の長い改良リリースを設ける。	
	(4)	CSRF 対策用トークンの発行、HTML への埋め込み、必要なひも付け、及びこれを検証する処理	

問 2

出題趣旨		
昨今、クラウドサービスが積極的に活用されるようになってきており、クラウドサービスへの移行が増加している。クラウドサービスへの移行では、情報セキュリティについて、オンプレミスのシステムとは異なる知識と技術、運用の知見が求められる。 本問では、クラウドサービスへの移行を題材として、各種認証の仕組み、認証に関するセキュリティ対策などの知識及び技術力を問う。		

設問	解答例・解答の要点		備考
設問 1	(1)	a キャッシュ	
	(2)	b DDoS	
	(3)	c Host	
	(4)	Y-CDN-U-FQDN を名前解決した IP アドレスと同じ IP アドレスをもつ Web サイト	
	(5)	d TLS の接続先サーバ名	
設問 2	(1)	ST は認証サーバに送られないから	
	(2)	総当たり攻撃はオフラインで行われ、ログインに失敗しないから	
設問 3	(1)	e ウ	
	(2)	f ア	
	(3)	g 偽造	
	(4)	h 1	
		i 3	順不同
		j 4	
設問 4	(1)	k ウ	
		l イ	
		m ア	
	(2)	n エ	
	(3)	o (2)	
		p (6)	
	(4)	q ウ	
設問 5	(1)	r オ	
		s エ	
		t ウ	
	(2)	u (8)	
	(3)	v イ	
	(4)	w 認証要求	
		x ID トークン	