

令和2年度 10月 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	
情報システムの構築時にはリスク分析を行うが、運用開始後の改修時やほかのシステムとの機能統合時にはリスク分析が行われていない場合が見受けられる。リスク分析は、システムのセキュリティを確保するための重要な工程の一つであり、ここで不備があると後続の工程に悪影響を及ぼす。 本問では、企業の合併に伴う複数の Web サイトの統合を題材に、リスク分析を行う能力、及び Web アプリケーションプログラムにおけるセキュアプログラミングの能力を問う。	

設問	解答例・解答の要点		備考
設問1	a	LDAP-P, LDAP-Q, LDAP-R	
	b	LDAP	
設問2	本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。		
設問3	(1)	c ウ	
		d ア	
		f ケ	
		g イ	
	(2)	e ウ	
		h キ	
	(3)	i NamingException を投げる前に、childChecked を false にする	
設問4	(1)	j パスワードを、本人以外のメールアドレスに送ることができる	
	(2)	k パスワードリセットの URL を、登録済みメールアドレスだけに送る	
	(3)	① ・サイト P でポイントが不正に利用される。 ② ・サイト Q で A 百貨店の商品が不正に購入される。	
設問5	(1)	(い) (2)	
		(う) (4)	
	(2)	(あ) SP	
		(い) IdP	
		(う) SP	
	(3)	(え) SP	
		(か) IdP	
		(き) IdP	
		(く) SP	

問 2

出題趣旨	
昨今、パブリッククラウドの活用が進んでいる。一方、パブリッククラウドを利用する上でのセキュリティ対策を利用者が適切に設計・設定していなかったことによる情報漏えい事故も多発している。 また、ゼロトラストという概念をよく聞くようになった。それに基づけば、通信相手を常に認証する必要があるが、例えば多要素認証に対応した、クラウドサービスの認証基盤（IDaaS）や MDM など、そのための技術、環境が整ってきている。 本問では、働き方改革のためのマルチクラウドを活用したテレワーク環境の構築を題材に、クラウドサービス利用時のリスクを適切に評価する能力を問う。	

設問	解答例・解答の要点		備考
設問 1	(1)	イ	
	(2)	第三者の OTP アプリで不正に OTP を生成される。	
	(3)	a ウ	
		b エ	
		c イ	
		d ア	
		e カ	
		f オ	
設問 2	社内情報を表示した画面をカメラで撮影するという方法		
設問 3	(1)	社内情報を表示した画面のスクリーンショットを取るという方法	
	(2)	ア, ウ, エ	
設問 4	セキュリティ対策についての第三者による監査報告書で確認するという方法		
設問 5	DaaS-V でのクライアント証明書によるデバイス認証		
設問 6	(1)	g パスワードの推測によってログイン	
	(2)	容易に推測可能な PIN コードを設定する。	
	(3)	クライアント証明書によるデバイス認証を行う仕組み	