令和７年度　春期　情報処理安全確保支援士試験　解答例

午後試験

問１

出題趣旨
サプライチェーンの侵害事例は増えてきており，サプライチェーンに関する脅威は IPA“情報セキュリティ 10 大脅威”の組織編にも 7 年連続で含まれている。 本問では，システム開発企業でのサプライチェーンリスク対策についての取組を題材として，サプライチェーンリスク対策に関する知識や，侵害発生時の対策検討の能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	企画・設計工程からセキュリティ対策を組み込むという考え方		
	(2)	L 社の業務委託先に要求する対策と同等のセキュリティ対策を再委託先にも要求させること		
設問２	(1)	スクリプト P をダウンロードしておき，システム Q のサーバ上に配置する方法		
	(2)	スクリプト P を読み込む箇所をソースコードから削除する。		
	(3)	項番	1	
		修正内容	連携している外部サービスを管理対象に含める。	
設問３	(1)	ア	10	
		イ	4	
		ウ	5	
		エ	11	
	(2)	a	開発環境の踏み台サーバで共用アカウントを利用している。	
		b	問題なし。	
		c	問題なし。	
設問４		利用しているソフトウェアやそのバージョンが明確になり，脆弱性の影響有無を容易に把握できるから		
設問５	(1)	d	踏み台サーバ	
	(2)	(あ)	ツール F で検知できるエラーをより早く発見することができる。	
		(い)	CI/CD パイプラインの管理機能を使って自動実行することができる。	

問２

出題趣旨
脆弱性対応の優先順位の判断は，脆弱性が悪用されることを防ぐために非常に重要である。 本問では，公開サイトの脆弱性診断で検出された脆弱性を題材として，脆弱性の深刻度レベルと対応優先度を判断する能力及び対応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		a	ア	
		b	ア	
		c	ア	
		d	ア	
		e	イ	
設問２		f	新たな脆弱性が発見されたこと	順不同
		g	リスクが変わったと評価し値を変えたこと	
設問３	(1)	ウ		
	(2)	OpenSSH のログに認証タイムアウトのメッセージの出力が多数あったらサイト担当者に電子メールでアラートを送る。		
	(3)	クライアント認証を行う。		
設問４	(1)	WA-1	パラメータ item の値が容易に推測できること	
		WB-1	・発注確認機能の URL が推測困難であること ・発注確認機能の URL を入手する必要があること	
	(2)	3		
設問５	(1)	現状値	攻撃コードなどの情報を多くの公開サイトにある情報から判断する必要があるから	
		EPSS 値	FIRST のサイトで公開されている値をそのまま使えばよいから	
	(2)	l	EPSS 値の監視	
	(3)	診断時に実際に悪用できることを確認しているから		
設問６		m	A	
		n	A	
		o	C	
		p	A	
		q	B	
		r	B	
		s	A	
		t	S	

問３

出題趣旨
JPCERT コーディネーションセンター及び IPA が運営する脆弱性対策情報ポータルサイト“JVN（Japan Vulnerability Notes)”には，国内企業が開発したスマートフォンアプリケーションプログラムの脆弱性が公表されている。 本問では，スマートフォン用アプリケーションプログラムの脆弱性を題材として，脆弱性への対策の能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	C サービスに送られた HTTP リクエストの Authorization ヘッダーから取り出す。		
	(2)	F アプリを解析し，暗号化されたアクセスキー並びに共通鍵及び初期ベクトルを入手し，暗号化されたアクセスキーを AES-CBC で復号する。		
	(3)	ファイル名に含まれる注文番号を 00000001 から順に増やしてダウンロードを試行する。		
	(4)	・https://www.a-sha.co.jp.k-sha.co.jp/ ・https://www.a-sha.co.jp@k-sha.co.jp/ ・https://k-sha.co.jp/		
設問２	(1)	www.a-sha.co.jp		
	(2)	a	オ	
		b	ケ	
		c	ウ	
		d	コ	
		e	ア	
		f	イ	
		g	カ	
		h	キ	
	(3)	通信解析ツールのプライベート認証局のルート証明書をインストールし，信頼設定を行う。		
設問３		i	(い)	
設問４	(1)	URL を確認する手段がない。		
	(2)	WebView を呼び出す前に，URL の先頭が https://www.a-sha.co.jp/であるかを検証する。		

問４

出題趣旨
企業で利用しなくなったのに残っていたドメインや公開されたままになっていた Web サーバを悪用するサイバー攻撃が多発している。 本問では，ある企業での IT 資産管理及び脆弱性管理を題材として，未把握の公開 IT 資産を発見し，管理するマネジメント能力を問う。

設問		解答例・解答の要点		備考
設問１		サーバ名	権威 DNS サーバ	
		変更内容	終了したサブドメインの CNAME レコードを削除する。	
設問２	(1)	a	レンタルサービスを契約して利用した	順不同
		b	他社データセンターを契約して利用した	
	(2)	c	WHOIS	
	(3)	あ	Z	
		い	X	
		う	Y	
	(4)	d	オ	
		e	ア	
		f	イ	
		g	ク	
		h	キ	
設問３	(1)	ポートスキャンで Web のポートだけが開いていることを確認する。		
	(2)	脆弱性スキャナーを実行して，脆弱性の有無を確認する。		
	(3)	する場合	一旦，サービスを停止し，脆弱性を修正後に再開する。	
		しない場合	速やかにネットワークから切り離し，機器を廃棄する。	
設問４	(1)	4.0		
	(2)	ウ		
	(3)	実際に悪用された。		
	(4)	項番１	情シ部が IT 資産管理台帳にある SW について，重要な脆弱性情報が発表されていないかを継続的に確認する。	
		項番２	該当 SW を保有する管理部門に対策の優先度を連絡し，対策実施を確認する。	