令和５年度　秋期　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
脆弱性を悪用されたインシデント発生時の対策立案においては，影響度の把握や適切な対策検討，及び優先度決定のため，どのような脆弱性がどのように悪用されたかを理解した上で対応を検討する必要がある。 本問では，Web アプリケーションプログラムの脆弱性を悪用されたことによるインシデント対応を題材に，HTML や ECMAScript から悪用された脆弱性と問題点を読み解き，対策を立案する能力を問う。

設問		解答例・解答の要点	備考
設問１	(1)	イ	
	(2)	レビュータイトルを出力する前にエスケープ処理を施す。	
設問２		HTML がコメントアウトされ一つのスクリプトになるような投稿を複数回に分けて行った。	
設問３	(1)	XHR のレスポンスから取得したトークンとともに，アイコン画像としてセッション ID をアップロードする。	
	(2)	会員のアイコン画像をダウンロードして，そこからセッション ID の文字列を取り出す。	
	(3)	ページ V にアクセスした会員になりすまして，Web アプリ Q の機能を使う。	
設問４		スクリプトから別ドメインの URL に対して cookie が送られない仕組み	

問２

出題趣旨
企業内ネットワークでは，無線 LAN が広く普及している。来客者用の無線 LAN が設置されている場合もあり，こういった環境では，第三者が接続しないように，セキュリティ対策を行うことが重要である。 本問では，アパレル業におけるセキュリティ対策の見直しを題材に，無線 LAN を使った環境における脅威を様々な角度から想定する能力及びセキュリティ対策を立案する能力を問う。

設問			解答例・解答の要点	備考
設問１	(1)	a	利用者 ID	順不同
		b	パスワード	
	(2)	c	このサーバ証明書は，信頼された認証局から発行されたサーバ証明書ではない	順不同
		d	このサーバ証明書に記載されているサーバ名は，接続先のサーバ名と異なる	
	(3)	HTTP のアクセスを HTTPS のアクセスに置き換えてアクセスする。その後，偽サイトからサーバ証明書を受け取る。		
設問２	(1)	外部共有者のメールアドレスに自身の私用メールアドレスを指定する。		
	(2)	e	MAC アドレス	
設問３	(1)	RADIUS		
	(2)	f	秘密鍵	
	(3)	g	業務 PC から取り出せないように	
	(4)	EAP-TLS に必要な認証情報は，業務 PC にしか格納できないから		
	(5)	来客用無線 LAN からインターネットにアクセスする場合の送信元 IP アドレスを a1.b1.c1.d1 とは別の IP アドレスにする。		
	(6)	h	DNS	
	(7)	表３	1	
		表４	1，4	

問３

出題趣旨
クラウドサービスが広く浸透している。様々なクラウドサービスの活用は，組織に多くの利便性をもたらす一方で，クラウドサービスで発生したインシデントが，自組織にも影響を及ぼし得る。このようなインシデントが発生した場合，迅速に状況を把握し，影響を考慮して対処することが重要である。 本問では，継続的インテグレーションサービスを提供する企業とその利用企業におけるインシデント対応を題材に，攻撃の流れと波及し得る影響を推測し，対策を立案する能力を問う。

設問		解答例・解答の要点		備考
設問１		ウ，エ		
設問２	(1)	偽サイトに入力された TOTP を入手し，その TOTP が有効な間にログインした。		
	(2)	ア		
	(3)	イ		
	(4)	/proc ファイルシステムから環境変数を読み取った。		
	(5)	認証に用いる情報に含まれるオリジン及び署名をサーバが確認する仕組み		
	(6)	a	ア	
設問３	(1)	有効なコード署名が付与された偽の P アプリを J ストアにアップロードする攻撃		
	(2)	J 社の Web サイトから削除する。		
	(3)	秘密鍵が漏れないという利点		
	(4)	影響	P アプリを起動できない。	
		対応	P アプリをアップデートする。	

問４

出題趣旨
情報資産を保護するためには，リスクを洗い出すことが出発点となる。リスクを洗い出した後，そのリスクによる情報資産への影響を分析した上で，対策の必要性を評価し，具体的な対策の内容を検討することが重要である。これらのリスクアセスメントからリスク対応までのプロセスを適切に行えることが，情報処理安全確保支援士（登録セキスペ）には要求される。 本問では，業務委託関係にある百貨店と運送会社を題材に，リスクアセスメントを実施する能力，及び個々のリスクを低減するための対策を立案する能力を問う。

設問					備考
設問１			ア	10，11，12，13	
			イ	大	
			ウ	C	
			エ	G 百貨店で，S サービスへログイン可能な IP アドレスを W 社プロキシだけに設定する。	
設問２	①	(1)	あ	G 百貨店からW社への連絡を装った電子メールに未知のマルウェアを添付して，配送管理課員宛てに送付する。	①～③の例に限らず，本文に示した状況設定に沿うリスクアセスメントの結果が記述されていること
		(2)	い	配送管理課員が，添付ファイルを開き，配送管理用 PC が未知のマルウェアに感染した結果，ID と PW を周知するメールが読み取られ，S サービスの ID と PW が窃取される。その ID と PW が利用されて，W 社外から S サービスにログインされて，Z 情報が漏えいする。	
			う	2，3，5，6，9，12	
			え	大	
			お	高	
			か	A	
			き	配送管理用 PC に EDR を導入し，不審な動作が起きていないかを監視する。	

	②	(1)	あ	配送管理課員がよく閲覧する Web サイトにおいて，脆弱性を悪用するなどして，配送管理課員が閲覧した時に，未知のマルウェアを別の Web サイトからダウンロードさせるように Web ページを改ざんする。	
		(2)	い	配送管理課員が，改ざんされた Web ページを閲覧した結果，マルウェアをダウンロードして PC がマルウェアに感染する。マルウェアがキー入力を監視して，配送管理課員が S サービスにアクセスした際に ID と PW が窃取される。その ID と PW が利用されて，W 社外から S サービスにログインされ，Z 情報が W 社外の PC などに保存される。	
			う	2，3，6	
			え	大	
			お	低	
			か	C	
			き	プロキシサーバの URL フィルタリング機能の設定を変更して，配送管理用 PC からアクセスできる URL を必要なものだけにする。	
	③	(1)	あ	W 社からアクセスすると未知のマルウェアをダウンロードする仕組みの Web ページを用意した上で，その URL リンクを記載した電子メールを，G 百貨店からW社への連絡を装って送信する。	
		(2)	い	配送管理課員が，電子メール内の URL リンクをクリックすると，配送管理用 PC が未知のマルウェアに感染する。PC 内に残っていた Z 情報を一括出力したファイルが，マルウェアによって攻撃者の用意したサーバに送信され，Z 情報が漏えいする。	
			う	2，3，5，6，9，10	
			え	大	
			お	高	
			か	A	
			き	全ての PC とサーバに，振舞い検知型又はアノマリ検知型のマルウェア対策ソフトを導入する。	
設問３			a	5，10，12	
			b	2，3，4	