令和７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
インシデント発生時は，インシデント対応を行うとともに，インシデントが攻撃によるものなのかどうか，脆弱性が悪用されたのかどうかを調べた上で，適切な再発防止策を検討する必要がある。 本問では，Web アプリケーションの脆弱性を悪用されたインシデントを通して，セキュアプログラミングに対する理解，並びに HTML 及び ECMAScript を読み解いて問題点及び原因を認識し，対策を講じる実践的能力を問う。

設問		解答例・解答の要点		備考
設問１		a	できない	
		b	できない	
設問２	(1)	ロール管理		
	(2)	c	タスク名	
	(3)	d	個人タスク<script src="/files/F1234567890.xlsx"></script>	
	(4)	e	管理者	
		f	タスクの締切日を過ぎる。	
		g	利用者のロールを管理者に設定する。	
	(5)	図３のスクリプトを S サービス内にアップロードする工夫		
設問３	(1)	h	アップロードされたファイルの形式が拡張子と整合しているかをチェックする。	
	(2)	i	プロジェクト進捗管理	
	(3)	出力時にエスケープ処理を施す。		
設問４		j	S サービスの仕様を理解した専門家による脆弱性検査	

問２

出題趣旨
近年，サイバー攻撃の増加に伴い，情報システムの設計，開発並びに運用等のあらゆる場面において，暗号技術を理解することがますます重要になっている。暗号の適切な利用によって情報の機密性や完全性を担保することができる一方，暗号の不適切な利用はシステムの脆弱性を生むことにつながる。 本問では，暗号資産交換業における暗号鍵の管理を題材として，情報の暗号化及び復号，並びにデジタル署名の生成及び検証のそれぞれの処理に関する基礎的な理解を問うとともに，暗号鍵の暗号化といった暗号技術の高度な応用力を問う。

設問		解答例・解答の要点		備考
設問１		ウ，エ		
設問２		施設 K の外から，鍵管理 PC の作動音や鍵管理 PC から放出される電磁波を観測し，署名鍵 S を推測する。		
設問３	(1)	(i)と(ii)の間	B コインを攻撃者に移転する移転情報を記録したファイルを業務用メディア内に追加する。	
		(vi)と(vii)の間	B コインを攻撃者に移転する署名済みの移転情報を記録したファイルを攻撃者に送信するとともに，業務用メディアから削除する。	
	(2)	a	メッセージ認証符号	
	(3)	当日担当者を複数名とし，互いに確認しながら作業を実施するように手順を変更する。		
設問４	(1)	作業 2 において，パスワードで暗号化した署名鍵 S と紙に書き留めたパスワードを一緒に移送している点		
	(2)	b	ウ	
		c	ア	
		d	エ	
		e	ウ	
		あ	オ	
		い	ク	
	(3)	復号鍵 D がないので，暗号化された署名鍵 S は復号できない。		
	(4)	攻撃者の生成した鍵ペアの暗号鍵		

問３

出題趣旨
働き方改革の一環としてリモートワークの導入が広まっている。リモートワークに使用するインフラの導入には，効率的な業務の実現に加え，必要なセキュリティレベルの確保を検討することが重要である。 本問では，リモートワーク環境の導入を題材として，IT 環境のセキュリティ対策及び VPN サービスの導入方法を問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	DNSSEC	
	(2)	b	DoH	
		c	TLS	
設問２		d	イ	
		e	ア	
設問３		K サービス設定サイトへのアクセスが許可される接続元 IP アドレスを a1.b1.c1.d1 に制限する。		
設問４	(1)	f	各取引先サービスへの接続を許可する IP アドレスとして，P 社専用の K サービス用固定グローバル IP アドレスを登録してもらう	
	(2)	Z-IB，OS ベンダーの OS アップデート配布サイト，認証基盤サービス及び K サービス設定サイトへの HTTPS サービス		
設問５	(1)	g	認証方式 1 の電話番号として，個人所有スマホの電話番号を登録する	
	(2)	K サービス接続時のログから OS がバージョン X の社有 PC を抽出し，アカウント名から利用者を特定後，利用者の所属する部の情報セキュリティ推進者に報告し，バージョン Y への移行を促してもらう。		

問４

出題趣旨
サプライチェーンにおけるセキュリティリスクの管理が進んでいる現在，サプライチェーンに組み込まれている企業では，より上流又は下流に位置する企業から情報セキュリティ管理体制の構築が求められることがよくある。 本問では，そのような場面を題材に，ある企業のシステム構成，ネットワーク構成及び業務の流れを前提として，攻撃シナリオの検討，並びに，その攻撃シナリオへの対策及び必要な運用手順の立案の能力を問う。

<table>
<tr><th colspan="2">設問</th><th colspan="5">解答例・解答の要点</th><th>備考</th></tr>
<tr><td colspan="2" rowspan="2">設問１</td><td>a</td><td colspan="4">未知の</td><td></td></tr>
<tr><td>b</td><td colspan="4">暗号化</td><td></td></tr>
<tr><td rowspan="11">設問２</td><td rowspan="4">(1)</td><td>c</td><td colspan="4">回避</td><td rowspan="3">順不同</td></tr>
<tr><td>d</td><td colspan="4">移転</td></tr>
<tr><td>e</td><td colspan="4">保有</td></tr>
<tr><td rowspan="8">(2)</td><td colspan="2">所属組織</td><td>読込権限</td><td>書込権限</td><td>権限変更権限</td><td></td></tr>
<tr><td colspan="2">総務部総務課</td><td>×</td><td>×</td><td>×</td><td></td></tr>
<tr><td colspan="2">総務部情報システム課</td><td>×</td><td>×</td><td>○</td><td></td></tr>
<tr><td colspan="2">営業部</td><td>○</td><td>○</td><td>×</td><td></td></tr>
<tr><td colspan="2">製造部設計課</td><td>○</td><td>×</td><td>×</td><td></td></tr>
<tr><td colspan="2">製造部製造課</td><td>○</td><td>×</td><td>×</td><td></td></tr>
<tr><td colspan="2">製造部品質保証課</td><td>○</td><td>×</td><td>×</td><td></td></tr>
<tr><td colspan="2" rowspan="2">設問３</td><td>f</td><td colspan="4">図 3 中の(け)の箇所に，追加で FW</td><td></td></tr>
<tr><td>g</td><td colspan="4">USB メモリを接続したときの動きを確認するためのソフトウェアを導入した，社内 LAN から切り離された検査用 PC</td><td></td></tr>
<tr><td rowspan="5">設問４</td><td rowspan="2">(1)</td><td>h</td><td colspan="4">SCADA 内の NC プログラムをバックアップ／リストアするための媒体とソフトウェア</td><td rowspan="2">左の例に限らず，本文の状況に沿った仕組み，手順が記述されていること</td></tr>
<tr><td>i</td><td colspan="4">SCADA に NC プログラムをリストアする手順</td></tr>
<tr><td rowspan="3">(2)</td><td>j</td><td colspan="4">マルウェアに感染した一般 PC が，正常な通信を妨害するパケットを大量に送信して，SCADA と工作機械の間の通信ができなくなる。</td><td rowspan="3">左の例に限らず，本文の状況に沿った被害のシナリオが記述されていて，有効な仕組み，手順が記述されていること</td></tr>
<tr><td>k</td><td colspan="4">SCADA，工作機械及び製造監視用 PC だけの独立した LAN を構成するためのネットワーク機器</td></tr>
<tr><td>l</td><td colspan="4">SCADA，工作機械及び製造監視用 PC を L 社のネットワークから切り離す手順</td></tr>
</table>