

午後 試験

問 1

出題趣旨	
<p>企業活動の効率向上を目的として、部門ごとの個別の業務を、外部ベンダに委託することがある。この場合、業務を遂行する段階で、外部ベンダに委託した業務が適切に履行されているかどうかを確認するとともに、社内における管理体制が適切に機能しているかどうかを確認することが必要となる。さらに、社内外の状況の変化に対応して、委託業務の内容や社内の管理体制を改善することが必要となる。</p> <p>本問では、日々新たな脆弱性が発見される状況下において、開発・運用を外部委託している Web 受注システムのセキュリティ対策の改善策を例に、情報セキュリティアドミニストレータとしての、問題分析能力、解決策立案能力を問う。</p>	

設問	解答例・解答の要点		備考
設問 1	a	オ	
	b	カ	
設問 2	(1)	シグネチャファイルを常に最新版に更新すること	
	(2)	入力された文字列が暗号化されているから	
設問 3	(1)	対策の実行が Web 受注システムに悪影響を与えないことを確認する必要があるから	
	(2)	<ul style="list-style-type: none"> <li>・規約どおりに Web 受注アプリを開発した証跡資料を提出させること</li> <li>・ソースコード検査ツールによる検査の結果資料を提出させること</li> </ul>	
設問 4	必須な項目	<ul style="list-style-type: none"> <li>・セキュリティ事故として X 社へ通報すべき問合せの範囲と内容</li> <li>・セキュリティ事故の発生を疑わせるような問合せへの対応手順</li> </ul>	
	方法	<ul style="list-style-type: none"> <li>・問合せ対応のテストを行う。</li> <li>・問合せ対応の記録を点検する。</li> </ul>	

問 2

出題趣旨	
<p>ノート PC などの普及によって、PC を社外に持ち出したり、社外に持ち出したノート PC を社内ネットワークへ接続したりするケースが増えている。このような PC のネットワーク利用形態の多様化に伴い、セキュリティレベルの確保が困難になるエンドポイントの脅威からネットワーク上の資源を適切に保護するための仕組みとして、検疫システムが注目されている。</p> <p>本問では、検疫システムについての基礎知識と、状況に応じた検疫システムの構築、運用についての実務的能力を問う。</p>	

設問	解答例・解答の要点		備考
設問 1	a	エ	
	b	イ	
設問 2	(11)		
設問 3	(1)	タイミング	IP アドレス取得後、パターンファイルやパッチが更新されるまで
		範囲	<ul style="list-style-type: none"> <li>・幹線 Q 社 L3SW を経由しない PC 間</li> <li>・幹線 Q 社 L3SW で隔離された業務用 VLAN 以外の範囲</li> </ul>
	(2)	<ul style="list-style-type: none"> <li>・検査が終了する前も IP 通信が可能だから</li> <li>・検査を行う前から IP 通信が可能となるから</li> </ul>	
設問 4	PC と D 社 L2SW の間にハブを接続し、複数台の PC を起動する。		

問3

出題趣旨	
<p>最近は、個人情報扱う部屋などの特別な区域への入退室管理において、記憶や持ち物による認証に替えて、忘れてたり紛失したりすることのない、指紋、静脈、虹彩などによる生体認証の採用が増えてきた。</p> <p>本問では、生体認証の特性やリスクを理解して高セキュリティの入退室管理システムを構築、運用するための知識と実践技術を問う。</p>	

設問	解答例・解答の要点	備考
設問1	a 才	
	b キ	
	c 力	
設問2	ア <ul style="list-style-type: none"> <li>・認証の速度</li> <li>・処理性能</li> <li>・応答性</li> </ul>	
	イ <ul style="list-style-type: none"> <li>・認証の精度</li> <li>・識別精度</li> </ul>	
設問3	(1) 指紋登録時に登録者本人であることを確認し、登録操作に立ち会う。	
	(2) ウ 特徴点を抽出して数値化	
設問4	(1) 来訪者の入退室を記録して保管する。	
	(2) 指紋登録できない人を対象に、入退室カードと暗証番号の入力による個人認証を導入する。	

問4

出題趣旨	
<p>Web サイトを活用した各種の会員向けサービスが様々な組織の Web サイトで一般的に行われている。しかしながら、ポイント付与などの附帯サービスを行うためには個人情報の管理がどうしても避けられず、法律にのっとった細心の注意を行使させる必要がある。</p> <p>本問では、情報セキュリティアドミニストレータとして、組織での個人情報保護施策実施の際の、全般的なセキュリティ対策のチェックを行う能力について問う。また、自社の Web サイトの安全性だけでは防ぎきれないフィッシングの問題に関して、消費者保護のための対応策への理解についても問う。</p>	

設問	解答例・解答の要点	備考
設問1	a 力	
	d ク	
	e 工	
設問2	b エスケープ処理 又は サニタイジング	
	c ファイル名を直接指定	
設問3	(1) <ul style="list-style-type: none"> <li>・SSL通信が行われていること</li> <li>・Webサイトとの通信経路の暗号化</li> </ul>	
	(2) 鍵マークをダブルクリックして表示される証明書の発行先が、J社のドメイン名であるかを確認してください。	
設問4	<ul style="list-style-type: none"> <li>・電話でパスワードなどの認証情報は答えないこと</li> <li>・J社側から電話で、パスワードなどの認証情報を聞くことはないこと</li> </ul>	