

平成 19 年度 春期 テクニカルエンジニア（情報セキュリティ）試験 解答例

午後Ⅱ試験

問 1

出題趣旨	
セキュリティは品質要件の一部である。実際のシステム設計においては、システムに対する機能要件、セキュリティ以外の品質要件、制約条件とのバランスをとりながらシステム全体の視点から判断して設計する必要がある。 本問では、大規模 Web システムにおけるセキュリティ設計を題材として、情報セキュリティ標準を遵守するための設計を行いつつ、実際の大規模システム開発において発生しがちな、セキュリティとほかの要件・制約とが相反する課題について、どのように解決すべきかを総合的に判断する能力を問う。	

設問		解答例・解答の要点						備考																																		
設問 1	a	物理																																								
	b	技術 又は 論理																																								
設問 2	(1)	制限エリアは必要最小限の運用管理者だけが入室可能なエリアとする。																																								
	(2)	・業務アプリケーション管理者が、機密情報と極秘情報が配置された制限エリアに入室することを防ぐ。 ・システム管理者と DB 管理者だけが機密情報と極秘情報にアクセスできるようにする。																																								
設問 3	(1)	アクセス記録中に記録される DB ユーザ ID からは個人を特定することができないから																																								
	(2)	業務アプリケーションで業務ユーザ ID を記録する。																																								
設問 4	(1)	変更前の暗号鍵による復号処理と変更後の暗号鍵による暗号化処理																																								
	(2)	計画停止時間を 2 時間以内とする品質要件が満たされないから																																								
	(3)	<table><tr><th>テーブル名</th><th>キー項目</th><th colspan="5">データ項目</th></tr><tr><td>変換 TBL</td><td>口座番号</td><td>内部 ID</td><td></td><td></td><td></td><td></td></tr><tr><td>検索 TBL_A</td><td>内部 ID</td><td>カナ姓</td><td></td><td></td><td></td><td></td></tr><tr><td>検索 TBL_B</td><td>内部 ID</td><td>カナ名</td><td></td><td></td><td></td><td></td></tr><tr><td>顧客 TBL (変更後)</td><td>内部 ID</td><td>暗証番号</td><td>住所</td><td>電話番号</td><td>生年月日</td><td>勤務先</td></tr></table>							テーブル名	キー項目	データ項目					変換 TBL	口座番号	内部 ID					検索 TBL_A	内部 ID	カナ姓					検索 TBL_B	内部 ID	カナ名					顧客 TBL (変更後)	内部 ID	暗証番号	住所	電話番号	生年月日
テーブル名	キー項目	データ項目																																								
変換 TBL	口座番号	内部 ID																																								
検索 TBL_A	内部 ID	カナ姓																																								
検索 TBL_B	内部 ID	カナ名																																								
顧客 TBL (変更後)	内部 ID	暗証番号	住所	電話番号	生年月日	勤務先																																				

問2

出題趣旨	
社内システムの構築においては、従業員の安全な認証や、リモートアクセス及び電子メールの的確な運用が求められる場合が多い。リモートアクセスでは SSL や IPsec がしばしば使われる。また、社外で使用する PC のセキュリティ対策も重要である。さらに、ウイルスメール、スパムメール対策も重要となる。 本問では、その際に必要とされるリモートアクセスや認証技術、社外で使用する PC や電子メールのセキュリティ対策技術に関する知識と能力を問う。	

設問	解答例・解答の要点		備考
設問1	(1)	a 停止	
		b アクセスログ	
	(2)	適切な本人確認を行わずに新しいパスワードを伝えている。	
設問2	(1)	c IKE	
		d ESP	
		e DH 又は Diffie-Hellman	
	(2)	・相手を認証するため ・相手がもつ事前共有鍵の正当性を検証するため	
	(3)	一時鍵情報 p や一時鍵情報 q を攻撃者が入手できないから	
	(4)	モード アグレッシブモード 理由 利用するインターネット接続環境では IP アドレスは固定ではないから	
設問3	(1)	f 生体 又は バイオメトリクス	
		g 本人	
		h 他人	
	(2)	登録されている事前共有鍵の無効化	
設問4	(1)	ネットワーク接続ができないところではデータを利用できない。	
	(2)	ノート PC のハードディスクを暗号化し、復号鍵を認証デバイスに保管する。	
設問5	(1)	社外からのスパムメールを送信する SMTP の送信元アドレスが FW のアドレスに書き変わってしまったから	
	(2)	感染してしまった原因 図 5 は偽のアラートメールであり、ウイルス付きのソフトウェアをダウンロードして実行してしまったから	
		検知できなかった理由 HTTP アクセスに関するウイルスチェックは行っていなかったから	
	(3)	セキュリティパッチや修正プログラムは、パッチサーバ以外からダウンロードしない。	