

平成 20 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	
最近では、Web を前提としたシステム開発が主流となっているが、アプリケーション開発時のセキュリティ対策は正しく実施されていないことが少なくない。 本問では、Web アプリケーションシステムで“SQL インジェクション”による不正アクセスがあった状況を想定し、適切なインシデント対応の在り方や、“ディレクトリトラバーサル”；“認可処理の欠如”などの多く見受けられる脆弱性に対する、適切なプログラミング手法を問題として取り上げた。	

設問	解答例・解答の要点			備考
設問 1	(1)	a	オ	
		c	エ	
	(2)	../bin/ifconfig		
	(3)	攻撃	OS コマンドの不正実行	
設問 2		問題点	非公開のファイル内容が不正参照されてしまう。	
	(1)	2007 年 10 月 13 日 4 時 28 分		
	(2)	d	query-string 又は クエリストリング	
	(3)	イ		
	(4)	b	各プログラムから DB へのアクセスに使用されている DB アカウントに付与する権限を最小化	
設問 3	(1)	①	・運用担当者が C 課長の許可なく DB にアクセスしている。	
		②	・運用担当者が DB アカウントを共用している。	
			・DB ログを収集していない。	
	(2)	不足している情報	TRN ログ単独 イ, エ	
			DB ログ単独 イ	
		改修内容	X システムにログインする利用者の識別子を DB 側に通知し、それを DB ログに出力して収集する。	
	(3)	①	・適切なインシデント対応手順を策定する。	
		②	・手順どおり対応できるように、定期的に訓練する。	

問2

出題趣旨	
近年，認証技術は身近なところに浸透しており，日常生活の中でも IC カードや生体認証などのデバイスを利用する機会が増えている。認証技術は情報セキュリティにおいて最も重要な技術分野の一つであり，その応用例は多岐にわたるが，その企画・設計においては様々な構成要素を適切に選択する必要がある。 本問では，専門学校における認証システムの企画・設計を題材として，Web やシングルサインオン，無線 LAN といった領域での認証に関する知識と設計の能力を問う。	

設問	解答例・解答の要点		備考
設問 1	(1)	a ダイジェスト 又は Digest	
	(2)	送受信されるデータ自体は暗号化されないから	
設問 2	(1)	b オ	
		c エ	
	(2)	・利用者 ID の移行に関するルールを定める。 ・認証情報の受渡しに関するルールを定める。	
	(3)	認証情報が漏えいした場合，なりすましによって利用可能なすべての情報システムにアクセスされる。	
設問 3	(1)	SSO 機能を提供するサーバに障害が発生すると，これを利用するすべての情報システムに利用者がアクセスできなくなる。	
	(2)	・クッキーはドメイン名の異なるサーバに送ることができないから ・ブラウザがクッキーをサーバに送信するかはドメイン名で判断するから	
設問 4	(1)	d オ	
		e カ	
		f キ	
		g ア	
	(2)	脅威 偽のアクセスポイントに接続させられてしまう。	
		被害 通信の内容を盗聴されたり改ざんされたりする可能性がある。	
設問 5	(1)	ア 利用者管理コストを軽減する	順不同
		イ 利用者の利便性を向上させる	
	(2)	将来想定される出席確認や入退室管理などへの応用に向くから	