

平成 26 年度 秋期 情報セキュリティスペシャリスト試験 解答例

午後Ⅱ試験

問 1

出題趣旨	
ビジネスを海外展開している企業においては、これまで地域や国ごとに行ってきた情報セキュリティ管理を統合するのに伴い、情報システムの利用者 ID 管理及びアクセス管理（ID and Access Management, 以下 IAM という）を統合する動きが起きている。IAM の統合においては、利用者の利便性並びに既存の情報システム及び運用管理プロセスへの影響を考慮し、最適なソリューションを選択する必要がある。 本問では、海外展開する大手金融機関における IAM の統合を題材に、IAM の設計及び運用上の考慮点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	認証 Cookie	
	(2)	b	アジアポータル	
	(3)	承認が行われず、社内システムにアクセスする必要がある者も ID を登録できてしまう。		
設問 2	(1)	G ポータルや G システムからエージェントを呼び出すための変更		
	(2)	GDS と各地域の DS 間で信頼関係を結ぶ。		
	(3)	日本と欧米地域の ID に重複があるという問題		
設問 3	(1)	契約社員の利用者情報が取り込まれない点		
	(2)	①	・日本 DS	
		②	・欧米 DS1	
設問 4		③	・アジア LDS	
	地域	日本		
	サーバ名	日本認証サーバ		
設問 5	(1)	①	・パスワード	
		②	・OTP トークン	
	(2)	多種の個人所有機器での利用者認証の動作検証		
設問 6	(3)	ネットワーク遅延が大きいことから、仮想デスクトップの操作に対するレスポンスが悪化する。		
	(1)	アジア地域		
	(2)		構成要素	設定内容
		①	アジア認証サーバ	SPNEGO の設定をする。
		②	アジア PC	SPNEGO の設定をする。
				①と②は順不同

問 2

出題趣旨	
Web サイトに対するセキュリティ対策が各企業で行われているが、企業によって対策の推進状況に差がある。Web サイトの基本的な脆弱性対策に抜けや漏れがあるケースや、最新の脆弱性への対応に追いついていないケースも見受けられる。 本問では、グループ企業のセキュリティインシデントと Web サイトのセキュリティ対策を題材として、SQL インジェクション、セキュリティ診断及び Web サイトの新しいセキュリティ対策に関する知識を問う。	

設問	解答例・解答の要点		備考
設問 1	(1)	a ウ	
		b ク	
	(2)	c /GoodsDetail	
		d goodsNo	
	(3)	残り 3 画面に SQL インジェクションの脆弱性があるかもしれないから	
	(4)	A 社情報システム部に事故発生後にすぐ報告していない点	
設問 2	(1)	e 診断ツールの IP アドレス	
	(2)	f ファイアウォールで遮断されているポート番号の通信に関わる脆弱性	
	(3)	修正によって新たな脆弱性が発生していないこと	
設問 3	(1)	g #	
		h </script>	
	(2)	診断方法	スクリプトを含むデータを Web アプリに入力し、それが Web サイトからの応答中に出力されているかを確認する。
		理由	Web サイトからの応答中に不正なスクリプトが含まれていないから
	(3)	サイト	サイト 5, サイト 6
		変更内容	X-FRAME-OPTIONS ヘッダの DENY を SAMEORIGIN にする。
	(4)	i ウ	
	(5)	j ブラウザのアドレスバーの情報で、https で通信していることを確認する	
	(6)	初回にブラウザで Web サイトへ http でアクセスした場合	