平成 23 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
社会インフラを担う情報システムでは，非常時にも業務を継続することが求められる。BCP 策定においては，情報システムに関する技術的な知識だけでなく，業務そのものに対する理解も必要となる。セキュリティ技術者には，こうした業務の観点からの取組みも求められるため，常日頃より幅広い視点でスキルの研さんと経験の積み重ねが要求される。 本問では，医療情報システムを題材にして，業務要件に応じたアクセス制御や，長期に渡るデータの真正性確保に関する技術についての知識と応用力を問うとともに，情報システムの可用性に加え，業務の非常時への対応についての経験と対応力を問う。

設問		解答例・解答の要点	備考
設問１	(1)	作成責任者以外の者による電子カルテへの署名	
	(2)	耐タンパ性	
設問２	(1)	医療行為に必要な範囲を超えて患者の医療情報にアクセスすることを抑止する効果	
	(2)	a　A，R，U，D，P	
	(3)	個別の利用者ごとに，電子カルテのデータ項目ごとに行うアクセス制御	
設問３	(1)	①　(J) ②　(K)	
	(2)	電子カルテのディジタル署名の有効期限が切れる前に，署名検証に必要な情報を含むアーカイブタイムスタンプを付与する。	
	(3)	b　ディジタル署名	
	(4)	バックアップから改ざん前の電子カルテを復旧する機能	
設問４	(1)	**日々行うべき業務**：患者ごとに，見読可能な画像データを電子カルテから生成し，USB ディスクに書き出しておく。	
		災害時に行うべき業務：電子カルテの画像データを保管した USB ディスクを端末に接続して，患者の電子カルテの画像データを医師に配布する。	
	(2)	① ② ・本人確認の方法と，認証に用いる IC カードの貸与及び利用者 ID の付与の方法 ・応援者の資格の確認方法と，応援者に付与するアクセス権限の内容と付与方法	

問２

出題趣旨
ログ管理システムの設計においては，セキュリティ技術だけでなく，既存システムの環境や運用全体を見渡す広い視野が必要になる。近年，実務を担当するセキュリティ技術者には，セキュリティに関する専門知識だけでなく，システムに求められる要件及び制約の一つとしてセキュリティをとらえ，多岐にわたる前提条件を収集整理した上で他の要件及び制約とのバランスをとりながら全体で最適となるセキュリティ機能を設計する能力が求められている。 本問では，大規模システムにおける，ログ管理システムの全体設計に関する，これらの能力と経験を問う。

設問		解答例・解答の要点		備考
設問１		a	DHCP	
		b	NTP	
設問２	(1)	通信内容が暗号化されており，ログの内容が分析できないから		
	(2)	**データ項目**	サーバのホスト名又はサーバの IP アドレス	
		判別できる場合	一つのウィンドウだけを使って特権操作を行った場合	
		判別の根拠となる情報	ログに記録された直前のログオン操作成功におけるサーバのホスト名又はサーバの IP アドレス	
	(3)	DBMS のログ取得機能がサーバ資源を大量に消費するから		
	(4)	**システム**	①　1 ②　2	
		理由	特権操作 2 以外の DB アクセスのログが大量に取得されるから	
	(5)	(F)，(G)，(H)		
設問３	(1)	東京 DC の電源設備の保守作業のとき		
	(2)	**最大データ量**	462	
	(3)	**伝送速度**	6	
	(4)	ログの改ざん防止のため		
	(5)	ログを保存する際は暗号化を行う。		
設問４	(1)	①　・管理端末と各サーバの時刻を同期させる。 ②　・管理端末と各サーバの ID 体系を統一する。		
	(2)	**役割名称**	オペレータ	
		理由	情報システム部の従業員はオペレータの具体的な作業内容を知らないから	
	(3)	**操作**	各社の管理責任者が行う特権操作	
		内容	特権操作を行った本人以外による確認	