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	