問３

出題趣旨
クラウドサービスの発展によって，企業におけるインターネット上の Web サービスの利用が増加傾向にある。Web サービスには SSL を用いることが多いが，プロキシで Web アクセス時のログを取得する場合，通信内容が暗号化されているので詳細なログを取得できない。 本問では，HTTPS 通信時におけるプロキシでのログ取得を題材として，HTTPS 通信時の動作及び証明書の検証についての理解を確認する。

設問		解答例・解答の要点		備考
設問１	(1)	ログを平文で記録できないから		
	(2)	(2)，(3)，(5)		
	(3)	ア		
設問２	(1)	a	中間者	
	(2)	① ②	・サーバ証明書のコモンネームとアクセス先のホスト名が一致すること ・サーバ証明書がブラウザで信頼する認証局から発行されていること	
設問３	(1)	b	L プロキシのルート証明書を信頼するルート証明書としてインストールする	
	(2)	証明書 2 はブラウザが信頼する認証局が発行したものではないから		
	(3)	サーバ証明書のコモンネームとアクセス先のホスト名を一致させるため		