問２

出題趣旨
DNS の名前解決通信は，主に UDP を用いる。UDP は，TCP と比べると送信元 IP アドレスの詐称の検知が難しく，キャッシュポイズニング攻撃の原因ともなっている。ファイアウォールの方式設計においては IP アドレス詐称対策を考慮する必要がある。さらに，インターネットに公開されているサーバの名前解決の方式設計においてはキャッシュポイズニング対策を考慮する必要がある。 本問では，送信元 IP アドレスを詐称した攻撃とその対応を題材にして，ファイアウォール，DNS サーバ及びメールサーバに関する技術要素への理解，設計能力について問う。

設問		解答例・解答の要点		備考
設問１	(1)	a	UDP	
		b	3way	
		c	DNSSEC	
	(2)	問合せ PT の送信元ポート番号をランダムに変えること		
	(3)	送信元が外部メールサーバの場合，再帰的な名前解決を許可する必要があるから		
	(4)	(d)，(e)，(f)		
	(5)	G 社のドメイン名になりすましたメールを外部メールサーバに送信すること		
設問２	(1)	IF-1 経由で届く支社プロキシサーバからの正規の問合せ PT と，詐称された問合せ PT とを識別できないから		
	(2)	リゾルバ機能及び DNS キャッシュ機能		