

平成 27 年度 秋期 ネットワークスペシャリスト試験 解答例

午後 I 試験

問 1

出題趣旨	
<p>シングルサインオンは、大規模な Web システム構築で用いられることが多くなってきた技術であるが、この技術を活用したシステム構築においては、アプリケーション技術者、サーバ技術者、ネットワーク技術者が協力して取り組むことが必要である。本問のように、負荷分散装置でシングルサインオンサーバを冗長化したシステムを安定して構築するためには、パケットレベルの詳細な流れが理解できるスキルが必要である。</p> <p>本問では、Cookie を利用したシングルサインオンについての基本的な仕組みの理解と、DSR 方式ロードバランサを用いたシングルサインオンサービス負荷分散について、実務上必要となる技術の理解を問う。</p>	

設問	解答例・解答の要点		備考
設問 1	ア	リバースプロキシ	
	イ	リダイレクト	
	ウ	Set-Cookie	
	エ	内部 DNS	
	オ	ループバック	
設問 2	⑤		
設問 3	(1)	a-sha.example.jp	
	(2)	Cookie に Secure 属性を付ける。	
設問 4	(1)	SYN パケットにはレイヤ 7 情報が含まれていないから	
	(2)	Gratuitous ARP 又は GARP	
	(3)	VIP アドレスに対する ARP リクエストに応答しないように設定する。	

## 問 2

出題趣旨	
<p>SaaS, PaaS などの利用が拡大しているが、これらを利用する企業ではインターネットとの通信量が格段に増加する。そのため、接続回線の増速、ファイアウォールやルータなどのネットワーク機器の性能拡張が必要になる場合もある。また、社内のトラフィックに変化が生じることによって、改めて社内ネットワークの検証が必要となることもある。</p> <p>負荷分散装置は、ネットワーク機器の性能拡張にも用いることができる。その場合は、一般に透過型負荷分散を用いる。これは、FW の他、IDS/IPS, ルータ, 接続回線などの負荷分散にも応用可能であり、ネットワーク技術者として理解しておきたい技術である。</p> <p>本問では、透過型負荷分散を題材として、TCP/IP の各レイヤの動作に関する理解と、性能設計、信頼性設計に関する基礎的な能力を問う。</p>	

設問	解答例・解答の要点		備考	
設問 1	ア	スループット		
	イ	パケット		
	ウ	維持		
設問 2	(1)	(A) 宛先 IP アドレス	機器 b	
		宛先 MAC アドレス	FW1	
	(B)	宛先 IP アドレス	機器 b	
		宛先 MAC アドレス	FW2	
	(2)	宛先 IP アドレスを書き換えられない。		
(3)	セッション単位に、2 台の LB が同じ FW を選択する。			
設問 3	(1)	故障発生時の性能を不足させないため		
	(2)	あ	99	
		い	180	
	(3)	FW を経由する LB 間の経路の障害を検出できる。		
(4)	リトライアウトを待たずに接続の切断を検知できる。			

問3

出題趣旨	
<p>近年インターネットのセキュリティ対策の重要性が増大し、その対策として侵入検知システム（IDS）や侵入防止システム（IPS）の導入が一般的となってきた。導入に当たっては、それぞれの機能と特徴を正しく理解し、不正アクセスに対して最適に対応できるように設計し、導入後も継続的にメンテナンスしていく必要がある。IDS と IPS はネットワークを構成する重要な機器であり、ネットワークエンジニアには、関連する知識が求められる。</p> <p>本問では、ネットワークのセキュリティ対策向上を題材に、IDS と IPS の機能と特徴について、基本的な知識と理解力を問う。</p>	

設問	解答例・解答の要点			備考		
設問1	ア	アノマリ 又は 異常検知				
	イ	ミラー 又は ミラーリング				
	ウ	プロミスキャス				
	エ	IP				
	オ	unreachable				
設問2	(1)	通信の範囲		IDSの接続箇所		
			SW1	SW2	SW3	
		インターネット⇔内部LAN	○	×	○	
	(2)	FWのACLを動的に変更して、遮断の対象とする送信元アドレスを追加する。				
(3)	不正アクセスの送信元アドレスが偽装されている可能性があるから					
設問3	(1)	保護する機器にセキュリティパッチを適用するまでの間、脆弱性を悪用する攻撃の通信を遮断する。				
	(2)	通信をそのまま通過させ、遮断しない機能				
	(3)	不正アクセスへの対応を最適化するために、ログを取得して解析する。				