平成 29 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
VPN 技術はリモートアクセスのための技術として様々な場面で活用されている。また，幾つかの VPN 技術の中でも SSL-VPN は，その使いやすさから多くの場面で利用されている。 SSL-VPN は，リモートアクセス技術として，組織外部ネットワークから内部ネットワークへのリモートアクセスに用いられることが多いが，VPN アクセス時の認証や通信の暗号化といった SSL-VPN に備わる機能は，組織内部ネットワークにおいてもセキュリティへの対応用途に利用可能である。 本問では，企業の内部と複数企業の間の両方の場合における SSL-VPN の活用を通じて，SSL-VPN に備わる認証や暗号化といった基本的な機能とネットワーク機器の機能とを組み合わせた，セキュアなネットワークの構築を行う能力を問う。

設問		解答例・解答の要点			備考
設問 1		ア	SHA-1		
		イ	1.2		
		ウ	Client_Hello		
		エ	Server_Hello		
		オ	リバースプロキシ		
設問 2	(1)	暗号アルゴリズム	①	・鍵交換	
			②	・認証	
		ハッシュアルゴリズム		メッセージ認証	
	(2)	顧客システムは，様々なプロトコルを利用している。			
	(3)	vNIC			
設問 3		カ	内部 LAN		
		キ	DMZ		
		ク	172.16.0.0/16		
		ケ	202.y.44.2/32		
設問 4	(1)	②，③，④，⑤			
	(2)	顧客システム構築ネットワークから他社の顧客システム構築ネットワークへの通信			
	(3)	⑥			

問２

出題趣旨
仮想デスクトップ基盤（以下，VDI という）は，情報セキュリティ強化やワークスタイル変革に取り組む企業や組織において導入する事例が多くなっている。VDI の導入では，従業員が利用していた PC のプログラム実行環境をサーバ上で集約管理するので，通信の変化に対応したネットワーク設計が必要になる。また，近年増加している標的型攻撃に特化した情報セキュリティ機器の導入や VDI におけるマルウェア感染時の対処など，ネットワークも含めて実施する情報セキュリティ対策に関する技術力もネットワークエンジニアには要求される。 本問では，VDI の導入を題材に，VDI 導入前後における通信の変化を把握し，それに応じた帯域制御方式や標的型攻撃対策に関するネットワーク設計技術について問う。

設問		解答例・解答の要点		備考
設問１		バーストトラフィック		
設問２	(1)	VDI 導入前に経由する通信	ファイル転送通信	
		VDI 導入後に経由する通信 ①	・画面転送通信	
		②	・プリント通信	
	(2)	a	1.25	
		b	100	
		c	10	
	(3)	理由	インターネット通信は本社の仮想 PC から行われるから	
		利点	情報セキュリティ対策を本社で集中的に行うことができる。	
設問３	(1)	プリント通信が画面転送通信を圧迫するから		
	(2)	送出タイミングを調整する。		
設問４		ア	仮想 SW	
		イ	任意	
		ウ	C&C サーバ	

問３

出題趣旨
近年，企業においてはクラウドサービスの利用が進んでいる。企業がクラウドサービスを利用する際には，自社ネットワークとクラウドサービスとのネットワーク接続を行う必要がある。ネットワーク接続を行う際には，業務要件を満たすとともに，ネットワークの可用性や拡張性を確保，運用時におけるネットワーク監視について考慮する必要がある。 本問では，ある企業の社内ネットワークを想定し，インターネット VPN を用いた接続，BGP を用いた経路制御，自社ネットワークとの経路情報の交換，及び ping を用いたネットワーク監視について考えられるかを問う。

設問		解答例・解答の要点		備考
設問１		ア	NAPT	
		イ	事前共有鍵	
		ウ	AS	
		エ	TCP	
		オ	ICMP	
		カ	echo reply	
設問２	(1)	暗号化対象の通信がグローバル IP アドレス間の通信だから		
	(2)	フラグメントとリアセンブルの処理が発生する。		
設問３	(1)	BGP によって回線断や機器障害を検知し，トラフィックをう回できる。		
	(2)	Hello パケットを出さない。		
	(3)	A	大きく	

	(4)	eBGP から OSPF へ再配布された経路を再び eBGP へ再配布しない。	
設問4		ネットワーク接続の冗長構成が失われたことを検出するため	