平成 26 年度　秋期　ネットワークスペシャリスト試験　解答例

午後Ⅱ試験

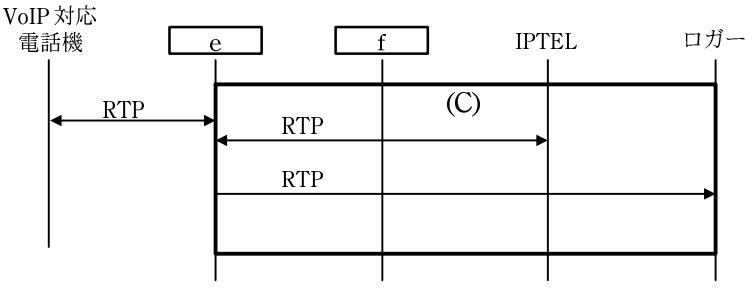
問 1

出題趣旨
最近，特定の企業や官公庁などを標的にして，その組織が保有する知財情報や個人情報などの重要な情報の窃取や破壊などを行う，標的型メール攻撃が増加してきた。標的型メール攻撃は，攻撃手口が巧妙なために，発見が難しく被害が増加している。 標的型メール攻撃の対策は，PC やサーバに対するセキュリティ対策だけでなく，ネットワークでの対策も欠かせない。そこで，標的型メール攻撃の対策には，セキュリティ技術者とネットワーク技術者が協力して実施策を立案することが求められている。 本問では，標的型メール攻撃の対策を題材として，セキュリティ技術者とネットワーク技術者が協力して実施策を立案する過程を記述した。その中で，ネットワーク技術者が実施すべきネットワークでの対策を取り上げ，その対策を通して，ネットワーク技術者に求められる，ネットワーク設計・構築技術とネットワークセキュリティ技術を基にした，ネットワークでのセキュリティ対策についての理解を問うた。

設問		解答例・解答の要点						備考
設問１		a	URL　又は　統一資源位置指定子					
		b	HTTP					
		c	IP アドレス					
		d	コンテンツフィルタリング					
		e	トンネリング					
設問２	(1)	添付ファイルを開いたり，メールに記載されたリンク先にアクセスしたりする。						
	(2)	メール送信元の MTA の IP アドレスが所属するドメインと，送信者のメールアドレスのドメイン						
	(3)	社外に送信されるメールの送信元 IP アドレスになるから						
	(4)	**サーバ名**	メール中継サーバ					
		理由	社外から Y 社宛てに送信されたメールを直接受信するから					
設問３	(1)	PC と Web サーバの間						
	(2)	プロキシサーバのルート証明書						
	(3)	プロキシサーバが，暗号化されたプリマスタシークレットを復号できないから						
設問４	(1)	**表 4**	**ポート A のポート ID**	P3	**通信の方向**	IN		
		表 5	**ポート B のポート ID**	P5	**通信の方向**	OUT		
	(2)	部署 1 と本社サーバセグメント間の疎通テスト						
	(3)	**動作**	許可	**送信元 IP アドレス**	192.168.1.0/24			
		宛先 IP アドレス	192.168.11.0/24	**プロトコル**	UDP			
		送信元ポート番号	any	**宛先ポート番号**	53			
		TCP 制御ビット	any					
	(4)	部署 1 の PC から管理 PC に対して確立する TCP コネクションは禁止するが，逆方向に確立する TCP コネクションは許可する。						
設問５	(1)	・社外の Web サーバとの間の SSL で暗号化された通信においても，認証された利用者と通信内容が取得できる。 ・プロキシサーバの認証に連続して失敗したことが記録されたログから，マルウェアの活動と推測できる情報が取得できる。						
	(2)	① ② ③	・メールに添付されたファイルを開かない。 ・メール本文に記載されたリンク先にアクセスしない。 ・メールが，正しい送信者から送信されたものか確認する。 ・不審なメールの内容を，セキュリティ担当者に報告する。 ・発見した不審なメールに関する情報を，全社で共有する。					
	(3)	マルウェアの社内での活動を，早期に発見できること						

問２

出題趣旨
サーバ仮想化技術の発展とともに，仮想化環境でシステムを構築する際に，従来と異なる課題が発生してくる。また，ネットワーク機器についても，最近，仮想サーバ上で動作させる試みも出てきている。 このような流れが進むと，サーバ，ネットワークの IT プラットフォームが仮想サーバという汎用的なプラットフォーム（サーバ）上に集約され，各種機能は仮想サーバで動作するソフトウェアに変わっていくことになる。このことによって，システム構築のスピードアップ，柔軟性や運用性の向上が期待される。 しかし，このような状況になっても，発生する新しい課題に対して，既存技術を活用して適切な対処をしていくためには，課題となる現象の基礎的・根本的な理解が不可欠である。本問では，その拡張性から応用範囲が広い SIP を取り上げ，SIP ベースのコミュニケーションシステムをネットワークも含め，仮想サーバ上に構築していくという状況を設定し，その構築過程で発生する課題とその解決を題材とした。 特に，仮想化が進んだシステム構築の中で，従来とは異なる課題が発生することの認識と，課題への対応といった観点で，基礎の理解に基づく状況把握力や技術応用力を問うた。

設問		解答例・解答の要点		備考
設問１	(1)	a	インスタントメッセージ　又は　チャット	
		b	RTP　又は　RTP と RTCP	
		c	UDP	
		d	テキスト	
	(2)	URI から相手の IP アドレスを求め，相手に INVITE メッセージを送る。		
設問２	(1)	公衆 IP 電話網の SIP サーバ，IP-PBX		
	(2)	アドレス変換対象外の SIP メッセージ内に送信者のプライベート IP アドレスが含まれている。		
	(3)	SIP メッセージ内の IP アドレス情報を送信元である VoIP-GW のグローバルアドレスに書き換える。		
設問３	(1)	仮想スイッチのポートに該当する VLAN の全てのフレームを出力し，仮想 NIC 側でそれらを全て取り込む動作		
	(2)	状態	流入するフレームの宛先 MAC アドレスが既にポート 3 側に存在するとして登録されている。	
		対応策	MAC アドレス学習機能を抑止できる SW を使用し，通過するポート 3 で学習を抑止する。	
設問４	(1)	音声パケットを中継しないから		
	(2)	e	VoIP-GW	
		f	IP-PBX	
	(3)			
	(4)	VoIP-GW には呼制御に関する SIP セッション情報も送られてくるから		
	(5)	ミラーポート出力フレームの転送用設定が不要だから		
設問５	(1)	ア	IP01	
		イ	Any	
		ウ	Any	
		エ	443	
	(2)	サービス提供用内部 LAN のネットワークに属する IP アドレス		
	(3)	ネットワーク機器ごとに異なるハードウェアを用意せずに済むから		