TAC

平成26年度秋期　情報処理技術者試験

ネットワークスペシャリスト　解答例

【午　後　Ⅰ】

問 1 （配点 50 点）

設問 1 （15 点:3 点×5）

ア: 帯域幅

イ: 0

ウ: TOS

エ: DiffServ

オ: 高く

設問 2 （21 点:(1)4 点×2, (2)3 点, (3)3 点×2, (4)4 点）

(1) （デフォルトゲートウェイの設定） ルータ 3 をマスタルータとする VRRP の仮想 IP アドレスを設定
（VRRP の設定） ルータ 3 とルータ 4 に同じ VRRP グループを設定し, ルータ 3 のプライオリティ値をルータ 4 より大きくする。

(2) 10.1.0.0/16

(3) a: ルータ 1→ルータ 3
b: ルータ 2→ルータ 1→ルータ 3

(4) 緊急でない業務は業務系システムにアクセスをしない。

設問 3 （14 点:(1)3 点×2, (2)4 点, (3)4 点）

(1) ① ポート番号
② IP アドレス

(2) データが大きく応答確認が頻繁に必要な通信

(3) 負荷が高まり, 高速化処理ができない場合

問 2 （配点 50 点）

設問 1 （15 点:3 点×5）

ア: NAPT

イ: ステートフル

ウ: データリンク

エ: GARP

オ: タグ

設問 2 （25 点:(1)4 点, (2)4 点, (3)5 点, (4)4 点, (5)4 点×2）

(1) SW3 と L3SW の間

(2) TCP の再送制御機能

(3) SW2 のミラーポートに PC を接続してフェールオーバリンク情報を取得し, 障害が発生した FW を特定できる。

(4) MAC アドレステーブル

(5) a: DNS サーバ, Web サーバ, ルータ

b: FW1 から設定情報が同期されたこと

設問 3 (10 点:(1)5 点, (2)5 点)

(1) L3SW と SW4 を相互に入れ替える。

(2) 企画部用の仮想 FW は FW1 を Active に設定し, 営業部用の仮想 FW は FW2 を Active に設定する。

問 3 (配点 50 点)

設問 1 (15 点:3 点×5)

ア: 分散

イ: Flood

ウ: 再帰

エ: リフレクション

オ: ペネトレーション

設問 2 (8 点:(1)3 点, (2)5 点)

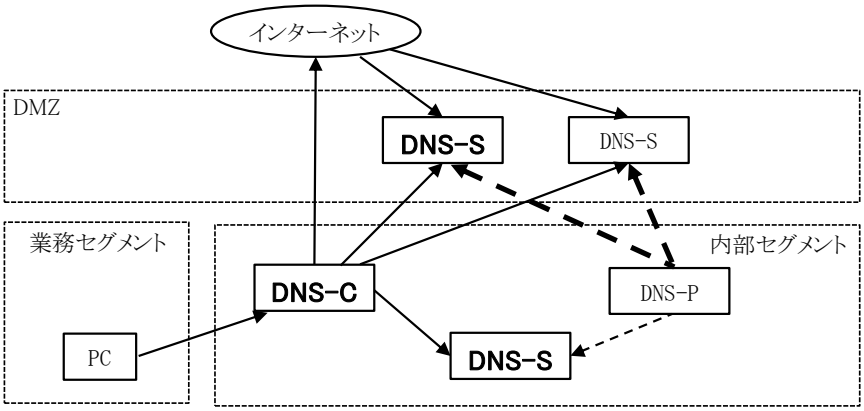
(1) a: 踏み台

(2) 設定したサイズ以上の ICMP エコー応答を遮断する機能

設問 3 (17 点:(1)4 点, (2)5 点, (3)4 点×2)

(1) DNS キャッシュポイズニングへの脆弱性

(2)



(3) ① 内部から外部へのパケットの通信ログを取得し, 監視する。

② 内部から外部への不要なポートの通信を遮断する。

設問 4 (10 点:(1)5 点, (2)5 点)

(1) b: システムをネットワークから切断

(2) 再発防止のセキュリティ対策の実施と, 対応手順の見直しを行う。

【午　後　Ⅱ】

問 1 （配点 100 点）

設問 1 （15 点：3 点×5）

a：URL

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 （19 点：(1)4 点，(2)4 点，(3)4 点，(4)（サーバ名）3 点，（理由）4 点）

（1） メールを信用して添付ファイルを開いたり，リンクをクリックしたりする。

（2） エンベロープ FROM アドレスのドメインと，メールの From ヘッダフィールドのアドレスのドメイン

（3） メール中継サーバのみグローバル IP アドレスを設定しているから

（4） （サーバ名） メール中継サーバ

（理由） 認証対象の外部からのメールが直接転送されるサーバだから

設問 3 （12 点：(1)4 点，(2)4 点，(3)4 点）

（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） Web サーバの公開鍵で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 （34 点：(1)3 点×4，(2)4 点，(3)2 点×7，(4)4 点）

（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） 業務用通信区間における疎通テスト通信を許可するため

（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） 本社部署 1 セグメントから管理セグメントへの TCP コネクションの確立は拒否し，管理セグメントから本社部署 1 セグメントへの TCP 通信は許可する。

設問 5 （20 点：(1)4 点，(2)4 点×3，(3)4 点）

（1） 外部への通信時のプロキシサーバの利用者認証の成功時と失敗時の情報と，HTTPS 通信で暗号化されていたデータの内容

（2） ① 不審なメールの添付ファイルや URL などを開かない。

② 不審なメールの送信元に電話などの信頼できる方法で問い合わせる。

③ 速やかにセキュリティ担当者に報告する。

（3） マルウェアに感染した場合，早期発見することができる。

問 2 （配点 100 点）

設問 1 （21 点：(1)4 点×4，(2)5 点）

（1） a：インスタントメッセンジャー

b：RTP

c：UDP

d：テキスト

（2） 登録されている接続相手の URI に対応する IP アドレスにメッセージを中継する。

設問 2 （14 点：(1)4 点，(2)5 点，(3)5 点）

（1） 公衆 IP 電話網の SIP サーバ，IP-PBX

（2） SIP ヘッダやボディ中の発信元 IP アドレスが企業内のプライベート IP アドレスのままで応答できないため

（3） INVITE メッセージと応答メッセージに含まれる IP アドレスを SBC に設定された IP アドレスで相互に変換する。

設問 3 （15 点：(1)5 点，(2)5 点×2）

（1） 受信したフレームを宛先 MAC アドレスにかかわらず仮想スイッチの接続ポートから同一 VLAN のロガーの仮想 NIC へ転送する。

（2）（状態） 送信元 MAC アドレスにより MAC アドレステーブルを更新したため，ポート 2 にフレームを転送したから

（対応策） MAC アドレステーブルにポート 3 からフレームを転送するように，静的に MAC アドレスを登録する。

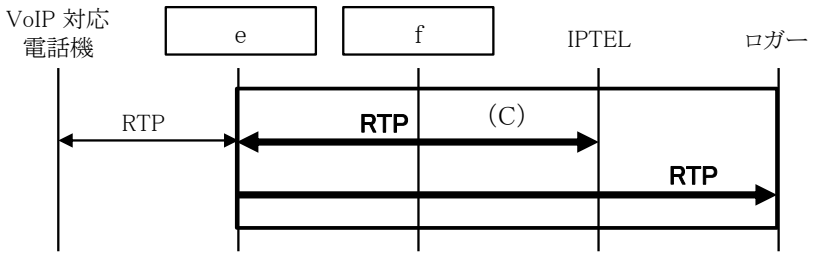
設問 4 （28 点：(1)5 点，(2)4 点×2，(3)5 点，(4)5 点，(5)5 点）

（1） IP-PBX は音声パケットを中継しない。

（2） e：VoIP-GW

f：IP-PBX

（3）



（4） ロガーが受信する INVITE メッセージに呼情報が含まれているから

（5） 通話用セッションが生成されたときのみ録音すればよい点

設問 5 （22 点：(1)3 点×4，(2)5 点，(3)5 点）

（1） ア：IP01

イ：any

ウ：any

エ：443

（2） サービス提供用内部 LAN のネットワークアドレスに所属する IP アドレス

（3） ネットワーク機器それぞれを冗長化せず，仮想サーバを冗長化すればよいから

以上