NW

平成26年度　秋期
ネットワークスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問3
選択方法	2問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を○印で囲んでください。○印がない場合は，採点されません。3問とも○印で囲んだ場合は，はじめの2問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問1，問3を選択した場合の例〕

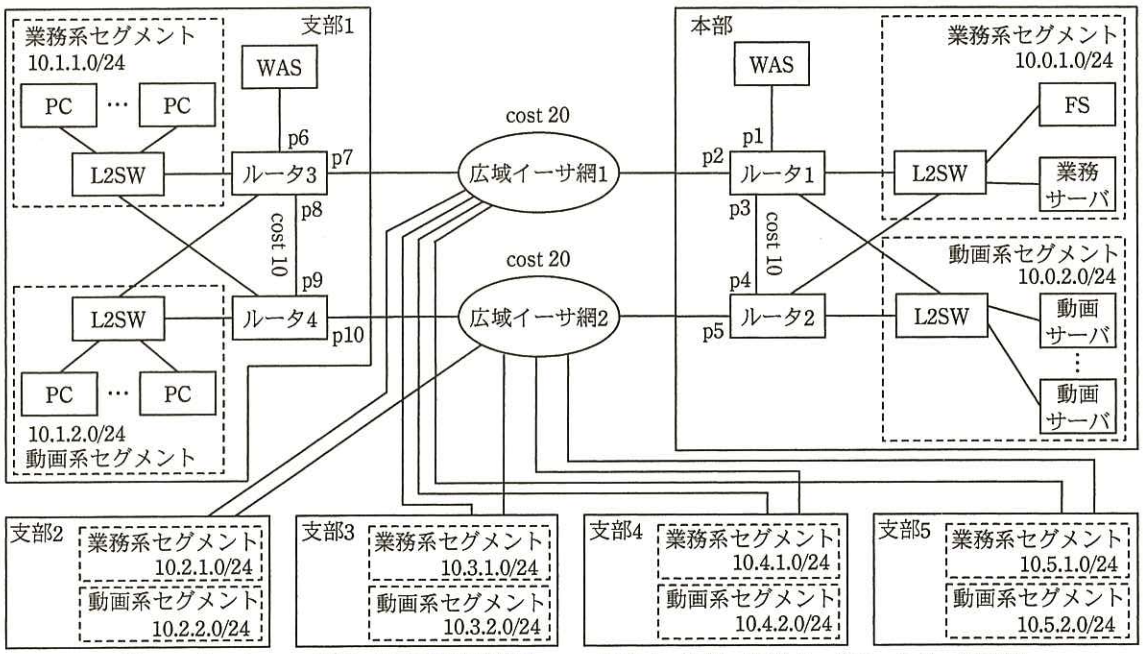
選択欄	
2問選択	(問1)
	問2
	(問3)

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　ネットワーク構成の見直しに関する次の記述を読んで，設問1～3に答えよ。

A 予備校は，東京に本部，全国に 5 支部がある。従来，本部で行った人気授業は録画して，物理媒体を各支部に配布していたが，各支部からの要望を受け，本部に動画サーバを置き，本部から各支部に授業の動画を配信することにした。また，運用管理の一元化と情報保護の強化のために，業務系のファイルサーバ（以下，FS という）を本部に集約することにした。

情報システム部の M 課長は，N 君に対し，A 予備校の新ネットワーク構成の方針を提示し，ネットワーク構成の見直しとその運用について検討するように指示した。N 君が考えた A 予備校の新ネットワーク構成を，図1に示す。



L2SW：レイヤ2スイッチ　WAS：WAN高速化装置　広域イーサ網：広域イーサネットサービス網

注記1　cost xは，OSPFで用いるコスト値を示す。

注記2　p1～p10は，ポートIDを示す。

注記3　支部2～支部5は，支部1と同じ機器構成である。

図1　A予備校の新ネットワーク構成（抜粋）

M 課長が提示した，A 予備校の新ネットワーク構成の方針を，次に示す。

・本部及び各支部では，業務系システムと動画系システムのセグメントを分け，それぞれ業務系セグメントと動画系セグメントとする。

・本部と各支部間は，異なる通信事業者の広域イーサ網 1 及び広域イーサ網 2 によって冗長化する。広域イーサ網 1 と広域イーサ網 2 は，等しい帯域とする。
・本部と各支部間のネットワーク経路は，業務系セグメント間を広域イーサ網 1 経由とし，動画系セグメント間を広域イーサ網 2 経由とする。
・一方の広域イーサ網が使用できなくなった場合には，他方の広域イーサ網によって業務系セグメント間及び動画系セグメント間の通信を行う。障害時には，動画系セグメント間の通信は，業務系セグメント間の通信よりも優先し，支障なく維持されるものとする。
・各支部からの FS のアクセスの高速化のために，WAS を導入する。

〔ネットワーク経路の検討〕

N 君は，まず，支部 1 と本部間のネットワーク経路について検討した。ルータ 1 とルータ 2 の組，及びルータ 3 とルータ 4 の組には，それぞれ業務系セグメント用と動画系セグメント用の VRRP を設定する。①PC 及びルータの設定を適切に行うことによって，業務系セグメント間のデータはルータ 1 とルータ 3 を経由させ，動画系セグメント間のデータはルータ 2 とルータ 4 を経由させることができる。

次に，採用する経路制御プロトコルを検討した。障害発生時には，できるだけ早く代替のネットワーク経路に切り替えて通信を回復させたい。よって，経路情報の再構成が高速な OSPF を採用することにした。一般的なルータの OSPF は，物理ポートの［　ア　］を基にしたコストをメトリックにしてネットワーク経路の選択を行う。しかし，ネットワーク経路を方針どおりにするために，コストを図 1 に示す値に設定した。

OSPF では，経路制御の範囲を設定する，エリアという概念がある。一つの OSPF のネットワークは，複数のエリアに分けることができる。エリア番号が［　イ　］であるエリアはバックボーンエリアと呼ばれ，必ず存在しなければならない。エリアを複数に分割する場合には，バックボーンエリアとその他のエリアが隣接するようにエリア分けを設計する。バックボーンエリアとその他のエリア間を相互接続するルータは，エリア境界ルータ（以下，ABR という）と呼ばれる。また，ABR ではエリア内の経路情報を集約して，他のエリアに送ることができる。N 君は，本部，広域イーサ網 1 及び広域イーサ網 2 をバックボーンエリアに，各支部をそれぞれ別のエリアに分

け，ABR で最もプレフィックスが短くなるように経路情報の集約を行う設計にした。

N 君の設計に基づく，本部から支部 1 への動画データの送信経路を，表 1 に示す。

表 1　本部から支部 1 への動画データの送信経路（抜粋）

事象	動画データの送信経路
通常時	動画サーバ → L2SW → ルータ2 → ルータ4 → L2SW → PC
ルータ2　本体の障害時	動画サーバ → L2SW → [a] → L2SW → PC
ルータ4　p10 の障害時	動画サーバ → L2SW → [b] → L2SW → PC

続いて，一方の広域イーサ網が使用できなくなった場合にも，動画系セグメント間の通信を支障なく維持する方法について検討した。広域イーサ網 1 及び広域イーサ網 2 の通信帯域には若干の余裕を見込んでいるが，帯域不足は避けられない。各ルータに QoS を設定し，動画系セグメント間の通信を優先することにした。ルータの QoS としては，RFC 2474 に基づいて，IP ヘッダの [ウ] フィールドを DS フィールドとして再定義して通信の優先評価を行う [エ] モデルが実装されている。

一方の広域イーサ網が使用できなくなった場合は，非優先である業務系セグメント間の通信はある程度の影響が予測される。FS と業務サーバは，散発的に利用されている。TCP で実装されている業務系システムの通信アプリケーションの場合は，データ転送速度が低下しても通信の維持とデータの保全は確保できる。しかし，業務によっては，応答時間の増大によって業務に支障が出る場合がある。よって，②業務系システムのアクセス集中を避けるための方策を定め，マニュアル配布及び掲示板で利用者に周知することにした。

〔WAS の導入〕

FS を本部に集約することに伴い，FS のアクセス速度の低下が懸念される。その対応策として WAS を導入することにした。WAS を導入したときの通信，WAS のデータ処理は，次のとおりである。

・ルータ 1 及びルータ 3 では，PBR（Policy Based Routing）を動作させる。PBR の動作によって，③ルータは FS で使用している CIFS（Common Internet File System）プロトコルのパケットを識別して WAS 宛てに転送する。PBR による経路制御は，

OSPF による経路制御よりも優先度が［　オ　］なっている必要がある。

・WAS は，データを受信した後に，“データの高速化処理”を行う。

N 君は，PC と FS 間での WAS によるデータの高速化処理について調査した。調査の結果，WAS 間では，データ圧縮機能による通信データ量の削減だけでなく，④データの送信元に対して代理応答を行ってデータをキャッシュに蓄積した後に，もう一方の WAS 宛てに一括してデータを送信することによって，高速化を図っていることが分かった。また，⑤データの高速化処理を自動的に停止する機能があることを確認した。

N 君がまとめた検討結果は M 課長に承認され，新ネットワークの構築準備を開始することになった。

設問 1　本文中の［　ア　］～［　オ　］に入れる適切な字句又は数値を答えよ。

設問 2　〔ネットワーク経路の検討〕について，(1) ～ (4) に答えよ。

(1) 本文中の下線①について，業務系セグメントの PC のデフォルトゲートウェイの設定を 30 字以内で述べよ。また，通常時，業務系セグメントの PC から送信されたパケットを適切な通信経路で中継するためには，ルータの VRRP の設定をどのようにすればよいか。50 字以内で具体的に述べよ。

(2) ルータ 3 がルータ 1 へ送る，業務系セグメントと動画系セグメントの経路情報のプレフィックスを答えよ。

(3) 表 1 中の［　a　］，［　b　］に入れる適切な動画データの送信経路を，表 1 中の表記に従ってそれぞれ答えよ。

(4) 本文中の下線②の方策を，運用の観点で，25 字以内で具体的に述べよ。

設問 3　〔WAS の導入〕について，(1) ～ (3) に答えよ。

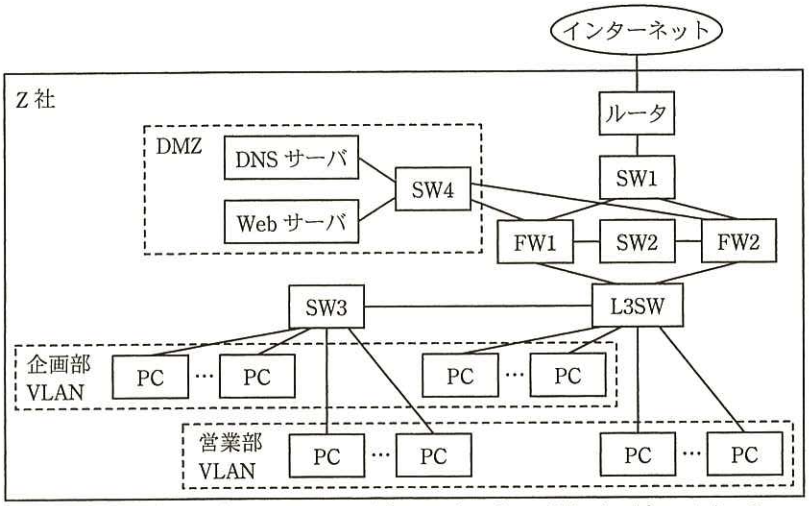
(1) 本文中の下線③の識別に使用される，OSI 基本参照モデルの第 3 層以上の情報を二つ答えよ。

(2) 本文中の下線④の処理の効果がより高くなるのは，本部と支部間の通信の特性がどのような場合か。20 字以内で具体的に述べよ。

(3) 本文中の下線⑤の機能はどのような場合に必要になるのか。20 字以内で具体的に述べよ。

問2　ファイアウォールの障害対応に関する次の記述を読んで，設問1～3に答えよ。

Z社は，美容用品・健康用品を扱う企業である。Z社には企画部と営業部があり，各部のPCは部ごとのVLANに属している。ネットワークの管理は，企画部システム課のO主任とU君が行っている。Z社の現在のネットワーク構成を，図1に示す。



FW：ファイアウォール　L3SW：レイヤ3スイッチ　SW：レイヤ2スイッチ

図1　Z社の現在のネットワーク構成（抜粋）

〔FWの構成と交換作業〕

Z社では，FW1を主系に設定し，FW2を副系に設定したActive-Standby冗長構成を採用し，運用を行っている。通常時，FWは，必ず主系がActive動作になり，副系がStandby動作になる仕様である。

FWでは，［　ア　］と呼ばれる機能によって，ネットワークアドレス及びポート番号の変換を行っている。また，主系から副系にフェールオーバした後も通信を継続させるために，FWが通信の中継のために管理している情報（以下，管理情報という）を自動的に引き継ぐ［　イ　］フェールオーバ機能を動作させている。FWがフェールオーバした後に，多くのアプリケーションでデータの保全性が保たれて平常どおり通信できるのは，①トランスポート層のプロトコルの機能によるところが大きい。

FW1とFW2の間にはフェールオーバリンクと呼ばれる専用接続があり，設定情報の同期，管理情報の複製，及び対向FWの動作状態の識別に使用されている。フェー

ルオーバリンクには，ケーブル直結にする構成と SW を挟む構成があるが，Z 社では，②障害切分けのために SW2 を挟む構成を採用している。FW の冗長構成及びフェールオーバに関する動作は，次のとおりである。

・FW の冗長化機能は，仮想アドレスを使用する方式ではなく，主系の IP アドレス及び MAC アドレスを副系が引き継ぐ方式である。
・新たに Active 動作になった FW は，切り替わったことを通知するフレームを FW の各ポートから送信する。FW に接続しているスイッチは，このフレームを受信することで，③レイヤ 2 機能で用いるテーブルを適切に更新することができる。
・Active 動作の FW を副系から主系に切り戻すためには，手動操作が必要である。
・FW は，起動時にフェールオーバリンクによって，他の Active 動作中の FW を認識すると，主系又は副系であるかにかかわらず Standby 動作に入る。このとき，FW は自己の設定情報を無視して，Active 動作中の FW から設定情報を同期する。

Z 社では，数日前に FW1 が故障して，FW2 にフェールオーバした。U 君は，通信に影響を与えずに交換できると考え，代替機を入手次第，交換作業を行うことにした。

作業当日，U 君は，FW1 を工場出荷時の設定のままの代替機と交換し，配線後に電源を投入した。少したってから SW2 を見ると，FW1 接続ポートで，OSI 基本参照モデルの［　ウ　］層での正常接続を表すリンク LED が消灯していた。そこで，UTP のコネクタを強く押し込んだところ点灯した。その直後から，システム課に DMZ 及び社外へのアクセスができないとの苦情が相次いだ。慌てて，FW1 と FW2 を確認すると，両方とも Z 社用のフィルタリングルールを含む設定情報が失われていたので，直ちに FW1 の設定情報を復元し，FW2 に設定情報を同期させた。しかし，その後もアクセスできないとの苦情が続いた。U 君は，事故の原因を特定して通信を回復した後，今回の交換作業における事故では，次の二つが関係していることを確認した。

・FW1 は，電源投入後に FW2 を認識できず，Active 動作になった。
・フェールオーバリンク接続時に，FW1 が主系設定であったので，副系の FW2 は FW1 から設定情報の同期と管理情報の複製を行い，Standby 動作に切り替わった。

次は，今回の交換作業に関する O 主任と U 君の会話である。

O 主任：今回，FW1 の交換作業のミスは，U 君らしくなかったわ。

U君　：すみません。うかつでした。

O主任：FW1とFW2の設定復元後も，通信が回復しなかったのはなぜかしら。

U君　：FW1を代替機に交換した結果，FW1の各ポートのMACアドレスが変わったので，通信ができなかったのです。FWには，自ポートに設定されたIPアドレスの解決を要求する［　エ　］を用いて接続機器のARPテーブルを更新する機能がないので，手動操作が必要でした。このようなミスの再発防止のために，FW故障時の交換作業手順を整理しておきます。

O主任：お願いするわ。それから，FWの管理の都合上，フィルタリングルールを企画部と営業部で分けたいので，仮想FWを導入する案の検討をお願いできないかしら。

U君　：はい，分かりました。

U君は，FW故障時の交換作業手順を整理し，表1にまとめた。

表1　FW故障時の交換作業手順

故障機器	作業順序	作業内容
FW1	(1) 設定確認	代替機の主系設定が解除されていることを確認する。
	(2) 交換及び接続	代替機の電源を切断し，交換及び接続を行う。
	(3) 電源投入	Standby動作に入り，FW2から設定情報が同期されたことを確認する。
	(4) 主系への切戻し	FW1をActive動作に切り戻し，主系設定を行う。
	(5) ARPテーブル初期化	L3SW，［　a　］について初期化する。
	(6) 通信確認	DMZ及び社外との通信が可能であることを確認する。
FW2	(1) 設定確認	代替機の主系設定が解除されていることを確認する。
	(2) 交換及び接続	代替機の電源を切断し，交換及び接続を行う。
	(3) 電源投入	Standby動作に入り，［　b　］を確認する。
	(4) 通信確認	DMZ及び社外との通信が可能であることを確認する。

〔仮想FW導入案の検討〕

まず，U君は，仮想FWについて調査した。仮想FWとは，FW1及びFW2の中に論理的なFWの機能を複数定義できる機能である。フィルタリングルールは，仮想

FW ごとに独立して設定できる。仮想 FW には，FW の各ポート（フェールオーバリンク用ポートを除く）に相当する仮想ポートがあり，それぞれに IP アドレス及び VLAN 番号を割り当てる。仮想 FW との通信は，［　オ　］VLAN を使用して 1 本のリンクに複数の VLAN を収容する接続（以下，トランク接続という）を行い，VLAN 番号を合致させることで可能になる。

U 君は，企画部用の仮想 FW 及び営業部用の仮想 FW の両方を，それぞれ FW1 及び FW2 に定義する構成案を考えた。仮想 FW の導入に伴い，企画部と営業部の VLAN 間通信を廃止する。DNS サーバ及び Web サーバは現在のままとし，トランク接続を使用しない。新たに機器を購入せずに，④2 台のスイッチを相互に入れ替えて対処する。

さらに，仮想 FW について調査を進めると，Active-Active 冗長構成にした物理 FW（FW1 及び FW2）に，⑤Active 動作に設定した仮想 FW を適切に配置すると，物理 FW 間での負荷分散が可能であることが分かった。

U 君は，これらの調査結果を O 主任に報告し，仮想 FW の導入案は了承された。仮想 FW の導入作業は，翌月の法定点検による全館停電日に合わせて行うことになった。

設問 1　本文中の［　ア　］～［　オ　］に入れる適切な字句を答えよ。

設問 2　〔FW の構成と交換作業〕について，(1) ～ (5) に答えよ。

(1) 図 1 において，機器間がトランク接続でなければならない箇所はどこか。図 1 中の機器名を用いて答えよ。

(2) 本文中の下線①のプロトコルの機能を，10 字以内で答えよ。

(3) 本文中の下線②を採用する利点は何か。50 字以内で具体的に述べよ。

(4) 本文中の下線③のテーブル名を，15 字以内で答えよ。

(5) 表 1 中の［　a　］に入れる機器名を，図 1 中の機器名を用いて三つ答えよ。また，［　b　］に入れる確認内容を，20 字以内で答えよ。

設問 3　〔仮想 FW 導入案の検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線④の入れ替えを，図 1 中の機器名を用いて答えよ。ただし，各機器のポートには，余裕があるものとする。

(2) 本文中の下線⑤の配置を，50 字以内で具体的に述べよ。

問3　ネットワークのセキュリティ対策に関する次の記述を読んで，設問 1～4 に答えよ。

X 銀行は，Q 県を本拠地とする中堅の地域金融機関である。X 銀行は，基幹システムである勘定系システムの運用を他行との共同センタに委託しているが，自行にもコンピュータセンタをもっており，インターネットバンキングは X 銀行独自のシステム（以下，IB システムという）で運用している。IB システムの構成を，図 1 に示す。

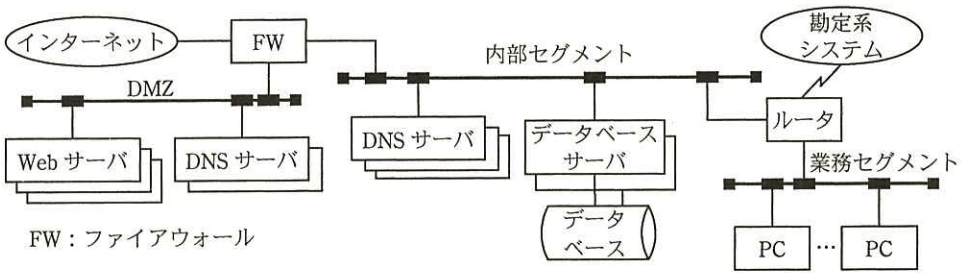


図 1　IB システムの構成（抜粋）

IB システムは，Web を使ったインターネット経由の顧客向けサービスである。IB システムは，勘定系システムで管理している口座残高などの情報を除き，独自のユーザ ID，パスワードなどの重要情報をデータベースに保有している。IB システムの Web サーバは，業務セグメントの PC からもアクセスできる。

最近，IB システムへのサイバー攻撃が増加している。金銭的な被害は発生していないが，セキュリティインシデントは頻繁に発見されている。

〔サイバー攻撃対策〕

X 銀行では，サイバー攻撃対策のためのセキュリティ担当者として，システム企画部の主任の F 氏が任命されている。次は，新たにシステム企画部に着任した G 君と，F 氏の会話である。

G 君：最近のサイバー攻撃にはどのようなものがあるのですか。

F 氏：最近，標的システムへの通信量を増大させて，ネットワークやサーバの処理能力を占有することによって，正常な取引の処理を妨害し，場合によってはサーバをダウンさせる DoS 攻撃が，頻繁に発生している。特に，多数のコンピュー

タが標的サーバを集中的に攻撃する［　ア　］型 DoS 攻撃は，発信元のコンピュータの特定が難しいので，被害が大きくなるといわれている。DoS 攻撃には，TCP のパケットを大量に送信し，応答待ちにして新たな接続を妨害する SYN［　イ　］攻撃や，コネクションレスの UDP パケットを使った UDP［　イ　］攻撃などがある。

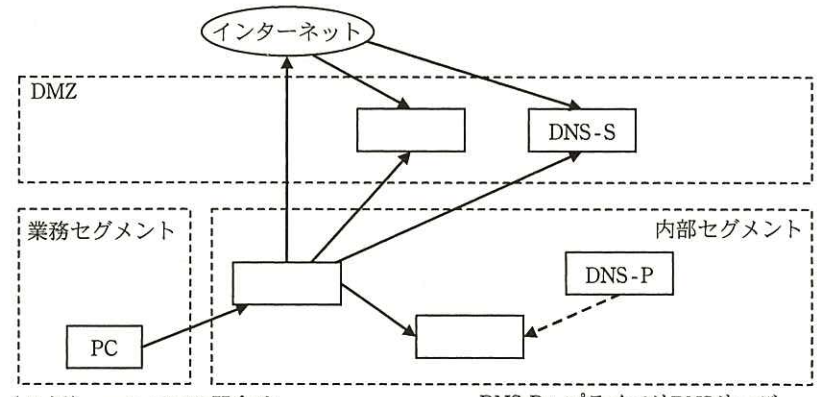
G 君：DoS 攻撃といえば，DNS の機能を悪用したものがあるそうですね。

F 氏：例えば，PC などから問合せを受けた DNS サーバが，他の DNS サーバにも問合せを行い，最終的な結果を返信する［　ウ　］的な問合せにおいて，発信元の IP アドレスを詐称して，その問合せの結果を標的サーバ宛てに送信させる DNS［　エ　］攻撃と呼ばれるものがある。このような，オープンリゾルバを用いた攻撃に関しては，自らも攻撃の［　a　］とならないようにすることが重要だ。サイバー攻撃に対応するためには，常に最新のセキュリティ対策を施しておく必要がある。

X 銀行では，DNS へのサイバー攻撃に対応するために，IB システムに様々な対策を施している。そのうちの一つが，DNS のセキュリティ対策である。

〔DNS のセキュリティ対策〕

IB システムの DNS 概念図を，図 2 に示す。



注記　設問のために，図の一部を省略している。

図 2　IB システムの DNS 概念図

図2のDNSは，次のセキュリティ対策方針に基づいて構築されている。

・DNS サーバが管理するドメインを，DMZ（外部向けゾーン）と内部セグメント（内部向けゾーン）に分け，それぞれゾーン転送を行う。

・①DMZ の DNS サーバは，キャッシュ機能を無効にしたセカンダリの冗長構成として，DMZ に設置されグローバル IP アドレスを割り当てられた Web サーバの名前解決に使用する。

・内部セグメントの DNS サーバは，プライマリ，セカンダリ，キャッシュをそれぞれ別のサーバ機器で稼働させる。

・内部セグメントのプライマリ DNS サーバには，DNS の問合せが来ないようにし，ゾーン転送の宛先は自行内のセカンダリサーバに限定する。

・内部セグメントのセカンダリ DNS サーバは，内部セグメントに設置されたデータベースサーバの名前解決に使用する。

・FW において，内部セグメントの DNS サーバから DMZ の DNS サーバへの通信は，TCP/UDP ともポート番号 53 番だけを許可する。

DNS の対応を含めた上記のセキュリティ対策を正しく実装し，実効性を確保することが必要である。

次は，侵入検査とインシデント管理に関する，F 氏と G 君の会話である。

G 君：被害が発生してからでは遅いのではないでしょうか。被害を未然に防ぐ対策はないのですか。

F 氏：そうだね。当行では，実際に脆弱(ぜい)性があるかどうか調査するための侵入検査，いわゆる［ オ ］テストを定期的に実施して，セキュリティ対策の状況を評価している。しかし，それだけでなく，平常時の状態をよく監視しておき，被害が発生する前の兆候をつかむことが大切だ。そのためにはインシデント管理が重要だと考えている。また，②外部からの不正アクセスだけでなく，内部から外部への通信にも十分に注意しなければならないね。

G 君：少しでも不審な動きがあったら，事前に定めておいた対応手順に従って，迅速に対応する必要があるということですね。

〔インシデント管理〕

IB システムにおいて，不正侵入などのサイバー攻撃に関わる重大なインシデントが発生した場合，社内のインシデント発見者又は社外からのインシデント連絡を受け付ける担当者が，定められた手順に従ってセキュリティ担当者への連絡を行う。インシデントの連絡を受け付けたセキュリティ担当者は，発生したインシデントの状況を把握し記録した後，必要な対処を実施することが定められている。

IB システムにおいて，サイバー攻撃に関わる重大なインシデントが発生したときのために，X 銀行が定めた対応手順を，図 3 に示す。

＜発見者又は受付担当者の対応＞
(1) 状況把握と記録
(2) 対処方法の確認
(3) セキュリティ担当者への連絡
(4) 対処結果の報告

＜セキュリティ担当者の対応＞
(1) 状況把握と記録
(2) 対処方法の確認
(3) [b]
(4) 原因の特定と対処
(5) システムの復旧
(6) 対処結果の報告

図 3　IB システムのサイバー攻撃に関わる重大なインシデント発生時の対応手順

X 銀行では現在，適切なセキュリティ対策を実施し，インシデント発生時に迅速に対応することによって，IB システムを順調に稼働させている。

設問 1　本文中の [ア] ～ [オ] に入れる適切な字句を答えよ。

設問 2　〔サイバー攻撃対策〕について，(1)，(2) に答えよ。

(1)　本文中の [a] に入れる適切な字句を答えよ。

(2)　大量のパケットを送信する攻撃として，大きなサイズの ICMP エコー応答を使ったものがある。この攻撃を防御するために，図 1 中の FW がもつべき機能は何か。30 字以内で具体的に述べよ。

設問 3　〔DNS のセキュリティ対策〕について，(1) ～ (3)に答えよ。

(1)　本文中の下線①の対策をとらなかった場合，どのようなセキュリティ上の脆弱性が考えられるか。20 字以内で述べよ。

(2) 本文中のセキュリティ対策を実施した場合の，図 2 中の空欄の DNS サーバと，DNS 問合せ及びゾーン転送について，凡例に従って図 2 を完成させよ。

(3) 本文中の下線②で，内部から外部への不正な通信を発見又は防止するために必要な，FW での対策を二つ挙げ，それぞれ 30 字以内で述べよ。

設問 4 〔インシデント管理〕について，(1)，(2) に答えよ。

(1) 図 3 中の［ b ］は，セキュリティ担当者の対応として必要な，ネットワークに係る作業である。その作業の内容を 15 字以内で答えよ。

(2) 対処結果の報告後，将来発生するインシデントへの対応として，セキュリティ担当者が実施すべき事項がある。その内容を 30 字以内で述べよ。

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるものは，次のものに限ります。
   なお，会場での貸出しは行っていません。
   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬
   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後Ⅱの試験開始は 14:30 ですので，14:10 までに着席してください。