平成 26 年度 秋期 午後Ⅰ問題の解答・解説

注：試験センターが公表している出題趣旨・採点講評・解答例を転載している。

問 1

出題趣旨

近年，データを 1 か所に置き，ネットワーク経由で様々なプロトコルやトラフィックの特性に合わせて利用するニーズが，ますます増えてきている。ネットワーク技術者には，ネットワークの冗長化による信頼性向上に必要なスキルや，プロトコルやトラフィックの特性を考慮したデータ転送の高速化のスキルが，一層要求される。

本問では，ネットワークの冗長化と，WAN 高速化装置を題材に取り上げ，OSPF による経路制御，ネットワーク機器や回線の障害時の運用，WAN 高速化装置によるデータの高速化処理の基本的知識を問う。

採点講評

問 1 では，ネットワークの冗長化と，WAN 高速化装置を題材とし，OSPF による経路制御，ネットワーク機器や回線の障害時の運用，WAN 高速化装置の基本的知識について出題した。全体として，正答率は低かった。

設問 1 では，ウとエの正答率が低かった。QoS に関する重要な用語なので把握しておいてほしい。

設問 2 では，(1)～(3) の正答率が低かった。(1) は，デフォルトゲートウェイの冗長化と，仮想ルータによる冗長化に着目せずに，単に通信経路を説明しただけの解答が散見された。図と本文をしっかり読み，設問で何が問われているかを，きちんと理解した上で解答してほしかった。(2) は，OSPF の経路集約を問う問題であり，(3) は，経路制御に VRRP と OSPF を用いた冗長化構成での，障害時の送信経路を問う問題である。単に暗記するだけでなく，そのプロトコルの役割や仕組み，活用方法について，しっかり理解しておいてほしい。(4) は，正答率が高かった。

設問 3 では，WAN 高速化装置や PBR（Policy Based Routing）に関する問題である。(2) の正答率が低かった。全般的に，ネットワークの基本的な知識について問う問題であり，図と本文をしっかり読み，その条件に沿って考えていけば，正答を導くことができるはずである。

設問		解答例・解答の要点		備考
設問 1		ア	帯域幅　又は　通信速度	
		イ	0	
		ウ	TOS	
		エ	DiffServ　又は　Differentiated Services	
		オ	高く	
設問 2	(1)	デフォルトゲートウェイの設定	業務系セグメントに対応した仮想ルータの IP アドレス	
		VRRP の設定	業務系セグメントの仮想ルータがルータ 3 でアクティブになるようにプライオリティ値を設定する。	
	(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)	利用者をグループ化して使用時間帯をずらす。		

（表は次ページに続く）

設問		解答例・解答の要点	備考
設問 3	(1)	① ・IP アドレス ② ・ポート番号	
	(2)	ラウンドトリップ時間が大きい場合	
	(3)	片側の WAS が故障した場合	

本事例のテーマは，ネットワーク構成の見直しである。

個々の設問の解説に入る前に，本事例の全体像をつかむことにしよう。

●ネットワーク構成の方針

第 3 段落に，本事例のネットワーク構成の方針が述べられている。各方針に項番①～⑤を付与して以下に示す。

①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。

②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。

③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。

④一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。

⑤各支部からの FS（ファイルサーバ）のアクセスの高速化のために，WAS（WAN 高速化装置）を導入する。

この方針を実現するため，次の表に示す三つのソリューションを検討している。

全体像をつかむため，これらソリューションの概要を一つずつ解説する。特に，(A)「業務系セグメント間と動画系セグメント間のトラフィック分散と冗長化」は，複数の要素技術を組み合わせた難易度の高い設計であるため，詳しく述べることにする。

表：本事例に登場する三つのソリューション

	ソリューション	使用する技術	方針
(A)	業務系セグメント間と動画系セグメント間のトラフィック分散と冗長化	OSPF，VRRP	①②③④
(B)	広域イーサ網の障害時における，動画系セグメント間の通信の優先制御	ルータの優先制御機能	④
(C)	FS のアクセスの高速化	PBR(Policy Based Routing)，WAS	⑤

●業務系セグメント間と動画系セグメント間のトラフィック分散と冗長化

方針③に基づき，本部と支部 1 間の業務系セグメントの通信は広域イーサ網 1 を経由し，動画系セグメントの通信は広域イーサ網 2 を経由する。

方針③，④に基づき，広域イーサ網 1 に障害が発生したとき，本部と支部 1 間の業務系セグメントの通信は広域イーサ網 2 を経由する。広域イーサ網 2 に障害が発生したとき，本部と支部 1 間の動画系セグメントの通信は広域イーサ網 1 を経由する。

ここでは，設問 2 で動画系セグメント間の通信経路が問われていることを踏まえ，動画系セグメントのトラフィック分散と冗長化について解説しよう。

業務系セグメントについては，動画系セグメントの説明に登場する広域イーサ網，ルータ，サーバの名称を，業務系セグメントで相当するものに読み替えればよい。すなわち，広域イーサ網 2 を広域イーサ網 1 に，ルータ 2 をルータ 1 に，ルータ 4 をルータ 3 に，動画サーバを業務サーバに，それぞれ読み替える。

・【ルータの冗長化】

ルータの冗長化について，〔ネットワーク経路の検討〕の第 1 段落に，次のように記述されている。

> 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。PC 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。

ここには，「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」とある。VRRP

では，一つのインタフェースに VRRP 設定を複数登録することができる。そのように設定するときは，VRRP の番号，仮想ルータの IP アドレス（仮想 IP アドレス）を，設定ごとに異なる値にする必要がある。

本事例では，VRRP を用いてルータを冗長化している。したがって，動画系セグメントのサーバ及び PC のデフォルトゲートウェイは，動画系セグメントの仮想ルータの IP アドレスにする。

通常時，動画系のトラフィックは広域イーサ網 2 を経由する。したがって，動画系セグメントのマスタルータは，広域イーサ網 2 側のルータである。バックアップルータは，同じ拠点内にある広域イーサ網 1 側のルータである。

以上をまとめると，動画系セグメント用の VRRP 設定，及び，サーバと PC のルーティングテーブルは，次のとおりである。

表：動画系セグメント用の VRRP 設定

拠点	マスタルータ	バックアップルータ
本部	ルータ 2	ルータ 1
支部 1	ルータ 4	ルータ 3

表：本部の動画サーバのルーティングテーブル

宛先ネットワーク／サブネットマスク	ネクストホップ	経路設定の方法
0.0.0.0/0	本部における 動画系セグメントの仮想ルータ	スタティック

表：支部 1 の動画系セグメントの PC のルーティングテーブル

宛先ネットワーク／サブネットマスク	ネクストホップ	経路設定の方法
0.0.0.0/0	支部 1 における 動画系セグメントの仮想ルータ	スタティック

（注）支部 2 ～ 5 の動画系セグメントの PC のルーティングテーブルは省略。

業務系セグメントはどのように設定するのだろうか。

業務系セグメントのサーバ及び PC のデフォルトゲートウェイは，業務系セグメントの仮想ルータの IP アドレスにする。

通常時，業務系のトラフィックは広域イーサ網 1 を経由する。したがって，業務系セグメントのマスタルータは，広域イーサ網 1 側のルータである。

要するに，業務系セグメントの設定は，動画系セグメントの設定に登場する「ルータ 2」を「ルータ 1」に，「ルータ 4」を「ルータ 3」に，「動画サーバ」を「業務サーバ」に，それぞれ読み替えればよい。それゆえ，VRRP の設定，及び，サーバと PC のルーティングテーブルは，次のとおりである。

表：業務系セグメント用の VRRP 設定

拠点	マスタルータ	バックアップルータ
本部	ルータ 1	ルータ 2
支部 1	ルータ 3	ルータ 4

表：本部の業務サーバのルーティングテーブル

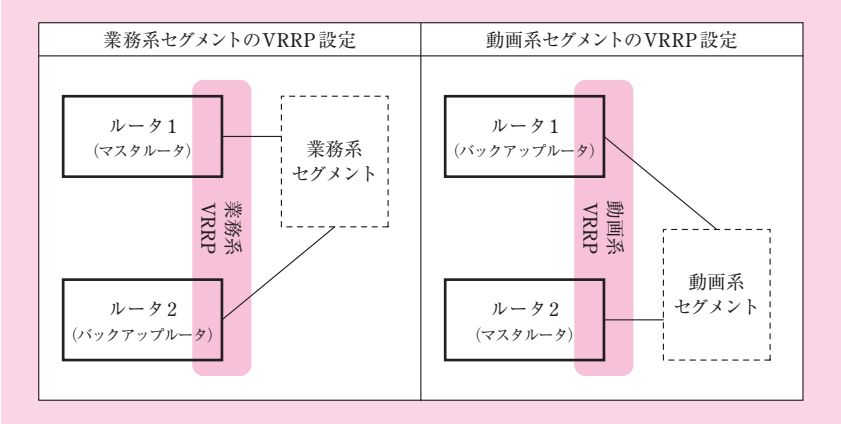
宛先ネットワーク／サブネットマスク	ネクストホップ	経路設定の方法
0.0.0.0/0	本部における 業務系セグメントの仮想ルータ	スタティック

表：支部 1 の業務系セグメントの PC のルーティングテーブル

宛先ネットワーク／サブネットマスク	ネクストホップ	経路設定の方法
0.0.0.0/0	支部 1 における 業務系セグメントの仮想ルータ	スタティック

（注）支部 2 ～ 5 の業務系セグメントの PC のルーティングテーブルは省略。

このように，各拠点の 2 台のルータには 2 種類の VRRP 設定が登録されており，かつ，マスタルータ，バックアップルータが互い違いに設定されている。この様子を，本部のセグメントを例にして次の図に示す。



図：本部のセグメントのマスタルータとバックアップルータ

・【ルータ間の経路の冗長化】

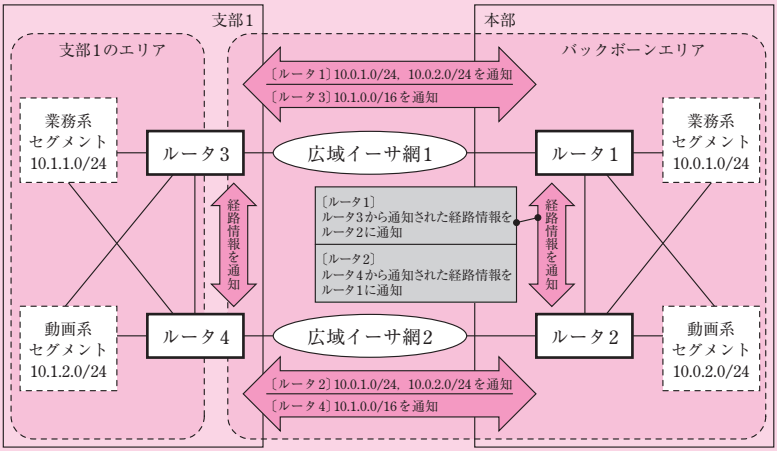
経路制御プロトコルについて，第 2 段落と第 3 段落に次のように記述されている。

OSPF を採用することにした。……（略）……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。……（略）……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（エリア境界ルータ）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。

支部 1 の ABR は，ルータ 3 とルータ 4 である。支部 1 の ABR は，エリア内の業務系セグメントと動画系セグメントを集約した経路情報を，本部のルータ，支部 2 ～ 5 の ABR との間で通知し合う。本部のルータは，支部 1 のルータ（広域イーサ網の向こう側にあるルータ）に対し，本部のセグメントの経路情報を集約せずに通知している。更に，本部のルータは，お互いに，支部 1 のルータから通知された経路情報を通知し合っている。

支部 1 のルータは，本部のルータ（広域イーサ網の向こう側にあるルータ）に対し，支部 1 のセグメントの経路情報を集約して通知している。更に，支部 1 のルータは，お互いに，本部のルータから通知された経路情報を通知し合っている。経路集約について設問 2（2）で問われているので，集約アドレスの求め方はそこで詳しく解説しよう。

次の図に，本部と支部 1 のルータ間で経路情報を通知する様子を示す。

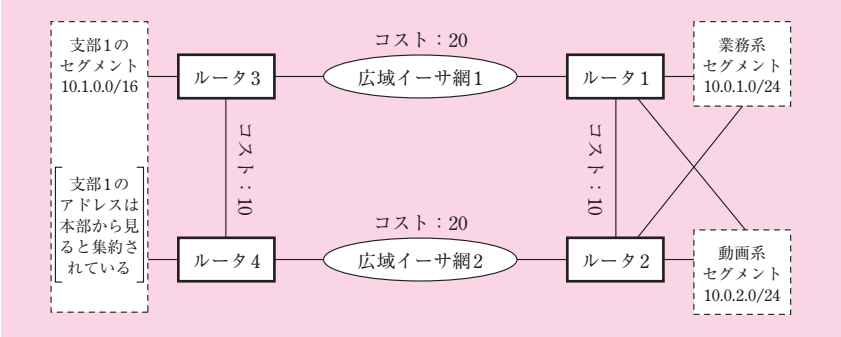


（注）他の支部から通知される経路情報は省略している。各拠点のルータ間のリンク（例：本部のルータ 1 とルータ 2 間）のネットワークアドレスは不明なので省略している。

：経路情報の通知　　：エリア

図：本部と支部 1 のルータ間の経路情報の通知

本部のルータから見た，本部と支部１間のネットワークは次の図のようになる。この図には，本文の図１に書かれたコストも記している。本部のルータからは，支部１のセグメントが集約されていることに着目できる。



図：本部のルータから見た，本部と支部１間のネットワーク

OSPF では，宛先ネットワークとそのサブネットマスクが等しい経路情報が複数存在する場合(つまり，ロンゲストマッチアルゴリズムでは同等の経路である場合)，コストが最小の経路を選択する。

本事例において，経路はどのように選択されるのだろうか。動画系セグメントのマスタルータであるルータ２とルータ４を例に取り上げて解説しよう。

ルータ２から支部１のネットワーク（10.1.0.0/16）に至る経路の候補を次の表に示す。経路①と経路②は，ロンゲストマッチアルゴリズムでは同等である。両者のコストを比較すると，経路②の方が小さい。したがって，ルータ２から支部１のネットワークに至る経路は，経路②となる。

表：ルータ２から支部１のネットワークに至る経路の候補

項番	宛先ネットワーク／サブネットマスク	ネクストホップ	コスト(*)
①	10.1.0.0/16	ルータ１	30
②	10.1.0.0/16	ルータ４	20

（＊）ルータ 4 から支部 1 のネットワークへのコストが本文に明記されていないため，コスト値の計算から除外している。経路①と経路②のコストの大小を比較できればよいので，計算から除外しても，経路選択の結論は変わらない。
以降の解説においても，OSPF のコストに言及する場合，本文に明記されていないコストは計算から除外する。
各拠点の業務系セグメントと動画系セグメントは，OSPF による経路制御を実施していない。それゆえ，ルータの業務系セグメント側のインタフェース，動画系セグメント側のインタフェースは，OSPF の経路制御を行わない設定（パッシブインタフェース）になっていると考えられる。

したがって，通常時のルータ 2 のルーティングテーブルは，次のとおりである。

表：ルータ 2 のルーティングテーブル（通常時）

宛先ネットワーク／サブネットマスク	ネクストホップ	経路設定の方法
（ルータ 1 とルータ 2 間のリンク）	（直接接続）	（直接接続）
10.0.1.0/24 （本部の業務系セグメント）	（直接接続）	（直接接続）
10.0.2.0/24 （本部の動画系セグメント）	（直接接続）	（直接接続）
10.1.0.0/16 （支部 1 のセグメントの集約アドレス）	ルータ 4	OSPF （ルータ 4 が通知した経路情報）
10.2.0.0/16（支部 2 のセグメント）	（省略）	OSPF （支部 2 のルータが通知した経路情報）
（支部 3 ～ 5 は省略）	（省略）	（省略）

（注）支部 2 ～ 5 の経路情報は，支部 1 と同様に，集約アドレスとなる。

ルータ 4 から本部の動画系セグメント（10.0.2.0/24）に至る経路を次の表に示す。経路①と経路②は，ロンゲストマッチアルゴリズムでは同等である。両者のコストを比較すると，経路②の方が小さい。したがって，ルータ 4 から本部の動画系セグメントに至る経路は，経路②となる。

表：ルータ 4 から本部の動画系セグメントに至る経路の候補

項番	宛先ネットワーク／サブネットマスク	ネクストホップ	コスト
①	10.0.2.0/24	ルータ 3	30
②	10.0.2.0/24	ルータ 2	20

したがって，通常時のルータ 4 のルーティングテーブルは，次のとおりである。

表：ルータ４のルーティングテーブル（通常時）

宛先ネットワーク／サブネットマスク	ネクストホップ	経路設定の方法
（ルータ３とルータ４間のリンク）	（直接接続）	（直接接続）
10.0.1.0/24 （本部の業務系セグメント）	ルータ２	OSPF （ルータ２が通知した経路情報）
10.0.2.0/24 （本部の動画系セグメント）	ルータ２	OSPF （ルータ２が通知した経路情報）
10.1.1.0/24 （支部１の業務系セグメント）	（直接接続）	（直接接続）
10.1.2.0/24 （支部１の動画系セグメント）	（直接接続）	（直接接続）
10.2.0.0/16（支部２のセグメント）	（省略）	OSPF （支部2のルータが通知した経路情報）
（支部３～５は省略）	（省略）	（省略）

（注）支部２～５の経路情報は，本部のルータ２のルーティングテーブルと同じである。

通常時の動画系セグメント間の経路についてまとめると，次のようになる。

- ルータ２から見た，支部１を宛先とする経路のネクストホップはルータ４である
- ルータ４から見た，本部を宛先とする経路のネクストホップはルータ２である

したがって，動画系のトラフィックは広域イーサ網２を経由することになる。

業務系セグメントについては，動画系セグメントの設定に登場する「ルータ2」を「ルータ1」に，「ルータ4」を「ルータ3」に，それぞれ読み替えればよい。したがって，通常時，業務系のトラフィックは広域イーサ網１を経由することになる。

・**【障害時の経路】**

マスタルータに障害が発生すると，VRRP の仕組みによりバックアップルータがマスタルータに切り替わる。

ルータ又は広域イーサネットに障害が発生すると，ルータ間で通知される経路情報が迂回経路を通るようになるため，ルーティングテーブルにエントリされる経路情報が動的に変化する。

障害時の経路については設問２（3）で問われているので，そこで詳しく解説しよう。

●広域イーサ網の障害時における，動画系セグメント間の通信の優先制御

一方の広域イーサ網が使用できなくなった場合，業務系セグメント間の通信と動画系セグメント間の通信は，他方の広域イーサ網を通ることになる。このとき，方針④に基づき，動画系セグメント間の通信を業務系セグメント間の通信よりも優先する。

この方針を実現するソリューションについて，〔ネットワーク経路の検討〕の第 5 段落に次のように記述されている。

> 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 TOS 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 DiffServ モデルが実装されている。

（注）説明の都合上，空欄ウ，エを補填した。

したがって，ルータの優先制御機能を用いていることが分かる。ルータは，到着したパケットを優先順位に従ってルーティングすることで，優先制御を実現している。

パケットの優先度は IP パケットの TOS フィールドに設定される。この設定は，送信元ホストで行うか，又は，優先制御機能を有するルータが一定のルールに基づいて行う。なお，本事例では，どのノードが優先度を設定しているかは明記されていない。

IP パケットの TOS フィールドについては設問 1 空欄ウ，エで問われているので，そこで詳しく解説しよう。

● FS のアクセスの高速化

FS のアクセスの高速化を実現するソリューションについて，〔WAS の導入〕の第 1 段落に次のように記述されている。

> ・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，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。……（略）……
>
> ・WAS は，データを受信した後に，“データの高速化処理”を行う。

PBR については設問 3（1），WAS が実施する「データの高速化処理」については設問 3（2）でそれぞれ問われているので，そこで詳しく解説しよう。

それでは，本事例のソリューションについて全体像をつかんだところで，いよいよ設問の解説に移ろう。

■設問 1

解答例

ア：帯域幅　又は　通信速度
イ：0
ウ：TOS
エ：DiffServ　又は　Differentiated Services
オ：高く

ア

空欄アを含む文章は，「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」と記述されている。OSPF は，コストを明示的に設定しない限り，物理ポートの帯域幅を基にコストを設定する。よって，空欄アに該当する字句は，「**帯域幅**」又は「**通信速度**」である。

イ

空欄イを含む文章は，「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」と記述されている。バックボーンエリアの番号は 0 番である。よって，空欄イに該当する数値は，「**0**」である。

ウ，**エ**

空欄ウを含む文章は，「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」と記述されている。

ルータの優先制御は，キューに着したパケットを優先順位に基づいてルーティングする仕組みになっている。パケットの優先度は，IP ヘッダの TOS フィールドに設定されている。RFC2474「Definition of the Differentiated Services Field（DS Field）in the IPv4 and IPv6 Headers」は，TOS フィールドを DS フィールドとして再定義した規格であり，この規格に基づく優先制御を DiffServ モデルと呼ぶ。

よって，空欄ウに該当する字句は「**TOS**」であり，空欄エに該当する字句は「**DiffServ**」である。

オ

空欄オを含む文章は，〔WAS の導入〕の第 1 段落の 1 番目の箇条書きにある。「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」と記述されている。

PBR は，通常の経路制御とは異なる方法で経路を選択する。そのため，PBR を動作させるには，この優先度を最も高くしておく必要がある。本事例では，ルータ 1 及びルータ 3 で PBR を動作させるが，ルータ 1 及びルータ 3 では OSPF による経路制御を行っているため，PBR の優先度を OSPF よりも高くしておく必要がある。よって，空欄オに該当する字句は，「**高く**」である。

■設問 2

(1)

解答例

デフォルトゲートウェイの設定：

業	務	系	セ	グ	メ	ン	ト	に	対	応	し	た	仮	想	ル	ー	タ	の	I	P	ア	ド	レ	ス

（25字）

VRRP の設定：

業	務	系	セ	グ	メ	ン	ト	の	仮	想	ル	ー	タ	が	ル	ー	タ	3	で	ア	ク	テ	ィ	ブ
に	な	る	よ	う	に	プ	ラ	イ	オ	リ	テ	ィ	値	を	設	定	す	る	。					

（45字）

著者解答例

VRRP の設定：

業	務	系	セ	グ	メ	ン	ト	用	の	V	R	R	P	設	定	の	プ	ラ	イ	オ	リ	テ	ィ	値
は	広	域	イ	ー	サ	網	1	側	の	ル	ー	タ	を	高	く	設	定	す	る	。				

（46字）

本問は，次の二つのことを問うている。

1. 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」
2. 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の「VRRP の設定」

それでは，一つずつ解を導こう。

●デフォルトゲートウェイの設定

下線①は，〔ネットワーク経路の検討〕の第 1 段落にある。そこには，「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。① PC 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」と記述されている。

ここで，冒頭の「業務系セグメント間と動画系セグメント間のトラフィック分散と冗長化」の解説を振り返ろう。【ルータの冗長化】で述べたとおり，業務系セグメントのサーバ及び PC のデフォルトゲートウェイは，業務系セグメントの仮想ルータの IP アドレスにする。

よって，正解は解答例に示したとおりとなる。

● VRRP の設定

通常時，業務系のトラフィックは広域イーサ網 1 を経由する。したがって，冒頭の【ルータの冗長化】で解説したとおり，業務系セグメントのマスタルータは，広域イーサ網 1 側のルータである。すなわち，本部においてはルータ 1，支部 1 においてはルータ 3 が該当する。

問題文は，「VRRP の設定をどのようにすればよいか」を問うている。解答に際しては，VRRP の設定内容が具体的に伝わるようにするとよい。VRRP を設定するルータの組においてマスタルータになるのは，プライオリティ値を高く設定したルータである。そこで，プライオリティ値の設定に着目して解答を記せばよい。

よって，正解は，「**業務系セグメント用の VRRP 設定のプライオリティ値は広域イーサ網 1 側のルータを高く設定する**」などとなる。

なお，試験センターの解答例は，「**業務系セグメントの仮想ルータがルータ 3 でアクティブになるようにプライオリティ値を設定する**」である。「広域イーサ網 1 側のルータ」ではなく，「ルータ 3」になっている。ルータ 3 は，支部 1 における広域イーサ網 1 側のルータである。問題文は「業務系セグメントの PC」に言及しているので，支部における設定を問うている。第 1 段落は本部と支部間のネットワークについて検討しているので，試験センターの解はその文脈を考慮したものである。とはいえ，自分の導いた解が「ルータ 3」に言及していなくても，広域イーサ網 1 側のルータのプライオリティ値を高くする旨を記していれば，論旨は伝わる。よって，著者解答例も正解である。

(2)

解答例

10.1.0.0/16

問題文は，「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」を問うている。

支部の経路情報の集約について，〔ネットワーク経路の検討〕の第 3 段落に，「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」と記述されている。したがって，業務系セグメントと動画系セグメントのネットワークアドレスを，「ABR で最もプレフィックスが短くなる」という条件に見合うように集約すればよい。

プレフィックスを短くすると，集約する対象となるアドレス空間が広くなる。「ABR で最もプレフィックスが短くなる」という条件は，言い換えると，「他のエリアのアドレスを含めることがない程度までアドレス空間を広げた上で，最もプレフィックスを短くする」ということである。

ルータ 3 は支部 1 の ABR である。通知する集約アドレスは，支部 1 のアドレスを含み，かつ，他の支部のアドレスを含まないようにしなければならない。

図 1 を見ると，各拠点のネットワークアドレスは，第 2 オクテットで識別されていることが分かる。すなわち，本部は「0」，支部 1 は「1」，支部 2 は「2」という具合だ。それゆえ，支部 1 のアドレスを含み，かつ，他の支部のアドレスを含まない集約アドレスは，「10.1.0.0/16」である。

よって，正解は「**10.1.0.0/16**」となる。

なお，ルータ 3 とルータ 4 間のセグメントについては，問題文中に指示がなく，図 1 中にアドレスも明記されていないため，考慮から外す(*)。

(*) 当然ながら，ルータ 3 とルータ 4 間のセグメントも，ABR から通知される。「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」という条件の下，通知する経路情報の数ができるだけ少なくなるようにアドレスを設計したければ，ルータ 3 とルータ 4 間のセグメントのアドレスが，設問 2（2）の解である「10.1.0.0/16」に含まれるようにすればよい。

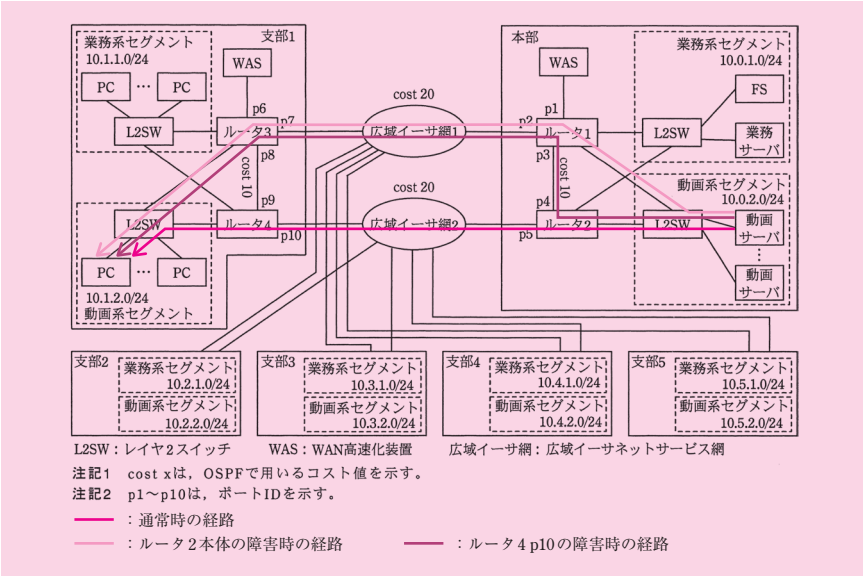
(3)

解答例

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

問題文は，「表 1 中の［ a ］，［ b ］に入れる適切な動画データの送信経路」を問うている。空欄 a は「ルータ 2　本体の障害時」の送信経路の一部であり，空欄 b は「ルータ 4　p10 の障害時」の送信経路の一部である。

結論から言うと，本部の動画サーバから支部 1 の PC 宛てのトラフィックは，次の図に示す経路を通る。



図：本部の動画サーバから支部 1 の PC 宛てのトラフィック経路

以下，障害を一つずつ取り上げて，解を導くことにしよう。

●ルータ 2 本体の障害

・動画サーバ

冒頭の【ルータの冗長化】で解説したとおり，ルータ 2 は，動画系セグメントのマスタルータになっている。ルータ 1 は，バックアップルータになっている。

ルータ 2 本体に障害が発生すると，動画系セグメントのバックアップルータであるルータ 1 が，マスタルータに昇格する。したがって，動画サーバのデフォルトゲートウェイは動画系セグメントに対応した仮想 IP アドレスのままであるが，動画データのパケットは，

動画サーバ → L2SW → ルータ 1

の順に送信される。

・ルータ 1

ルータ 2 本体に障害が発生すると，ルータ 1 は，支部 1 の集約アドレスを宛先とする経路情報を，ルータ 3 のみから通知される。したがって，動画データのパケットは，

ルータ 1 → ルータ 3

の順に送信される。

・ルータ 3

ルータ 3 は動画系セグメントを直接接続しているので，動画データのパケットは，

ルータ 3 → L2SW → PC

の順に送信される。

・まとめ

まとめると，ルータ 2 本体の障害時，本部から支部 1 への動画データの送信経路は，次のようになる。

動画サーバ → L2SW → ルータ 1 → ルータ 3 → L2SW → PC

●ルータ 4 の p10（ポート 10）の障害

・動画サーバ

ルータ 2 に障害が発生しない限り，VRRP のマスタルータは切り替わらない。したがって，動画データのパケットは，

動画サーバ → L2SW → ルータ 2

の順に送信される。

・ルータ 2，ルータ 1

ルータ 4 のポート 10 に障害が発生すると，OSPF の経路情報が変化する。ルータ 2 は，支部 1 の集約アドレスを宛先ネットワークとする経路情報を，ルータ 1 を経由して，ルータ 3 から通知される。したがって，動画データのパケットは，

ルータ 2 → ルータ 1 → ルータ 3

の順に送信される。

・ルータ 3

ルータ 3 は動画系セグメントを直接接続しているので，動画データのパケットは，

ルータ 3 → L2SW → PC

の順に送信される。

・まとめ

まとめると，ルータ 4 のポート 10 の障害時，本部から支部 1 への動画データの送信経路は，次のようになる。

動画サーバ → L2SW → ルータ 2 → ルータ 1 → ルータ 3 → L2SW → PC

●解の導出

a

ルータ 2 本体の障害時，本部から支部 1 への動画データの送信経路は，「動画サーバ → L2SW → ルータ 1 → ルータ 3 → L2SW → PC」である。よって，空欄 a に該当する経路は「**ルータ 1 → ルータ 3**」であるので，これが正解となる。

b

ルータ 4 のポート 10 の障害時，本部から支部 1 への動画データの送信経路は，「動画サーバ → L2SW → ルータ 2 →ルータ 1 → ルータ 3 → L2SW → PC」である。よって，空欄 b に該当する経路は「**ルータ 2 → ルータ 1 → ルータ 3**」であるので，これが正解となる。

(4)

解答例

利用者をグループ化して使用時間帯をずらす。（21字）

問題文は，「本文中の下線②の方策」を，「運用の観点」で解答するように求めている。

下線②は，〔ネットワーク経路の検討〕の第 6 段落にある。そこには「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」と記述されている。

これは一般的な知識から解を導く。

一般的に言って，アクセス集中によって応答時間が増大する理由は，高い使用率に起因する待ち時間の増大である。使用率は，「到着率×サービス時間／窓口数」で求まるので，使用率を下げるには，到着率を低くするか，サービス時間を短くするか，サーバ（窓口）の数を増やす方法が考えられる。

このうち，運用の観点で対応できるのは，到着率を下げる方法である。下線②中の「アクセス集中を避ける」という記述は，アクセスが集中しないよう，利用者が意識してアクセスを分散させることを示唆している。つまり，利用者間でアクセスを分散し，到着を平準化させることで，到着率を下げるわけだ。

運用上の対応でこれを実現するには，利用者をグループ化し，グループごとにアク

セスする時間帯を定めておき，かつ，そのことを利用者に周知すればよい。よって，正解は，「**利用者をグループ化して使用時間帯をずらす**」となる。

一方，サービス時間を短くすること，サーバの数を増やすことは，いずれも運用で対応できることではないため，正解ではない。

サービス時間を短くするには，処理内容を少なくするか，サーバの処理性能を高めるか，いずれかの方策が求められる。とはいえ，処理内容を少なくするには業務の見直しが必要となるため，運用では対応できない。サーバの処理性能を高めることは，そのリソースを増強することを意味しており，「運用の観点」という趣旨から外れてしまう。

サーバの数を増やすことは，システム構成を変更することを意味しており，こちらも「運用の観点」という趣旨から外れてしまう。

■設問 3

(1)

解答例

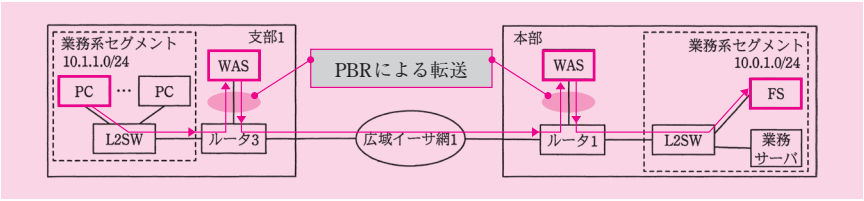
① IP アドレス
②ポート番号

問題文は，「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」問うている。

下線③は〔WAS の導入〕の第 1 段落の 1 番目の箇条書きの中にある。第 1 段落には「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」と記述されている。WAS を導入したときの通信について述べているのが，下線③を含む 1 番目の箇条書きである。そこには次のように記述されている。

> 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。

ルータ 1 及びルータ 3 が実施する，WAS 宛ての転送の様子を次の図に示す。



図：ルータ 1 及びルータ 3 が実施する，WAS 宛ての転送

PBR は，支部の PC と本部の FS が WAS 経由でファイル転送を行うために実施する。ここで問われているのは，ルータ 1 及びルータ 3 がパケットのどの情報に基づいて PBR による経路制御を行うか，ということである。

本問の解を導く前に，まずは CIFS について解説する。それを踏まえて，解を導こう。

● CIFS，SMB

CIFS（Common Internet File System）は，主として Windows 系のプラットフォームで使用されているファイル共有プロトコルである。下位層のトランスポートプロトコルに TCP を使用しており，ポート番号は 445 番である。

CIFS は，IBM が開発した SMB（Server Message Block）が基になっている。これを Microsoft が拡張し，1996 年に CIFS という名称で仕様を公開した。Microsoft は SMB をバージョンアップして SMB 2.0 とし，2008 年にリリースした OS（Windows Vista，Windows Server 2008）に搭載した。SMB 2.0 の登場により，CIFS はバージョン 1（SMB 1.0）に位置付けられている。その後も SMB はバージョンアップを重ねており，新しい OS に搭載されている。2010 年にリリースした OS（Windows 7）には SMB 2.1，2012 年にリリースした OS（Windows 8，Windows Server 2012）には SMB 3.0 が搭載されている。

SMB（CIFS を含む）は Windows に搭載されたファイル共有プロトコルであり，Windows ネットワークで他の PC にアクセスするとき，暗黙裡に使用されるものである。例えば，Windows のエクスプローラーを開いて「ネットワーク」をクリックすると他の PC が見えたり，他の PC 上で共有設定したディレクトリが見えたりするが，このときに SMB のやり取りが行われている。

●解の導出

CIFS について分かったところで，いよいよ解を導こう。

本事例では，FS のアクセス速度の低下に対応するため，WAS を導入する。ルータ 1 及びルータ 3 は，CIFS を用いたファイル転送を本部の FS と支部 1 の PC 間で行う場

合に限り，同じ拠点内の WAS にパケットを転送する。これ以外のホスト間で CIFS の通信を行うときは（例えば，Windows ネットワークで他の PC にアクセスする，など），WAS に転送しない。

したがって，ルータから WAS に転送される通信は，次の条件に合致したものでなければならない。

1. プロトコルが CIFS である
2. 支部の PC と本部の FS 間の通信である

1 番目の条件は，TCP ヘッダのポート番号から識別できる。2 番目の条件は，IP ヘッダの IP アドレスから識別できる。

よって，正解は，「**ポート番号**」「**IP アドレス**」となる。

(2)

解答例

ラ	ウ	ン	ド	ト	リ	ッ	プ	時	間	が	大	き	い	場	合

（16字）

問題文は，「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」と記述されている。

下線④は〔WAS の導入〕の第 2 段落にある。そこには次のように記述されている。

> WAS 間では，……，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。

この解を導くには，まず，CIFS でファイル転送を行う仕組みを知る必要がある。その仕組みを知ることで，どのような場合に WAS で「一括してデータを送信する」と効果的であるのかが分かるからだ。それを踏まえて，解を導こう。

● CIFS でファイル転送を行う仕組み

あらかじめ断っておくと，SMB には様々なコマンドがあり，バージョンアップを重ねるうちに機能強化も図られている。ここでは SMB の詳細に立ち入らず，本問を解

くのに最低限必要となる，基本的な仕組みについて解説する。

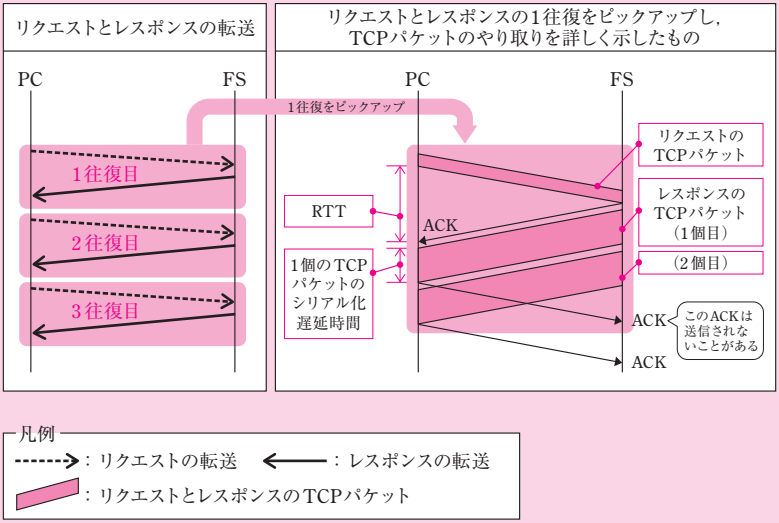
CIFS（SMB 1.0）では，基本的に，「リクエストとレスポンス」の組（1 往復）を単位にして，やり取りが行われる。例えば，PC が FS からファイルを読み出すとき，PC はリクエスト（読出しのコマンド）を送信する。FS はレスポンス（指定されたファイルのデータ）を返信する。

CIFS の仕様上，リクエストとレスポンスの 1 往復でやり取りできるデータサイズには，上限がある。したがって，この上限値よりも大きいファイルサイズを読み出すには，リクエストとレスポンスの組が何往復もやり取りされることになる(*)。

（*） 本問は CIFS（SMB 1.0）を扱っているため，「リクエストとレスポンスの組（1 往復）」を単位にやり取りするとシンプルに考えて，解を導いている。
参考までに，SMB 2.0 は，1 回のリクエストパケットで複数のコマンドを送信する機能，直前のリクエストに対するレスポンスを待たずに次のリクエストを送信する機能など，数々の機能強化が図られている。

更に，リクエストとレスポンスの 1 往復でやり取りできるデータサイズとして，TCP パケットの最大長よりも大きな値を指定することができる。このとき，レスポンスは複数の TCP パケットに分割される。

ここまで解説した内容に基づき，PC が FS から 1 個のファイルを読み出すときのシーケンスを次の図で示す。



図：リクエストとレスポンスの転送シーケンス

ここで，図の左側は，CIFS のリクエストとレスポンスのやり取りを示している。ここでは，1 個のファイルを読み出すのに 3 往復のやり取りをしている。

図の右側は，リクエストとレスポンスの 1 往復をピックアップし，TCP パケットのやり取りを詳しく示している。ここでは，リクエストのサイズは TCP パケットの 1 個分，レスポンスのサイズは TCP パケットの 2 個分としている。FS から PC 宛てにレスポンスを転送するとき，TCP の連続転送の仕組みにより，2 個の TCP パケットを，ACK（確認応答パケット）を待たずに転送している。

ピックアップした図の PC 側に示した「シリアル化遅延時間」は，パケットを 1 ビットずつ伝送するのに要する時間である。シリアル化遅延時間は「伝送時間」ともいう。伝送効率を無視すると，シリアル化遅延時間は次の式で求められる。

$$\text{シリアル化遅延時間［秒］} = \frac{\text{パケットサイズ［ビット］}}{\text{帯域［ビット／秒］}}$$

同じくピックアップした図の PC 側に示した「RTT」（Round Trip Time）は，パケットの往復時間（相手ノードに TCP パケットを送信してから，相手ノードからの ACK パケットを受信するまでの時間）である。

したがって，1 往復の所要時間は，シリアル化遅延時間と RTT の合計値となる。

$$\text{1 往復当たりの所要時間［秒］} = \text{シリアル化遅延時間［秒］} + \text{RTT［秒］}$$

前述のとおり，CIFS は，「リクエストとレスポンス」の組（1 往復）を単位に，やり取りを行う。支部の PC と本部の FS 間で CIFS のやり取りを行うとき，PC は，リクエストを送信すると，RTT が経過してレスポンスを受信するまで，新たなリクエストを送信できない。したがって，1 個のファイルを読み出すのに何往復も必要とする場合，転送の所要時間はその往復分の時間となる。つまり，次の式で求められる。

$$\text{転送の所要時間［秒］} = \text{1 往復当たりの所要時間［秒］} \times \text{往復数}$$

●解の導出

CIFS でファイル転送を行う仕組みが分かったところで，いよいよ解を導こう。

本事例では，本部と支部間を広域イーサ網で接続している。WAN 回線を経由した通信では，RTT の値は数十ミリ秒に達する。

具体例として，転送の所要時間を次の条件に従って求めてみよう。

表：転送の所要時間を求めるための条件

広域イーサ網の帯域幅	100×10^6［ビット／秒］
広域イーサ網の RTT	30×10^{-3}［秒］
ファイルサイズ	60,000,000 バイト
1 往復当たりの転送データサイズ	3,000 バイト
往復数	20,000 回（＝ 60,000,000 ÷ 3,000）

$$\text{シリアル化遅延時間［秒］} = \frac{3000 \times 8\text{［ビット］}}{100 \times 10^6\text{［ビット／秒］}} = 0.24 \times 10^{-3}\text{［秒］}$$

$$\begin{aligned}\text{1 往復当たりの所要時間［秒］} &= 0.24 \times 10^{-3}\text{［秒］} + 30 \times 10^{-3}\text{［秒］} \\ &= 30.24 \times 10^{-3}\text{［秒］}\end{aligned}$$

$$\begin{aligned}\text{転送の所要時間［秒］} &= 30.24 \times 10^{-3}\text{［秒］} \times 20000 \\ &= 604.8\text{［秒］}\end{aligned}$$

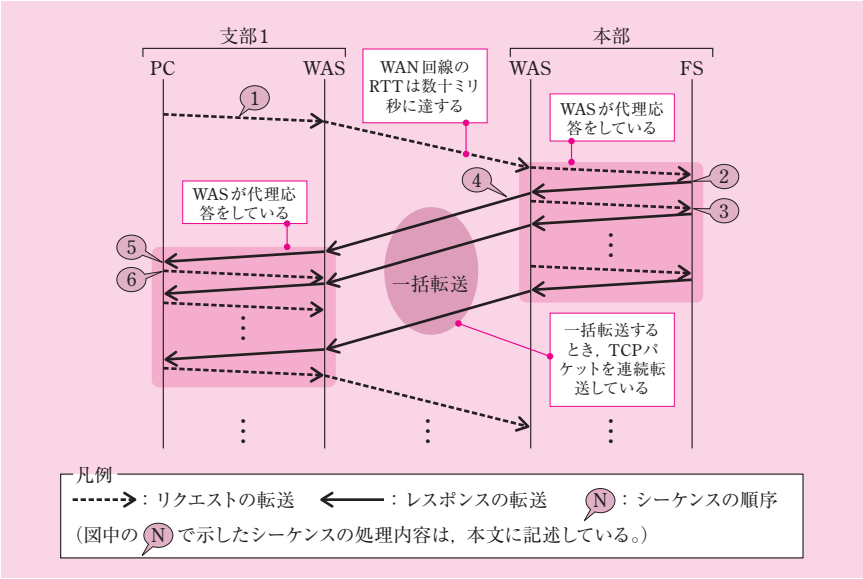
WAS の高速化処理について，下線④には「データの送信元に対して代理応答を行ってデータをキャッシュに蓄積した後に，もう一方の WAS 宛てに一括してデータを送信する」とある。「代理応答」という記述から，

- 支部 1 においては，支部 1 の WAS があたかも FS であるかのように振る舞う
- 本部においては，本部の WAS があたかも PC であるかのように振る舞う

ということが推論できる。

そのような代理をする目的は，WAS 間で一括してデータを送信するためであり，この一括転送こそ高速化の鍵を握っている。

この様子を次の図に示す。



図：WAS を用いた，リクエストとレスポンスの転送シーケンス

1. 支部 1 の PC は，支部 1 の WAS にリクエスト（1 回目）を転送する。支部 1 の WAS は，本部の WAS にこれを転送する。本部の WAS は，FS にこれを転送する。
2. FS は，リクエストを受信すると，本部の WAS にレスポンス（1 回目）を転送する。
3. 本部の WAS は，すぐに，FS にリクエスト（2 回目）を転送する。この WAS の振舞いが，下線④で「代理応答」と呼ばれている。この代理応答は，何度も行われる。LAN 上でやり取りしているため，RTT はほぼゼロである。
4. 本部の WAS は，WAS は代理応答をすると共に，レスポンスをキャッシュする。このキャッシュしたデータを支部 1 の WAS に一括転送する。支部 1 の WAS も，一括転送されたデータをキャッシュする。
5. 支部 1 の WAS は，PC にレスポンス（1 回目）を転送する。
6. 支部 1 の PC は，すぐに，支部 1 の WAS にリクエスト（2 回目）を転送する。支部 1 の WAS は，キャッシュしたデータからレスポンス（2 回目）を転送する。この WAS も，「代理応答」をしている。

（以下，略）

この代理応答と一括転送によって，転送の所要時間はどのように改善されるのだろうか。先ほどの具体例で確かめてみよう。

新たに付け加える条件として，一括転送するデータサイズをレスポンスの 10 回分としてみる。その結果，1 往復当たりの転送データサイズは 10 倍に，往復数は 0.1 倍になる。

表：転送の所要時間を求めるための条件

一括転送するデータサイズ	レスポンスの 10 回分
1 往復当たりの転送データサイズ	30,000 バイト（＝ 3,000 × 10）
往復数	2,000 回（＝ 20,000 ÷ 10）

$$\text{シリアル化遅延時間［秒］} = \frac{30000 \times 8\text{［ビット］}}{100 \times 10^6\text{［ビット／秒］}} = 2.4 \times 10^{-3}\text{［秒］}$$

$$\begin{aligned}\text{1 往復当たりの所要時間［秒］} &= 2.4 \times 10^{-3}\text{［秒］} + 30 \times 10^{-3}\text{［秒］} \\ &= 32.4 \times 10^{-3}\text{［秒］}\end{aligned}$$

$$\begin{aligned}\text{転送の所要時間［秒］} &= 32.4 \times 10^{-3}\text{［秒］} \times 2000 \\ &= 64.8\text{［秒］}\end{aligned}$$

この例では，転送の所要時間は約 1/10 になることが分かる。その理由は，往復数が 0.1 倍になったからである。1 往復当たりの所要時間の大半を RTT（30 ミリ秒）が占めているため，往復数が減った分だけ転送の所要時間が短くなるわけだ。

このように，RTT が大きい場合，WAS の高速化処理の効果がより高くなることが分かる。

よって，この旨を解答すればよい。正解は，「**ラウンドトリップタイムが大きい場合**」となる。

参考までに，WAS は平成 20 年度午後 I 問 3 で出題されている。時間があるときに確認しておくとよいだろう。

(3)

解答例

片側のWASが故障した場合（13字）

問題文は，「下線⑤の機能はどのような場合に必要になるか」を問うている。

下線⑤は〔WAS の導入〕の第 2 段落にある。そこには，「⑤データの高速化処理を自動的に停止する機能」と記述されている。

これは一般的な知識から解を導く。

WAS は，データを一括転送したり，圧縮して送受信したりする機能をもっている。これらの機能は，対向側が故障したら正しく動作しなくなる。したがって，対向側を監視し，その故障を検知したら，高速化処理を自動的に停止する機能が必要である。さもないと，ファイル転送を継続できなくなってしまうからだ。

よって，正解は，「**片側の WAS が故障した場合**」となる。

問 2

出題趣旨
ネットワークの保守作業では，ネットワークの構成，機器の動作及び実装を理解して障害箇所の特定と機器の交換を行い，短時間のうちに通信を復旧させる必要がある。保守対象のネットワークは，自ら設計，構築に携わったものでないことも多く，ネットワーク構成図を読み解く能力も必要である。これらの業務に従事するネットワーク技術者には，高度な知識と経験が要求される。 本問では，ファイアウォールの保守作業でのミス，仮想ファイアウォールの導入検討を題材に，通信プロトコル，ファイアウォール及び周辺機器の動作，保守作業手順のまとめ，VLAN 設計，ファイアウォール負荷分散の考え方について基本的な要素を問う。

採点講評
問 2 では，ファイアウォール（以下，FW という）の障害対応を題材に取り上げ，FW の冗長化構成と，VLAN 及び仮想 FW の設計について出題した。加えて，OSI 基本参照モデルの第 1 層から第 4 層までの各層と，隣接する層間の関係について問うことも意図した。全体として，正答率は低かった。 設問 1 では，イの正答率が低かった。FW の冗長化構成における重要な機能なので把握しておいてほしい。 設問 2 では，(1) をアプリケーション間の通信に着目せずに，FW に着目した解答が散見された。機能を曖昧に説明した解答も多く，TCP の信頼性のある通信を実現する機能は何であるかを端的に解答してほしかった。(3) は，SW2 を挟む構成にすることで，第 2 層を透過しつつ第 1 層を分離している観点から解答してほしかった。(5) a は正答率が低かった。(4) にも関係するが，通信の第 2 層と第 3 層の違いを把握しておいてほしい。 設問 3 は，本文を読解して，VLAN 及び仮想 FW の構成図が描ければ難しくない問題である。(2) では，仮想 FW の配置の目的を主体に説明して，肝心の配置の具体性に欠ける記述になっていた解答が散見された。

設問			解答例・解答の要点	備考
設問 1		ア	NAPT	
		イ	ステートフル	
		ウ	物理　又は　第 1	
		エ	Gratuitous ARP　又は　GARP	
		オ	タグ　又は　Tag	
設問 2	(1)		SW3 と L3SW の間	
	(2)		TCP の再送機能	
	(3)		一方のポート故障による対向ポートのリンク断を防ぎ，どちらの FW の障害か特定が容易になる。	
	(4)		MAC アドレステーブル	
	(5)	a	ルータ，DNS サーバ，Web サーバ	
		b	FW1 から設定情報が同期されたこと	
設問 3	(1)		SW4 と L3SW を相互に入れ替える。	

（表は次ページに続く）

設問		解答例・解答の要点	備考
設問 3	(2)	・FW1 で企画部用の仮想 FW を，FW2 で営業部用の仮想 FW を，それぞれ Active にする。 ・FW2 で企画部用の仮想 FW を，FW1 で営業部用の仮想 FW を，それぞれ Active にする。	

■設問 1

解答例

ア：NAPT
イ：ステートフル
ウ：物理　又は　第 1
エ：Gratuitous ARP　又は　GARP
オ：タグ　又は　Tag

ア

空欄アを含む文章は，「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」と記述されている。

FW は，非公開セグメントと公開セグメントの境界に設置される。通常，非公開セグメントではプライベートアドレスを使用しているので，非公開セグメントのホストからインターネットにアクセスするときは，送信元 IP アドレスをグローバルアドレスに変換する必要がある。非公開セグメントには多数のホストが存在するため，1 個のグローバルアドレスを複数のホストで共有して変換する必要がある。

TCP/IP の通信は，送信元／宛先 IP アドレス，送信元／宛先ポート番号，（IP ヘッダの）プロトコル番号の組で識別される。宛先 IP アドレス，宛先ポート番号，プロトコル番号が等しい複数の通信が FW を経由する場合でも，通信の識別性は保たれなければならない。そこで，送信元 IP アドレスをグローバルアドレスに変換する際，このグローバルアドレスを共有する複数のホスト間で通信を識別できるようにするため，送信元ポート番号も同時に変換する。

アドレス及びポート番号を変換するこの機能のことを NAPT（Network Address and Port Translation）という。よって，空欄アに該当する字句は，「**NAPT**」である。

イ

空欄イを含む文章は，「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」と記述されている。

冗長構成を採用している FW 間では，フェールオーバした後も通信を継続させる機能をもっている。この機能のことを「ステートフルフェールオーバ」という。よって，空欄イに該当する字句は，「**ステートフル**」である。

［ウ］

空欄ウを含む文章は，〔FW の構成と交換作業〕の第 5 段落にある。そこには，FW を SW（L2 スイッチ）に接続したところ，FW1 接続ポートで「正常接続を表すリンク LED が消灯していた」と記述されている。空欄ウは，この正常接続が OSI 基本参照モデルのどの層に該当するかを問うものである。

SW や NIC のリンク LED は，ケーブルを介して相手側と電気的に接続している状態になると点灯する。これは，OSI 基本参照モデルの物理層（第 1 層）での正常接続を表すものである。よって，空欄ウに該当する字句は「**物理**」又は「**第 1**」である。

［エ］

空欄エを含む文章は，「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」と記述されている。

自ポートに設定された IP アドレスを目標アドレスに指定するアドレス解決を，Gratuitous ARP（GARP）という。Gratuitous ARP を受信したノードは，ARP テーブルを更新する仕様になっている。

Gratuitous ARP について，詳しくは本書の第 3 章「3.4.2　特別な用途の ARP」を参照されたい。

空欄エの文脈は，FW を代替機に交換したときに ARP テーブルを更新する必要があると述べている。その理由は，代替機に交換した結果，「各ポートの MAC アドレスが変わった」からである。

実は，この交換を行った後，本来の設定情報を代替機に復元している（〔FW の構成と交換作業〕第 5 段落を参照）。したがって，代替機には，FW に割り当てられた IP アドレスが正しく設定されていることが分かる。

交換前に FW のアドレス解決を行ったノードは，FW の IP アドレスに対応する MAC アドレスとして，アドレス解決時点のものを ARP テーブルにキャッシュしている。すなわち，交換後には存在していない「古い MAC アドレス」を，FW の IP アドレスに対応付けてキャッシュしているわけだ。

この状態でノードが FW 経由の通信を行うと，ノードが送信する MAC フレームの

宛先 MAC アドレスには古い MAC アドレスが格納されてしまう。当然ながら，FW 経由の通信に失敗してしまう。

したがって，FW を代替機に交換した後，ノードの ARP テーブルを更新する必要がある。そのために用いられるのが，Gratuitous ARP である。対象となるノードは，FW 経由の通信を行う際に ARP 要求を送信するノード，すなわち，同一ブロードキャストドメイン内の全てのノードである。この点，Gratuitous ARP はブロードキャストパケットであるため，これを用いれば対象となる全てのノードに到達できる。

よって，正解は，「**Gratuitous ARP**」又は「**GARP**」である。

オ

空欄オを含む文章は，「［オ］VLAN を使用して 1 本のリンクに複数の VLAN を収容する接続を行（う）」と記述されている。

同一の物理リンクに，複数の異なる VLAN のリンクを束ねる技術は，タグ VLAN である。よって，空欄オに該当する字句は，「**タグ**」又は「**Tag**」である。

タグ VLAN について，詳しくは本書の第 1 章「1.4.3　VLAN」を参照されたい。

■設問 2

(1)

解答例

SW3 と L3SW の間

本問は，「トランク接続でなければならない箇所」を問うている。

「トランク接続」の定義は，〔仮想 FW 導入案の検討〕の第 1 段落にある。そこには，「タグ VLAN を使用して 1 本のリンクに複数の VLAN を収容する接続」と記述されている（空欄オを補填）。

SW3 は，企画部 VLAN の PC と営業部 VLAN の PC を収容している。SW3 はレイヤ 2 スイッチであり，二つの VLAN を収容するため，ポートに VLAN を割り当てている。

PC の収容ポートに割り当てる VLAN は，当該 PC の所属 VLAN だけでよい。それでは，L3SW の収容ポートに割り当てる VLAN については，どうだろうか。

PC が L3SW を経由して他のホストと通信するとき，その通信は SW3 と L3SW 間の物理リンクを通る必要がある。したがって，SW3 と L3SW の間の物理リンクは，企画部 VLAN と営業部 VLAN の二つのリンクを通す設定になっていなければならない。つ

まり，L3SW の収容ポートに割り当てる VLAN は，企画部 VLAN と営業部 VLAN の二つである。対向側の L3SW のポートも同様に VLAN を割り当てる。したがって，この物理リンクは，トランク接続でなければならない。

よって，正解は，「**SW3 と L3SW の間**」となる。

(2)

解答例

T C P の 再 送 機 能　（8字）

下線①は，〔FW の構成と交換作業〕の第 2 段落にある。そこには，「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」と記述されている。

そもそも，FW のフェールオーバ時にデータの保全性を気に掛けるべきなのはなぜだろうか。

FW に障害が発生した瞬間，たまたま FW を経由していたパケットは損失してしまう。加えて，下線①の直前の文章に記述されているとおり，本事例の FW はステートフルフェールオーバ機能を動作させている。主系から副系にフェールオーバする際，この機能により管理情報が副系に引き継がれる。短いとはいえ引継ぎには時間がかかるので，フェールオーバが完了するまで，FW 経由の通信は一時的に中断せざるを得ない。この中断が原因でパケットが損失する可能性もある。

そのようなわけで，FW のフェールオーバ時にデータの保全性を気に掛けるべき理由は，FW のフェールオーバによってパケット損失が生じるリスクがあるからだ。

したがって，下線①が言及しているトランスポート層プロトコルの機能とは，「たとえパケットが損失しても，アプリケーション層のデータの保全性が保たれる機能」と言い換えることができる。本問はその機能が何であるかを問うている。

問われている内容が判明したので，ここから先は一般的な知識から解を導くことができる。

本事例のネットワークは IP ネットワークであるため，インターネットのプロトコルスイートを前提に考える。そのトランスポート層プロトコルには，TCP と UDP がある。

TCP，UDP は，通信する両端のアプリケーション間でパケットを送受信するプロトコルであるが，TCP はコネクション型であり，UDP はコネクションレス型である。

TCP は，コネクションを確立した後，コネクション単位でパケットの順序を管理している。パケット順序の入れ替わりやパケットの損失などのエラーを検出し，パケットを再送する機能をもっている。それゆえ，アプリケーションデータの保全性が保証される。

一方，UDP はコネクションを確立せず，単純にパケット単位で通信を行うのみである。それゆえ，パケット順序の入れ替わりやパケットの損失を検出する機能をもたず，アプリケーションデータの保全性は保証されない。

したがって，前述のとおり FW のフェールオーバ時にパケット損失が生じたとしても，トランスポート層プロトコルが TCP であれば，再送機能によってアプリケーションのデータの保全性は保たれることが分かる。つまり，下線①が言及している機能は，「**TCP の再送機能**」である。よって，これが正解となる。

(3)

解答例

一	方	の	ポ	ー	ト	故	障	に	よ	る	対	向	ポ	ー	ト	の	リ	ン	ク	断	を	防	ぎ	,
ど	ち	ら	の	F	W	の	障	害	か	特	定	が	容	易	に	な	る	。						

（44 字）

下線②を含む文章は，〔FW の構成と交換作業〕の第 3 段落にある。下線②の文脈は，FW1 と FW2 間のフェールオーバリンクの構成について説明しており，「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」と記述されている。したがって，本問は，「ケーブル直結にする構成」と「SW を挟む構成」を障害切分けの観点から比較し，「SW を挟む構成」の利点を解答することを求めている。

一般的に言って，障害の切分けは，故障を含む範囲と含まない範囲を明確にし，故障部位を含む範囲を徐々に絞り込むことによって達成される。範囲を明確にするには，仮説検証型のアプローチを用いればよい。すなわち，切分け対象となる範囲に障害がある（又は，障害がない）という仮説を立て，その仮説から導かれる事象の発生を検証すればよい。

それでは，これから障害の例を幾つか取り上げ，障害をどのように切り分けるかを述べる。その切分けにおいて，前述の二つの構成（ケーブル直結にする構成と SW を挟む構成）のどちらかに優位性があるかどうかを考察してみよう。もし SW を挟む構成の方に利点があるならば，それが正解となる。

一つ目の例として，本体の電源系統が故障したケースを取り上げる。このときは，

本体に電気が供給されていないはずだ。そこで，電源ランプが消灯していることを確認することで，障害を切り分けることができる。この切分けについては，二つの構成に差異はない。

二つ目の例として，本体のシステム（OS 等）に障害が発生したケースを取り上げる。このときは，コマンド操作を行えないはずだ。そこで，機器にログインできること，ログイン後に適切な操作を行えることを確認することで，障害を切り分けることができる。この切分けについても，二つの構成に差異はない。

さて，とりあえず二つのケースを列挙したが，そのどちらも，本体がそもそも動作しないケースである。ここまでの考察から，この種の障害の切分けにおいて，二つの構成に差異はないことが分かる。それゆえ，本体の障害については，これ以上深入りしないことにしよう。

三つ目の例として，物理ポートに障害が発生したケースを取り上げる。このとき，例えば，物理層の故障であれば，その物理ポートがリンクダウンしているはずなので，リンク LED の消灯を確認すれば障害を切り分けることができる。ネットワーク層以下の故障であれば，IP パケットが到達可能ではないので，ping コマンドを投入すれば障害を切り分けることができる。

フェールオーバリンク以外の物理ポートについては，前述の方法で障害が発生している箇所を特定できるので，二つの構成に差異はない。

一方，フェールオーバリンクの物理ポートについては，どうだろうか。ケーブル直結にする構成では，故障が発生したポートだけでなく，対向側の FW のポートもリンクダウンしてしまう。これでは，どちらの FW の障害であるかを特定することができない。これに対し，SW を挟む構成では，ポート故障によるリンクダウンは SW の対向ポートにのみ波及するので，リンク LED を確認することで障害を切り分けることができる。したがって，フェールオーバリンクの物理ポートの故障の切分けにおいて，SW を挟む構成の方に利点がある。

よって，正解は解答例に示したとおりとなる。

(4)

解答例

M	A	C	ア	ド	レ	ス	テ	ー	ブ	ル

（11字）

問題文は，「下線③のテーブル名」を問うている。

下線③を含む文章は，〔FW の構成と交換作業〕の第 3 段落の 2 番目の箇条書きにある。下線③の文脈は，FW の冗長構成及びフェールオーバに関する動作について述べ，箇条書きで列挙している。1 番目と 2 番目の箇条書きは，次のように記述されている。

・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。

本問を解くには，スイッチのレイヤ 2 機能に関する一般的な知識が必要である。そこで，まずはその点について解説する。それを踏まえて，解を導こう。

●スイッチの機能

どのレイヤ 2 スイッチも必ず装備している機能は，アドレス学習機能と転送機能である。

スイッチは，MAC フレームの受信を契機に，受信したポートの先に送信元ノードが存在していることを学習する。ただし，直接収容しているのか，別のスイッチを経由して存在しているのかまでは分からない。

このとき学習した内容（受信ポートと送信元 MAC アドレスの対応付け）を，MAC アドレステーブルに登録する。これがアドレス学習機能である。

スイッチは，MAC フレームを受信すると，どのポートの先にどのノードがあるかを MAC アドレステーブルから判定し，特定のポートからフレームを送り出す。これが転送機能である。

転送する際，受信フレームの宛先 MAC アドレスが MAC アドレステーブルに登録されていない場合，つまり，宛先ノードがどのポートの先に存在するかをまだ学習していない場合，スイッチは，（受信ポートを除く）各ポートから一斉にフレームを送り出す。これをフラッディングという。スイッチがフレームを特定のポートのみから転送できるのは，アドレス学習が適切に行われているからに他ならない。

言うまでもなく，ポートと MAC アドレスの対応付けは，変化し得るものである。例えば，PC をスイッチからいったん切り離し，別のポートにつなぎ直すかもしれない。その点を考慮し，スイッチは，エージングタイムと呼ばれる期間内に同一の内容を再学習しないと，MAC アドレステーブルからその登録を抹消する。多くの製品ではエージングタイムは 300 秒である。

●解の導出

レイヤ 2 スイッチの機能について分かったところで，いよいよ解を導こう。

第 3 段落の 1 番目の箇条書きにあるとおり，主系から副系にフェールオーバすると，IP アドレスと MAC アドレスが主系から副系に引き継がれる。したがって，フェールオーバの結果，主系（FW1）と副系（FW2）の別々のポートに収容している SW においては，ポートと MAC アドレスの対応付けが変化してしまう。すなわち，FW の MAC アドレスは，フェールオーバ前は主系（FW1）の収容ポートの先に存在していたが，フェールオーバ後は副系（FW2）の収容ポートの先に存在することになる。

アドレス学習は，あくまでフレームの受信を契機に行われる。したがって，副系（FW2）からフレームを受信しない限り，エージングタイムが満ちるまで，FW を宛先とする MAC フレームを主系（FW1）の収容ポートから送り出してしまう。当然ながら，FW を経由する通信に失敗してしまう。

そこで，Active になった後，副系は，FW の MAC アドレスを送信元 MAC アドレスとする MAC フレームを送信する。これが，第 3 段落の 2 番目の箇条書きに記述された，「切り替わったことを通知するフレーム」の正体である。

よって，下線③のテーブルは「**MAC アドレステーブル**」であり，これが正解となる。

参考までに，このフレームの宛先 MAC アドレスは，ブロードキャストアドレスである。なぜなら，主系と副系を別々のスイッチに収容するなど，様々なネットワーク構成が一般的にあり得るため，FW から同一ブロードキャストドメイン内の全てのスイッチに通知する必要があるからだ。

このフレームのタイプ（上位層プロトコル）は，このブロードキャストフレームを受信するノードに悪影響を与えないものであれば何でもよい。

(5)

解答例

a：ルータ，DNS サーバ，Web サーバ
b：FW1 から設定情報が同期された こと （17字）

a

空欄 a は，表 1「FW 故障時の交換作業手順」の，FW1 の作業順序（5）の中にある。順序（5）の作業は，「ARP テーブル初期化」である。その作業内容は，「L3SW，a について初期化する」と記述されている。したがって，ここで問われてい

るのは，主系である FW1 を代替機に交換した後，どのノードの ARP テーブルを初期化する必要があるか，ということだ。すでに L3SW は記されているので，それ以外のノードを解答すればよい。

設問 1 の空欄エで解説したとおり，FW を代替機に交換した後，同一ブロードキャストドメイン内の全てのノードの ARP テーブルを更新する必要がある。

図 1 を見ると，FW1 及び FW2 と同一ブロードキャストドメインにあるノードは，L3SW（正確に言うと，L3SW 内のルータ），インターネットとの境界にあるルータ，DMZ にある DNS サーバ及び Web サーバである。したがって，L3SW 以外のノードで ARP テーブルを初期化する必要があるのは，ルータ，DNS サーバ，Web サーバの三つである。よって，これが正解となる。

b

空欄 b は，表 1「FW 故障時の交換作業手順」の，FW2 の作業順序（3）の中にある。順序（3）の作業は，「電源投入」である。その作業内容は，「Standby 動作に入り，［ b ］を確認する」と記述されている。したがって，ここで問われているのは，副系である FW2 を代替機に交換した後，Standby 動作に入った後に何を確認するか，ということだ。

FW が Standby 動作に入ったときの動作について，〔FW の構成と交換作業〕の第 3 段落の 4 番目の箇条書きには，「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」と記述されている。

この記述は「起動時」に当てはまる。順序（3）の作業は「電源投入」であることから，順序（3）の作業内容は，この記述どおりに動作していることを確認することであるはずだ。

FW2 を代替機に交換する前，FW1 は Active 動作をしている最中である。この点を踏まえて，表 1 の FW2 の作業順序（1）～（3）を見てみよう。

順序（1）は，「設定確認」である。その内容は，「代替機の主系設定が解除されていることを確認する」ことだ。したがって，順序（1）の完了時点で，FW2 の代替機は副系になっている。

順序（2）は，「交換及び接続」である。その内容は，「代替機の電源を切断し，交換及び接続を行う」ことだ。したがって，順序（2）の完了時点で，FW2 は代替機と交換されている。ただし，電源は投入されていない。

そして，いよいよ順序（3）に移る。まず，作業者は FW2 の電源を投入する。する

と，4 番目の箇条書きの記述に従い，FW2 はフェールオーバリンクの先にある FW1 を認識し，Standby 動作に入る。次いで，FW2 は，Active 動作中の FW1 から設定情報を同期する。この同期は自動的に行われるので，同期が正しく行われているか作業者は確認する必要がある。この確認作業が，空欄 b に該当する。

よって，正解は，「**FW1 から設定情報が同期されたこと**」となる。

この解は，FW1 を代替機に交換するときの作業順序（1）～（3）と見比べることでも導ける。

FW1 を代替機に交換する前，FW2 は Active 動作をしている最中である。この点を踏まえて，表 1 中の FW1 の順序（1），（2）を見てみると，このときに行う作業は，FW2 と同じことが書かれている。すなわち，（1）副系の設定，（2）交換及び接続，である。それゆえ，続く作業（3）の「電源投入」を行うと，FW2 と同じく，Standby 動作に入るはずだ。実際，表 1 中の FW1 の順序（3）には，次のように記述されている。「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」。

したがって，FW1 の順序（3）に「FW2 から設定情報が同期されたことを確認する」と記述されている以上，FW2 の順序（3）も同じ内容であると推論できる。ただし，同期する相手が対向側であることに留意し，「FW2」を「FW1」に置換する。こうして，先ほど導いた解と同じものが得られる。

参考までに，FW1 と FW2 の交換作業は，順序（4）以降が異なっている。FW1 は，順序（4）で主系への切戻し，順序（5）で ARP テーブルの初期化，順序（6）で通信確認を行う。FW2 は，順序（4）で通信確認を行う。FW1 の順序（6）と FW2 の順序（4）は同じ内容である。

つまり，FW1 の方は，主系への切戻しと ARP テーブルの初期化が，順序（3）の後に追加されているわけだ。その目的は，故障した FW1 を代替機に交換した後，これを主系として動作させるためである。順序（4）は，まさにこのための作業である。

順序（5）が必要な理由は，設問 1 の空欄エで解説したとおりである。FW1 を代替機に交換すると物理ポートの MAC アドレスが変わるため，ARP テーブルを更新する必要があるからだ。

■設問 3

（1）

解答例

SW4 と L3SW を相互に入れ替える。

本問を解くには，本事例に登場する仮想 FW の機能，仮想 NW を導入した後のネットワーク構成について理解しておく必要がある。そこで，まずはその点について解説する。それを踏まえて，解を導こう。

●仮想 FW の機能

仮想 FW を導入する目的について，〔FW の構成と交換作業〕の第 6 段落の O 主任の 3 番目の発言には，「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」と記述されている。では，このために仮想 FW を用いるのはなぜだろうか。それを知るには，仮想 FW の機能を見てみるとよい。〔仮想 FW 導入案の検討〕の第 1 段落には次のように記述されている。

> 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，タグ 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。

したがって，企画部用の仮想 FW と営業部用の仮想 FW を別々に設けることにより，部ごとにフィルタリングルールを分けるという目的を達成できる。

企画部と営業部は VLAN が異なっているので，企画部用の仮想 FW と営業部用の仮想 FW は，IP アドレスが異なっていなければならない。この点については，それぞれの仮想 FW の仮想ポートに「IP アドレス及び VLAN 番号」を割り当てることによって対応できる。

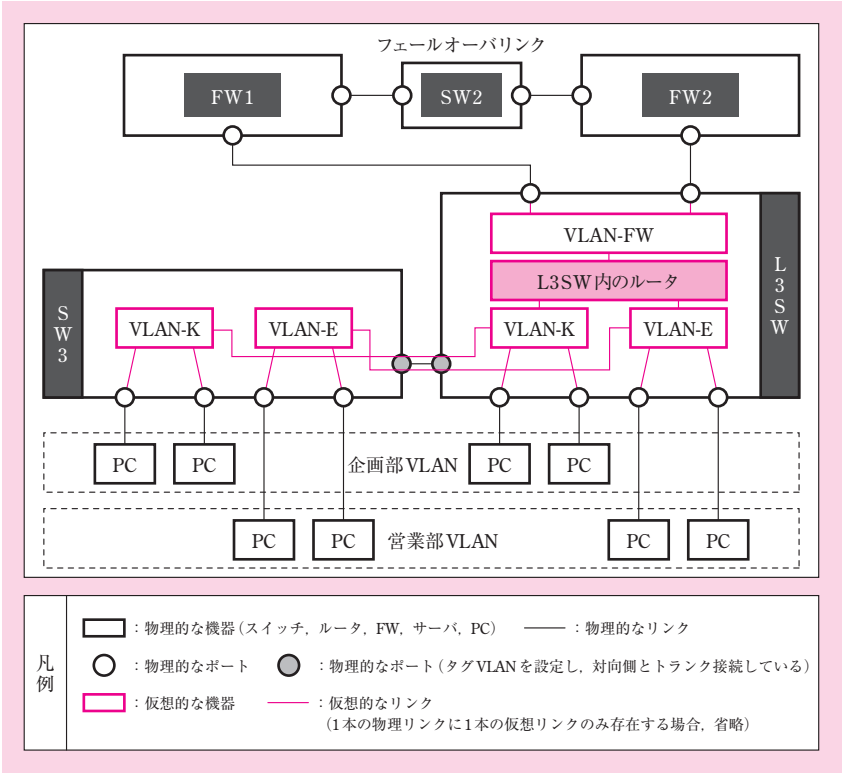
FW の内部では，企画部 VLAN のリンクを企画部用の仮想 FW に，営業部 VLAN のリンクを営業部用の仮想 FW に，それぞれ仮想的に接続する。それゆえ，FW の社内側の物理ポートは，二つの VLAN を収容しなければならない。この点については，「仮想 FW との通信は，タグ VLAN を使用して 1 本のリンクに複数の VLAN を収容する接続を行い，VLAN 番号を合致させることで可能になる」とあるので，物理ポートにタグ VLAN を設定することによって対応できる。

●仮想 FW を導入した後のネットワーク構成

仮想 FW の機能について分かったので，次に仮想 FW を導入した後のネットワーク構成について考察してみよう。その後，本問の解を導くことにする。

・企画部 VLAN，営業部 VLAN，FW の接続

第 2 段落に「企画部と営業部の VLAN 間通信を廃止する」とある。図 1「Z 社の現在のネットワーク構成」を見ると，企画部 VLAN と営業部 VLAN の間に L3SW がある。L3SW は内部にルータをもっており，このルータに直接接続された VLAN をルーティングする。「企画部と営業部の VLAN 間通信」とは，要するに，ルータによる経路制御のことだ。現在のネットワーク構成に VLAN を書き加えると，次の図のようになる。



図：現在のネットワーク構成（企画部，営業部）

図中の VLAN は，次の表に示すセグメントを指している。

表：「現在のネットワーク構成」におけるセグメント

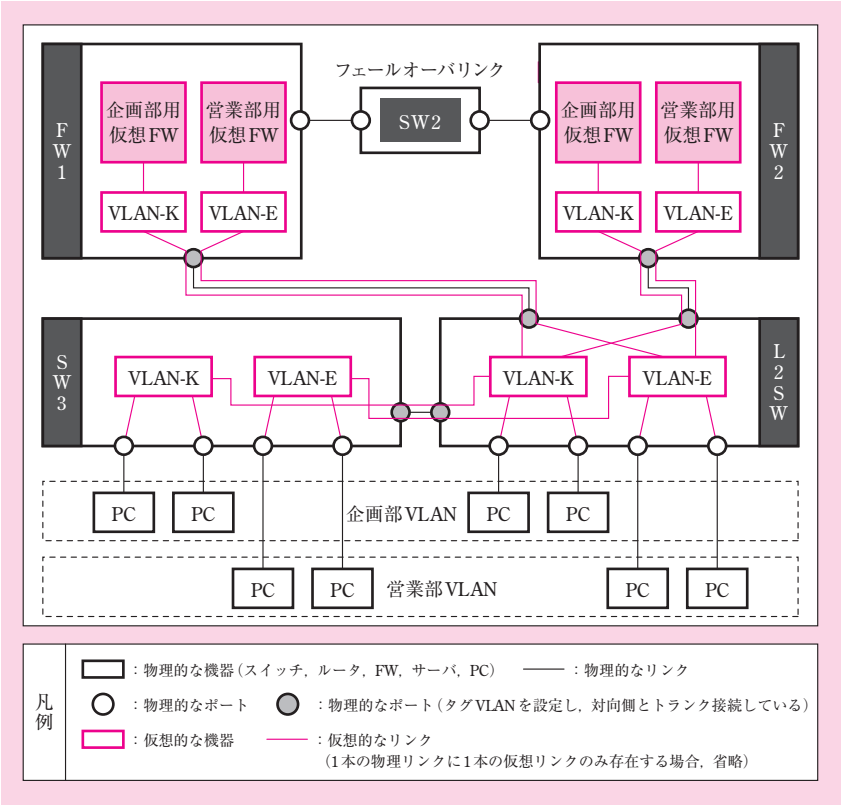
名前	セグメント
VLAN-K	企画部 VLAN
VLAN-E	営業部 VLAN
VLAN-FW	L3SW と FW 間のセグメント

L3SW に直接接続された VLAN 間の通信を廃止するには，L3SW をレイヤ 2 スイッチに置き換えるか，L3SW 内のルータを経由しないようにするか（事実上，L2SW として使用するか），L3SW の FW 機能を用いてパケットを破棄するか，などの対応が考えられる。この点について，第 2 段落に「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」とあるので，L3SW を既設のレイヤ 2 スイッチと入れ替える。

図 1 中のスイッチを見ると，L3SW 以外のスイッチ（SW1 ～ SW4）はすべてレイヤ 2 スイッチである。

入れ替えたレイヤ 2 スイッチの内部は，企画部 VLAN と営業部 VLAN の二つに分割される。この構成でレイヤ 2 スイッチが FW に接続される。前述のとおり，FW の社内側の物理ポートにタグ VLAN を設定し，企画部 VLAN と営業部 VLAN の二つを収容する。したがって，FW の対向側となるレイヤ 2 スイッチのポートにも同じタグ VLAN を設定する。それゆえ，レイヤ 2 スイッチと FW 間はトランク接続になる。このようにすれば，企画部 VLAN は企画部用の仮想 FW に，営業部 VLAN は営業部用の仮想 FW に，それぞれ接続できる。

具体的にどのレイヤ 2 スイッチと入れ替えるかは後述するが，ここまで考察した内容に基づき，レイヤ 2 スイッチに入れ替えた後のネットワーク構成は次の図のようになる。なお，図中の VLAN は，図「現在のネットワーク構成（企画部，営業部）」と同一である。



図：L3SW をレイヤ 2 スイッチに入れ替えた構成

・DMZ，FW の接続

DMZ のサーバは，社内の PC（企画部及び営業部の PC）と通信する。現在のネットワーク構成において，DMZ のサーバのルーティングテーブルはどのようになっているだろうか。DMZ のサーバは FW を経由して PC と通信するので，社内の PC があるサブネットワーク（企画部 VLAN 及び営業部 VLAN）を宛先とする経路のネクストホップは，FW の DMZ 側の IP アドレスである。

このルーティングテーブルを念頭に置きながら，第 3 段落にある「DNS サーバ及び Web サーバは現在のままと（する）」という条件に見合うように，新しいネットワーク構成を考察しよう。

このたび，企画部用の仮想 FW と営業部用の仮想 FW の 2 台が導入される。第 1 段落に「（仮想 FW の仮想ポートに，）それぞれに IP アドレス及び VLAN 番号を割

り当てる」とあるので，企画部用の仮想 FW，営業部用の仮想 FW の DMZ 側の仮想ポートには，それぞれ別々の IP アドレスが割り当てられる。

この構成で，DMZ のサーバのルーティングテーブルを現在のままにして，社内の PC と通信するにはどうすればよいだろうか。

ここでヒントになるのは，「2 台のスイッチを相互に入れ替えて対処する」という記述である。先ほど「企画部 VLAN，営業部 VLAN，FW の接続」で，L3SW をレイヤ 2 スイッチに入れ替えると解説したが，不要となった L3SW を活用できないだろうか。

そこで，DMZ のサーバと FW 間に L3SW を挟む構成を考えてみる。SW4 を L3SW に入れ替えるわけだ。この L3SW 内のルータの DMZ 側の IP アドレスは，現在の構成で FW の DMZ 側に割り当てている IP アドレスとする。このようにすれば，DMZ のサーバのルーティングテーブルを変更する必要がない。

とはいえ，L3SW のルーティングテーブルには，明示的に経路を登録する必要がある。それは，企画部 VLAN を宛先とする経路，営業部 VLAN を宛先とする経路である。企画部 VLAN を宛先とする経路のネクストホップは，企画部用の仮想 FW の DMZ 側の IP アドレスである。同様に，営業部 VLAN を宛先とする経路のネクストホップは，営業部用の仮想 FW の DMZ 側の IP アドレスである。

以上より，現在ある SW4 を L3SW と入れ替えなければならないことが分かる。本問はこの入替えを問うているので，ここまでの考察により解を導くことができた。

・ルータ，FW の接続

つい先ほど解を導いたばかりだが，せっかくなので，導入後のネットワーク構成について余すことなく考察しよう。

〔FW の構成と交換作業〕の第 2 段落に述べられているとおり，FW では NAPT 機能を動作させている。PC がインターネットにアクセスするとき，FW により，送信元 IP アドレスが FW のルータ側の IP アドレスに変換される。

現在のネットワーク構成において，ルータと FW は同一のサブネットワーク上にあり，ルータと FW 間の通信は，直接ルーティングとなる。つまり，ルーティングテーブルを参照しない。

このたび，企画部用の仮想 FW，営業部用の仮想 FW が導入され，それぞれに IP アドレスが割り当てられる。とはいえ，NAPT 機能によってアドレスが変換されることに変わりはなく，ルータと仮想 FW 間の通信も直接ルーティングのままだ。したがって，PC のインターネットアクセスに関しては，ルータのルーティングテーブルに変更は生じない。それゆえ，本問で問われている機器の入替えも必要ない。

DMZ のサーバは，グローバルアドレスが割り振られていると考えられる。それゆえ，ルータとサーバ間の通信は FW を経由することになる。

現在のネットワーク構成において，DMZ を宛先とする経路のネクストホップは，FW のルータ側の IP アドレスである。

仮想 FW を導入した後はどうなるだろうか。本文には明記されていないが，どちらかの仮想 FW を新たなネクストホップに指定することになる。当然，その仮想 FW には，DMZ とインターネット間の通信のフィルタリング設定が必要となる。

本文にはルータを変更してはならないとは明記されていないので，このルーティングテーブルの変更は許容されていると考えてよい。

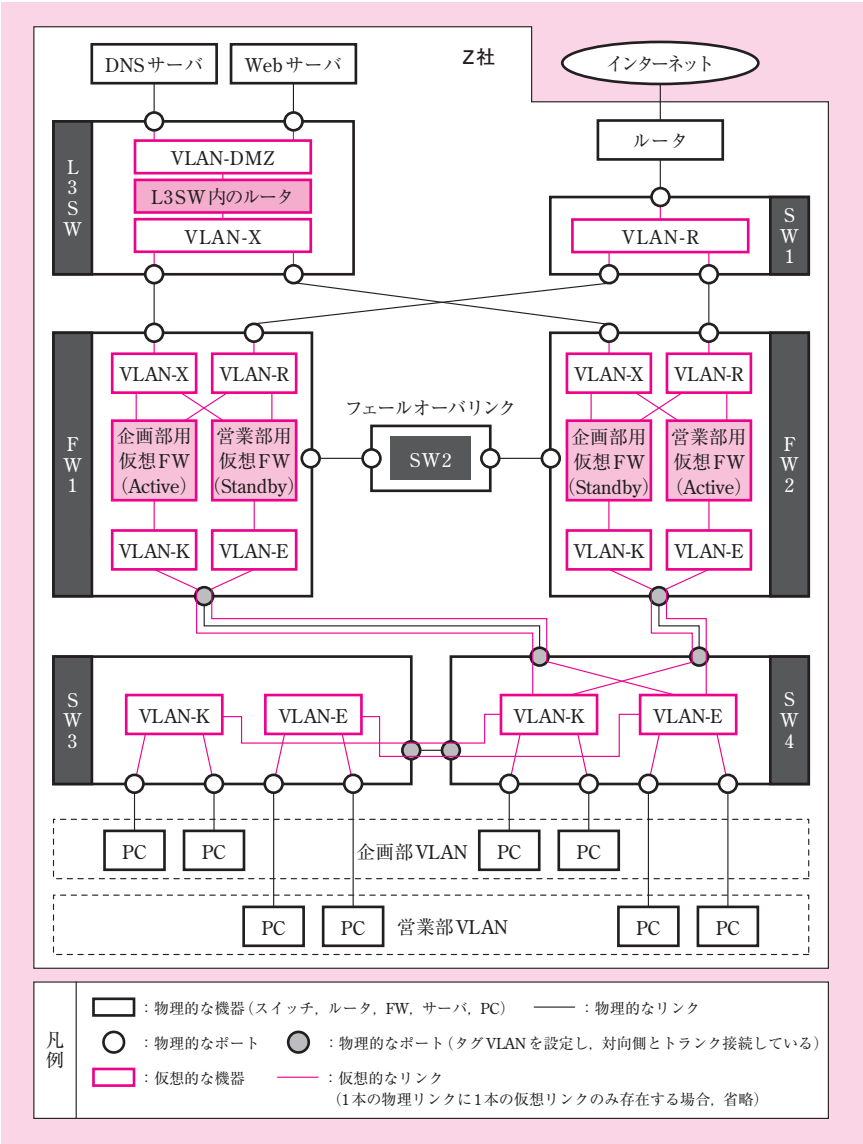
加えて，L2SW のルーティングテーブルには，DMZ とインターネット間の通信を行うためにデフォルトルートが設定されなければならない。デフォルトルートのネクストホップは，その仮想 FW となる。

●解の導出

本問は，下線④で言及している機器の入替えについて問うている。下線④は，〔仮想 FW 導入案の検討〕の第 2 段落にある。そこには，「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」と記述されている。

「DMZ，FW の接続」の最後でまとめたとおり，入れ替える機器は，SW4 と L3SW である。よって，これが正解となる。

参考までに，仮想 FW を導入した後のネットワーク構成を次の図に示す。なお，この図には，次の設問 3（2）の解（仮想 FW の配置）も記している。



図：仮想 FW 導入後のネットワーク構成

図中の VLAN は，次の表に示すセグメントを指している。

表：「仮想 FW 導入後のネットワーク構成」におけるセグメント

名前	セグメント
VLAN-K	企画部 VLAN
VLAN-E	営業部 VLAN
VLAN- DMZ	DMZ
VLAN-X	入替え後の L3SW と FW 間のセグメント
VLAN-R	ルータと FW 間のセグメント

(2)

解答例

- FW1で企画部用の仮想FWを，FW2で営業部用の仮想FWを，それぞれActiveにする。（44字）
- FW2で企画部用の仮想FWを，FW1で営業部用の仮想FWを，それぞれActiveにする。（44字）

本問は，下線⑤で言及している仮想 FW の配置について問うている。下線⑤は，〔仮想 FW 導入案の検討〕の第 3 段落にある。そこには，「Active-Active 冗長構成にした物理 FW（FW1 及び FW2）に，⑤ Active 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」と記述されている。

冗長構成について「Active-Active」と記述されているので，FW1 と FW2 が同時に Active 動作をするように，仮想 FW を配置していることが分かる。つまり，FW1 にも FW2 にも Active 動作をする仮想 FW が稼働しているわけだ。

具体的に言うと，例えば，FW1 で企画部用の仮想 FW を Active にし，FW2 で営業部用の仮想 FW を Active にすればよい。このとき，FW1 で営業部用の仮想 FW は Standby になり，FW2 で企画部用の仮想 FW は Standby になるので，仮想 FW 間の冗長化も実現できる。

このように配置するならば，企画部の通信は一方の物理 FW を経由し，営業部の通信は他方の物理 FW を経由することになるため，物理 FW 間の負荷も分散される。

よって，正解は，「**FW1 で企画部用の仮想 FW を，FW2 で営業部用の仮想 FW を，それぞれ Active にする**」となる。当然ながら，Active にする FW1 と FW2 を交互に入れ替えてもよく，そのように置換した文章も正解である。

問 3

出題趣旨

DDoS 攻撃を始めとするサイバー攻撃は年々増加し，ネットワークのセキュリティの重要性が増している。ネットワークの様々な機器やサービスにおいてセキュリティ対策が必要であるが，ネットワークの基本機能の一つである DNS は，未だに適切な対策が施されていないサーバも多く，サイバー攻撃の踏み台となっている場合がある。対策には，平常時の状況を把握し，異常なアクセスを早期に発見して対処することが必要だが，そのためにはインシデントの発生状況に注意を払い，事前に定めた手順に従って適切に対応することが重要である。

本問では，ネットワークのセキュリティ対策を題材に，DNS のセキュリティ対策とインシデント管理について，基本的な知識と理解力を問う。

採点講評

問 3 では，ネットワークのセキュリティ対策を題材に，DNS に関わる基本的な知識と，重要なインシデントが発生した場合のネットワークの運用対処について出題した。いずれも基礎的な知識を問うたものであり，全体として正答率は高かった。

設問 1 は，基本的な用語と知識に関する問題だが，DNS に関わる用語は正答率が低かった。正確に理解してほしい。

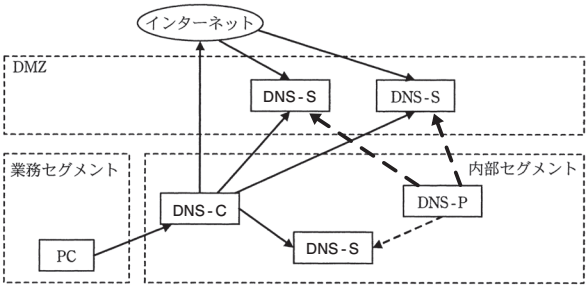
設問 2（1），（2），設問 3（1）は，DNS やファイアウォールのセキュリティ対策に関する問題であり，比較的高い正答率であった。受験者の関心も高く，よく学習されていると思われる。

設問 3（2）は，DNS サーバの配置と DNS 問合せやゾーン転送を，本文に記載した条件に従って図示する問題であるが，本文の条件をよく読まず，自身の経験や一般的な知識だけで解答しているものが非常に多かった。また，DNS 問合せやゾーン転送は，DNS の基本的な機能であるが，正しく理解されていない解答が散見された。DNS はネットワークの基礎的な要素であり，用語を覚えるだけでなく仕組みを理解して，構築方法などについてもきちんと理解しておいてほしい。

設問 4 は，インシデント発生時の運用手順について問うたものであるが，ネットワーク技術者としてシステムの運用を理解しておくことが大切である。特に PDCA サイクルに従った改善手法については，実務に応用できるように身に付けておくことが重要である。

設問		解答例・解答の要点		備考
設問 1		ア	分散	
		イ	フラッド	
		ウ	再帰	
		エ	リフレクタ	
		オ	ペネトレーション	
設問 2	(1)	a	踏み台	
	(2)		断片化されたエコーパケットを許可しない機能	

（表は次ページに続く）

設問		解答例・解答の要点	備考
設問 3	(1)	DNS キャッシュが改ざんされる。	
	(2)		
	(3)	① 内部から外部への通信に対する遮断ルールを設定する。 ② FW で遮断した通信の結果ログを監視する。	
設問 4	(1)	b ネットワークの切断	
	(2)	対処結果の評価を行い，インシデントの対処方法を見直す。	

■設問 1

解答例

ア：分散
イ：フラッド
ウ：再帰
エ：リフレクタ
オ：ペネトレーション

ア

空欄アを含む文章は，〔サーバ攻撃対策〕の第 1 段落，F 氏の 1 番目の発言の中にある。そこには「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」と記述されている。

DoS 攻撃の中で，多数のコンピュータが標的サーバを集中的に攻撃するものは，分散型 DoS（Distributed DoS）攻撃である。よって，空欄アに該当する字句は，「**分散**」である。

イ

空欄イを含む文章は，空欄アと同様，F 氏の 1 番目の発言の中にある。そこには，「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」と記述されている。

結論から言うと，空欄イに該当する字句は，「**フラッド**」である。

ここでは，SYN フラッド攻撃と UDP フラッド攻撃について述べられている。

両者の名称に含まれる「フラッド」（flood）とは，「洪水」を意味している。両者とも，「洪水のごとく一度に大量のパケットがやってくる」という特徴を有しているからだ。そして，まさにこの特徴が DoS 攻撃の本質であると言えよう。短時間で大量にやってくるパケットがネットワークやサーバの処理能力を占有することにより，正常なサービスが妨害されるからである。

攻撃の種類によって，処理能力が占有される要因は異なっている。そこで，SYN フラッド攻撃，UDP フラッド攻撃を一つずつ解説しよう。「フラッド」という特徴を念頭に置きながら，具体的にどのようにサービス妨害をもたらすのかを理解していただきたい。

● SYN フラッド攻撃

TCP のコネクション確立フェーズは，スリーウェイハンドシェークと呼ばれる，3 個のパケットのやり取りからなる。パケットの送信元とヘッダ中のビットに着目すると，その内訳は次のとおりである。TCP のコネクション確立について，詳しくは本書の第 3 章「3.3.4　TCP コネクション」を参照されたい。

表：TCP コネクション確立フェーズでやり取りされるパケットの送信元とヘッダ中のビット

順序	送信元	ビット
1	クライアント（コネクションの要求元）	SYN ビット
2	サーバ（コネクションの要求先）	SYN ビット，ACK ビット
3	クライアント（コネクションの要求元）	ACK ビット

1 番目のパケットは，TCP のコネクション確立を要求するものである。これを SYN パケットと呼ぶ。SYN パケットを受信したホストは，要求元に 2 番目のパケットを返信すると共に，コネクションのためにリソースを確保する。そして，要求元から 3 番目のパケットが送られるのを待っている。この，3 番目のパケットを待っている状態を，ハーフオープンと呼ぶ。

SYN フラッド攻撃は，SYN パケット受信時のホストの振舞いを悪用した，DoS 攻撃である。

攻撃者は，標的サーバに SYN パケットを送信する際，送信元 IP アドレスを詐称する。そして，攻撃者は，この詐称した SYN パケットを短時間に大量に送信するのである。

標的サーバは，これを受信すると，詐称された送信元に返信する。2 番目のパケットを受け取った相手は，そもそもコネクション確立を要求していないので，3 番目のパケットを送ることはない。あるいは，詐称した IP アドレスはそもそもホストが存在していないことも多く，そのときは，3 番目のパケットが来ることはない。この結果，標的サーバはハーフオープン状態のままになり，リソースを無駄に消費させられてしまう。更に，F 氏の 1 番目の発言にあるとおり，新たな接続も妨害されてしまう。

このような SYN フラッド攻撃の仕組みにより，サーバの処理能力を占有され，正常なサービスを提供できなくなってしまうのである。

● UDP フラッド攻撃

ホストは UDP パケットを受信すると，通常は次の順序に従って動作する。これを基本フローと呼ぶことにしよう。

〔基本フロー〕

（1）OS は，宛先ポート番号に対応するアプリケーションが自ホストで動いているかを調べる

（2）アプリケーションが動いている場合，OS は UDP パケットのペイロード部分を取り出し，これをアプリケーションに渡す

（3）アプリケーションは，ペイロードの内容を処理する

〔基本フロー〕の順序（1）で，もしもアプリケーションが動いていなかった場合，次の順序に従って動作する。これを代替フローと呼ぶことにしよう。順序（1）は基本フローと同じである。

〔代替フロー：アプリケーションが動いていない場合〕

（1）OS は，宛先ポート番号に対応するアプリケーションが自ホストで動いているかを調べる

（2a）アプリケーションが動いていない場合，OS は，ICMP の Destination Unreachable メッセージ（Port Unreachable コード）を送信元ホストに返信する

UDP フラッド攻撃は，この代替フローの振舞いを悪用した，DoS 攻撃である。

攻撃者は，標的サーバに UDP パケットを送信する際，宛先ポート番号として，対応するアプリケーションが到底存在しないようなポート番号を指定する。加えて，送信元 IP アドレスを詐称する。そして，攻撃者は，この詐称した UDP パケットを短時間に大量に送信するのである。

標的サーバは，これを受信すると，ICMP パケットを詐称された送信元に返信する。この結果，ネットワークの帯域は，攻撃用の UDP パケットとその返信用の ICMP パケットを伝送する分だけ無駄に消費させられる。更に，標的サーバの CPU 時間も，代替フローを処理する分だけ無駄に消費させられる。一方，送信元は詐称されているため，攻撃者は ICMP パケットを受信することはなく，その分のリソース消費は免れている。

このような UDP フラッド攻撃の仕組みにより，ネットワークやサーバの処理能力が占用され，正常なサービスを提供できなくなってしまうのである。

ウ

空欄ウを含む文章は，「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」と記述されている。

DNS サーバの問合せには，再帰的問合せと反復的問合せの 2 種類がある。

PC などのクライアントから問合せを受けた DNS サーバは，最終的な答えを得られるまで他の DNS サーバに問合せを行い，最終的な結果をクライアントに返信する。このクライアントが行う問合せを再帰的問合せという。

再帰的問合せの要求を受け付けた DNS サーバは，他の DNS サーバに対して問合せを行う。この DNS サーバが行う問合せを反復的問合せという。

よって，空欄ウに該当する字句は，「**再帰**」である。

DNS の再帰的問合せと反復的問合せについて，詳しくは本書の第 4 章「4.2.2　名前解決の仕組み」を参照されたい。

エ

空欄エを含む文章は，「再帰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」と記述されている。

結論から言うと，空欄エに該当する字句は，「**リフレクタ**」である。

DNS の問合せは，トランスポート層プロトコルとして，コネクションレス型である

UDP を使用する(*)。DNS リフレクタ攻撃は，送信元の詐称が容易であるというコネクションレス型通信の脆弱性を悪用した DoS 攻撃である。まずはその脆弱性を解説し，次いで，DNS リフレクタ攻撃について解説しよう。

（*）DNS は，問合せ及び応答メッセージのサイズが 512 バイト以下であるとき，UDP を使用する。メッセージのサイズが 512 バイトを超えるとき，TCP を使用するか，又は，EDNS0 で標準化された手続きに則って UDP を使用するか，いずれかの方法を採る。

●送信元の詐称が容易であるというコネクションレス型通信の脆弱性

コネクション型である TCP は，送信元を詐称して通信することができない。そのことが分かれば，コネクションレス型である UDP が，送信元を詐称できるという脆弱性をもっていることを理解できる。

UDP の脆弱性を理解しやすくするため，TCP では送信元を詐称できない理由について，まずは説明する。

コネクション型の TCP では，アプリケーション層プロトコルの通信に先立って TCP のコネクションを確立する。このとき，もしも送信元 IP アドレスが詐称されていたら，コネクション確立フェーズのやり取りに失敗するので，データ通信フェーズに遷移しない。コネクション確立フェーズに成功したら，そのフェーズで交換したシーケンス番号に従ってデータ通信フェーズのやり取りが順番どおりに行われるため，悪意のある第三者がコネクションをハイジャックすることは至難の業となる。それゆえ，ひとたびコネクションを確立すれば，パケットの送信元 IP アドレスは，そのパケットを本当に送信したホストのものであることが保証される。

これに対し，コネクションレス型の UDP では，コネクションを確立せず，最初のパケットからアプリケーション層プロトコルのやり取りが始まる。それゆえ，パケットの送信元 IP アドレスが，パケットを本当に送信したホストのものであるのか，あるいは詐称されたものであるのかを（少なくとも，トランスポート層以下のヘッダ情報だけでは），見分けることができない。

したがって，トランスポート層プロトコルに UDP を使用するアプリケーションは，送信元 IP アドレスの詐称が容易であるという脆弱性をもっている。

● DNS リフレクタ攻撃

DNS リフレクタ攻撃は，送信元の詐称が容易であるというコネクションレス型通信の脆弱性を悪用している。

DNS の問合せパケットを送信する際，送信元 IP アドレスを詐称したらどうなるだ

ろうか。問合せを受けた DNS サーバは，問合せパケットの送信元 IP アドレスを通信相手であると判断するので，その相手に対し，応答パケットを返信してしまう。

攻撃者は，DNS の問合せパケットの送信元 IP アドレスとして，標的となるサーバの IP アドレスを格納する。そして，この問合せを，オープンリゾルバと呼ばれる DNS サーバに送信する。オープンリゾルバとは，インターネット上に存在し，どの端末からも再帰的問合せを受け付ける DNS サーバのことである。

攻撃者から問合せを受けたオープンリゾルバは，当然ながら，これに対する応答を標的サーバに返信する。攻撃者は，この問合せを大量に送り付けることによって，標的サーバへの DoS 攻撃を仕掛けることを企図している。

DNS リフレクタ攻撃では，攻撃側といえども，問合せパケットを送信する以上，ネットワークとサーバのリソースを消費する。とはいえ，DNS の応答パケットのサイズは，問合せパケットのサイズより大きくなる。攻撃する際は，応答のサイズが何倍にも，何十倍にも増大するように，問い合わせる内容を巧妙に指定する。攻撃側よりも標的側の方がリソース消費のダメージがはるかに大きくなるので，DNS リフレクタ攻撃は DoS 攻撃になるのだ。

より巧妙な攻撃として，攻撃者はリフレクタ攻撃を直接実行せず，インターネット上に用意した大量のボットに指示を与えて，ボットがリフレクタ攻撃を行う方法がある。個々のボットのリソース消費を小さく抑えつつ，これを一斉に大量に行うことで，標的サーバへの分散型 DoS 攻撃を仕掛けるのである。

参考までに，「DNS リフレクタ攻撃」のことを「DNS Amplification 攻撃」（略して，「DNS Amp 攻撃」）という文献もある。これは，応答のサイズが問合せに比べて何十倍にも増幅されるという特徴に由来する呼び名である。ただし，RFC5358 では「DNS リフレクタ攻撃」と呼んでいるので，試験センターの解答例はこちらに合わせたのであろう。

オ

空欄オを含む文章は，「実際に脆弱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」と記述されている。

脆弱性があるかどうかを調査する目的で，擬似的に攻撃を仕掛ける検査のことを，ペネトレーションテストという。よって，空欄オに該当する字句は，「**ペネトレーション**」である。

■設問 2

(1)

解答例

a：踏み台

本問は，空欄 a に入れる適切な字句を問うている。

空欄 a は，〔サーバ攻撃対策〕の第 1 段落，F 氏の 2 番目の発言の中にある。その文脈は，オープンリゾルバを用いた DNS リフレクタ攻撃について説明しており，「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」と記述されている。

設問 1 の空欄エで解説したとおり，攻撃者は，DNS の問合せパケットの送信元 IP アドレスとして，標的となるサーバの IP アドレスを格納する。そして，この問合せを，オープンリゾルバに送信する。標的サーバから見ると，DNS の応答パケット，すなわち，DoS 攻撃の被害をもたらす攻撃パケットが，オープンリゾルバから送信される。したがって，オープンリゾルバは，悪意はなくとも，攻撃の踏み台になっているわけだ。

よって，空欄 a に該当する字句は，「**踏み台**」である。

(2)

解答例

断片化されたエコーパケットを許可しない機能（21 字）

問題文は，「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」と記述されている。

問題文にわざわざ「大量のパケット」「大きなサイズ」「ICMP エコー応答」と書かれているので，この方向付けに沿って解を導く必要がある（付録 PDF「午後問題の解答テクニック」の「0.3.6　問題を解く②：応用テクニック」の「5. 条件を読み落としたり，自分勝手に条件を加えたりしない」を参照されたい）。

本問は，「この攻撃を防御するために，図 1 中の FW がもつべき機能」を問うている。本問を解くには，「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」に関する一般的な知識が必要である。そこで，まずはその点について解説する。それを踏まえて，解を導こう。

●大きなサイズの ICMP エコー応答を使った，大量のパケットを送信する攻撃

問題文には，「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」と記述されている。

IP は，パケットサイズが MTU（Max Transmission Unit：最大転送単位）を超えると，MTU に収まるようにパケットを分割して伝送する仕組みになっている。これをフラグメンテーションという。したがって，MTU をはるかに超える大きなサイズを指定することによって，大量のフラグメントパケットが送信されるので大量のパケットを送信することができる。フラグメンテーションについて，詳しくは本書の第 3 章「3.2.2　IP ヘッダ」を参照されたい。

分割されたパケットを再構築する処理（以下，デフラグメント処理という）を行うのは，宛先ホストである。フラグメントは元の順番どおりに到着するとは限らないので，デフラグメント処理が完了するまで，フラグメントをバッファに保持しておかなければならない。それゆえ，デフラグメント処理は宛先ホストに一定の負荷をかけることが分かる。したがって，大量のフラグメントパケットを送信することは，宛先ホストに対する DoS 攻撃となる。

更に，問題文には「ICMP エコー応答」とあるが，これにはどのような意味があるのだろうか。ICMP は IP の上位層プロトコルであるが，IP はコネクションレス型の通信を行うので，「送信元の詐称が容易である」という脆弱性を有している。これを悪用し，攻撃者は次のように攻撃を仕掛ける。

攻撃者は，ICMP エコー要求パケットの送信元 IP アドレスとして，標的となるサーバの IP アドレスを格納する。そして，このエコー要求を，ICMP エコー要求を受け付けるホストに送信する。このホストは踏み台である。この結果，踏み台から ICMP エコー応答が送信される。

ここで，問題文にある「大きなサイズの ICMP エコー応答」という記述を思い起こそう。ICMP エコー要求のメッセージに大きなサイズのデータを格納すると，ICMP エコー応答のメッセージにもそれと同じデータが格納される。そこで，攻撃者は，標的サーバが大量のフラグメントパケットを受信するように，大きなサイズのデータを格納した ICMP エコー要求を送信する。こうして，標的サーバに DoS 攻撃を仕掛けるのである。

●解の導出

本問は「図 1 中の FW がもつべき機能」を問うているが，FW のもつ基本的な機能は，パケットフィルタリングによるアクセス制御である。そこで，大きなサイズの ICMP エコー応答を使った DoS 攻撃を FW で防御する方法は，分割された ICMP エコー応答パケットを通過させないことである。

よって，正解は解答例に示したとおりとなる。

このように，解を導くときは，問題文にある「大量のパケット」「大きなサイズ」「ICMP エコー応答」という記述を読み落とさないようにしなければならない。ただ単に「ICMP エコーパケットを許可しない」と述べただけでは不十分である。

■設問 3

(1)

解答例

D	N	S	キ	ャ	ッ	シ	ュ	が	改	ざ	ん	さ	れ	る	。

（16字）

問題文は，「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」と記述されている。

下線①は，〔DNS のセキュリティ対策〕の第 1 段落の 2 番目の箇条書きにある。そこには，「① DMZ 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」と記述されている。

したがって，本問は，図 2 の DNS サーバにおいて，DMZ の DNS サーバのキャッシュ機能を無効にしなかった場合の脆弱性を問うている。本問を解くには，DNS のキャッシュサーバに関する一般的な知識が必要である。そこで，まずはその点について解説する。それを踏まえて，解を導こう。

●DNS のキャッシュサーバ

DNS サーバの役割には，再帰的要求を受け付ける役割を担うキャッシュサーバと，反復的問合せを受け付ける役割を担うコンテンツサーバの二つがある。キャッシュサーバは，キャッシュ機能を有効にすること（再帰的要求の受付を許可すること）で，その役割を果たすようになる。

キャッシュサーバは，フルサービスリゾルバサーバとも呼ばれ，クライアントから

の名前解決の再帰的要求を受け付けると，コンテンツサーバに反復的問合せを実行し，そこで得られた結果をクライアントに応答する。

キャッシュサーバは，名前解決の過程で得られた情報をすぐに破棄せずに，キャッシュとして一定期間保存する。それぞれの情報にはキャッシュの有効期間が付与された状態で返答され，キャッシュが有効である間は，コンテンツサーバに対する反復的問合せを省略する。これにより，名前解決にかかる時間の高速化を図っている。

●解の導出

インターネット上に公開しているキャッシュサーバは，キャッシュが汚染されるという脆弱性をもっている。

キャッシュ汚染について簡単に解説すると，これは「改ざんされた名前解決情報をキャッシュさせられる」というものである。改ざんされている点を具体的に言うと，ホスト名に対応付ける IP アドレスを，本物の IP アドレスではなく，攻撃者が用意したサーバの IP アドレスにすることである。キャッシュサーバのキャッシュが汚染されると，この名前解決を問い合わせたとき，汚染されたキャッシュが応答される。この結果，クライアントは，当該ホストにアクセスしているつもりで，実際には攻撃者のホストにアクセスさせられることになる。

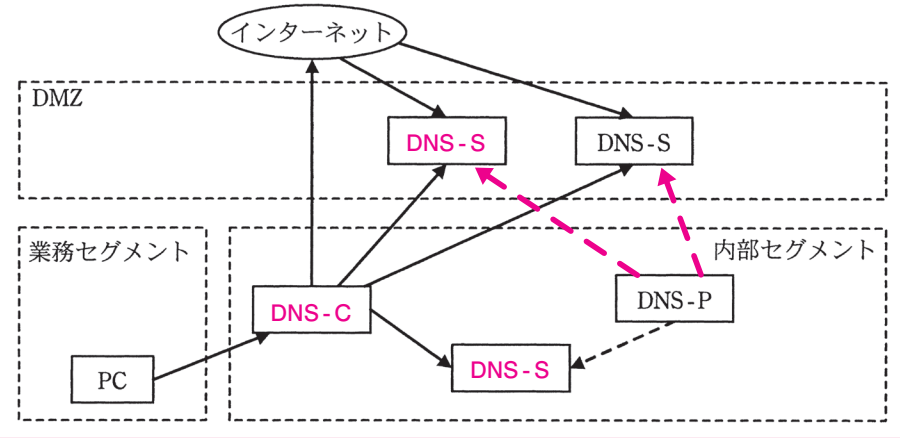
キャッシュの汚染は外部からの攻撃によってもたらされる。詳しくは本書の第 4 章「4.2.7　DNS キャッシュ汚染」で解説しているので，そちらを参照されたい。具体的な攻撃方法については割愛する。

下線①は「DMZ の DNS サーバ」に言及している。下線①に続く記述には，DMZ 上の Web サーバにグローバル IP アドレスが割り当てられているとあるので，同じ DMZ にある DNS サーバも公開されたサーバであり，悪意ある第三者がアクセスできることが分かる。したがって，DMZ の DNS サーバがキャッシュサーバとしての役割を担ってしまうなら，キャッシュが汚染される可能性がある。

よって，正解は，「**DNS キャッシュが改ざんされる**」となる。

(2)

解答例



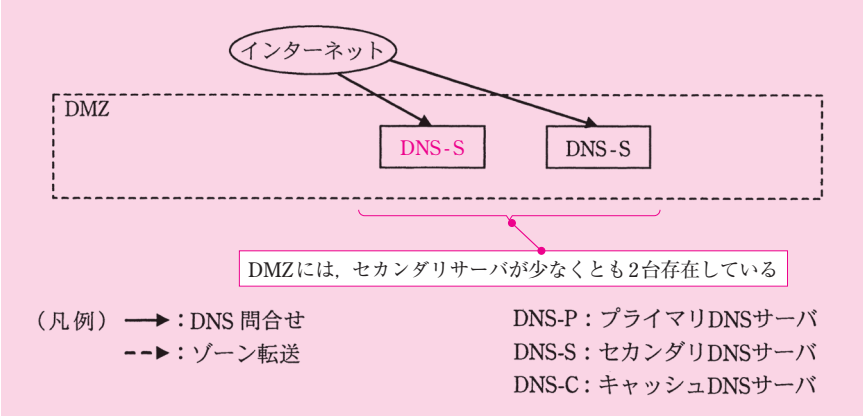
本問は図 2 中の空欄に該当する DNS サーバを埋め，図 2 を完成させることを求めている。

〔DNS のセキュリティ対策〕の第 2 段落は，図 2 の DNS のセキュリティ対策方針を箇条書きで列挙しており，全部で 6 項目ある。これらの条件を踏まえて，一つずつ解を導こう。

● DMZ に設置された DNS サーバ

2 番目の箇条書きは，「DMZ 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」と記述されている。したがって，DMZ の DNS サーバは，セカンダリサーバであり，かつ，冗長構成をとっている。つまり，DMZ には，セカンダリサーバが少なくとも 2 台存在していることが分かる。また，「キャッシュ機能を無効にした」とあるので，DMZ にはキャッシュサーバは存在していないことも分かる。

図 2 を見ると，DMZ には 2 台の DNS サーバが配置されている。そのうちの 1 台は「DNS-S」（セカンダリサーバ）と記されている。したがって，もう 1 台もセカンダリ DNS サーバであるはずだ。よって，次の図に示すとおり，空欄には「DNS-S」（セカンダリ DNS サーバ）が該当する。



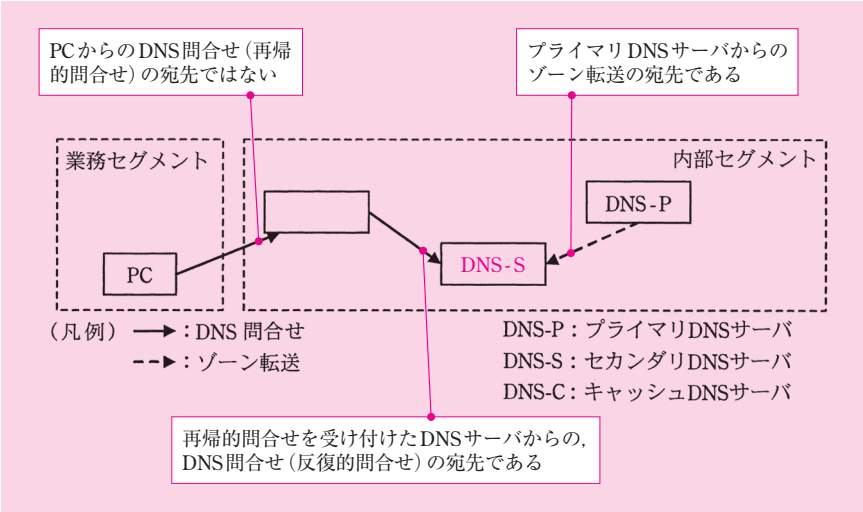
図：DMZ に設置されたセカンダリ DNS サーバ

●内部セグメントに設置された DNS サーバ

4 番目の箇条書きは，「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」と記述されている。したがって，内部セグメントのプライマリ DNS サーバのゾーン転送の宛先は，セカンダリサーバである。

5 番目の箇条書きは，「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」と記述され，3 番目の箇条書きは，「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」と記述されている。したがって，セカンダリ DNS サーバは内部セグメントのコンテンツサーバとして振る舞うが，キャッシュサーバとしては振る舞わないことが分かる。それゆえ，キャッシュサーバから反復的問合せを受け付けるが，PC から再帰的問合せを受け付けないことが分かる。

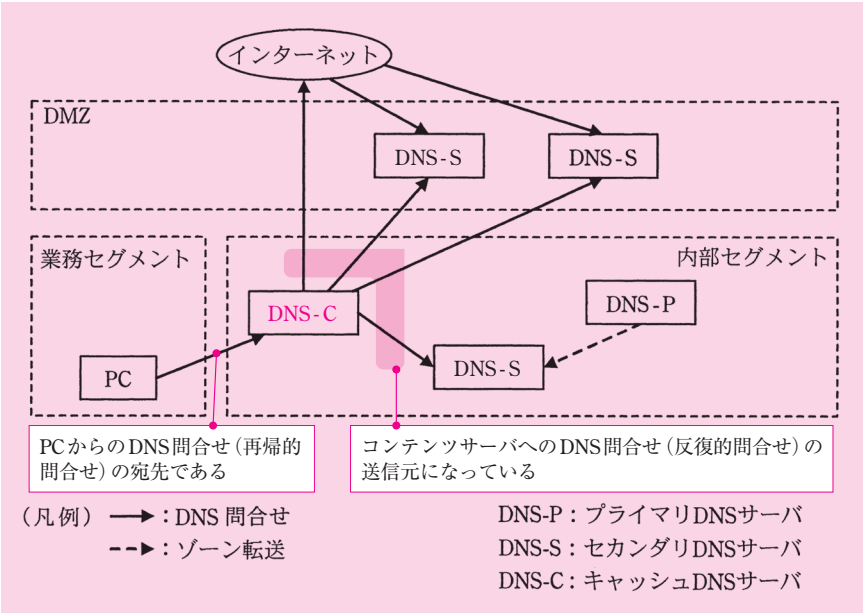
図 2 を見ると，プライマリ DNS サーバからのゾーン転送の宛先であり，かつ，再帰的問合せを受け付けた DNS サーバからの，DNS 問合せの宛先にもなっているサーバが存在する。これがセカンダリ DNS サーバである。よって，次の図に示すとおり，空欄には「**DNS-S**」（セカンダリ DNS サーバ）が該当する。



図：内部セグメントに設置されたセカンダリ DNS サーバ

3 番目の箇条書きは，「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」と記述されている。したがって，業務セグメントにある PC からの再帰的問合せの宛先は，キャッシュサーバだけであることが分かる。更に，キャッシュサーバである以上，コンテンツサーバ宛てに反復的問合せを送信していることも分かる。

前述のセカンダリ DNS サーバを埋めた状態で図 2 を見ると，PC からの DNS 問合せ（再帰的問合せ）の宛先におり，インターネット上のコンテンツサーバと自ネットワーク内のコンテンツサーバ（セカンダリ DNS サーバ）の DNS 問合せ（反復的問合せ）の送信元になっているサーバが存在する。これがキャッシュサーバである。よって，次の図に示すとおり，空欄には「**DNS-C**」（キャッシュサーバ）が該当する。



図：内部セグメントに設置されたキャッシュサーバ

(3)

解答例

①内部から外部への通信に対する遮断ルールを設定する。（25字）
②FWで遮断した通信の結果ログを監視する。（20字）

問題文は，「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（よ）」と記述されている。

下線②は，〔DNS のセキュリティ対策〕の第 3 段落，F 氏の 1 番目の発言の中にある。そこには，「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」とある。問題文はこれを引用した上で，不正な通信の発見，防止を一つずつ解答することを求めている。

これは一般的な知識から解を導く。

FW がもつ機能には，

- 決められた通信だけを許可し，それ以外の通信を遮断する機能
- 通信のログを採取し，これを監視する機能

などがある。

このうち，防止に役立つのは一つ目の機能であり，発見に役立つのは二つ目の機能である。これらの機能を，問題文に合わせて「内部から外部への通信」に適用し，解を導けばよい。

すなわち，内部から外部への不正な通信を FW で防止するには，内部から外部への通信に対する遮断ルールを設定すればよい。よって，これが一つ目の解となる。

不正な通信を FW で発見するには，FW で遮断した通信のログを監視すればよい。よって，これが二つ目の解となる。

■設問 4

(1)

解答例

b：ネットワークの切断　(9字)

問題文は，図 3 中の空欄 b を埋めることを求めている。問題文には，空欄 b が「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」と記述されているので，これを手掛かりにして解を導こう。

図 3 には，その表題どおり，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が記されている。空欄 b は，その 3 番目の作業である。

〔インシデント管理〕の第 1 段落には，「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」と記述されている。この記述と図 3 の＜セキュリティ担当者の対応＞を照らし合わせてみると，1 番目の作業は「状況把握と記録」とあり，2 番目の作業は「対処方法の確認」とあるので，3 番目の作業とは，「インシデントの状況を把握し記録した後」に実施すべき，「必要な対処」であることが分かる。2 番目の作業は，3 番目に行う作業の内容を事前に確認するためのものである。

4 番目の作業は「原因の特定と対処」とある。通常，原因の特定には時間がかかる。図 3 は「重大なインシデントが発生している」という状況下での作業手順であることを考えるなら，3 番目の作業は原因の特定よりも緊急度の高いものであり，迅速に行

うべき作業であると推論できる。

第 3 段落には，図 3 の対応手順に則っているゆえに，「インシデント発生時に迅速に対応（している）」と記述されている。それゆえ，図 3 には「迅速な対応」が盛り込まれていることが分かる。この記述は，「3 番目の作業は迅速に行うべきものである」との推論を裏付けるものだ。

ここまで考察した内容を整理すると，3 番目の作業は次のようなものである。

- サイバー攻撃に関わる重大なインシデントが発生しており，原因はまだ特定されていないが，インシデントの状況は把握できている
- 発生したインシデントの状況を把握し記録した後，迅速に実施すべきものである
- 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

これらを総合的に考え合わせると，このときに行う作業は，「ネットワークから切断すること」であると言える。

なぜなら，DoS 攻撃などの重大なインシデントが発生していることが明らかになっているわけだから，これ以上の攻撃を受けないよう迅速に対応しなければならない。その有効な手段は，標的となっているサーバをネットワークから切断することである。こうすれば，少なくとも，攻撃を止めることができるからだ。これは，原因の特定よりも優先して行うべきことであるのは言うまでもない。

更に，ネットワークから切断することは，セキュリティ担当者が実施すべきものであり，まさしくネットワークに係るものであるから，問題文中の手掛かりとも合致している。

よって，正解は，「**ネットワークの切断**」となる。

(2)

解答例

対	処	結	果	の	評	価	を	行	い	,		イ	ン	シ	デ	ン	ト	の	対	処	方	法	を	見	直	す	。

（27字）

問題文は，「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」を問うている。

これは一般的な知識から解を導く。

インシデントに対処した後に行えることは,

- インシデント対処の評価及び改善
- 再発防止策の検討及び実施

などである。

問題文は「将来発生するインシデントへの対応」とあるので，同じようなインシデントが将来発生した場合を想定した解を求めている。そこで,「インシデント対処の評価及び改善」を解答するとよい。よって，正解は解答例に示したとおりとなる。