平成 29 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

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。

採点講評

問 1 では，企業における SSL-VPN を活用したリモートアクセス VPN 環境構築を題材に，SSL-VPN の基本機能を利用したセキュアなネットワーク構築について出題した。全体として，正答率は低かった。

設問 1 は，SSL-VPN の動作とプロトコルの基本について出題したが，正答率は低かった。特に，TLS の安全性を考慮したプロトコル選定やバージョン選定については，ネットワーク技術者として必須の項目なので，是非知っておいてほしい。

設問 2(1)は，暗号スイート中のアルゴリズム項目の用途を出題したが，正答率は低かった。これは SSL/TLS に関する基本事項なので，正しく把握してほしい。

設問 2(2)は，SSL-VPN の動作方式選定についてその選定根拠を求めたが，正答率は低かった。SSL-VPN の動作方式について理解した上で問題文全体を読み取り，正答を導き出してほしい。

設問 3 は，社内ネットワークに SSL-VPN を導入しようとする場合の FW ルール設定について出題したが，正答率は高かった。

設問 4 は，特定のセキュリティ要件実現のために L3SW に設定すべきアクセスリストについて出題したが，正答率は高かった。ただし，L3SW に隣接する FW 設定内容の考慮に欠けると思われる誤った解答も散見された。

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			

(表は次ページに続く)

設問		解答例・解答の要点		備考
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		

本問は，SSL-VPN を用いたリモートアクセスネットワークを構築する事例を取り上げている。

本問は，TLS 及び SSL-VPN の様々な技術的要素を出題している。これらについて，詳しくは本書の第 8 章「8.4.6　SSL，TLS」を参照していただきたい。特に，本問で中心的な役割を果たしている SSL-VPN の L2 フォワーディング方式の仕組みについて，同節の「● SSL-VPN の仕組み」及び「● L2 フォワーディング方式」を参照していただきたい。

●本問の全体像

・現行ネットワークの特徴

事例に登場する H 社は，顧客の業務システムを構築するシステム開発会社である。開発期間中，顧客システムは H 社の拠点の内部 LAN に構築される。最終的に顧客の拠点に納入されたシステムは，顧客社内の PC などから利用される。

H 社では，受注した顧客システムごとに構築専用のネットワーク（以下，顧客システム構築ネットワークという）をそれぞれ設ける。

現行の顧客システム構築ネットワークの主な特徴は，次のとおりである。

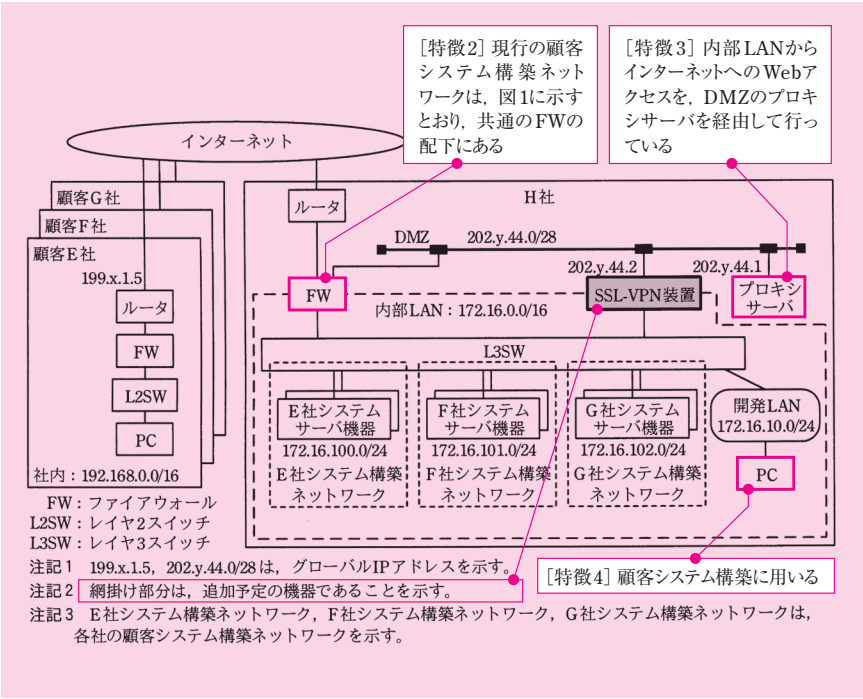
［特徴 1］顧客システムは，様々なサーバ機器，OS，ミドルウェアなどを組み合わせて構築され，利用されるプロトコルも様々である（序文の第 1 段落）。

［特徴 2］現行の顧客システム構築ネットワークは，図 1 に示すとおり，共通の FW の配下にある。なお，図 1 中の網掛けで示された SSL-VPN 装置は，これから追加する予定の機器である。

［特徴 3］内部 LAN からインターネットへの Web アクセスを，DMZ のプロキシ

サーバを経由して行っている（〔H 社の現行ネットワーク〕の第 1 段落）。

［特徴 4］顧客システムを構築する際，開発 LAN に接続された PC から顧客システム構築ネットワークにアクセスして行っている（〔H 社の現行ネットワーク〕の第 1 段落）。



図：H 社の現行ネットワーク構成（図 1 の抜粋）

・現行ネットワークが抱える問題点

H 社では，顧客システム構築業務において，二つの問題を抱えている。

〔顧客システム構築業務の問題とその解決策〕の第 1 段落の中で，次のように記述されている。

（問題 1）顧客システム構築ネットワークに対して，当該構築業務とは関係がない PC から不正なアクセスを受ける可能性がある。

（問題 2）顧客システム構築を H 社の拠点で行っているので，顧客はシステムが納入されるまで動作確認ができない。

・解決策の検討

これらの問題に対処するために，SSL-VPN の利用を検討した。その点は第 2 段落の「(1) SSL-VPN について」「(2) SSL-VPN の動作方式」に記述されている。

この検討を踏まえ，問題の解決策を考案した。その点について，第 3 段落の中で，次のように記述されている。

> これらの検討結果から，開発 LAN 及び顧客各社の PC から顧客システム構築ネットワークに対する必要なアクセスを全て SSL-VPN 経由で行うようにすることで，問題 1 と問題 2 に対処できると考え（た）。

ここに「顧客システム構築ネットワークに対する必要なアクセスを全て SSL-VPN 経由で行うようにする」とある。その目的は「問題 1 と問題 2 に対処」するためだ。

SSL-VPN 経由でアクセスする PC として，次の 2 種類を挙げている。

- 開発 LAN の PC
- 顧客社内の PC

それぞれの PC からのアクセスを SSL-VPN 経由にすることは，二つの問題への対処と，どのように関係しているのだろうか。

結論から言うと，次のように整理できる。

表：問題と PC の関係

問題	SSL-VPN 経由にする PC	狙い
1	開発 LAN の PC	内部 LAN 経由で直接アクセスできないようにし，適正な通信だけをアクセスできるようにするため
2	顧客社内の PC	インターネット経由でアクセスできるようするため

まず，問題 1 について解説しよう。

前述の［特徴 4］にあるとおり，開発 LAN の PC は顧客システム構築ネットワークに直接アクセスが可能である。開発 LAN と顧客システム構築ネットワークは L3SW を介して接続しているため，開発者は自分が担当していない顧客システムに無制限にアクセスできてしまうのだ。

この問題に対処するには，直接アクセスできないようにした上で，構築業務に関係する適正な通信だけをアクセスできるようにする必要がある。そのための方策が SSL-

VPN 経由でのアクセスとなる。

次に，問題 2 について解説しよう。

一般的に言って，インターネット経由で内部 LAN にアクセスできるようにするには，リモートアクセスの仕組みの導入が必要となる。その代表的な技術が SSL-VPN である。

前述の［特徴 1］を踏まえると，SSL-VPN の L2 フォワーディング方式が，この問題への適切な解決策となる（詳しくは設問 2（2）で後述する）。

・問題解決のための具体的な設定

以上より，問題に対応するには，SSL-VPN 装置の導入が必要であることが分かった。そのために必要な設定について，〔SSL-VPN 装置の導入のための検討〕の中で記述されている。

さらに，問題に対応するには，「FW，L3SW などの設定変更」も必要になる（〔顧客システム構築業務の問題とその解決策〕の第 3 段落）。

具体的に言うと，FW のフィルタリングルールの設定については，〔SSL-VPN 装置の導入のための検討〕の中で記述されている。L3SW のアクセスリストの設定については，〔問題 1 の解決策〕の中で記述されている。

・本問の構成

以上を踏まえて本問の構成を概観すると，次のように整理できる。

表：本問の構成

見出し	主な内容	主に対応する出題箇所	
		設問	小問
なし（序文）	現行ネットワークの構成 図 1　H 社の現行ネットワーク構成	—	—
H 社の 現行ネットワーク			
顧客システム 構築業務の問題と その解決策	問題 1，2 の列挙	—	—
	問題 1，2 の解決策	1	空欄ア～オ
	（1）SSL-VPN について （2）SSL-VPN の動作方式	2	（1）～（3）
SSL-VPN 装置の導入 のための検討	（1）SSL-VPN 装置の設置位置 （2）SSL-VPN 装置へのユーザに対する情報登録 （3）IP アドレスの割当て	—	—
	（4）FW のルール変更	3	空欄カ～ケ

（表は次ページに続く）

見出し	主な内容	主に対応する出題箇所	
		設問	小問
検討後の ネットワーク構成	図 2　検討後のネットワーク構成	—	—
問題 1 の解決策	問題 1 の解決策 (1) VLAN 間の不正通信制限 (2) SSL-VPN 接続する PC の通信制限	4	(1) ～ (3)

それでは，設問の解説に移ろう。

■設問 1

解答例

ア：SHA-1
イ：1.2
ウ：Client_Hello
エ：Server_Hello
オ：リバースプロキシ

空欄ア～オは SSL/TLS プロトコル，SSL-VPN 動作方式の基礎知識を問うている。

ア

空欄アは，〔顧客システム構築業務の問題とその解決策〕の第 2 段落，「(1) SSL-VPN について」の 1 番目の箇条書きの中にある。そこには，「十分な安全性を確保できないとされるハッシュアルゴリズムである MD5 又は［　ア　］」と記述されている。

かつて使用されていたものの，もはや十分な安全性を確保できないとみなされているハッシュアルゴリズムとして，MD5, SHA-1 を挙げることができる。執筆時点（2017 年 12 月）では，これらに代わり，SHA-1 を改良した SHA-2 の使用が推奨されている。

したがって，MD5 と相並んで，「十分な安全性を確保できないとされるハッシュアルゴリズム」とみなされているものは，SHA-1 である。

よって，正解は「**SHA-1**」となる。

イ

空欄イは，空欄アの直後にある。そこには，「十分な安全性を確保できないとされるハッシュアルゴリズムである MD5 又は SHA-1（空欄ア）を使用しないで済むように，

TLS プロトコルのバージョン［　イ　］以上を利用する」と記述されている。

2008 年に RFC5246 で規格化された TLS バージョン 1.2 は，より安全な暗号スイートを選択できるように改良されている。具体的に言うと，ハッシュアルゴリズムでは SHA-2（SHA-256，SHA-384）を，認証付暗号利用モードでは GCM，CCM を，それぞれ利用できるようになった。

したがって，安全とはみなされていない MD5 又は SHA-1 を使用しないで済むように，TLS プロトコルのバージョンを指定する際には，1.2 以上としなければならない。

よって，正解は「**1.2**」となる。

なお，執筆時点では，TLS バージョン 1.3 の規格はドラフト段階であるため，市場の製品でバージョンを実際に指定する際は「1.2」を選択する。

●参考

IPA のサイトで提供されている「SSL/TLS 暗号設定ガイドライン」（2015 年発行）は，SSL/TLS サーバの構築時の設定，ブラウザの設定，SSL/TLS を安全に使うために考慮すべき事柄などを分かりやすく解説している。

https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html

［　ウ　］，［　エ　］

空欄ウ，エは，〔顧客システム構築業務の問題とその解決策〕の第 2 段落，「（1）SSL-VPN について」の 2 番目の箇条書きの中にある。そこには，「SSL/TLS のコネクション開設時に，クライアント側から送られる［　ウ　］メッセージと，サーバ側から送られる［　エ　］メッセージの交換が行われる。このとき，それ以降で用いられる暗号スイート（アルゴリズムの組合せを示した情報）が決定される」と記述されている。

SSL/TLS のコネクション開設は，通常，クライアント側から開始する。

最初に，クライアントは Client_Hello メッセージを送る。このメッセージには，自分が対応可能な暗号スイート（複数）が含まれている。

サーバがこれを受け取ると，クライアントとサーバの双方が対応できる暗号スイートを一つ選択し，Server_Hello メッセージを送る。このメッセージには，このとき選んだ暗号スイート（一つ）が含まれている。

その後のやり取りでは，選択された暗号スイートが適宜使用される。

よって，空欄ウに該当する字句は「**Client_Hello**」となり，空欄エに該当する字句は「**Server_Hello**」となる。

なお，ここで問われているメッセージ名の表記は，RFC5246「TLS Protocol Version 1.2」では「ClientHello」，「ServerHello」となっている。おそらく，採点に際して，多

少の表記上のバリエーションは許容されるものと著者は考えている。例えば，RFC に倣った表記はもちろん，全て小文字にした表記，アンダーバーの代わりに空白にした表記なども，メッセージ名として遜色のないものだからだ。

オ

空欄オは，〔顧客システム構築業務の問題とその解決策〕の第 2 段落，「(2) SSL-VPN の動作方式」の中にある。そこには，「SSL-VPN の基本的な動作には，［　オ　］，ポートフォワーディング，L2 フォワーディングの 3 方式がある」と記述されている。

SSL-VPN は，TLS プロトコルを利用した VPN 技術である。

拠点内のアプリケーションサーバ（以下，AP サーバと称する）に，PC がインターネット経由でリモートアクセスするときに利用する。

SSL-VPN の動作方式は，リバースプロキシ，ポートフォワーディング，L2 フォワーディングの 3 方式がある。

よって，正解は「**リバースプロキシ**」となる。

■設問 2

(1)

解答例

暗号アルゴリズム：鍵交換，認証
ハッシュアルゴリズム：メッセージ認証

問題文は，「本文中の下線（Ⅰ）について，2 種類の暗号アルゴリズムと 1 種類のハッシュアルゴリズムのそれぞれの用途を答えよ」と記述されている。

下線（Ⅰ）は，〔顧客システム構築業務の問題とその解決策〕の第 2 段落，「(1) SSL-VPN について」の 2 番目の箇条書きの中にある。そこには，「SSL/TLS のコネクション開設時に，クライアント側から送られる Client_Hello メッセージと，サーバ側から送られる Sever_Hello メッセージの交換が行われる。このとき，それ以降で用いられる暗号スイート（アルゴリズムの組合せを示した情報）が決定される。その情報には，アプリケーション層の暗号化に使われる暗号アルゴリズム以外に，（Ⅰ）2 種類の暗号アルゴリズムと 1 種類のハッシュアルゴリズムが含まれる」と記述されている（空欄ウ，エを補填）。

TLS では，暗号アルゴリズムとハッシュアルゴリズムを様々な場面で用いている。

大別すると，TLS セッションを用いたアプリケーション層の暗号化通信のとき，及び，TLS セッションを確立するときである。

それらアルゴリズムの組合せは，TLS セッション確立時の最初のやり取り（Client_Hello，Server_Hello）で取り交わされた，暗号スイートに含まれている。つまり，この段階で決定したアルゴリズムを，その後のやり取りで用いているわけだ。

そのうち,「アプリケーション層の暗号化に使われる暗号アルゴリズム」は既に本文中で言及されている。本問が問うているのは，それ以外のものとなる。

そこで，アプリケーション層の暗号化通信，TLS セッション確立のための通信のそれぞれについて，暗号アルゴリズムとハッシュアルゴリズムがどのように用いられているかをまずは解説する。次いで，解を導こう。

●アプリケーション層の暗号化通信

TLS では，アプリケーション通信の暗号化通信の際，暗号アルゴリズムとハッシュアルゴリズムを用いる。

暗号アルゴリズムの用途は，言うまでもなく，パケットのペイロード（アプリケーション層全体）の暗号化である。暗号化処理の高速化のため，通常，この暗号アルゴリズムは共通鍵方式に基づくものを使用する。その代表例は AES，RC4 などである。

この共通鍵は，TLS セッション確立時の鍵交換によって得られた，セッション鍵（セッションごとに乱数から生成された鍵）である。

一方，ハッシュアルゴリズムの用途は，ペイロードのメッセージ認証である。その代表例は SHA-2 である。

TLS の仕様では，アプリケーション層の暗号化とメッセージ認証で用いるアルゴリズムを，TLS セッションの確立時に決定することを規定している。具体的に言うと，そのタイミングは暗号スイートが決定される手順 1，2（Client_Hello，Server_Hello）である。

これまでの解説を整理すると，使用されているアルゴリズムは次のようになる。

表：使用されているアルゴリズム

アルゴリズムの種別	用途	本問で問われているか
暗号アルゴリズム	ペイロード（アプリケーション層）の暗号化	No
ハッシュアルゴリズム	ペイロード（同上）のメッセージ認証	Yes

● TLS セッション確立のための通信

TLS では，TLS セッションを確立するために，クライアントとサーバ間でハンドシェークプロトコルのやり取りが行われる。その際，別の暗号アルゴリズムも用いられている。

TLS セッションを確立する手順は，おおよそ次のとおりである。

1. クライアントは，暗号スイートの候補（複数），及び，クライアントが生成した乱数を送信する。
2. サーバは，実際に使用する暗号スイート（一つ）を決定する。これをクライアントに送信する。同時に，サーバが生成した乱数を送信する。
3. サーバは，サーバ証明書（サーバ公開鍵の証明書）を送信する。
4. クライアントは，サーバ証明書を用いてサーバを認証する。
5. クライアントは，プリマスタシークレットと呼ばれる乱数を生成する。この乱数から，アプリケーション層の暗号化通信に用いる共通鍵（セッション鍵）が生成される。これをサーバの公開鍵で暗号化して送信する。
6. サーバは自分の秘密鍵で復号することで，プリマスタシークレットを得る。この時点で，クライアントとサーバはプリマスタシークレットを共有する。
7. クライアントとサーバはそれぞれ，手順 1，2 で生成し交換した乱数及びプリマスタシークレットから，マスタシークレットを生成する。さらに，マスタシークレットから共通鍵を生成する。
8. 共通鍵を生成したクライアントとサーバは，「暗号アルゴリズムの使用を開始すること」をお互いに通知し合う。この後，全てのメッセージ（手順 9，及び，SSL セッション確立後のアプリケーション通信）は，暗号化される。
9. 前述の一連のやり取りが攻撃者によって改ざんされていないかを確認するため，クライアントとサーバは，メッセージ認証コードを交換し合う。このときやり取りされるメッセージは暗号化されている。

この説明では，サーバ認証（手順 3，4）にはサーバ証明書を用い，鍵交換（手順 5，6）にはサーバ公開鍵を用いるものとしている。それらの処理には，公開鍵方式に基づく暗号アルゴリズムが用いられている。その代表例は RSA である。

実を言うと，これ以外の手順も規定されている。

例えば，サーバの要求に基づき，クライアント認証が行われる場合がある。それは手順 4 と 5 の間で行われる。この認証処理には，サーバ認証と同じ暗号アルゴリズム（RSA 等）が用いられる。

他にも，鍵交換の手順として，Diffie-Hellman 鍵交換を用いることもできる。その処理には，暗号アルゴリズム（Diffie-Hellman）が用いられている。

ここでは詳細を割愛するが，公開鍵証明書を用いたサーバ認証について，詳しくは本書の第 8 章「8.2.2　認証方式」の「●第三者認証と電子証明書」を参照していただきたい。鍵交換について，同じ章の「8.2.1　暗号化方式」の「●鍵交換」を参照していただきたい。

さて，TLS の仕様では，主体認証（サーバ，クライアント）と鍵交換の手順，並びに，その際に用いる暗号アルゴリズムを，TLS セッションの確立時に決定することを規定している。具体的に言うと，そのタイミングは暗号スイートが決定される手順 1，2（Client_Hello，Server_Hello）である。

それらアルゴリズムの組合せは様々なバリエーションがある。例えば，主体認証と鍵交換の組を挙げると，「両方とも RSA」「主体認証は RSA，鍵交換は DH」「主体認証は DSA，鍵交換は DH」といった具合だ。

これまでの解説を整理すると，使用されているアルゴリズムは次のようになる。

表：使用されているアルゴリズム

アルゴリズムの種別	用途	本問で問われているか
暗号アルゴリズム	主体認証	Yes
暗号アルゴリズム	鍵交換	Yes

この表には明記しなかったが，厳密に言うと，手順 9 では，パケットの暗号化とメッセージ認証が行われている。ここで使用されるアルゴリズムは，アプリケーション層の暗号化通信と同じものだ。

●解の導出

これまでの解説から明らかなとおり，TLS では，暗号アルゴリズムの用途は 3 種類あり，ハッシュアルゴリズムの用途は 1 種類ある。

このうち，本文で言及されていないものを解答すればよい。

よって，正解は解答例に示したとおりとなる。

なお，試験センターの解答例では「主体認証」の代わりに「認証」となっている。本書ではメッセージ認証と区別するために，主体認証という用語を使って解説した。

(2)

解答例

顧客システムは，様々なプロトコルを利用している。（24字）

問題文は，「本文中の下線（Ⅱ）について，判断の根拠となった，H 社が構築する顧客システムの特徴を……答えよ」と記述されている。

下線（Ⅱ）は，〔顧客システム構築業務の問題とその解決策〕，の第 2 段落，「(2) SSL-VPN の動作方式」の中にある。そこには，「SSL-VPN の基本的な動作には，リバースプロキシ，ポートフォワーディング，L2 フォワーディングの 3 方式がある。（Ⅱ）H 社の場合は L2 フォワーディング方式が望ましいと，S さんは判断した」と記述されている（空欄オを補填）。

SSL-VPN の動作方式の特徴をまとめると，次の表のとおりとなる。

表：SSL-VPN 動作方式の種類と特徴

動作方式	専用モジュール	使用できるアプリケーション
リバースプロキシ方式	不要	ブラウザ上で動作できるアプリケーションに限定される
ポート フォワーディング方式	必要	ポート番号が実行時に変化しないアプリケーションに限定される
L2 フォワーディング方式	必要	アプリケーションには制限がない

動作方式を選定する上で重要な判断基準となるのは，使用できるアプリケーションの種類である。当然ながら，もしも業務で使用するアプリケーションに対応していないなら，SSL-VPN によるリモートアクセスを行えなくなるからだ。

本問は「H 社が構築する顧客システムの特徴」を問うているので，顧客システムで使用するアプリケーションに着目し，解を導こう。

冒頭で解説したとおり，現行の顧客システム構築ネットワークには次のような特徴がある。念のため再掲しよう。

［特徴 1］顧客システムは，様々なサーバ機器，OS，ミドルウェアなどを組み合わせて構築され，利用されるプロトコルも様々である（序文の第 1 段落）。

序文の第 1 段落に「利用されるプロトコルも様々である」と記述されている。

さらに，冒頭で解説したとおり，〔顧客システム構築業務の問題とその解決策〕の（問題 2）を解決するために，顧客各社の PC から SSL-VPN を経由して内部 LAN の自顧客システム構築ネットワークにアクセスできるようにすることが求められている。

以上より，SSL-VPN 経由で顧客が使用するアプリケーションは様々なものがあることが分かる。ゆえに，使用できるアプリケーションの制限がないことが選定の必要条件になる。

これに見合う SSL-VPN の方式を，前述の表「SSL-VPN 動作方式の種類と特徴」の中から選ぶなら，L2 フォワーディング方式以外に選択肢がない。

したがって，この方式が望ましいと判断する根拠となった「H 社が構築する顧客システムの特徴」とは，「様々なプロトコルを利用している」ことである。

よって，正解は解答例に示したとおりとなる。

(3)

解答例

vNIC

問題文は，「本文中の下線（Ⅲ）について，割り当てられた IP アドレスは，PC のどのネットワークインタフェースに設定されるか。図 2 中の字句を用いて答えよ」と記述されている。

下線（Ⅲ）は，〔顧客システム構築業務の問題とその解決策〕，の第 2 段落，「(2) SSL-VPN の動作方式」の 2 番目の箇条書きにある。そこには，「（Ⅲ）接続時の認証に応じて，PC に適切な IP アドレスを割り当てる」と記述されている。

前後の文脈を含めると，この箇条書きは，L2 フォワーディング方式の動作概要を述べたものである。箇条書きを全て列挙すると，このように記されている。

・PC にインストールするクライアントモジュールから SSL/TLS 接続を行う。
・接続時の認証に応じて，PC に適切な IP アドレスを割り当てる。
・PC と SSL-VPN 装置間の SSL/TLS 接続トンネル上で，レイヤ 2 の中継を行う。

3 番目の箇条書きに「PC と SSL-VPN 装置間の SSL/TLS 接続トンネル上で，レイヤ 2 の中継を行う」とある。具体的に言うと，この方式では，仮想的な L2 ネットワーク

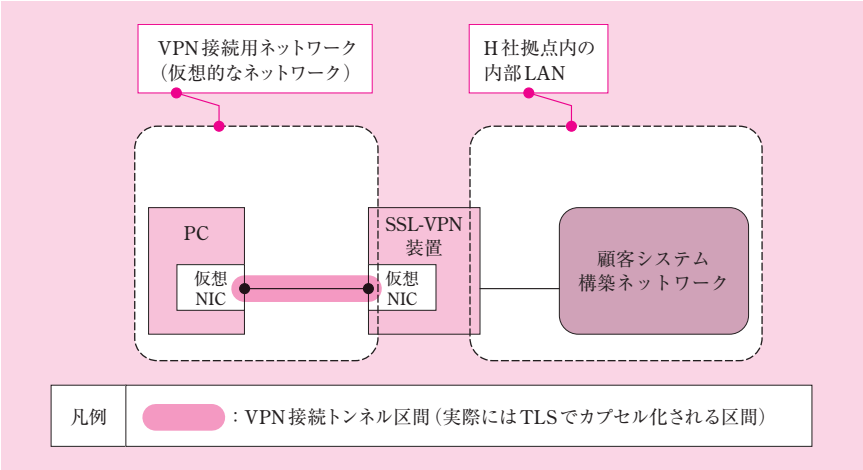
（一つのサブネットワーク）に，SSL-VPN 装置と PC が存在する仕組みになっている。

この仮想的な L2 ネットワークを実現するため，利用者の PC に，専用モジュールをインストールする必要がある。これが 1 番目の箇条書きで述べられた「クライアントモジュール」である。

L2 フォワーディング方式では，この専用モジュールを起動して SSL-VPN 装置に接続すると，仮想 NIC が構築される。さらに，この仮想 NIC と SSL-VPN 装置を接続する仮想的な L2 ネットワークが，VPN 接続トンネル上に構築される。SSL-VPN 装置は，仮想 NIC に対し，この L2 ネットワークの IP アドレスを割り当てる。

2 番目の箇条書きにある「PC に適切な IP アドレスを割り当てる」とは，このことを指している。

仮想的な L2 ネットワークの構成を次の図に示す。



図：L2 フォワーディング方式における，仮想的なネットワーク構成

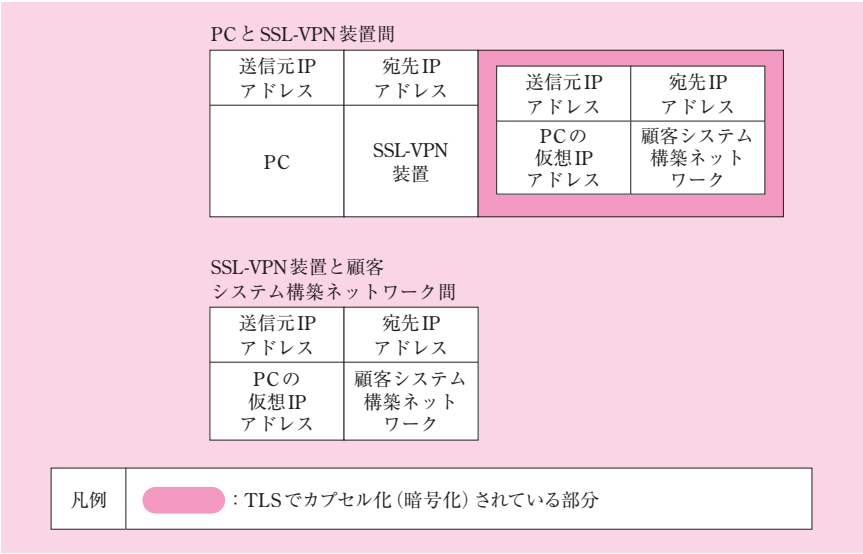
仮想的に見ると，同じ L2 ネットワークに，SSL-VPN 装置と PC が存在している。

顧客社内の PC と顧客システム構築ネットワークは，SSL-VPN 装置を介し，直接アクセスできるようになる。

要するに，仮想的なネットワーク上で，顧客社内の PC から送信されたパケットは，SSL-VPN 装置でルーティングされ，顧客システム構築ネットワークに到達するのである。そのパケットは，送信元 IP アドレスが仮想 IP アドレスとなり，宛先 IP アドレスが顧客システム構築ネットワークの IP アドレスとなる。

もちろん，実際のネットワークでは，PC と SSL-VPN 装置間は TLS でカプセル化

（暗号化）されている。PC がパケットを送信したときにカプセル化され，SSL-VPN 装置がこれを受信したときにカプセル化が解除される仕組みになっている。



図：L2 フォワーディング方式における，IP パケットのアドレス

この点を踏まえ，本文の図 2「検討後のネットワーク構成（抜粋）」を見ると，このネットワークには，SSL-VPN トンネルが 2 個記されている。

一つ目は，顧客 E 社の PC の vNIC と H 社の SSL-VPN 装置の間である。二つ目は，H 社内開発 LAN の PC の vNIC と H 社の SSL-VPN 装置の間である。

二つの SSL-VPN トンネルは，送信元の PC が異なるものの，PC の vNIC と SSL-VPN 装置の間に構築されている。

この「vNIC」について，図 2 の中で「仮想ネットワークインタフェースカード」と記述されている。この表現，及び，ここが SSL-VPN トンネルのエンドポイントになっていることから，vNIC は L2 フォワーディング方式で構築される仮想 NIC に他ならない。

したがって，仮想的な L2 ネットワークは，PC の vNIC と SSL-VPN 装置の間に構築されることが分かる。それゆえ，2 番目の箇条書き（つまり下線（Ⅲ））で述べられた IP アドレスの割当ては vNIC に対して行われる。

よって，正解は「**vNIC**」となる。

●参考：仮想的なネットワークにおける SSL-VPN 装置の役割

SSL-VPN 技術は標準化されたものではない。それゆえ，L2 フォワーディング方式に分類される技術であったとしても，細かな仕組みはベンダによって異なっている。

仮想的なネットワークにおける SSL-VPN 装置の役割は，そのようなベンダ依存性が見られる例である。その役割は，ルータであったり，L2SW であったりするのだ。

本事例の場合は，ルータである。

そのように言える理由は，顧客社内の PC の仮想 NIC に割り当てられる仮想 IP アドレスと，H 社拠点内の顧客システム構築ネットワークの IP アドレスが，異なるサブネットワークに属しているからだ。

この点は，本文の〔SSL-VPN 装置の導入のための検討〕の「(3) IP アドレスの割当て」の記述から確認できる。そこには，SSL-VPN で用いるアドレスが記されている。

PC の仮想 IP アドレスは，SSL-VPN 装置にプールされたものから払い出されている。その IP アドレスは「10.100.*k*.1 ～ 10.100.*k*.200」（*k*：顧客番号）となっている。一方，H 社拠点内の顧客システム構築ネットワークの IP アドレスは，「172.16.*z*.0/24」（$z = k + 99$）となっている。それゆえ，両者は異なっていることが分かる。両者を中継し得るのはルータ以外にない。

もし，SSL-VPN 装置を介して接続されたクライアントとサーバが，両者とも同じサブネットワークに属しているなら，SSL-VPN 装置の役割は L2SW であると判断できる。参考までに，平成 20 年度午後Ⅱ問 1 で出題された SSL-VPN の L2 フォワーディング方式は，そのような仕組みになっていた。

■設問 3

解答例

カ：内部 LAN
キ：DMZ
ク：172.16.0.0/16
ケ：202.y.44.2/32

設問 3 は表 1「通信を許可する FW ルール設定（抜粋）」中の空欄カ～ケを問うている。表 1 は，SSL-VPN 導入後の FW ルール設定の内容を示したものである。

冒頭で解説したとおり，SSL-VPN の導入は，顧客システム構築業務に関わる二つの問題を解決するために実施されたものである。

本設問の解を導くには，顧客システム構築業務の問題を解決するため新たに発生する通信を，ピックアップする必要がある。もしそれが FW を経由するならば，パケットフィルタリングのルールを新たに設定する必要が生じるからだ。なお，もしかすると不要になった通信があるかもしれず，その場合はルールを削除する必要が生じる。

求められている解は，それだけではない。表 1 のすぐ上の本文に「SSL-VPN 導入後の FW のルール」とあるので，従来許可していたルールも解答する必要がある。

そこで，解を導くために，まず，問題解決のために必要となる通信，不要になった通信，及び，従来どおり存続する通信を考察する。とりわけ，その通信の経路上に FW があるものをピックアップしてみよう。次に，その通信を許可するためのルールを考察する。最後に，表 1 のルールと照らし合わせて，解を導こう。

●問題解決のために必要となる通信

問題の解決策について，〔顧客システム構築業務の問題とその解決策〕の第 3 段落の中に，次のように記述されている。

> これらの検討結果から，開発 LAN 及び顧客各社の PC から顧客システム構築ネットワークに対する必要なアクセスを全て SSL-VPN 経由で行うようにすることで，問題 1 と問題 2 に対処できると考え（た）。

したがって，新たに発生する通信は次の 2 種類となる。

（通信 1）開発 LAN の PC から SSL-VPN を経由して顧客システム構築ネットワークにアクセスする通信

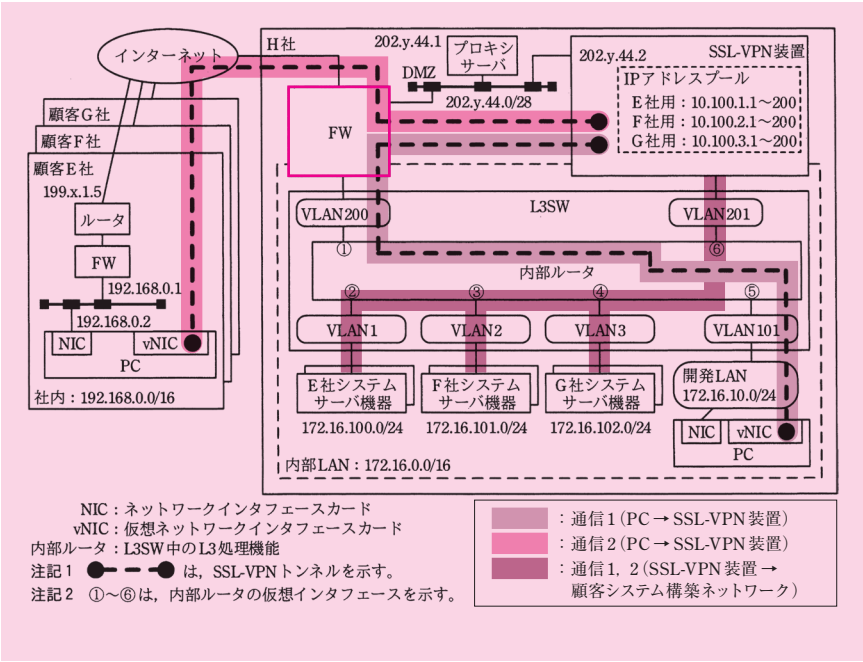
（通信 2）顧客各社の PC から SSL-VPN を経由して顧客システム構築ネットワークにアクセスする通信

これら二つの通信は，いずれも SSL-VPN 装置を経由する。その通信の経路全体について，〔SSL-VPN 装置の導入のための検討〕の「(1) SSL-VPN 装置の設置位置」の中に，次のように記述されている。

・顧客からインターネット経由で VPN 接続することと，開発 LAN から VPN 接続することを考慮して，SSL-VPN 装置の設置位置は DMZ と L3SW の間とする。
・SSL-VPN 装置から内部 LAN への通信用に，L3SW に新たな VLAN（VLAN201）を設け，SSL-VPN 装置の内側のインタフェースを L3SW に接続する。PC から顧客システム構築ネットワークへのアクセス経路が［PC → SSL-VPN 装置 → VLAN201 →顧客システム構築ネットワーク］となるように経路を設定する。

この経路のうち，「PC → SSL-VPN 装置」の部分が，図 2「検討後のネットワーク構成（抜粋）」に描かれた SSL-VPN トンネルである。

この二つの通信を次の図に示す。これを見ると明らかなとおり，「PC → SSL-VPN 装置」の部分，すなわち，SSL-VPN トンネルは，FW を経由している。それゆえ，この通信を許可するルールを FW に設定しなければならないことが分かる。



図：新たに発生する二つの通信

●問題解決の結果，不要になった通信

SSL-VPN 装置を導入した結果，問題 1 で指摘されていた通信が廃止される。

（問題 1）顧客システム構築ネットワークに対して，当該構築業務とは関係がない PC から不正なアクセスを受ける可能性がある。

この通信は，内部 LAN の中でやり取りされるものである。

図 1 に示された現行ネットワークを見ると明らかなとおり，この通信は FW を経由していない。それゆえ，この通信の廃止に伴って，FW のルールを変更する必要はないことが分かる。

●従来どおり存続する通信

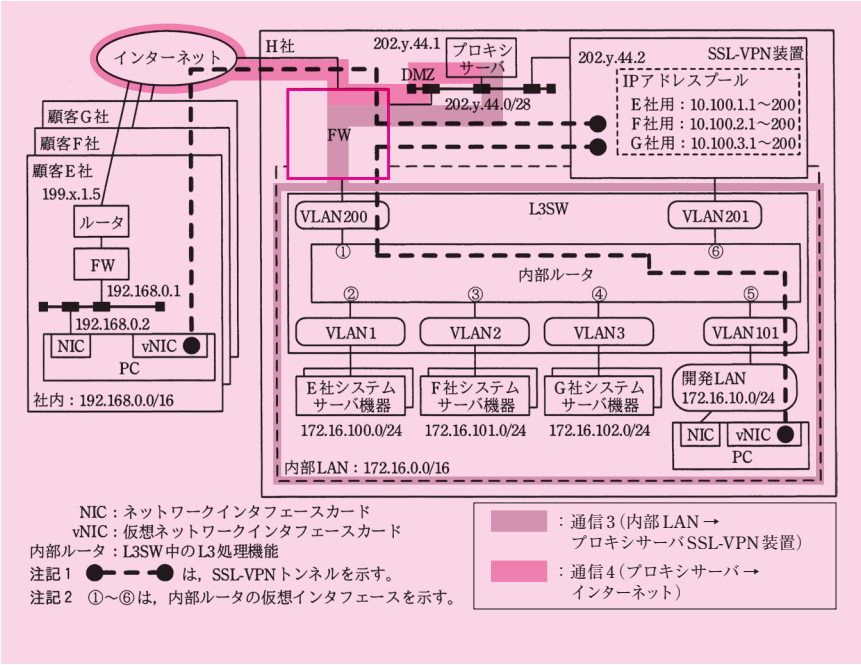
従来からある通信について，〔H 社の現行ネットワーク〕の第 1 段落に，「H 社は，内部 LAN からインターネットへの Web アクセスを，DMZ のプロキシサーバを経由して行っている」と記述されている。

したがって，この通信は，内部 LAN とプロキシサーバ間，及び，プロキシサーバとインターネット間でやり取りされるものである。

プロキシサーバが TCP コネクションの終端となることを考慮し，便宜上，二つに分けてみよう。

（通信 3）内部 LAN から DMZ のプロキシサーバにアクセスする通信
（通信 4）DMZ のプロキシサーバからインターネットにアクセスする通信

この二つの通信を図 2（検討後のネットワーク）に描き込んだものを次の図に示す。



図：従来どおり存続する通信

これを見ると明らかなとおり，どちらの通信も FW を経由している。

この通信を廃止する旨の記述はどこにもないため，これは存続すると推論できる。それゆえ，この通信を許可するルールを FW に設定したままにする必要がある。

なお，この通信のプロトコルについて，本文には「インターネットへの Web アクセス」とだけ述べられている。HTTP，TLS，FTP など複数考えられるが，本文からは特定できない。

当然ながら DNS（UDP/53）のやり取りもあるはずだが，DNS サーバの存在が明記されていないため，考察の対象から外すことにしよう。

● FW に設定するルール

これまで解説したとおり，四つの通信を FW で許可する必要がある。表 1 の表記に従い，それぞれの通信について，往路と復路を区別して，アクセス経路，送信元 IP アドレス，宛先 IP アドレス，プロトコル，宛先ポートを考察しよう。

ここで，表 1 の表記ルールを念のために確認しておこう。アクセス経路の表記では，FW の入口側インタフェースと出口側インタフェースを示し，通信の向きを矢印で示

す。送信元 IP アドレスと宛先 IP アドレスの表記では，IP アドレスにサブネットマスク長を付記する。それでは，四つの通信を一つずつ見ていこう。

（通信 1）開発 LAN の PC から SSL-VPN を経由して顧客システム構築ネットワークにアクセスする通信

往路は，アクセス経路が「内部 LAN → DMZ」である。送信元 IP アドレスが開発 LAN（172.16.10.0/24）であり，宛先 IP アドレスが SSL-VPN 装置（202.y.44.2/32）である。プロトコルが TCP，宛先ポートが TLS（443）である。

復路は，アクセス経路の向き，送信元／宛先の IP アドレスが，それぞれ入れ替わる。プロトコルが TCP，宛先ポートが任意である。

（通信 2）顧客各社の PC から SSL-VPN を経由して顧客システム構築ネットワークにアクセスする通信

往路は，アクセス経路が「インターネット→ DMZ」である。送信元 IP アドレスが任意であり，宛先 IP アドレスが SSL-VPN 装置（202.y.44.2/32）である。プロトコルが TCP，宛先ポートは TLS（443）である。

復路は，送信元／宛先の IP アドレスが入れ替わる。プロトコルが TCP，宛先ポートは任意である。

（通信 3）内部 LAN から DMZ のプロキシサーバにアクセスする通信

往路は，アクセス経路が「内部 LAN → DMZ」である。送信元 IP アドレスが内部 LAN（172.16.0.0/16）であり，宛先 IP アドレスがプロキシサーバ（202.y.44.1/32）である。プロトコル／宛先ポートについては，前述のとおり特定できないため，どちらも任意としておく。

復路は，アクセス経路の向き，送信元／宛先の IP アドレスが，それぞれ入れ替わる。プロトコル／宛先ポートが任意である。

（通信 4）DMZ のプロキシサーバからインターネットにアクセスする通信

往路は，アクセス経路が「DMZ →インターネット」である。送信元 IP アドレスがプロキシサーバ（202.y.44.1/32）であり，宛先 IP アドレスが任意である。プロトコ

ル／宛先ポートについては，通信 3 と同様，どちらも任意としておく。

復路は，アクセス経路の向き，送信元／宛先の IP アドレスが，それぞれ入れ替わる。プロトコル／宛先ポートが任意である。

●解の導出

表 1 には三つの通信を許可するルールが記されている。これらに該当するものを，先ほど考察した通信 1 ～ 4（往路と復路を含めると 8 個のルール）の中から選んでみよう。なお，表 1 のタイトルに「抜粋」とあるので，表 1 に記されていないルールがあるかもしれない。

説明の便宜上，まずは表 1 の 3 行目から解説しよう。表 1 の 3 行目は，アクセス経路が「インターネット→ DMZ」であり，プロトコル／宛先ポートが「TCP/443」である。このルールによって許可される通信は，通信 2（往路）である。

したがって，宛先 IP アドレスの空欄ケは「**202.y.44.2/32**」となる。

次に，表 1 の 1 行目を解説しよう。表 1 の 1 行目は，宛先 IP アドレスが DMZ のネットワークアドレス「202.y.44.0」であり，プロトコル／宛先ポートが任意である。

このルールによって許可される通信は，通信 1（往路），通信 3（往路），および，通信 2（往路）である。しかし，通信 2 は表 1 の 3 行目で許可されているので，対象外とする。

通信 1（往路），通信 3（往路）の宛先は DMZ 上のサーバなので，このルールで許可される。通信 1 のプロトコル／宛先ポートは通信 3 のそれに包含されており，通信 3 は「任意」となっているので，このルールで許可される。

したがって，アクセス経路の空欄カは「**内部 LAN**」，空欄キは「**DMZ**」となる。

送信元 IP アドレスの空欄クについては，通信 1 の送信元は通信 3 のそれに包含されるので，通信 3 の方に合わせて設定すればよい。それゆえ，「**172.16.0.0/16**」となる。

表 1 の 2 行目は，アクセス経路が「DMZ →インターネット」である。他の項目は省略するが，このルールによって許可される通信は，通信 2（復路），通信 4（往路）である。

■設問 4

設問 4 は，〔問題 1 の解決〕から出題されている。

設問 4 の解説に入る前に，この見出しで記述されている内容を概観してみよう。

冒頭で解説したとおり，現行ネットワークにおいて，開発 LAN は，全ての顧客システム構築ネットワークと L3SW を介して接続できる。それゆえ，開発者は自分が担当していない顧客システムに無制限にアクセスできてしまう。それが問題 1 で指摘され

ていた点である。

この解決策として SSL-VPN 装置を導入したが，他にもやるべきことがある。その具体策が，〔問題 1 の解決〕の中で説明されているのだ。

第 1 段落には，「問題 1 の解決策として，二つの通信制限をする」と記述されている。続く副見出しが，これを記している。

（1）VLAN 間の不正通信制限
（2）SSL-VPN 接続する PC（以下，VPN-PC という）の通信制限

設問 4 の小問（1）（2）は一つ目の，小問（3）は二つ目の通信制限について，それぞれ問うている。

以上で，見出し〔問題 1 の解決〕の全体像を把握できた。それでは，いよいよ小問の解説に移ろう。

(1)，(2)

解答例

(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（37字）

解説を分かりやすくするため，小問（1）と（2）を同時に扱うことにする。

小問（1）の問題文は，「本文中の下線（Ⅳ）について，表 2 のアクセスリストを設定すべきインタフェースを，図 2 中の①～⑥の記号で全て答えよ。ここで，アクセスリストはインタフェースの入力方向に設定するものとする」と記述されている。

小問（2）の問題文は，「本文中の下線（Ⅴ）について，禁止される通信は何か。本文中の字句を用いて……答えよ」と記述されている。

下線（Ⅳ）と（Ⅴ）は，〔問題 1 の解決〕の第 1 段落，「（1）VLAN 間の不正通信制限」の中にある。ここでは，問題 1 の解決策として，二つの通信制限を設けることについて述べている。

その一つ目である VLAN 間の不正通信制限について，「（Ⅳ）表 2 に示すアクセスリストを L3SW に設定して通信制限する。表 2 のアクセスリストは，H 社内の VLAN 通信のうちで不正なものを禁止する。具体的には，開発 LAN から顧客システム構築ネッ

トワークへの直接アクセス（SSL-VPN を経由しないアクセス）と，（V）それ以外の不正な通信を禁止する」と記述されている。

ここでは，H 社内の VLAN 通信のうち不正なものとして，2 種類を挙げている。

一つ目は問題 1 で指摘された通信である。

二つ目は下線（V）の通信であり，この点が小問（2）で問われている。

この二つの通信を禁止するために，表 2 のアクセスリストが設定されている。この点が小問（1）で問われている。

そこで，まず，禁止されている二つの通信を考察する。これが分かると小問（2）の正解が導ける。次に，通信を禁止するためにアクセスリストを設定する必要があるインタフェースを考察する。これが分かると小問（1）の正解が導ける。

●禁止する通信：小問（2）の解の導出

冒頭で解説したとおり，問題 1 に書かれている「当該構築業務とは関係がない PC」には，開発 LAN の PC が含まれている。これが記されている文脈から読み取れるが，開発 LAN の PC から顧客システム構築ネットワークへ直接アクセスさせず，SSL-VPN 装置を経由させることで，この問題を解決しようとしているからだ。

しかし，内部 LAN の中でやり取りされる通信が一切制限されていないならば，SSL-VPN 装置の導入など意に介さず，直接アクセスを試みる開発者がいるかもしれない。それゆえ，内部 LAN の通信を中継している L3SW において，通信を制限する必要がある。

その点を踏まえ，禁止する通信として，下線（V）の直前で，

- 開発 LAN から顧客システム構築ネットワークへの直接アクセス

を挙げているわけだ。

それでは，下線（V）が引かれた，他に禁止する通信とは，一体何であろうか。

ここで，SSL-VPN 装置の導入によって，問題 2 も解決しているという事実を思い起こしてみよう。これにより，顧客はインターネット経由で，自分の顧客システム構築ネットワークにアクセスすることが可能となる。

この結果，顧客システム構築ネットワークのサーバ機器上で，何らかのアプリケーションが動作するかもしれない。そして，同アプリケーションから，他の顧客システム構築ネットワークに不正な通信が行われるようになるかもしれない。

言うなれば，問題 2 を解決することによって，問題 1 と同等の「当該構築業務とは関係がないサーバ機器から不正なアクセスを受ける可能性がある」という問題が新た

に浮上してきたわけだ。

したがって，下線（V）が挙げている通信は，

- 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

であると結論できる。

よって，小問（2）の正解は，解答例に示したとおりとなる。

●アクセスリストを設定する必要があるインタフェース：小問（1）の解の導出

表 2 のアクセスリストは，問題文にあるとおり，「インタフェースの入力方向に設定」されている。要するに，L3SW にパケットが入ってくると，表 2 のアクセスリストに従って，通信が禁止又は許可される仕組みになっている。

表 2　VLAN 間通信制限のためのアクセスリスト

項番	動作	送信元 IP アドレス	宛先 IP アドレス
1	禁止	Any	172.16.0.0/16
2	許可	Any	Any

注記 1　Any は，パケットフィルタリングにおいてチェックしないことを示す。
注記 2　アクセスリストは，項番が小さい順に参照され，最初に該当したルールが適用される。
注記 3　どのルールにも該当しないものは禁止される。

図：問題文の表 2「VLAN 間通信制限のためのアクセスリスト」

前述のとおり，L3SW で禁止する通信は 2 種類ある。一つ目は，開発 LAN と顧客システム構築ネットワーク間の通信である。二つ目は，異なる顧客システム構築ネットワーク間の通信である。

L3SW から見て，開発 LAN はインタフェース⑤の配下にあり，顧客システム構築ネットワーク間の通信はインタフェース②～④の配下にある。つまり，②～⑤のインタフェース間は，相互の通信を禁止する必要がある。

この点を踏まえ，表 2 の 1 行目に記された「禁止」のルールを見てみる。その送信元 IP アドレスは「Any」であり，宛先 IP アドレスは「172.16.0.0/16」である。「172.16.0.0/16」は，内部 LAN のネットワークアドレスだ。

1 行目のルールをインタフェース②～④に設定すると，その配下にある顧客システムネットワークから，他社の顧客システムネットワーク及び開発 LAN への直接アクセ

スが禁止される。同様に，このルールをインタフェース⑤に設定すると，その配下にある開発 LAN から，顧客システムネットワークへの直接アクセスが禁止される。

したがって，インタフェース②～⑤に設定することによって，禁止する通信が全て網羅されることが分かる。

よって，小問（1）の正解は，「②，③，④，⑤」となる。

●参考：SSL-VPN 装置を経由する通信

設問 3 で解説したとおり，開発 LAN の PC は SSL-VPN による通信 1 を行っている。顧客社内の PC は SSL-VPN による通信 2 を行っている。この通信は，SSL-VPN 装置の VLAN201 側インタフェースを経由している。

設問 2（3）で解説したとおり，SSL-VPN トンネルが構築されると，PC と顧客システム構築ネットワークは，仮想的なネットワークを通って直接アクセスできるようになる。

PC から顧客システム構築ネットワークにパケットを送信する際，仮想的に見ると，送信元 IP アドレスは PC の仮想 IP アドレスとなり，宛先 IP アドレスは顧客システム構築ネットワークの IP アドレスとなる。

つまり，この通信において，SSL-VPN 装置の VLAN201 側インタフェースの IP アドレスは，送信元にも宛先にも指定されることがない。それゆえ，表 2 のアクセスリストの影響を受けないことが分かる。

(3)

解答例

⑥

問題文は，「本文中の下線（Ⅵ）について，表 3 のアクセスリストを設定すべきインタフェースを，図 2 中の①～⑥の記号で答えよ。ここで，アクセスリストはインタフェースの入力方向に設定するものとする」と記述されている。

表 3 の 1 ～ 3 行目はいずれも許可する通信となっている。注記 2 に「どのルールにも該当しないものは禁止される」とあるので，表 3 以外の通信を全て禁止することを目的として設定されたものである。

図 2 を見ると，表 3 の送信元 IP アドレスは，SSL-VPN 装置にプールされた IP アドレスであることが分かる。そして，表 3 の宛先 IP アドレスは，内部 LAN の顧客シス

テム構築ネットワークのアドレスであることが分かる。

SSL-VPN 装置にプールされた IP アドレスについて，〔SSL-VPN 装置の導入のための検討〕の「(3) IP アドレスの割当て」の 3 番目の箇条書きに，「VPN 接続時には，認証されたユーザに対応する……IP アドレスプールを選択する」と記述されている。したがって，この IP アドレスは，顧客社内の PC が SSL-VPN でリモートアクセスする際に使用されることが分かる。すなわち，設問 3 で解説した，通信 2 である。

顧客社内の PC は，手始めに SSL-VPN 装置に接続し，そこで認証を受ける。認証に成功すると SSL-VPN トンネルが構築され，PC の仮想 NIC に仮想 IP アドレスが割り当てられる。この仮想 IP アドレスは，SSL-VPN 装置にプールされた IP アドレスから払い出されているわけだ。

設問 2 (3) で解説したとおり，SSL-VPN トンネルが構築された後，仮想的には，顧客社内の PC から顧客システムネットワークに直接アクセスしているように見える。

仮想的なネットワーク上で，PC が送信するパケットは，送信元 IP アドレスが仮想 IP アドレス（プールされた IP アドレス）であり，宛先 IP アドレスが顧客システム構築ネットワークのアドレスである。実際には，PC と SSL-VPN 装置間は TLS でカプセル化されている。

この点を踏まえ，表 3 と図 2 に記された IP アドレスの対応を見てみよう。

1 行目は E 社用の通信に，2 行目は F 社用の通信に，3 行目は G 社用の通信にそれぞれ割り当てられた IP アドレスになっている。つまり，1 行につき 1 社ずつ対応していることが分かる。

したがって，表 3 のアクセスリストで許可しているパケットは，SSL-VPN 装置でカプセル化の解除後に取り出されたものであり，仮想的なネットワーク上で PC が顧客システム構築ネットワーク宛てに送付したものである。

表：表 3 と図 2 に記された IP アドレスの対応

			SSL-VPN 装置にプールされた IP アドレス			顧客システム構築ネットワークの IP アドレス		
表 3 の項番	1	送信元	E 社					
		宛先				E 社		
	2	送信元		F 社				
		宛先					F 社	
	3	送信元			G 社			
		宛先						G 社

〔SSL-VPN 装置の導入のための検討〕の「(1) SSL-VPN 装置の設置位置」を見ると，

PC から顧客システム構築ネットワークへのアクセス経路は，「PC → SSL-VPN 装置 → VLAN201 →顧客システム構築ネットワーク」と記述されている。

SSL-VPN 装置でカプセル化が解除されたアクセス経路を細かく見てみると，SSL-VPN 装置の VLAN201 側インタフェースから出ていき，L3SW のインタフェース⑥に入る。その後，L3SW でルーティングされ，宛先の顧客システム構築ネットワークに至る。

したがって，L3SW のインタフェース⑥が，表 3 のアクセスが設定されるべきところとなる。よって，これが正解となる。

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。

採点講評

問 2 では，仮想デスクトップ基盤（以下，VDI という）の導入を題材に，VDI 導入前後の通信要件の把握，ネットワーク帯域の見直し，帯域制御の設計，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ついて出題した。全体として，正答率は高かった。

設問 2(1)は，正答率は高かったが，VDI 導入後のシンクライアント及び仮想 PC で行われる通信を，本文から読み取れていない解答も散見された。ネットワーク技術者にとって，ネットワークで行われる通信，通信を行う装置，通信特性などを把握することは重要であると理解してほしい。

設問 2(2)は，VDI 導入後の広域イーサ網に関する計算を出題したが，正答率は低かった。問題文中に示された条件を正しく読み取り，正答を導き出してほしい。

設問 2(3)は，正答率は高かったが，情報セキュリティ対策上の利点についての言及がない解答も散見された。設問で何が問われているかを正しく理解し，注意深く解答してほしい。

設問 3 は，帯域制御に関して出題したが，(1)は通信特性を把握できている受験者が多く，正答率が高かった。(2)は“バケットを破棄する”と誤って解答した受験者が多かった。シェーピングやポリシングなどの帯域制御で用いられる機能に関する知識が不十分である結果と思われる。

設問 4 は，マルウェア感染時の対処に関して出題したが，正答率は高かった。

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	

本問は，仮想デスクトップ基盤（以下，VDI という）の導入を検討する事例を取り上げている。VDI の導入に伴って，セキュリティ対策（SSL 可視化，標的型攻撃対策，マルウェア感染時の対応）と帯域制御設計も検討している。

このように数多くの要素技術が登場するが，個々の要点はそれほど深く掘り下げられてはいない。本文の内容を落ち着いて整理すれば，解を導くことができるはずだ。

●本問の全体像

・現行ネットワークの概要

事例に登場する T 社は，本社と全国 10 か所の支店をもつ。

〔現行ネットワークの概要〕には，現行のネットワークの概要が記述されている。その主な特徴は，次のとおりである。

［特徴 1］本社と各支店が広域イーサ網で結ばれている。アクセス回線の契約帯域は，本社が 1G ビット／秒，各支店が 100M ビット／秒である（第 2 段落）。

［特徴 2］本社と各支店がそれぞれインターネットに接続している。契約帯域は，本社が 100M ビット／秒，各支店が 40M ビット／秒である（第 2 段落）。

［特徴 3］各従業員の PC 内のハードディスクには，T 社の秘密情報を含む書類が保存されている（序文の第 1 段落）。

［特徴 4］次に示す 3 種類の通信を行っている（第 3 段落）。

(1) ファイル転送通信
(2) プリント通信
(3) インターネット通信

これら 3 種類の通信に関する説明が，第 3 段落の副見出し (1) ～ (3) の中で記述されている。一つの副見出しが一つの通信に対応している。

次の表に，その目的と帯域をまとめておこう。

表：3 種類の通信の目的と帯域

通信の種類	目的	帯域
(1)ファイル転送通信	資料の共有 バックアップ	本社：200M ビット／秒 全支店：800M ビット／秒
(2)プリント通信	資料の印刷	必要な帯域は把握していない。 一時的に大量の帯域を使用する
(3)インターネット通信	Web サイト閲覧 メール	（記載なし）

宛先及び送信元も，同じ箇所に記述されている。

送信元と宛先を整理すると，広域イーサ網を経由する通信がどれであるかが明らかになる。結論から言うと，ファイル転送通信だ。

表：3 種類の通信の送信元と宛先

通信の種類	送信元	宛先	広域イーサ網の経由の有無
(1)ファイル転送通信	PC	本社のファイルサーバ	支店 PC が転送する場合，経由する
(2)プリント通信	PC	自拠点のプリントサーバ	経由しない
(3)インターネット通信	PC	インターネット上のサーバ	経由しない

(1) ファイル転送通信

この通信について，「(1) ファイル転送通信」の中で，「PC がファイルサーバと通信を行う」と記述されている。

支店 PC が本社のファイルサーバに転送する場合，支店 PC を送信元とし自拠点のプリントサーバを宛先とするトラフィックが発生する。それゆえ，広域イーサ網を経由する。

本社 PC が本社のファイルサーバに転送する場合は，本社拠点内で閉じたトラフィックが発生するため，広域イーサ網を経由しない。

(2) プリント通信

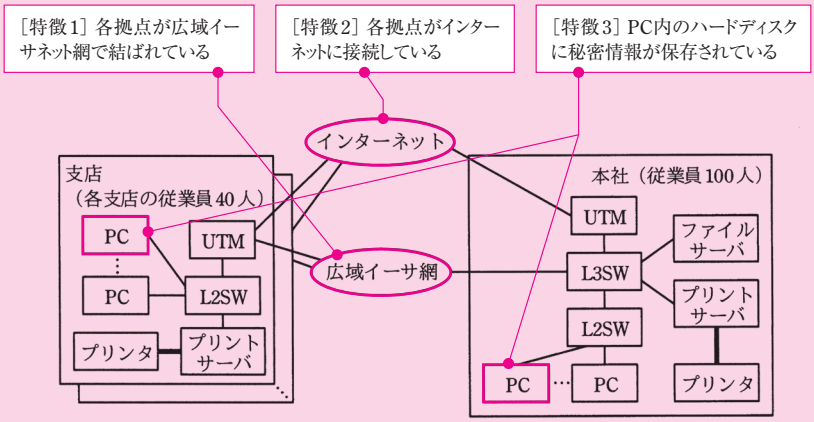
この通信について，「(2) プリント通信」の中で，「PC から自拠点のプリントサーバに印刷データを転送する」と記述されている。

それゆえ，本社にせよ支店にせよ，自拠点内で閉じたトラフィックが発生するため，広域イーサ網を経由しない。

(3) インターネット通信

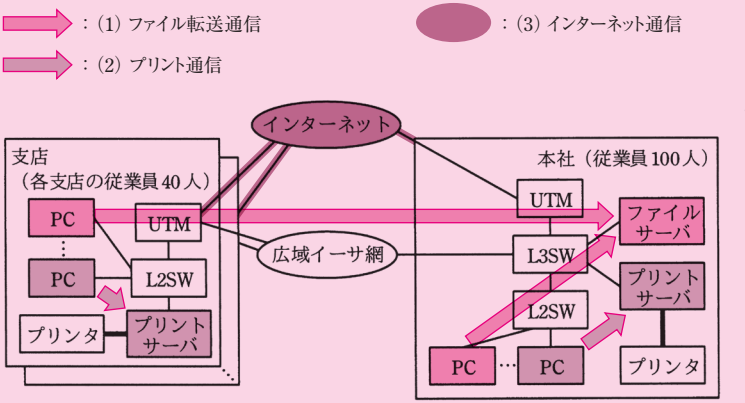
［特徴 2］で述べたが，〔現行ネットワークの概要〕の第 2 段落に「インターネット接続回線は，拠点ごとに契約して（いる）」。

それゆえ，本社にせよ支店にせよ，自拠点の接続回線を経由してインターネットにアクセスするため，広域イーサ網を経由しない。



L2SW：レイヤ2スイッチ　L3SW：レイヤ3スイッチ　UTM：Unified Threat Management
広域イーサ網：広域イーサネットサービス網
注記1　L2SW，L3SW，UTMは，全てのポートがギガビットイーサネットである。
注記2　プリンタとプリントサーバは，USBケーブルで接続されている。

図：T社の現行ネットワーク構成（図1の抜粋）



L2SW：レイヤ2スイッチ　L3SW：レイヤ3スイッチ　UTM：Unified Threat Management
広域イーサ網：広域イーサネットサービス網
注記1　L2SW，L3SW，UTMは，全てのポートがギガビットイーサネットである。
注記2　プリンタとプリントサーバは，USBケーブルで接続されている。

図：現行ネットワークの３種類の通信

・新ネットワークの概要

［特徴 3］で述べた，秘密情報が PC のハードディスクに保存されている事態を重く見た T 社は，情報セキュリティ強化を図るために，VDI の導入を決定した。

加えて，インターネット通信のセキュリティ強化を図ることにした。

一連の変更を反映するため，ネットワーク構成を大きく変更することにした。

これらを整理すると，七つの変更が行われることになる。本問を首尾よく解くには，数々の要点をきちんと整理する必要がある。そこで，設問の解説に入る前に，一つずつ詳しく述べておこう。

［変更 1］VDI の導入

本社に VDI サーバを設置し，秘密情報を VDI サーバで一括管理する。

VDI について，〔VDI の事前調査〕の中で詳しく説明されている。その内容を抜粋すると，次のようになる（適宜要約している）。

- VDI は，PC 単位のプログラム環境（以下，仮想 PC という）を提供するソフトウェアである。VDI サーバは，VDI を組み込んだサーバである。
- 各従業員には，ハードディスクなどの情報蓄積機能がない PC，すなわち，シンクライアント（以下，TC という）を支給する。従業員はこの TC を用いて仮想 PC を操作し，仮想 PC は画面を TC に転送する。
- VDI サーバは，VDI サーバ上に TC と 1 対 1 に対応する仮想 PC を生成する。このとき，VDI は仮想 PC に対して IP アドレスを動的に割り当てる。
- VDI サーバは，VDI サーバ上に仮想スイッチ（以下，仮想 SW という）を生成する。仮想 PC は仮想 SW との接続によって，外部との通信が可能になる。

［変更 2］画面転送通信の追加

VDI 導入に伴い，TC と仮想 PC 間の画面転送通信が新たに加わる。

この通信について，〔VDI の事前調査〕の「(3) 仮想 PC から行われる通信」の中で記述されている。便宜上，通信の項番を (4) とした上で，その目的と帯域を次の表にまとめておこう。

表：通信の目的と帯域

通信の種類	目的	帯域
(4) 画面転送通信	仮想 PC の画面を TC に転送する	TC1 台当たり 最大 200k ビット／秒

［変更 3］支店のインターネット接続回線の廃止，本社のインターネット接続回線の帯域増強

〔ネットワーク構成の検討〕の第 2 段落に「支店のインターネット接続回線を廃止し，本社のインターネット接続回線の帯域を 1G ビット／秒に変更する」と記述されているとおり，インターネット接続回線を変更する。

［変更 4］広域イーサ網のアクセス回線の帯域変更

通信の送信元が，現行ネットワークでは各拠点の PC だったのに対し，VDI 導入後には本社 VDI サーバ上の仮想 PC になることから，通信経路が変化する。さらに，各支店の TC と仮想 PC との間でやり取りされる画面転送通信が，広域イーサ網を経由することになる。

これら通信の送信元と宛先を整理すると，広域イーサ網を経由する通信がどれであるかが明らかになる。結論から言うと，プリント通信と画面転送通信だ。

表：通信の送信元と宛先

通信の種類	送信元	宛先	広域イーサ網の経由の有無
(1)ファイル転送通信	仮想 PC	本社のファイルサーバ	経由しない
(2)プリント通信	仮想 PC	TC から見た，自拠点のプリントサーバ	支店 TC が印刷する場合，経由する
(3)インターネット通信	仮想 PC	インターネット上のサーバ	経由しない
(4)画面転送通信	仮想 PC	TC	支店 TC に画面転送する場合，経由する

(1) ファイル転送通信

送信元が仮想 PC であり，宛先が本社のファイルサーバである。本社拠点内で閉じたトラフィックが発生するため，広域イーサ網を経由しない。

(2) プリント通信

支店 TC が自拠点で印刷する場合，仮想 PC を送信元とし自拠点のプリントサーバを宛先とするトラフィックが発生する。それゆえ，広域イーサ網を経由する。本社 TC が印刷する場合は，本社拠点内で閉じたトラフィックが発生するため，広域イーサ網を経由しない。

(3) インターネット通信

送信元が仮想 PC であり，宛先がインターネット上のサーバである。［変更 3］で述べたとおり，インターネット接続回線は本社のみ使用するため，広域イーサ網を経由しない。

（4）画面転送通信

送信元が仮想 PC であり，宛先が TC である。支店 TC の場合，広域イーサ網を経由する。本社 TC の場合は，これを経由しない。

広域イーサ網のアクセス回線の帯域は，ここを経由する二つの通信の品質や特性を踏まえて，適切な値に変更する必要がある。

この点が〔ネットワーク構成の検討〕の「(2) VDI 導入後の広域イーサ網」の中に記述されており，設問 2 (2) で問われている。帯域の具体的な数値については，当小問を解説する際に導くことにしよう。

［変更 5］帯域制御装置の導入

［変更 4］で述べたとおり，広域イーサ網を経由する通信は，プリント通信と画面転送通信の二つである。

このうち，画面転送通信は，TC の操作性が劣化しないように，帯域を確保する手段を講ずる。この点について，〔ネットワーク構成の検討〕の「(2) VDI 購入後の広域イーサ網」の中で，「全従業員が同時に仮想 PC を利用しても，TC の操作に遅れが発生しないようにするためには，画面転送通信の帯域を確保する必要がある」と記述されている。

一方，プリント通信用の帯域について，〔ネットワーク構成の検討〕の「(2) VDI 購入後のイーサネット網」に記述されているとおり，「印刷量を把握できない」ため，通信用の帯域を確保しない。

画面転送通信の品質を確保するため，帯域制御装置を導入する。

［変更 6］インターネット通信のセキュリティ強化

SSL/TLS で暗号化されたインターネット通信を監視し，標的型攻撃を検知するため，SSL 可視化装置と標的型攻撃対策装置を導入する。インターネット通信がこれらの装置を経由するように，ネットワーク構成を変更する。

この二つの装置に関する説明が，〔SSL 可視化装置・標的型攻撃対策装置の導入〕の中に記述されている。

SSL 可視化装置：

SSL/TLS 暗号化通信の復号，復号した通信データを標的型攻撃対策装置に転送，復号した通信データを再度暗号化する装置

標的型攻撃対策装置：

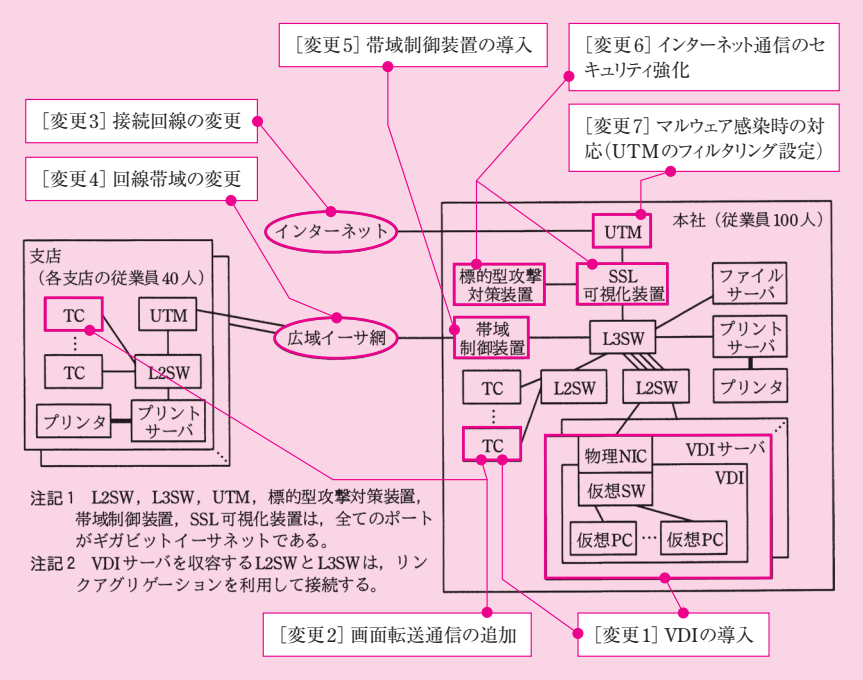
マルウェアに感染した仮想 PC がインターネット上の C & C（Command & Control）サーバと行う不正通信を検知し，C & C サーバの IP アドレスを特定する装置

［変更 7］仮想 PC のマルウェア感染時の対応

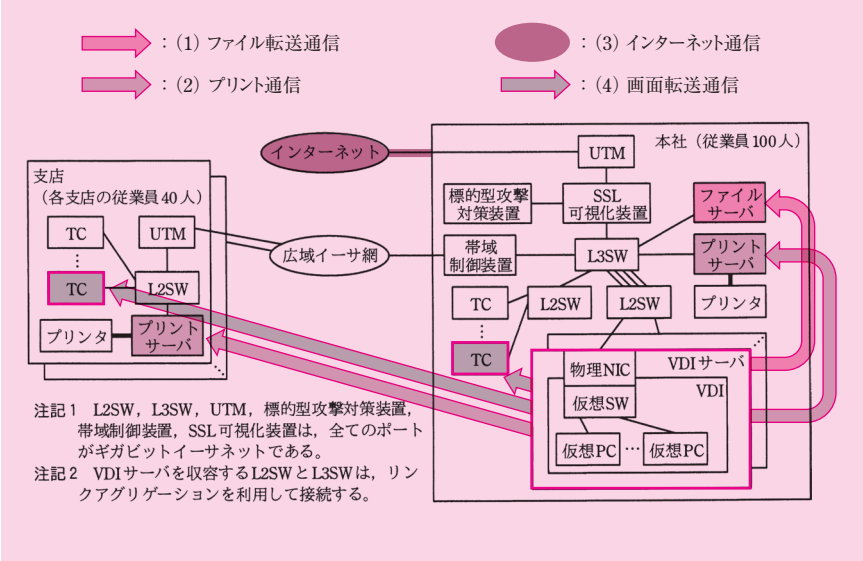
VDI 及び標的型攻撃対策装置の導入を踏まえ，仮想 PC のマルウェア感染時の対策を新たに設ける。

この点について，〔仮想 PC のマルウェア感染時の対応〕の中で，二つの対策が記述されている。その内容を抜粋すると，次のようになる（適宜要約している）。

- ある仮想 PC でウイルス対策ソフトがマルウェア感染を検知したとき，情報セキュリティ管理者がその仮想 PC を隔離すべきか否かを判断する。隔離するときは，VDI コンソールを使って，その仮想 PC を仮想 SW から切り離す。
- 標的型攻撃対策装置が，ある仮想 PC の通信から C&C サーバの IP アドレスを特定したとき，他の仮想 PC も含めて C&C サーバとの通信を遮断する必要がある。そのため，本社の UTM にフィルタリングルールを設定する。



図：VDI 導入後のネットワーク構成案（図 2 の抜粋）



図：VDI 導入後の 4 種類の通信

・本問の構成

以上を踏まえて本問の構成を概観すると，次のように整理できる。

表：本問の構成

見出し	主な内容	主に対応する出題箇所	
		設問	小問
なし（序文） 現行ネットワークの概要	現行ネットワークの構成 現行ネットワークの通信 図 1　T 社の現行ネットワーク構成	1	—
VDI の事前調査	［変更 1］	2	(1) ～ (3)
SSL 可視化装置・標的型攻撃対策装置の導入	［変更 6］		
ネットワーク構成の検討	［変更 2］［変更 3］［変更 4］ 図 2　VDI 導入後のネットワーク構成案		
帯域制御の設計	［変更 5］	3	(1) ～ (3)
仮想 PC のマルウェア感染時の対応	［変更 7］	4	—

七つの変更点を整理するのに紙面を結構割いたが，これで全体像はつかめたはずだ。それでは，いよいよ設問の解説に移ろう。

■設問 1

解答例

バ	ー	ス	ト	ト	ラ	フ	ィ	ッ	ク

（10字）

問題文は，「本文中の下線①の現象を引き起こすトラフィックを何というか」と記述されている。

下線①は，〔現行ネットワークの概要〕の第 3 段落，「(2) プリント通信」の 2 番目の箇条書きの中にある。そこには，「PC からプリントサーバに印刷データを送信したときは，①一時的に大量の帯域を使用する」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，「短時間に大量のパケットが流れる」という特性を有するトラフィックのことを「バーストトラフィック」と呼ぶ。

ここで使われている英単語の「バースト」(burst) とは，「爆発する」「噴出する」「はち切れる」「決壊する」等の意味をもつ。言うなれば，トラフィックが爆発的に生じる様を表している。

よって，正解は「**バーストトラフィック**」となる。

■設問 2

(1)

解答例

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：画面転送通信，プリント通信

問題文は，「本文中の下線③について，VDI 導入前に広域イーサ網を経由する通信を一つ，VDI 導入後に経由する通信を二つ，本文中の通信名を用いてそれぞれ答えよ」と記述されている。

本問は，大きく分けて二つのことを問うている。

一つ目は，「VDI 導入前に広域イーサ網を経由する通信」である。二つ目は，「VDI 導入後に経由する通信」である。それでは，一つずつ解を導くことにしよう。

●解の導出：VDI 導入前に広域イーサ網を経由する通信

「VDI 導入前」とは，要するに，現在のことを指している。

現行ネットワークの通信については，冒頭の「現行ネットワークの概要」の［特徴 4］で既に解説済みである。繰り返しになるが，次の 3 種類の通信がある。

(1) ファイル転送通信
(2) プリント通信
(3) インターネット通信

冒頭の［特徴 4］で導いた表を再掲しよう。詳しい解説はそこの説明を参照していただきたい。広域イーサ網を経由するものを，網掛けで強調しておく。

表：3 種類の通信の送信元と宛先（再掲）

通信の種類	送信元	宛先	広域イーサ網の経由の有無
(1)ファイル転送通信	PC	本社のファイルサーバ	支店 PC が転送する場合，経由する
(2)プリント通信	PC	自拠点のプリントサーバ	経由しない
(3)インターネット通信	PC	インターネット上のサーバ	経由しない

よって，VDI 導入前に広域イーサ網を経由する通信は，「**ファイル転送通信**」となる。

●解の導出：VDI 導入後に広域イーサ網を経由する通信

VDI 導入後，新たに画面転送通信が加わり，通信は全部で 4 種類になる。この点については，冒頭の「新ネットワークの概要」の［変更 2］で既に解説済みである。

冒頭の［変更 4］で導いた表を再掲しよう。詳しい解説はそこの説明を参照していただきたい。広域イーサ網を経由するものを，網掛けで強調しておく。

表：通信の送信元と宛先（再掲）

通信の種類	送信元	宛先	広域イーサ網の経由の有無
(1)ファイル転送通信	仮想 PC	本社のファイルサーバ	経由しない
(2)プリント通信	仮想 PC	TC から見た，自拠点のプリントサーバ	支店 TC が印刷する場合，経由する
(3)インターネット通信	仮想 PC	インターネット上のサーバ	経由しない
(4)画面転送通信	仮想 PC	TC	支店 TC に画面転送する場合，経由する

よって，VDI 導入後に広域イーサ網を経由する通信は，「**プリント通信**」「**画面転送通信**」となる。

(2)

解答例

a：1.25
b：100
c：10

本問は空欄 a ～ c に入れる適切な数値を問うている。

この空欄は，〔ネットワーク構成の検討〕の「(2) VDI 導入後の広域イーサ網」の中に記述されている。

順番に解説しよう。

a

空欄 a は 1 番目の箇条書きの中にある。そこには次のように記述されている。

> ・現行のアクセス回線の安全率は，“アクセス回線の契約帯域÷ピーク時に必要な帯域＝ a ”である。VDI 導入後も現行の安全率を確保する。

現行の広域イーサ網のアクセス回線について，〔現行ネットワークの概要〕の第 2 段

落の中で，「本社が 1G ビット／秒，各支店が 100M ビット／秒である」と記述されている。

現行のネットワークに関し，ピーク時に必要な帯域について言及されているのは，第 3 段落の「(1) ファイル転送通信」の 2 番目の箇条書きの中だけである。そこには，「本社従業員向けに 200M ビット／秒，全ての支店従業員向けの合計が 800M ビット／秒である」と記述されている。支店の数は「10 か所」（序文の第 1 段落）なので，支店 1 か所当たりに必要な帯域は「80M ビット／秒」となる。

冒頭及び設問 2（1）で解説したとおり，現行ネットワークの通信のうち，広域イーサ網を経由するのは，ファイル転送通信だけである。

ファイル転送通信の宛先は，本社にあるファイルサーバである。本社従業員によるファイル転送通信は，送信元が本社 PC であるので本社拠点内で閉じており，広域イーサ網を経由しない。一方，支店従業員によるものは，送信元が支店 PC であることから，広域イーサ網を経由する。

したがって，広域イーサ網を経由する通信に関し，ピーク時に必要な帯域は，全ての支店の合計が 800M ビット／秒であり，1 か所の支店が 80M ビット／秒である。

全ての支店から受けるファイル転送のトラフィックは，本社側のアクセス回線を通る。ここの帯域が 1G ビット／秒なので，安全率は次式より求まる。

安全率 = 1G ビット／秒 ÷ 800M ビット／秒
= 1.25　（式 1）

念のため，支店側のアクセス回線の安全率も確認しておこう。ここの帯域は 100M ビット／秒であり，本社側と比べて 1/10 の大きさになっている。ピーク時に必要な帯域も本社側と比べて 1/10 の大きさなので，安全率は同じである。

よって，空欄 a の正解は「**1.25**」となる。

b ，c

空欄 b，c は 4 番目の箇条書きの中にある。この文脈では VDI 導入後の帯域を求めているので，2 番目と 3 番目の箇条書きの記述も併せて確認してみよう。

そこには次のように記述されている。

・全従業員が同時に仮想 PC を利用しても，TC の操作に遅れが発生しないようにするためには，画面転送通信の帯域を確保する必要がある。
・印刷量を把握できないプリント通信の帯域は確保しない。
・VDI の導入でアクセス回線の契約帯域を下げることができる。契約帯域は現行の安全率を考慮した最低限必要な帯域とし，本社は［ b ］M ビット／秒，各支社は［ c ］M ビット／秒に変更する。

冒頭及び設問 2（1）で解説したとおり，VDI 導入後のネットワークの通信のうち，広域イーサ網を経由するのは，画面転送通信とプリント通信である。

帯域確保の要否に関し，画面転送通信については，2 番目の箇条書きの中で「確保する必要がある」と記述されている。一方，プリント通信については，3 番目の箇条書きの中で「確保しない」と記述されている。ここでは最低限必要な帯域を求めるので，帯域確保が必要となる画面転送通信にのみ着目すればよい。

画面転送通信の帯域について，〔VDI の事前調査〕の「(3) 仮想 PC から行われる通信」の 1 番目の箇条書きの中に「TC1 台が使用する帯域は，最大 200k ビット／秒」と記述されている。

各支店の従業員の人数は，図 2 より「40 人」である。支店の数は「10 か所」なので，全ての支店にある TC の合計数は 400 台となる。

したがって，これらが同時に仮想 PC を利用した場合，本社側と支店側のそれぞれのアクセス回線を流れるトラフィックの帯域は，次式より求まる。

本社側アクセス回線を流れるトラフィックの帯域
＝ TC400 台分の最大帯域
＝ 400 × 200k ビット／秒＝ 80M ビット／秒　（式 2）

支店側アクセス回線を流れるトラフィックの帯域
＝ TC40 台分の最大帯域
＝ 40 × 200k ビット／秒＝ 8M ビット／秒　（式 3）

現行の安全率（式 1）を維持するので，式 2，式 3 で求めた帯域に安全率を乗じた値が，アクセス回線の契約帯域となる。つまり，次式より求まる。

本社側アクセス回線の契約帯域
＝ 80M ビット／秒（式 2）× 1.25 ＝ 100M ビット／秒　（式 4）

支店側アクセス回線の契約帯域
＝ 8M ビット／秒（式 3）× 1.25 ＝ 10M ビット／秒　（式 5）

よって，空欄 b の正解は「100」となり，空欄 c の正解は「10」となる。

(3)

解答例

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
（25字）

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。（27字）

問題文は，「本文中の下線②について，インターネット接続回線を廃止する理由を，インターネット通信に着目して……述べよ。また，現行ネットワーク構成と比べたときの情報セキュリティ対策上の利点を……述べよ」と記述されている。

本問は，大きく分けて二つのことを問うている。

一つ目は，「下線②について，インターネット接続回線を廃止する理由」である。

下線②は，〔ネットワーク構成の検討〕の第 2 段落の中にある。そこには「VDI 導入後は，②支店のインターネット接続回線を廃止し，本社のインターネット接続回線の契約帯域を 1G ビット／秒に変更する」と記述されている。

つまり，一つ目に問うていることは，支店のインターネット接続回線を廃止する理由である。

二つ目は，「現行ネットワーク構成と比べたときの情報セキュリティ対策上の利点」である。

それでは，一つずつ解を導くことにしよう。

●解の導出：支店のインターネット接続回線を廃止する理由

問題文は「インターネット通信」に着目して答えるよう求めている。

インターネット通信に関し，VDI 導入の前と後で異なっている点がある。それは送信元である。送信元が変化すれば，通信経路も変化する。それゆえ，支店側の接続回線の廃止，及び，本社側の接続回線の帯域増強は，この送信元の変化に起因しているに違いないと推察できる。

VDI 導入前の現行ネットワークでは，冒頭の［特徴 4］で解説したとおり，送信元が PC である。各拠点はインターネットに接続しているので，PC からのインターネットアクセスは，自拠点の接続回線を経由する。

一方，VDI 導入後には，冒頭の［変更 4］で解説したとおり，送信元が仮想 PC となる。仮想 PC は，本社の VDI サーバ上に生成されたものであり，仮想 PC の IP アドレスは本社のネットワークアドレスの中から割り当てられる。それゆえ，仮想 PC からのインターネット通信は，本社の接続回線を経由することになる。

したがって，支店の TC からインターネットに接続することがないため，もはや支店側の接続回線を契約する必要がない。

よって，支店側の接続回線を廃止した理由は，「**インターネット通信は本社の仮想 PC から行われるから**」となる。これが求める解である。

さて，ここまでで解を導くことができたが，念のため確認しておきたい点がある。

それは，本社側の接続回線の帯域増強である。

仮想 PC は TC と 1 対 1 に対応して生成されるため，全拠点（本社及び支店）の TC からのインターネット通信に持ちこたえられるように，本社側の接続回線は帯域を増強する必要があるはずだ。

この点について，下線②の直後で「本社のインターネット接続回線の契約帯域を 1G ビット／秒に変更する」と述べられている。

本文の他の記述から，これが十分な大きさであることを裏付けてみよう。

まず，現行ネットワークの接続回線の帯域について，〔現行ネットワークの概要〕の中で，「本社が 100M ビット／秒，各支店が 40M ビット／秒」と記述されている。10 か所全ての支店を合計すると「400M ビット／秒」となる。

VDI 導入後に，本社側の接続回線を流れるインターネット通信の帯域は，従来の本社分（100M ビット／秒）と全ての支店分（400M ビット／秒）を合計した，500M ビット／秒相当となる。

実際，下線②の直後に記述された，変更後の契約帯域は「1G ビット／秒」である。したがって，「インターネット通信は本社の仮想 PC から行われる」ことを踏まえた，十分な大きさの契約帯域になっていることを確認できた。

●解の導出：現行ネットワークと比べたときの情報セキュリティ対策上の利点

「情報セキュリティ対策上の利点」が問われているので，VDI 導入後の情報セキュリティ対策に着目してみよう。すると，冒頭の解説で述べた，次の二つの点が該当することが分かる。

［変更 6］インターネット通信のセキュリティ強化
［変更 7］仮想 PC のマルウェア感染時の対応

冒頭の解説を簡潔に振り返ってみよう。

「インターネット通信のセキュリティ強化」は，〔SSL 可視化装置・標的型攻撃対策装置の導入〕の中で述べられている。T 社のサイバーセキュリティ対策の一環として，SSL 可視化装置と標的型攻撃対策装置が本社拠点に設置されている。仮想 PC からのインターネット通信は，SSL 可視化装置及び標的型攻撃対策装置で監視されている。

「仮想 PC のマルウェア感染時の対応」は，〔仮想 PC のマルウェア感染時の対応〕の中で述べられている。標的型攻撃対策装置が C & C サーバを特定したとき，本社の UTM にフィルタリングを設定するように対応策を練っている。

もし支店にもインターネット接続回線があったなら，支店側にもこれらの装置を設置し，合計 11 拠点分の監視を行わなければならなくなる。UTM のフィルタリングルール設定も 11 拠点分を同時に行わなければならなくなる。

一方，本事例のとおり本社にのみインターネット接続回線があるなら，この 1 拠点に集中してセキュリティ対策を実施すればよい。

両者を比較すると，本社で集中管理する方が，設置費用と運用負荷の面で利点があることが分かる。

よって，正解は「**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**」となる。

●参考：SSL 可視化装置

昨今では，情報セキュリティ意識の高まりを受け，Web ページ上のやり取りを全て TLS で暗号化するサイトが普及しつつある。「常時 SSL」と呼ばれる手法だ。

2017 年にはインターネット通信の半分が TLS で暗号化されると言われている(*)。

（*）HALF THE WEB IS NOW ENCRYPTED. THAT MAKES EVERYONE SAFER
https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/
URL は執筆当時（2017 年 12 月）のものである。

暗号化の普及により，通信の秘匿性は高まったと言えよう。

その反面，C & C サーバから標的型攻撃を受けて機密情報が窃取されたとしても，その通信が暗号化されていたなら，検知できなくなるという問題が懸念されるようになった。

これを解決すべく，TLS 暗号化通信を監視する機能を装備した SSL 可視化装置が，近年脚光を浴びている。

良い機会なので，参考までに，その仕組みを簡潔に解説しよう。なお，詳細の仕様は製品依存であることを申し添えておく。

SSL 可視化装置は，自社の PC とインターネット上のサーバとの通信を中継するプロキシである。TLS セッション確立を含む，全てのやり取りを中継し，監視している。

通常のプロキシであれば，TLS セッション確立の通信にせよ，TLS 暗号化の通信にせよ，ただ単にパケットを転送しているだけである。暗号化された通信の中身を解読することはできない。

これに対し，SSL 可視化装置は，自社 PC と接続先サーバが TLS セッションを確立する段階で，両者の通信に介入する。

まず，自社 PC が接続先サーバと TLS セッションを確立するため，いったん接続先サーバにアクセスする。接続先サーバはこれに応答して，公開鍵証明書を送信する。このときから，SSL 可視化装置の介入が始まる。

SSL 可視化装置は，接続先サーバの公開鍵証明書を自社 PC にそのまま転送しない。その代わり，自分自身の公開鍵証明書を自社 PC に送り返すのである。

この公開鍵証明書は，一見すると接続先サーバのものとそっくりだが，そこに格納された公開鍵が，SSL 可視化装置の公開鍵にすり替えられている。

こうして，SSL 可視化装置は，自社 PC に対して，あたかも接続先サーバであるかのように振る舞い，自社 PC との間で TLS セッションを確立する。これを TLS セッション A と呼ぼう（実は，自社 PC との TLS セッション確立を成功させるには，ある準備が必要である。詳しくは後述する）。

一方で，接続サーバに対しては，あたかも自社 PC であるかのように振る舞い，接続先サーバとの間で TLS セッションを確立する。これを TLS セッション B と呼ぼう。

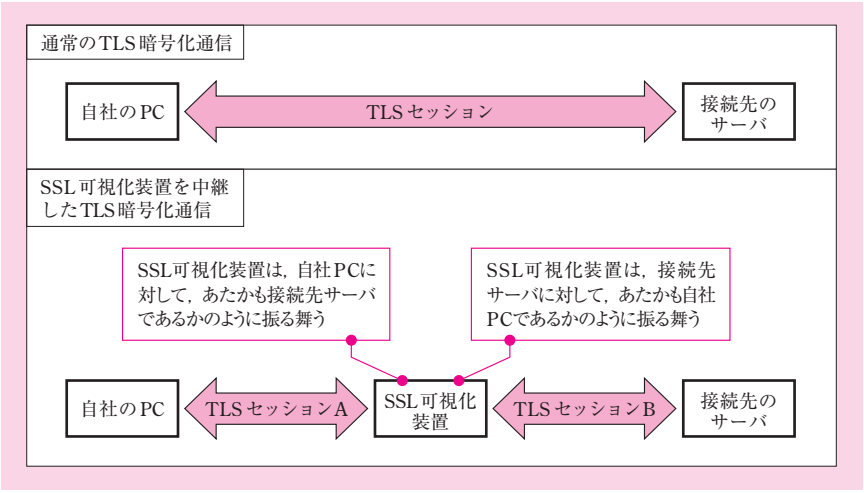
この結果，SSL 可視化装置は，二つの TLS セッション A，B のエンドポイントになる。当然ながら，それぞれの TLS セッションの共通鍵を有している。それぞれを鍵 A，鍵 B と呼ぼう。

前述のとおり，SSL 可視化装置は，自社 PC と接続先サーバの通信を中継する。このとき，自社 PC との間では TLS セッション A を，接続先サーバとの間では TLS セッション B を用いて通信するのである。

自社 PC が接続先サーバにパケットを送信する際，自社 PC は鍵 A を用いて暗号化する。SSL 可視化装置はこれを復号し，監視する。その後，SSL 可視化装置はこのパケットを接続先サーバに中継するが，鍵 B を用いて暗号化する。

接続先サーバが自社 PC にパケットを返信する際も，これと同様である。

このようにして，SSL 可視化装置は，TLS 暗号化通信を中継しながら，これを監視することができる。



図：SSL 可視化装置が TLS 暗号化通信を中継する仕組み

以上で SSL 可視化装置が暗号化通信を監視する仕組みを述べたが，この通信がうまくいくためには，あらかじめ準備しておくことがある。それは次の 2 点である。

- SSL 可視化装置の内部に，プライベート認証局（以下，プライベート CA という）を設置する。
- 自社 PC のブラウザに対し，このプライベート CA を「信頼できる CA のリスト」に加えるよう設定する。

前述のとおり，SSL 可視化装置は，自社 PC に対し，あたかも接続先サーバであるかのように振る舞っている。実を言うと，この振る舞いを首尾よく達成するには，TLS セッション確立時にブラウザが実施するサーバ認証に，成功しなければならない。さもないと，自社 PC との間で TLS セッションを確立できないからだ。

このサーバ認証では，信頼できる CA が発行した，公開鍵証明書が用いられている。そのため，前述のプライベート CA の準備が必要となるのである。

TLS セッションを自社 PC との間で確立する際，自社 PC は，SSL 可視化装置の公開鍵証明書を受け取る。これは，SSL 可視化装置が，公開鍵を自分のものにすり替えた上で，接続先サーバの公開鍵証明書に見せかけて発行したものであり，プライベート

CA による署名が付されている。自社 PC のブラウザはプライベート CA を信頼しているので，サーバ認証に成功するのだ。

当該証明書に格納された公開鍵は SSL 可視化装置が発行したものであり，これと対となる秘密鍵も自分が発行している。ゆえに，サーバ認証以降の TLS セッション確立のやり取りは全てうまくいくので，このときに生成された共通鍵をもつ。

この結果，SSL 可視化装置は，この TLS セッションでの暗号化通信を復号することができるのである。

興味深いことに，SSL 可視化装置が TLS 通信を中継・解読する方法は，SSL/TLS 通信における中間者攻撃（Man in the Middle 攻撃）の手口と同じである。

■設問 3

設問 3 は，〔帯域制御の設計〕について出題されている。

この設問を首尾よく解くには，この中で記述されている，帯域制御装置の機能，及び，この機能を使った帯域制御方式の設計を理解する必要がある。

そこで，小問の解説に入る前に，これらの点について解説しよう。

●帯域制御装置の機能

「(1) 帯域制御装置の機能」の 1 番目の箇条書きに記述されているとおり，宛先ごとに，分類制御，送出制御が可能である。以下，二つの機能の説明を抜粋しよう。

> ・分類制御では，IP アドレス，ポート番号などでパケットを分類し，グループ化する。グループ化の単位をクラスとし，クラス単位でキューを割り当て，パケットを格納する。
> ・送出制御では，クラス単位の帯域確保の制御と，同一支店への複数クラスのパケットに対するシェーピングが可能である。

シェーピングは，送出制御方式の一つである。この方式では，キューに到着したパケットを，送出レートを一定値以下に保って転送している。設定速度を超過したパケットはキューに蓄積し，後から転送する。

実は，このシェーピングの仕組みを説明した記述が，「(2) 帯域制御方式の設計」の 4 番目の箇条書きの中にある。そこには，帯域確保の制御を行わないクラスに分類されたパケットについて，「帯域が空いているときにだけ送出される」と記されている。

分類制御の説明と照らし合わせるなら，この帯域制御装置が，「帯域が空いていないとき，パケットはキューに格納される。帯域が空いたら，パケットはキューから送出

される」という送出制御を行っていることが分かるはずだ。名称こそ明記されていないが，まさしくシェーピングを説明した記述である。

たとえシェーピングという用語を知らなかったとしても，前後の記述を注意深く読めば，問題を解くことができるように配慮されていると言えよう。

●帯域制御方式の設計

冒頭の［変更 4］で解説したとおり，VDI 導入後に広域イーサ網を経由する通信は，画面転送通信とプリント通信である。冒頭の［変更 5］で解説したとおり，画面転送通信は帯域を確保する必要がある。一方，プリント通信はその必要がない。

画面転送通信の帯域を確保するというこの要件を実現するため，本事例では，帯域制御装置を導入する。

帯域制御装置は送出制御を行っているので，送信方向（本社から各支店の方向）の通信に対する帯域制御が必要となる。広域イーサ網を経由する通信は，送信元が本社（仮想 PC）なので，本社 1 か所にだけ帯域制御装置を設置すればよい。

この点を踏まえ，「(2) 帯域制御方式の設計」の記述を見てみよう。要約すると次のようになる。

- パケットがキューに到着すると，宛先ごとに，分類制御，送出制御の順に送られる。
- 分類制御では，ポート番号に基づいて，画面転送通信のクラスとプリント通信のクラスにパケットが分類される。
- 送出制御では，画面転送通信とプリント通信のクラスは，それぞれ異なる方法で送出される。

画面転送通信は，「(2) 帯域制御方式の設計」の 3 番目の箇条書き（下線④）にあるとおり，「各支店の従業員が同時に仮想 PC を利用するときに，最低限必要な帯域を確保する設定」を行う。それゆえ，このクラスに分類されたパケットは，必要な帯域が常に確保された状態になっているため，遅延なく送出される。

プリント通信は，帯域を確保する必要がないクラスである。4 番目の箇条書きにあるとおり，このクラスに分類されたパケットは，「帯域が空いているときにだけ送出される」。つまり，シェーピングされる。それゆえ，混雑時には遅延を余儀なくされる。

以上より，帯域制御装置の機能，及び，この機能の機能を使った帯域制御方式の設計を理解できたはずだ。それでは，いよいよ小問の解説に移ろう。

(1)

解答例

プ	リ	ン	ト	通	信	が	画	面	転	送	通	信	を	圧	迫	す	る	か	ら

（20字）

問題文は，「本文中の下線④について，帯域確保の設定を行わなかった場合，TC の操作性が悪化することが懸念される。TC の操作性が悪化する原因を，プリントの特性に着目して……述べよ」と記述されている。

帯域確保の設定を行わないクラスの通信について，「(2) 帯域制御方式の設計」の 4 番目の箇条書きの中で，「帯域が空いているときにだけ送出される」と記されている。

それでは，画面転送通信とプリント通信の両方とも，帯域確保の設定を行わないクラスに分類されると，どうなるだろうか。

当然ながら，帯域が空いていれば遅延は生じないが，帯域が空いていなければ遅延が生じるはずだ。

プリント通信の特性について，〔現行ネットワークの概要〕の第 3 段落の「(2) プリント通信」の中で，「一時的に大量の帯域を使用する」とある。したがって，ひとたびプリント通信が発生するなら，回線の帯域を使い切ってしまう事態が想定できる。

このとき，画面転送通信が同時に行われているとしたら，お互いに帯域を奪い合い，通信が圧迫される状況に陥ってしまう。画面転送のパケットがキューに蓄積されると，画面転送に遅延が生じることになる。

この状況を指して，問題文は，「TC の操作性が悪化することが懸念される」と述べているわけだ。本問はこの原因を問うているので，前述の内容を字数に収まるように答えればよい。

よって，正解は，「**プリント通信が画面転送通信を圧迫するから**」となる。

(2)

解答例

送	出	タ	イ	ミ	ン	グ	を	調	整	す	る	。

（13字）

問題文は，「本文中の下線⑤について，本社から各支店方向の通信の帯域が，各支店のアクセス回線の契約帯域を超過したときに，帯域制御装置がパケットに対して行う

制御の内容を，……述べよ」と記述されている。

設問 3 全体の解説の中で，本事例に登場する帯域制御装置が，シェーピング機能を装備していることを説明した。繰り返しになるが，シェーピングとは，「帯域が空いていないとき，パケットはキューに格納される。帯域が空いたら，パケットはキューから送出される」という仕組みをもつ送出制御方式である。

シェーピングの設定について，「(2) 帯域制御方式の設計」の 5 番目の箇条書きの中で，「各支店における広域イーサ網のアクセス回線の契約帯域とする」と記述されている。

設問 2 で解説したとおり，アクセス回線の契約帯域は，画面転送通信に必要な帯域に安全率 1.25 を乗じた，余裕のある大きさになっている。支店の全従業員が TC を操作したとしても，回線帯域はなお 20%の余裕がある（0.2 ＝（1.25 － 1）÷ 1.25）。

バースト性のあるプリント通信のパケットを帯域制御が受け取ったとき，もしも回線帯域の余裕分を超過してしまったならば，パケットをいったんキューに蓄積する。そして，帯域の空きを見計らって，送出タイミングを調整しながら，プリント通信のパケットを少しずつキューから取り出して転送していくのである。

よって，正解は「**送出タイミングを調整する**」となる。

■設問 4

解答例

ア：仮想 SW
イ：任意
ウ：C & C サーバ

本問は空欄ア～ウに入れる適切な字句を問うている。

この空欄は，〔仮想 PC のマルウェア感染時の対応〕の中に記述されている。

順番に解説しよう。

ア

空欄アは 1 番目の箇条書きの中にある。

1 番目の箇条書きは，ある仮想 PC で，ウイルス対策ソフトがマルウェアの感染を検知したときの対応を述べている。

そこには，「情報セキュリティ管理者がその仮想 PC を隔離すべきか否かを判断す

る。隔離するときは，VDI のコンソールを使って，その仮想 PC を［ア］から切り離す」と記述されている。

通常の PC がマルウェアに感染した場合，感染の拡大を防ぐため，当該 PC を隔離する必要がある。このときは，物理的に LAN ケーブルを引き抜いてネットワークから切り離せばよい。

しかし，仮想 PC には LAN ケーブルがつながっていないので，これとは異なる方法を用いてネットワークから切り離す必要がある。

仮想 PC がどのようにネットワークに接続しているかについて，〔VDI の事前調査〕の「(2) VDI の動作概要」の 2 番目の箇条書きに，「仮想 PC は仮想 SW との接続によって，外部との通信が可能になる」と記述されている。

したがって，仮想 PC を仮想 SW から切り離せば，外部との通信が不可能となるので，隔離に成功することが分かる。

よって，空欄アの正解は，「**仮想 SW**」となる。

［イ］，［ウ］

空欄イ，ウは 2 番目の箇条書きの中にある。

2 番目の箇条書きは，標的型攻撃対策装置が，ある仮想 PC の通信から C&C サーバの IP アドレスを特定したときの対応を述べている。

そこには，「本社の UTM にフィルタリングを設定する。被害の拡大を防ぐために，他の仮想 PC も含めて C & C サーバと通信を行うことを防ぐ必要があるので，“送信元＝［イ］，宛先＝［ウ］，ポート番号＝任意，動作＝拒否”のフィルタリングルールを設定し，インターネット方向の通信を遮断する」と記述されている。

「他の仮想 PC も含めて C & C サーバと通信することを防ぐ」「インターネット方向の通信を遮断する」とあるので，フィルタリングルールの宛先は，標的型攻撃対策装置が特定した，「C & C サーバ」となる。

フィルタリングルールの送信元は，全ての仮想 PC を対象としている。

一般的に考えれば，仮想 PC に対して VDI サーバから払い出される IP アドレスは，本社拠点内で使用されているプライベート IP アドレスだ。

インターネット通信をする際はどこかの機器でグローバル IP アドレスに NAPT 変換するが，それはどこの機器で行っているのだろうか。UTM から見た送信元を正しく見極めるため，この点を考察しておく必要がある。

本文には明記されていないが，現行ネットワークの構成（図 1）を見る限り，NAPT 変換は UTM で行っているに違いない。そして，このたびの VDI，SSL 可視化装置及び標的型攻撃対策装置の導入後も，この点は変更されていないものと考えられる（SSL

可視化装置の仕様がはっきりしないため，判断が難しい)。

UTM より内側ではアドレスが変換されない以上，今問われているフィルタリングルールの送信元は，仮想 PC に払い出される IP アドレスプール全体となる。本文には特にこれが明記されていないので，「任意」とすればよいだろう。

よって，空欄イ（送信元）の正解は「**任意**」となり，空欄ウ（宛先）の正解は「**C & C サーバ**」となる。

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。

採点講評

問 3 では，クラウドサービスとのネットワーク接続を題材に，インターネット VPN 接続，BGP と OSPF を用いた経路制御，ping を用いたネットワーク監視について出題した。

設問 2(1)は，トランスポートモードを選択した根拠を求める出題だが，正答率は低かった。ネットワーク設計を行う際には，それぞれの環境に応じて，最適な手法を選択できることは重要である。VPN やトンネリングの技術について，ネットワーク技術者として正確に理解をしてもらいたい。

設問 3(4)は，経路のループを防止するために必要な経路制御について出題したが，誤って，STP（スパニングツリープロトコル）について解答したものが散見された。IP の経路制御においても容易にループが発生し得ることを，是非知っておいてもらいたい。

設問 4 は二つある VPN トンネルの監視目的を求める出題だが，正答率は低かった。ネットワークに問題が発生した際の状況を正しく把握するために，目的を明確にして監視を行うことの必要性を理解してほしい。

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		

本問は，社内ネットワークとクラウドサービスのネットワークを VPN 接続する事例を取り上げている。

本問は，IP in IP と IPsec を使用した VPN トンネルの構築，ダイナミックルーティングプロトコル（BGP，OSPF）を使用した VPN トンネル接続の冗長化，及び，VPN トンネルの監視について問うている。

●本問の全体像

・ネットワーク接続構成の概要

事例に登場する K 社は，販売管理システムを更改し，当システムのサーバと DB（データベース）をクラウドに移行する計画を立てている。

その移行先として，L 社が提供しているクラウドサービスが有力視されている。

L 社クラウドサービスを試験的に利用するため，これを K 社ネットワーク（以下，K 社 NW）と接続する。

その主だった特徴は次の 6 点である。

［特徴 1］K 社 NW の VPN セグメントと L 社クラウドサービスのサーバセグメントは，どちらもプライベート IP アドレスが割り当てられている（図 1）。

［特徴 2］二つのネットワークをインターネット経由で VPN 接続するため，双方のネットワークに VPN ルータを設置する。
その際，次に示すように，VPN 接続を二重化する（〔クラウドサービスとのネットワーク接続の検討〕の 2 ～ 3 番目の箇条書き）。

表：VPN 接続の二重化の概要

実施する内容	場所
VPN ルータの設置	K 社側：VPNa1，VPNb1 L 社側：VPNa2，VPNb2
VPN トンネルの構成	VPNa1 と VPNa2 の間 VPNb1 と VPNb2 の間
アクティブ／スタンバイの設定	VPNa1 側の VPN トンネルをアクティブ

［特徴 3］K 社 VPN セグメント内にある VPNa1，VPNb1 及び L3SW の間では，OSPF を用いた経路情報の交換を行う（〔クラウドサービスとのネットワーク接続の検討〕の 4 番目の箇条書き）。

［特徴 4］VPN ルータ間は，IP in IP を用いたトンネルを構成する。このトンネルの通信を，IPsec を用いて暗号化する（〔インターネット VPN 接続の検討〕の第 1 段落）。

［特徴 5］ネットワーク接続の経路を二重化し，BGP を用いた動的経路制御を行う（〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕の第 1 段落）。

［特徴 6］二つある VPN トンネルがそれぞれ正常に動作しているかを常に確認するため，ping を用いる（〔ネットワーク監視の検討〕の第 1 段落）。

・本問の構成

以上を踏まえて本問の構成を概観すると，次のように整理できる。

表：本問の構成

見出し	主な内容	主に対応する出題箇所	
		設問	小問
なし（序文）	［特徴 1］［特徴 2］［特徴 3］ 図 1　L 社クラウドサービスとのネットワーク接続構成	1	空欄ア
クラウドサービスとのネットワーク接続の検討			
インターネット VPN 接続の検討	［特徴 4］	1	空欄イ
		2	(1) ～ (2)
K 社 NW と L 社クラウドサービスとの経路情報の交換の検討	［特徴 5］［特徴 3］ 図 2　K 社 NW と L 社クラウドサービスとの経路情報の交換の概要	1	空欄ウ，エ
		3	(1) ～ (4)
ネットワーク監視の検討	［特徴 6］	1	空欄オ，カ
		4	—

それでは，いよいよ設問の解説に移ろう。

■設問 1

解答例

ア：NAPT
イ：事前共有鍵
ウ：AS
エ：TCP
オ：ICMP
カ：echo reply

ア

空欄アは，〔クラウドサービスとのネットワーク接続の検討〕の第 2 段落の 7 番目の箇条書きにある。そこには，「K 社 NW の PC とサーバには，プライベート IP アドレスを割り当てる。PC 及びサーバからインターネットへの Web 閲覧などの通信は，FW で IP アドレスとポート番号の変換処理である［ア］を行う」と記述されている。

K 社 NW の PC 及びサーバがインターネットアクセスする際の経路について，同じ段落の 6 番目の箇条書きの中で，「（PC 及びサーバ）には，L3SW をデフォルトゲートウェイとして設定する。また，L3SW には，FW をデフォルトゲートウェイとして設定する」と記述されている。

したがって，PC やサーバがインターネットアクセスする経路は，次のとおりとなる。

PC，サーバ→ L3SW → FW →インターネット

7 番目の箇条書きにあるとおり，PC とサーバにはプライベート IP アドレスが割り当てられているため，インターネットアクセスの経路上のどこかの機器で，NAPT 変換（IP アドレスとポート番号の変換）が必要となる。それを FW が行っている旨を，7 番目の箇条書きは述べているのだ。

よって，正解は「**NAPT**」となる。

イ

空欄イは，〔インターネット VPN 接続の検討〕の第 3 段落の中にある。

このたびの VPN 接続は，トンネル技術は IP in IP を用い，トンネル区間の通信の暗号化には IPsec を用いる。第 2 ～第 3 段落は，IPsec の暗号化について述べている。

そこには，「暗号化は，フェーズ 1 と呼ばれる IKE SA の確立，フェーズ 2 と呼ばれる IPsec SA の確立を経て行われる。フェーズ 1 では，接続する相手を認証する方式として，両方の機器であらかじめ，［　イ　］と呼ばれる同じ鍵を共有する方式を利用する」と記述されている。

IPsec のフェーズ 1 では，VPN ルータ同士が互いに主体認証し合う。一般的によく利用されているのは，事前共有鍵方式である。第 3 段落にある，「両方の機器であらかじめ，同じ鍵を共有する方式」とは，この事前共有鍵方式のことを指している。

空欄イは，そこで用いられる鍵の名称を問うている。

よって，正解は「**事前共有鍵**」（Pre-Shared Key）となる。

IPsec について，詳しくは本書の第 8 章「8.4.5　IPsec」を参照していただきたい。

［　ウ　］

空欄ウは，〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕の第 3 段落の中にある。そこには，「BGP はルーティングプロトコルの一つであり，特定のルーティングポリシで管理されたルータの集まりを示す［　ウ　］の間で，経路情報の交換を行うために開発されたプロトコルである」と記述されている。

BGP は，AS（Autonomous System，自律システム）間を接続するダイナミックルーティングプロトコルであり，経路ベクトル型が採用されている。

AS とは，同一の管理ポリシによって管理されるネットワーク群であり，2 オクテット又は 4 オクテットの AS 番号によって識別される。

したがって，ここに記述された「特定のルーティングポリシで管理されたルータの集まり」は，AS を指していることが分かる。空欄ウはこの名称を問うている。

よって，正解は「**AS**」となる。

［　エ　］

空欄エは，〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕の第 4 段落の中にある。そこには，「BGP 接続を行う 2 台のルータ間ではトランスポートプロトコルの一つである［　エ　］のポート 179 番を使用し，経路情報の交換を行う。このコネクションのことを BGP ピアと呼ぶ」と記述されている。

BGP は，BGP 接続を行う 2 台のルータ間で TCP コネクションを確立し，ポート 179 番を使用して経路情報の交換を行う。

よって，正解は「**TCP**」となる。

空欄エを解く手掛かりとして，「トランスポートプロトコルの一つ」「ポート番号」「コネクション」といったキーワードが与えられている。BGP に詳しくなかったとし

ても，TCP という解答を導けたことだろう。

オ，**カ**

空欄オ，カは，〔ネットワーク監視の検討〕の第 1 段落の中にある。そこには，「監視には ping を用いる。ping は，［　オ　］の echo request パケットを監視対象に送り，［　カ　］パケットが監視対象から返ってくることで到達性を確認する」と記述されている。

ping は，ネットワーク機器の到達性（reachability）を監視する目的でよく用いられている。使用しているプロトコルは ICMP である。

監視用機器上で，監視対象機器に向けて ping コマンドを投入すると，監視用機器から ICMP echo request パケットが送信される。監視対象機器がこれを受け取ると，ICMP echo reply パケットを返信する仕様になっている。この 1 往復のやり取りをもって，監視用機器は，監視対象機器に到達可能であること，さらには，監視対象機器のレイヤ 3 機能（IP ノードとしての機能）が正常に稼働していることを確認できる。

この点を踏まえて，まず，空欄オを見てみよう。文脈上，ここに該当する字句は，echo request パケットが属するプロトコルである。

よって，空欄オの正解は「**ICMP**」となる。

次に，空欄カを見てみよう。ここに該当する字句は，監視対象機器が返信するパケットの名称である。

よって，空欄カの正解は「**echo reply**」となる。

■設問 2

設問 2 は〔インターネット VPN 接続の検討〕について出題している。

本設問を首尾よく解くには，トンネル技術である IP in IP の仕組み，及び，本事例において VPN トンネルでどのように使用されているかを理解しておく必要がある。そこで，これらの点について，概要をまず解説する。

● IP in IP

IP in IP とはトンネル技術の一つであり，RFC1853 で標準化されている。

IP in IP は，その名のとおり，IP パケットの中に，IP パケットをカプセル化する仕組みになっている。

次に示す図「IP in IP パケットの構造」を使って解説しよう。

図：IP in IP パケットの構造

オリジナル IP パケット，すなわち，カプセル化前のパケットは，オリジナルの IP ヘッダ①と IP ペイロードから構成されている。

これを IP in IP でカプセル化した後のパケットは，外部用の IP ヘッダ②が，オリジナルの IP ヘッダ①の前に付与されている。

さらに，この図では，IP ヘッダ②と①の間に「トンネル用ヘッダ」が挿入されている。RFC1853 によれば，構築されたトンネルに関わるヘッダが，IP ヘッダ②と①の間に挿入されることがあると規定している。

実を言うと，詳しくは後述するが，本事例ではトンネル区間が IPsec のトランスポートモードを用いて暗号化される。この暗号化によって挿入される IPsec の ESP ヘッダが，このトンネル用ヘッダに相当する。

IP ヘッダ②のプロトコル番号（上位層プロトコルを示す値）は，トンネル用ヘッダがない場合，「4」（IP in IP）となる。ESP 等のトンネル用ヘッダが挿入されている場合，プロトコル番号はそれを示す値になる。

●本事例の VPN 接続における，IP in IP と IPsec の使用

本事例では，K 社 NW と L 社クラウドサービスをインターネット経由で接続する。

この VPN トンネルについて，〔インターネット VPN 接続の検討〕の第 1 段落で，「L 社クラウドサービスの VPN ルータと K 社 NW の VPN ルータでは，互いのグローバル IP アドレスを利用して，……IP in IP を用いて，トンネルが構成される。このトンネルの通信を，IPsec を用いて暗号化する」と記述されている。

まずは，この記述にある「グローバル IP アドレス」という語に着目してみよう。

グローバル IP アドレス又はプライベート IP アドレスが割り当てられているネットワークについて，本文の記述を整理した内容を次の表に示す。

表：グローバル IP アドレスとプライベート IP アドレスが割り当てられているネットワーク

場所	ネットワーク	グローバル／プライベート	本文中の根拠
L 社	サーバセグメント	**プライベート**	図 1（g）（h）
インターネット		**グローバル**	―
K 社	DMZ	**グローバル**	〔インターネット VPN 接続の検討〕の第 1 段落
	VPN セグメント	**プライベート**	図 1（a）（b）
	FW セグメント	**プライベート**	設問 1 空欄アより，NAPT が FW で実施されるから
	サーバセグメント	**プライベート**	〔クラウドサービスとのネットワーク接続の検討〕の第 2 段落，7 番目の箇条書き
	クライアントセグメント	**プライベート**	

表中の「本文中の根拠」欄に示した内容を，一部補足しておこう。

図 1 の（a）～（h）は，注記 4 に記述されているように「VPN ルータに割り当てたプライベート IP アドレス」である。

したがって，（a）と（b）を収容している K 社 NW の VPN セグメント，（g）と（h）を収容している L 社クラウドサービスのサーバセグメントは，プライベート IP アドレスが割り当てられている。

なお，（c）～（f）は，VPN のトンネルインタフェースに割り当てられている。この点については後述する。

L 社拠点の VPN ルータの WAN インタフェース（インターネット側のインタフェース）は，インターネットに直に接していることから明白であるが，グローバル IP アドレスをもつ。

K 社拠点の VPN ルータの WAN インタフェース，及び，このインタフェースが接続している DMZ には，どのような IP アドレスが割り当てられているだろうか。

この点について，先ほど引用した，〔インターネット VPN 接続の検討〕の第 1 段落に，「L 社クラウドサービスの VPN ルータと K 社 NW の VPN ルータでは，互いのグローバル IP アドレスを利用して……トンネルが構成される」と述べられている。つまり，VPN ルータの WAN インタフェースはグローバル IP アドレスをもつことが分かる。それゆえ，これが接続している DMZ は，同じくグローバル IP アドレスが割り当

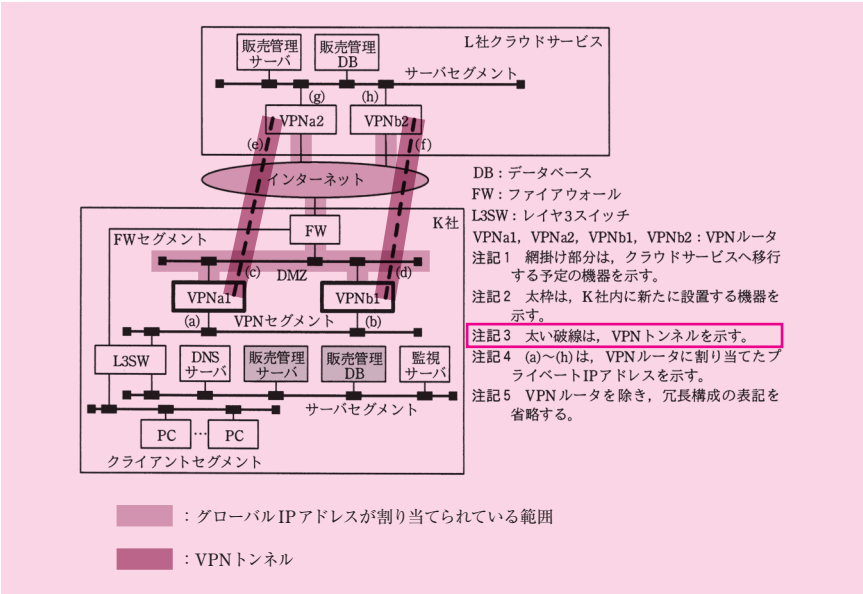
てられている。

したがって，K 社拠点の VPN ルータの WAN インタフェースには，グローバル IP アドレスが割り当てられている。

K 社 NW の FW セグメントについては，設問 1 空欄アより，NAPT が FW で実施されることが分かる。それゆえ，FW の内側に位置する FW セグメントは，プライベート IP アドレスが割り当てられている。

K 社 NW のサーバセグメントとクライアントセグメントは，〔クラウドサービスとのネットワーク接続の検討〕の第 2 段落の 7 番目の箇条書きに，プライベート IP アドレスを割り当てる旨，記述されている。

以上で，グローバル IP アドレス又はプライベート IP アドレスが割り当てられているネットワークを整理できた。まとめとして，VPN トンネル，及び，グローバル IP アドレスの範囲を，ネットワーク接続構成に書き加えたものを，次の図に示そう。



図：L 社クラウドサービスとのネットワーク接続構成（図 1 の抜粋）

IP アドレスの割当てが分かったので，〔インターネット VPN 接続の検討〕の第 1 段落の解説に戻ろう。

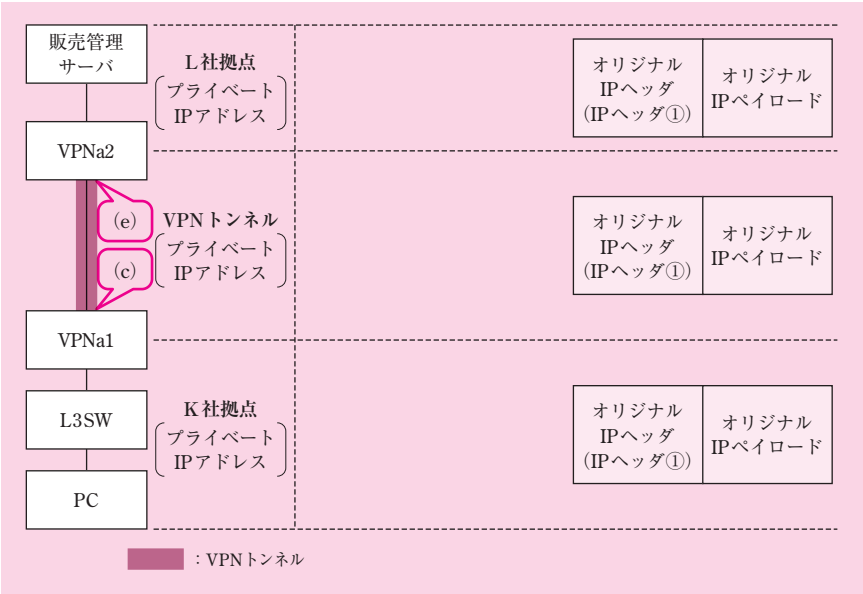
次に着目するのは，「IP in IP を用いて，トンネルが構成される。このトンネルの通信を，IPsec を用いて暗号化する」という記述である。

VPN トンネルは，簡単に言うと，2 拠点間を仮想的な専用線で接続することに相当する。この 2 拠点が，プライベート IP アドレスを割り当てているネットワークであっても，そして，この 2 拠点の間にインターネットが介在していても，VPN トンネルを通って直接通信することができるのだ。

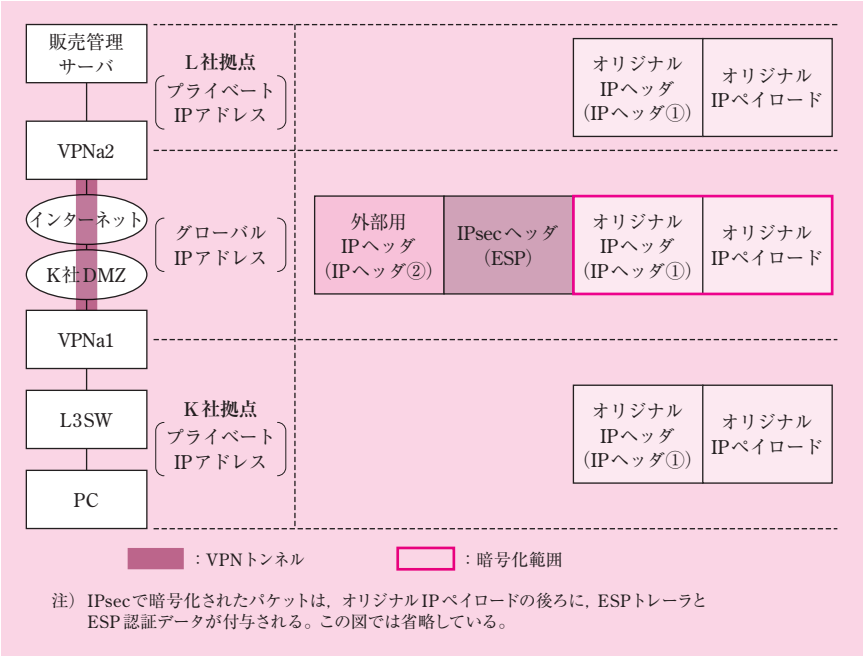
VPN ルータのトンネルインタフェース，すなわち，仮想的な専用線の両端に位置するインタフェースには，プライベート IP アドレスを割り当てることができる。

実は，図 1 の VPN ルータがもつ IP アドレス（c）～（f）は，このトンネルインタフェースに割り当てられたものである。

K 社と L 社の 2 拠点を VPN トンネルで接続したときに，仮想的に見えるネットワーク構成を次の図に示す。比較のために，実際のネットワーク構成をそのすぐ後に示そう。なお，説明を簡単にするため，ここではアクティブな VPN トンネル（VPNa1 と VPNa2 間）のみ図示する。



図：仮想的なネットワーク構成（アクティブな VPN トンネルのみ図示）



注）IPsecで暗号化されたパケットは，オリジナルIPペイロードの後ろに，ESPトレーラとESP認証データが付与される。この図では省略している。

図：実際のネットワーク構成（アクティブな VPN トンネルのみ図示）

二つの図で大きく異なっているところは，K 社拠点の VPN ルータ（VPNa1）と L 社拠点の VPN ルータ（VPNa2）に挟まれた区間である。

仮想的なネットワーク構成では，その区間にプライベート IP アドレスが割り当てられている。この区間に接している VPN ルータのインタフェースは，トンネルインタフェース（仮想的なインタフェース）である。図 1 の IP アドレス（c）は VPNa1 のトンネルインタフェースに，IP アドレス（e）は VPNa2 のそれに設定されている。

一方，実際のネットワーク構成では，両 VPN ルータに挟まれた区間はインターネットを経由しており，グローバル IP アドレスが割り当てられている。この区間に接している VPN ルータのインタフェースは，WAN インタフェース（実際のインタフェース）である。

二つの図に記したパケットは，K 社 NW のクライアントセグメントにある PC から，L 社クラウドサービスのサーバセグメントにある販売管理サーバ宛てに送信したものである。パケットの構造が，区間ごとにどのように遷移していくかを示している。

どちらの図においても，PC がサーバ宛てに送信するオリジナルの IP パケットは，IP ヘッダ①と IP ペイロードからなる。IP ヘッダ①の送信元は PC であり，宛先はサー

バである。そのどちらもプライベート IP アドレスだ。このオリジナル IP パケットを，サーバは受信する。つまり，通信の両端に位置する PC とサーバにしてみれば，仮想的なネットワークと実際のそれとは区別がつかないわけだ。

仮想的なネットワークにおいて，K 社拠点と L 社拠点の間は，VPN トンネルで直接接続されている。ここでは，オリジナル IP パケットは，K 社拠点，VPN トンネル，L 社拠点のどの区間においても，姿かたちを変えることなく，そのまま宛先に到達するかのように見えている。

しかしながら，実際のネットワークにおいて，K 社拠点と L 社拠点の間には，インターネットが横たわっている。このグローバル IP アドレスの区間を経由するとき，カプセル化を実施する必要がある。

実際のネットワークにおける振る舞いを，順を追って示そう。

［K 社拠点内の区間］

1. PC は，サーバ宛てにオリジナルの IP パケットを送信する。ここは仮想的なネットワークと同じ振る舞いである。
2. K 拠点の VPN ルータは，このパケットを受け取る。宛先 IP アドレスが L 社拠点のサーバセグメントなのでトンネルインタフェースに向けて転送する。
3. トンネルインタフェースはあくまで仮想的に存在しているものなので，このタイミングでカプセル化を実施する。このとき使用されるトンネル技術が IP in IP であり，カプセル化によって外部用の IP ヘッダ②が付与される。
   IP ヘッダ②の送信元は K 拠点の VPN ルータであり，宛先は L 拠点の VPN ルータである。そのどちらもグローバル IP アドレス，すなわち，VPN ルータの WAN インタフェースに割り当てられた IP アドレスだ。
4. K 拠点の VPN ルータは，カプセル化を実施した IP in IP パケットを，IPsec で暗号化する（詳しくは後述する）。
5. K 拠点の VPN ルータは，カプセル化と暗号化を実施したパケットを，WAN インタフェース（K 社 DMZ 側）に向けて転送する。

［K 社拠点と L 社拠点に挟まれた区間］

6. 当パケットは，K 社拠点から送出され，インターネットを経由して L 社拠点に到達する。

［L 社拠点内の区間］

7. 拠点の VPN ルータは，当パケットを WAN インタフェースから受け取ると，

復号とカプセル化解除を実施する。この時点でオリジナル IP パケットに戻る。

8. K 拠点の VPN ルータは，オリジナル IP パケットを，LAN インタフェース（サーバセグメント側）に向けて転送する。
9. サーバは，PC からのオリジナル IP パケットを受信する。ここも仮想的なネットワークと同じ振る舞いである。

項番 4 の段階で，VPN ルータは，IP in IP パケットを暗号化している。この点を補足しておこう。

暗号化の実施について，〔インターネット VPN 接続の検討〕の第 1 段落の中で，「トンネルの通信を，IPsec を用いて暗号化する」と記述されている。

IPsec の通信モードについて，第 4 段落の中で，「IP ヘッダを暗号化対象としないトランスポートモードを選択する」と記述されている。ここで言う IP ヘッダは，IP in IP トンネルを通るときの IP ヘッダを指している。すなわち，先ほどの図「実際のネットワーク構成（アクティブな VPN トンネルのみ図示）」に示した，外部用の IP ヘッダ②である。トランスポートモードで暗号化するため，外部用の IP ヘッダ②の直後に，ESP ヘッダが挿入される。

IPsec の通信モードの説明をここでは割愛するが，詳しくは本書の第 8 章「8.4.5 IPsec」を参照していただきたい。

ここまで理解できれば，設問 2 を解く準備は整った。それでは，いよいよ小問の解説に移ろう。

(1)

解答例

暗	号	化	対	象	の	通	信	が	グ	ロ	ー	バ	ル	I	P	ア	ド	レ	ス	間	の	通	信	だ	か	ら

（27 字）

問題文は，「本文中の下線①について，今回の構成では，トランスポートモードを選択している。選択した根拠を，IP アドレスに着目して……述べよ」と記述されている。

下線①は，〔インターネット VPN 接続の検討〕の第 4 段落にある。そこには，「フェーズ 2 では，① IP ヘッダを暗号化対象とするトンネルモードではなく，IP ヘッダを暗

号化対象としないトランスポートモードを選択する」と記述されている。

設問 2 全体の解説で述べたとおり，VPN ルータはトンネルの通信を IPsec で暗号化する。このとき暗号化対象となるパケットは，IP in IP でカプセル化されたパケットである。

IPsec で暗号化する際，2 種類の通信モードがある。一つ目はトンネルモード，二つ目はトランスポートモードである。

トンネルモードによる暗号化は，IPsec でトンネリングしてから暗号化するときに使用される。その典型例は，二つの拠点がインターネット経由で接続されており，インターネットの区間だけをトンネリングするケースだ。このように，トンネル区間は，オリジナル IP パケットの通信区間の一部となる。

トンネルモードのパケット構造は，外部用の IP ヘッダと ESP ヘッダが先頭に付与される。外部用の IP ヘッダの送信元と宛先は，トンネル区間の両端となる。

これに対し，トランスポートモードによる暗号化は，IPsec でトンネリングせずに暗号化するときに使用される。その典型例は，既に別のプロトコルでトンネリングされたパケットを暗号化するケースだ。

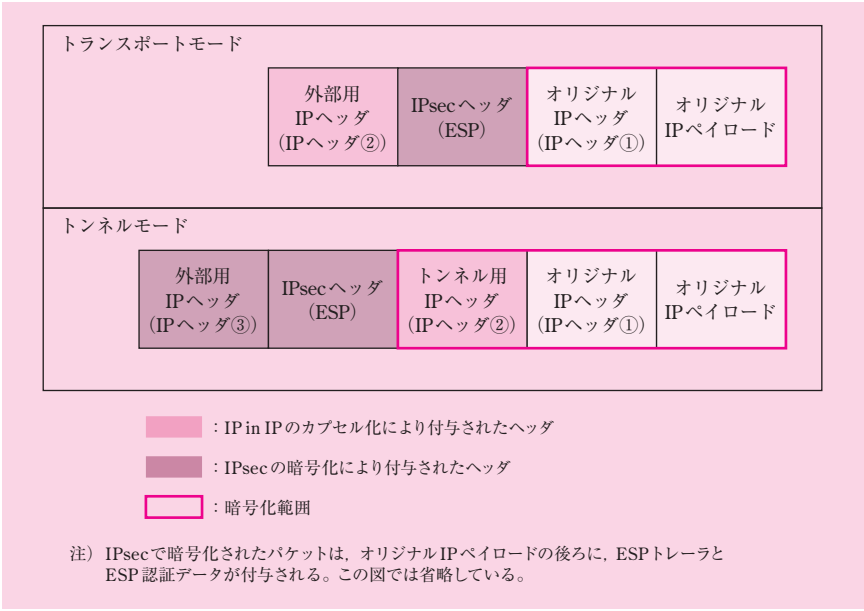
トランスポートモードのパケット構造は，IP ヘッダと IP ペイロードの間に，ESP ヘッダが挿入される。IP ヘッダの送信元と宛先は，暗号化に伴って変化することがない。

それでは，本事例で用いるべき通信モードは，どちらがよいだろうか。これを判断するには，IPsec でトンネリングする必要があるか否かが分かればよい。

この点について，〔インターネット VPN 接続の検討〕の第 1 段落に，「トンネルの通信を，IPsec を用いて暗号化する」と記述されている。ここから，IPsec の暗号化区間は，IP in IP トンネル区間と同一であることが分かる。それゆえ，IPsec でわざわざトンネリングする必要がないわけだ。したがって，トランスポートモードが適切である。

参考までに，本事例に登場する IP in IP パケットを IPsec で暗号化した場合の，通信モードによるパケット構造の違いを次の図に示そう。

なお，この図で用いられている IP ヘッダ①，②は，設問 2 全体の解説中の図「実際のネットワーク構成（アクティブな VPN トンネルのみ図示）」と同じである。



図：IP in IP パケットを暗号化した場合の，通信モードによるパケット構造の違い

トンネルモードで暗号化した場合，IP in IP パケット全体が暗号化の対象となる。このパケットの先頭には，IPsec が付与した外部用の IP ヘッダ③がある。この IP ヘッダ③の送信元と宛先は，IP ヘッダ②のそれと同じになる。IPsec と IP in IP のトンネル区間が同じだからだ。それゆえ，IPsec によるトンネリングは意味をなさない。それどころか，MTU が小さくなるというデメリットすらある。

トランスポートモードで暗号化した場合，IP in IP パケットの外部用 IP アドレスは，トンネル区間の両端のグローバル IP アドレスだ。このヘッダを使用してインターネットを通過できるので，IP ヘッダ②をそのまま使用すればよい。つまり，暗号化はオリジナル IP ヘッダ①とオリジナル IP ペイロードにのみ実施すればよい。

本小問が問うているのは，「トランスポートモードを選択した根拠」であるから，前述の内容をまとめればよい。

ただし，問題文には「IP アドレスに着目して述べよ」という条件が付いている。そこで，IP アドレスについて本文が与えている情報を手掛かりに，解を導くことにしよう。

ここで再び，〔インターネット VPN 接続の検討〕の第 1 段落の記述を思い起こすと，そこには「L 社クラウドサービスの VPN ルータと K 社 NW の VPN ルータでは，互い

のグローバル IP アドレスを利用して，……IP in IP を用いて，トンネルが構成される。このトンネルの通信を，IPsec を用いて暗号化する」とある。

IP in IP トンネルに関し ,「グローバル IP アドレスを利用して……トンネルが構成される」と記述されていることから，IPsec で暗号化する際，改めて IPsec でトンネリングする必要がないということが分かる。ゆえに，通信モードはトランスポートモードでよいという結論を導くことができる。

したがって，「グローバル IP アドレス」というキーワードを解答に含めて，内容をまとめればよい。

よって，正解は「**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**」となる。

(2)

解答例

フ|ラ|グ|メ|ン|ト|と|リ|ア|セ|ン|ブ|ル|の|処|理|が|発|生|す|る|。（22字）

問題文は，「本文中の下線②について，IP in IP で作成されたトンネルインタフェースの MTU の値を 1,500 とした場合，VPN ルータで発生する処理を，……述べよ。ここで，インターネットを含む全てのインタフェースの MTU の値を 1,500 とする」と記述されている。

設問 2 全体の解説中の図「仮想的なネットワーク構成（アクティブな VPN トンネルのみ図示）」に示したとおり，トンネルインタフェースから VPN トンネルに出ていくときのパケット構造は，次のものからなる。

オリジナル IP ヘッダ＋オリジナル IP ペイロード

同じく，図「実際のネットワーク構成（アクティブな VPN トンネルのみ図示）」に示したとおり，インターネットに出ていくときのパケット構造は，次のものからなる。

外部用 IP ヘッダ＋ ESP ヘッダ＋オリジナル IP ヘッダ
＋オリジナル IP ペイロード＋ ESP トレーラ＋ ESP 認証データ

トンネルインタフェースの MTU が 1,500 バイトである場合，オリジナル IP パケッ

トのサイズは，最大で 1,500 バイトになり得る。

では，もし 1,500 バイトのサイズをもつオリジナル IP パケットを VPN ルータが受け取り，これにカプセル化と暗号化を実施したら，どうなるだろうか。

このとき，カプセル化と暗号化を実施した IP パケットは，WAN インタフェースから出ていく。こちらの IP パケットには，外部用 IP ヘッダ，ESP ヘッダなどが付与されており，サイズが大きくなっている。したがって，WAN インタフェースの MTU が 1,500 バイトであるとしたら，MTU を超過してしまう。

ルータは，IP パケットを転送する際，そのサイズが転送先インタフェースの MTU を超過している場合，MTU のサイズに収まるようペイロードを分割する。分割したペイロードに IP ヘッダを各々付与し，複数の IP パケットにしてから，転送する仕様になっている。これをフラグメント（fragment，分割）という。

分割された IP パケットは，宛先ノードまで転送される。宛先ノードは，フラグメント化された IP パケットを全て受信し終えたら，元の IP パケットを組み立てる。これをリアセンブル（reassemble，再構築）という。

このような IP パケットのフラグメントとリアセンブルの処理負荷をかけないようにする工夫として，送信元ノードにおいて MTU を調整する方法が採られる。

トンネル区間におけるカプセル化と暗号化の処理を見越した，適切なサイズの MTU をあらかじめ送信元ノードに設定しておけば，仮に大きなサイズのアプリケーションデータを送信するときでも，送信元の段階で適切な MTU 単位で IP パケットを生成して送信してくれる。つまり，トンネル区間の入口で分割する処理が不要となるわけだ。

問題文に述べられた，「インターネットを含む全てのインタフェースの MTU の値を 1,500 とする」という設定は，このような MTU の調整が適切に行われていないことを言い表している。したがって，この状況下でパケットを送信するなら，VPN ルータでフラグメント処理が，宛先ノードでリアセンブル処理が発生し得る。

よって，正解は「**フラグメントとリアセンブルの処理が発生する**」となる。

■設問 3

設問 3 は〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕について出題している。

本設問を首尾よく解くには，経路情報交換に用いている BGP の仕組み，BGP ピア，及び，本事例において BGP がどのように使用されているかを理解しておく必要がある。そこで，これらの点について，概要をまず解説する。

● BGP の仕組み

インターネットでは，IP アドレスの全空間を ICANN が管理しており，AS と呼ばれる組織に IP アドレスをまとめて割り振っている。そして，この AS 内で独自にポリシを定めて経路情報を維持運用し，他の組織に IP アドレスを割り当てている。

この AS は，具体的に言うと，大規模な ISP，地域ネットワークなどである。そして，AS が IP アドレスブロックを割り当てる，より小規模のサイトには，中規模の ISP，企業，大学などがある。

このように経路情報は階層構造で管理されており，そこで使用されるルーティングプロトコルもそれぞれ異なっている。

プロトコルを大別すると，AS 間で使用される EGP（Exterior Gateway Protocol），AS 内で使用される IGP（Interior Gateway Protocol）に分類できる。

本問に登場する BGP は，EGP の代表的なプロトコルである。

同じく本問に登場する OSPF は，IGP の一種である。これは，比較的大規模な AS 内でよく用いられている。

今日，インターネットのバックボーンで交換される経路情報の総数（フルルート）は，IPv4 が 60 万超，IPv6 が 4 万超もある（2017 年 12 月現在）。

BGP は，この膨大な数に上る経路情報の交換を実現するために，様々な工夫が取り入れられている。

その主なものを幾つか挙げよう。

1. 経路が変化したときだけ差分を送信する仕組みにより，経路情報の交換にかかるトラフィックを抑えている。
2. 交換する経路情報は，NLRI（Network Layer Reachability Information）とパスアトリビュートである。経路選択はパスアトリビュートによって行われる。これには様々な種類があり，AS のポリシに基づく柔軟な経路選択を可能にしている。

2 番目に挙げた点を簡潔に補足する。

NLRI は，ネットワークアドレスとサブネットマスクの組である。

パスアトリビュートは，数ある経路の候補の中からベストパス（NLRI）を一つ選択するために用いられる。このベストパスが，ルーティングテーブル上の経路選択に使用される。

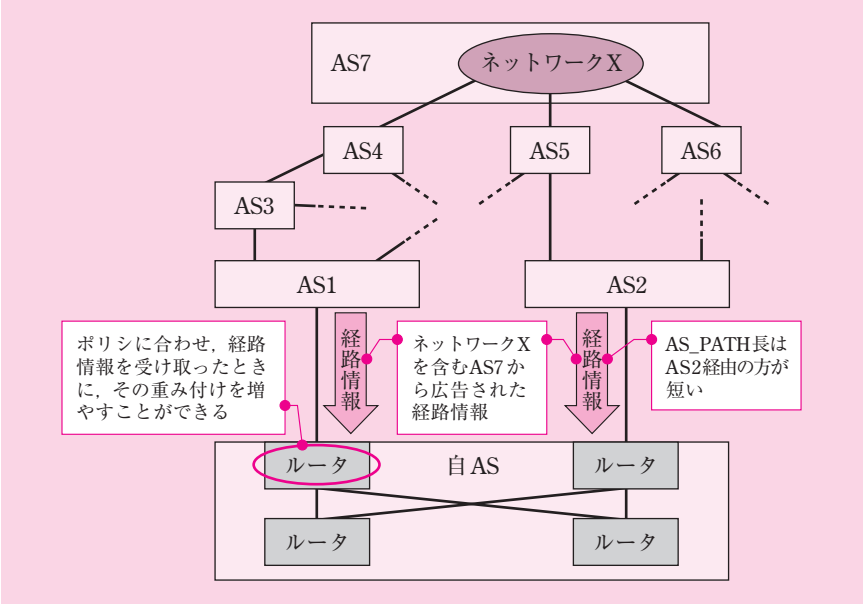
パスアトリビュートは，他のルーティングプロトコルのメトリックに相当するものだ。RIP では距離が，OSPF ではコストが用いられているのに対し，BGP では様々な

種類の属性が定義されているという特徴をもつ。

本問に登場するものだけでも，MED，AS_PATH がある。他にも LOCAL_PREF などがあり，それら属性には優先順位が定められている。

数々のパスアトリビュートを調整することで，AS は，自ら定めたポリシに基づいてベストパスを選択することができる。

例として，次の図に示すネットワークを使って説明する。自 AS は，あるネットワーク X に至る経路情報を AS1 と AS2 から受け取っているとしよう。要は，自 AS からネットワーク X に到達できる経路として，AS1 経由と AS2 経由の 2 通りがあるわけだ。



図：BGP のパスアトリビュートを活用した経路制御

このとき，例えば次のような経路制御が可能となる。

- パスアトリビュートの AS_PATH を見ると，ネットワーク X に到達するまでに通過する AS のパス長は，AS1 経由が「AS1 → AS3 → AS4 → AS7」の 4 個分であり，AS2 経由が「AS2 → AS5 → AS7」の 3 個分なので，AS2 経由の方が短い。そこで，AS2 経由の方をベストパスにしよう。

- パスアトリビュートの AS_PATH に基づけば，AS2 経由の方を選択するのが適切だ。しかし，このたびは意図的に AS1 経由の方を選択したい。これを実現するため，AS1 から受け取った経路情報に，パスアトリビュートの LOCAL_PREF を設定して重み付けを増やし，AS1 経由がベストパスになるように自 AS 内の全 BGP ルータに学習させよう（これは，LOCAL_PREF の方が AS_PATH より優先順位が高いことを利用した設定である）。

この例に示したように，ポリシに基づくきめ細かな設定を実施することで，AS は膨大な経路情報の交換を適切に制御し，日々運用しているのである。

● BGP ピア

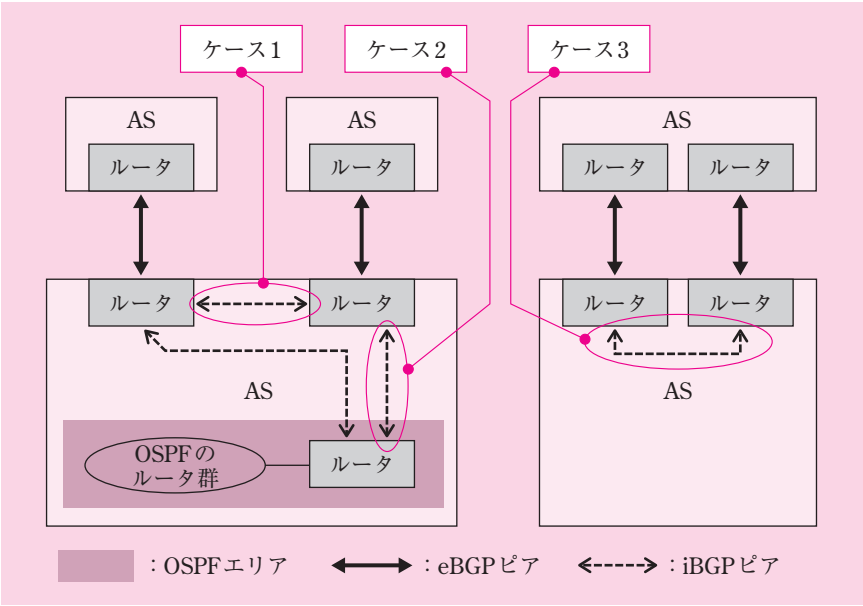
BGP 接続を行う 2 台のルータ間では，TCP の 179 番ポートを使用し，経路情報の交換を行う。このコネクションを BGP ピアと呼ぶ。

自 AS の BGP ルータは，他 AS の BGP ルータと BGP ピアを設定し，経路情報を交換している。このように，異なる AS に属するルータ間で設定される BGP ピアを，eBGP ピア（external BGP ピア）と呼ぶ。

自 AS の BGP ルータは，自 AS 内の別の BGP ルータとも BGP ピアを設定し，経路情報を交換している。このように，同じ AS に属するルータ間で設定される BGP ピアを，iBGP ピア（internal BGP ピア）と呼ぶ。

iBGP ピアを設定する目的は，自分が受け取った経路情報を，ピアを張る相手に伝えるためである。ただし，どのように伝え合うかに着目すると，その役割には幾つか種類がある。

主だったケースを三つ示す。本事例はケース 3 に該当するので，頭に入れておこう。



図：eBGP ピアと iBGP ピア

・ケース 1：他 AS の情報を共有する

この iBGP ピアは，自 AS の境界に位置する 2 台の BGP ルータが，それぞれ異なる AS から経路情報を受けている。この経路情報を自 AS 内で共有している。

・ケース 2：自 AS の内部に情報を伝える

この iBGP ピアは，自 AS の境界に位置する BGP ルータが，自 AS の内部に位置する BGP ルータに経路情報を伝えている。AS 内では OSPF が稼働しており，この内部 BGP ルータに接続している。

この内部 BGP ルータでは，BGP と OSPF の二つが稼働している。このルータは，OSPF ルータから転送されたパケットを受け取った後，今度は BGP の経路情報を使ってルーティングし AS 外へと転送する役割をもつ。さらに，境界 BGP ルータから転送されたパケットを受け取った後，今度は OSPF の経路情報を使ってルーティングし AS 内へと転送する役割をもつ。いわば，このルータは OSPF と BGP の間を橋渡しする存在だ。

なお，小規模なネットワークであれば，境界のルータが橋渡しする役割も兼

務すればよい。ケース 2 のような，橋渡しするための BGP ルータを内部に別途設ける必要はない。

本事例の K 社拠点は，そのような小規模なネットワークの例と言える。ここでは，境界に位置するルータ（VPNa1，VPNb1）で，BGP と OSPF の二つが稼働しており，OSPF と BGP の橋渡しも併せて実施している。

・ケース 3：隣接 AS 間の経路を冗長化する

この iBGP ピアは，隣接 AS との経路の冗長化を目的に，iBGP ピアを張る 2 台の BGP ルータがともに隣接 AS と接続している。

本事例では，K 社 NW と L 社クラウドサービスが隣接 AS となっており，両 AS 間を接続する VPN トンネルを冗長化している。

通常，iBGP ピアは，AS 内の全ての BGP ルータ同士でフルメッシュ接続する。iBGP ピアを張る相手から学習した経路情報は，他の iBGP ピアに通知しない。これは，AS 内で BGP によるルーティングループを防ぐためである。

本事例では，K 社拠点の BGP ルータ（VPNa1，VPNb1）は 2 台しかないので，両者で iBGP ピアを設定した時点でフルメッシュが完成している。

iBGP ピアで結ばれた 2 台の BGP ルータは，直に接続していなくてもよい。つまり，非 BGP ルータ（BGP が稼働していないルータ）を中継していても構わない。その場合，それら 2 台の BGP ルータ，及び，それらを中継する位置にある非 BGP ルータは，全て，何らかの IGP（例えば OSPF）が稼働している必要がある。2 台の BGP ルータがやり取りするパケットは，IGP の経路制御により，AS 内でルーティングされる。

本事例では，K 社拠点の BGP ルータは同じ VPN セグメントに収容されているので，この iBGP ピアは直に接続している。

●本事例における BGP の使用

先の「● BGP の仕組み」では，インターネットバックボーンにおける BGP の利用を念頭に置いて，ごく一般的な説明を述べた。

しかしながら，本事例に登場する BGP は，K 社 NW と L 社クラウドサービスのネットワーク接続でのみ使用する。インターネットバックボーンで取り交わされる膨大な経路情報を広告する目的で使用しているわけではないのだ。

このように用途を限定していると言える根拠は，本文中の 2 か所の記述である。

一つ目の根拠は，〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕の第 7 段落に記されている。そこには，「VPNa2 と VPNb2 は，それぞれ VPNa1 と VPNb1

に対し，L 社クラウドサービス内のサーバセグメントの経路だけ BGP で経路広告する」とある。L 社拠点のサーバセグメントだけとあるので，K 社 NW と L 社クラウドサービスのネットワーク接続でのみ使用することが分かる。

二つ目の根拠は，K 社拠点が使用する AS 番号が，プライベート AS 番号（64512 ～ 65534）だからである。この点は，第 5 段落に記されている。そこには，K 社拠点にある VPN ルータについて「VPNa1 と VPNb1 では 65505 を使用（する）」とあるので，プライベート AS 番号であることが分かる。

プライベート AS 番号は，自 AS 内で閉じたネットワークでのみ使用することができ，インターネットに経路広告してはならない。ちょうど，IPv4 のプライベート IP アドレスをインターネットで使用できないのと同じだ。したがって，本事例に登場する BGP は，K 社 NW と L 社クラウドサービスのネットワーク接続でのみ使用することが分かる。

なお，「VPNa2 と VPNb2 では L 社クラウドサービスが割当てを受けている 64496 を使用する」とある。L 社はクラウド事業者なので，インターネットで経路広告するために ICANN から AS 番号を割り当てられている。本事例の K 社拠点との閉じたネットワーク接続に際し，この AS 番号を流用している。

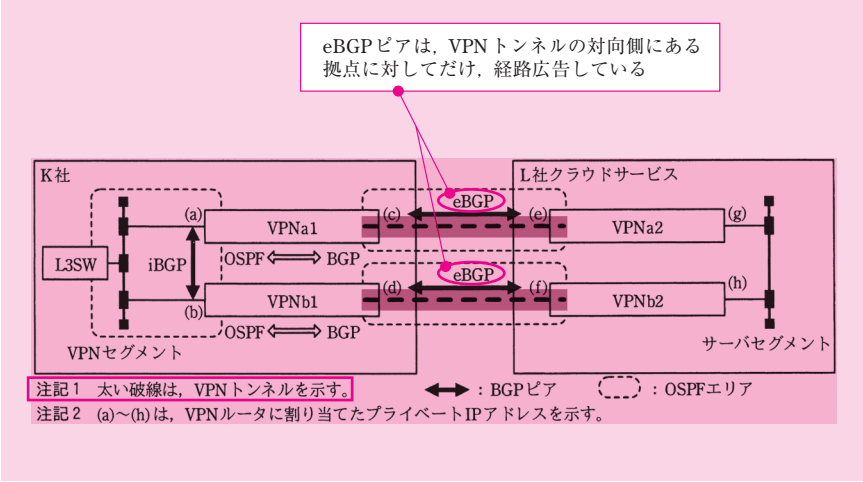
この点を踏まえて，本文の図 2「K 社 NW と L 社クラウドサービスとの経路情報の交換の概要」を見てみよう。

注目すべきは，K 社拠点と L 社拠点を接続しているのが，VPN トンネルである，という点だ。先ほど，「本事例に登場する BGP は，K 社 NW と L 社クラウドサービスのネットワーク接続でのみ使用する」「インターネットバックボーンで取り交わされる膨大な経路情報を広告する目的で使用しているわけではない」と述べたとおり，この図 2 においては，K 社拠点と L 社拠点の間に，インターネットが介在していないのだ。

要するに，図 2 のネットワークは，設問 2 全体の解説中の「●本事例の VPN 接続における，IP in IP と IPsec の使用」で述べた，「仮想的に見えるネットワーク」なのである。

この VPN トンネルは，仮想的な専用線の役割を果たしている。2 本の VPN トンネルの両端には，プライベート IP アドレス（c）～（f）が割り当てられている。

1 本の VPN トンネルの両端に BGP ルータが接続しており，これら 2 台の BGP ルータ間で eBGP ピアを設定している。この eBGP ピアは，VPN トンネルの対向側にいる相手ルータに対してのみ，経路広告している。



図：K 社 NW と L 社クラウドサービスとの経路情報の交換の概要（図 2 の抜粋）

なお，〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕の第 7 段落では，L 社拠点の VPN ルータのみ取り上げて，自拠点の経路を広告する旨，述べている。

それでは，本文には明記されていないものの，K 社拠点の VPN ルータも，同じように，自拠点の経路を広告していると言えるのだろうか。

eBGP ピアを設定している以上，そのように考えるのが自然である。しかも，このたびのネットワーク接続では，拠点間をつなぐ経路を冗長化している。VPN トンネルの障害発生時に，両拠点の BGP ルータが双方同時に経路情報を動的に切り替えるためにも，BGP を用いた経路制御を双方が同じように実施しているものと考えられる。

実を言うと，同見出しの第 10 段落，O さんと I 主任の会話を注意深く読むと，K 社拠点の VPN ルータが L 社側に経路広告していることが見て取れる。その点は設問 3 (3) のところで解説しよう。

試験では，正解を導くのに必要な手掛かりは記載しているが，あまり関係がない詳細な情報をあえて省略し，受験者の注意をそらさないように配慮することがある。L 社拠点側の設定（iBGP ピアや IGP の設定，等）に深入りしていないのは，そうした事情による。

本書では，「eBGP ピアを張る 2 台の VPN ルータが互いに経路広告している」と素直に解釈して，以降の解説を述べることにする。

ここまで理解できれば，設問 3 を解く準備は整った。それでは，いよいよ小問の解

説に移ろう。

(1)

解答例

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。 (33字)

問題文は,「本文中の下線③について，静的経路制御と比較して動的経路制御を選択した利点を……述べよ」と記述されている。

下線③は,〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕の第 1 段落にある。そこには,「L 社クラウドサービスとのネットワーク接続では，静的経路制御，又は BGP を用いた動的経路制御を選択できる。O さんは，③ BGP を用いた動的経路制御を選択した」と記述されている。

一般的に言って，静的経路制御と比較して動的経路制御がもつ利点は，経路障害の発生を動的に検知し，適切な迂回経路を選択してルーティングテーブルを動的に更新してくれることである。もちろん，この動的な更新は迂回経路があるときに限るが。

この障害検知は,「経路」，すなわち，経路上にある機器，回線の全てが対象に含まれる。

したがって，経路の耐障害対策を講ずる場合，この利点を活かし，迂回経路を用意した上で，動的経路制御を導入するのが一般的である。

本事例では，L 社クラウドサービスとのネットワーク接続に，VPN トンネルを採用している。この VPN トンネルは冗長化されている。この点について,〔クラウドサービスとのネットワーク接続の検討〕の第 2 段落の 3 番目の箇条書きに,「VPN トンネルは，VPNa1 側をアクティブ，VPNb1 側をスタンバイとする」と記述されている。

したがって，VPN トンネルの冗長化，すなわち，経路の耐障害対策を意図していることが分かる。

動的経路制御を採用すれば，前述のとおり人手を介さずに，VPN トンネルのフェールオーバを実現できる。

一方，静的経路制御では，機器や回線の障害を検知することにせよ，ルーティングテーブルを変更して迂回経路を設定することにせよ，全て手動で行わなければならない。障害切替えにかかる時間と労力を考えると，動的経路制御が勝っている。

したがって，この内容を字数に収まるように解答すればよい。

よって，正解は解答例に示したとおりとなる。

(2)

解答例

H	e	l	l	o	パ	ケ	ッ	ト	を	出	さ	な	い	。

（15字）

問題文は，「本文中の下線④について，パッシブインタフェースの動作の特徴を，……述べよ」と記述されている。

下線④は，〔K社 NW と L社クラウドサービスとの経路情報の交換の検討〕の第 8 段落にある。そこには，OSPF の設定について，次のように記述されている。

> K社 NW の VPN セグメントと接続する VPNa1, VPNb1 及び L3SW の各インタフェースでは OSPF のエリア 0 を構成し経路情報の交換を行う。さらに，IP in IP で作成されたトンネルインタフェースでは，OSPF のエリア 0 を構成するが，④経路情報の交換を行う必要がないのでパッシブインタフェースとする。

これは一般的な知識から解を導くことができる。

複数の OSPF ルータから構成された OSPF のエリアを，頭に思い描いてみよう。

ある OSPF ルータは，エリアの内側に位置しており，他の OSPF ルータに囲まれている。この OSPF ルータは，全てインタフェースで，他の OSPF ルータとの間で OSPF の通信を行う。すなわち，互いに Hello パケットで死活監視し，隣接関係にある OSPF ルータに対してリンクステート情報を送信する。

これとは異なり，別の OSPF ルータは，エリアの縁側に位置している。すなわち，自分が接続しているネットワークのうち，一部は OSPF ルータが隣接しているものの，残りには OSPF ルータが存在していない（ルータが全く存在していないか，あるいは，非 OSPF ルータのみ存在している）。この OSPF ルータは，他の OSPF ルータが存在するインタフェースでのみ，OSPF の通信を行っている。

今，注目したいのは，後者の OSPF ルータである。

この縁側にいる OSPF ルータは，OSPF ルータが存在していないインタフェース上で，OSPF の通信を行う必要がないが，そのネットワークの経路情報を伝える必要がある。このとき，当該のインタフェースをパッシブインタフェースに設定するのだ。

通常，OSPF ルータが稼働していると，ルータが接しているネットワークの経路情

報は，（ルータのインタフェースが通常であるかパッシブであるかにかかわらず），リンクステート情報としてエリア内に通知される。

インタフェースが通常であるかパッシブであるかの相違点は，OSPF のパケットをそのインタフェースから送信するか否かである。

通常のものであれば，インタフェースから Hello パケットを定期的に送信する。その結果，インタフェースに接しているネットワークにおいて，隣接関係を結んだ OSPF ルータとの間で経路情報を交換する。その逆に，パッシブインタフェースにすると，Hello パケットを送信しない。その結果，隣接関係を結ぶ相手がそもそもいないわけだから，リンクステート情報も送信しなくなるである。

よって，正解は「**Hello パケットを出さない**」となる。

正解は導いたが，第 8 段落の記述を振り返り，OSPF の設定を確認しておこう。

ここには，まず，「VPN セグメントと接続する VPNa1，VPNb1 及び L3SW の各インタフェースでは OSPF のエリア 0 を構成し経路情報の交換を行う」と記述されている。「OSPF エリア 0 を構成している」とあるので，VPN トンネルのネットワークは，経路情報としてエリア内に広告される。「経路情報の交換を行う」とあるので，VPN セグメントに接続するルータのインタフェースは，通常のものに設定している。

次いで，「IP in IP で作成されたトンネルインタフェースでは，OSPF のエリア 0 を構成するが，経路情報の交換を行う必要がないのでパッシブインタフェースとする」と記述されている。

こちらも「OSPF エリア 0 を構成している」とあるので，VPN トンネルのネットワークも，経路情報としてエリア内に広告される。「経路情報の交換を行う必要がない」とあるが，その理由は，トンネルの対向側にある L 社拠点の VPN ルータは OSPF ルータではないからだ。そのため，経路情報（OSPF のリンクステート情報）を交換する必要がない。この点は VPNb1 も同様だ。それゆえ，トンネルインタフェースは，「パッシブ」に設定している。

(3)

解答例

A：大きく

問題文は，「本文中の［ A ］に入れる適切な字句を答えよ」と記述されている。

空欄 A は，〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕の第 10

段落，O さんの 2 番目の発言の中にある。

この第 10 段落では，「VPNa1 側をアクティブ，VPNb1 側をスタンバイとする構成」を検討している。この文脈を押さえつつ，空欄 A の解を導くことにしよう。

●発言の要旨

I 主任の 1 番目の発言，これを受けた O さんの 2 番目の発言を要約すると，次のように整理できる。

- 通信の方向それぞれについて経路設計する必要がある。
- 社内から L 社クラウドサービスの方向は，L 社クラウドサービスを利用する PC からのパケットは全て L3SW に届くので，L3SW がパケットの転送先として，VPNa1 と VPNb1 のどちらを選択するか，転送先を決められるようにすればよい。
- VPNa1 と VPNb1 が，BGP で受けた経路情報を OSPF に再配布する際に，異なるコストを付与すると転送先を決めることができる。
- その処置として，VPNb1 側のコストを VPNa1 側と比べて［ A ］する。

●再配布

一連の発言の中で，「BGP で受けた経路情報を OSPF に再配布する」と記述されている。解を導くには，再配布について理解しておく必要がある。次にこの点を解説する。

BGP と OSPF など，複数のダイナミックルーティングプロトコルが稼働しているネットワークでは，一方のダイナミックルーティングプロトコルの経路情報を，他方のものに変換して受け渡すことができる。これを再配布（redistribution）という。

本事例に合わせて具体的に説明しよう。

・VPNa1 のルーティングテーブルと再配布

VPNa1 は，VPNa2 から L 社拠点のサーバセグメントの経路を広告される。VPNa1 のルーティングテーブルには，次のような経路情報がエントリされる。

宛先ネットワーク：L 社拠点のサーバセグメント
ネクストホップ　：VPNa2 のトンネルインタフェース（e）

この経路情報は BGP から得たものである。これを L3SW に経路広告したい

が，L3SW は BGP に対応していないので，そのまま伝えることができない。

そこで，VPNa1 上で再配布の設定を行い，この経路情報を OSPF の形式に変換してから，VPN セグメントに経路広告する。これが L3SW に伝わる。

・L3SW のルーティングテーブル

L3SW は，VPNa1 から L 社拠点のサーバセグメントの経路を広告される。それは次のような経路情報である。

宛先ネットワーク：L 社拠点のサーバセグメント
ネクストホップ　：VPNa1 の LAN インタフェース（a）

・VPNb1 のルーティングテーブルと再配布

VPNb1 は，VPNb2 から L 社拠点のサーバセグメントの経路を広告される。VPNb1 のルーティングテーブルには，次のような経路情報がエントリされる。

宛先ネットワーク：L 社拠点のサーバセグメント
ネクストホップ　：VPNb2 のトンネルインタフェース（f）

VPNb1 も同様に再配布の設定を行い，VPN セグメントに経路広告する。これも L3SW に伝わる。

・L3SW のルーティングテーブル

L3SW は，VPNb1 からも L 社拠点のサーバセグメントの経路を広告される。それは次のような経路情報である。

宛先ネットワーク：L 社拠点のサーバセグメント
ネクストホップ　：VPNb1 の LAN インタフェース（b）

こうして，L3SW は，L 社拠点のサーバセグメントに到達する経路情報を二つもつことになる。一つは VPNa1 から広告されたもの，もう一つは VPNb1 からのものである。

二つの経路情報に異なる優先度を設定することにより，優先度の高い方をアクティブ，低い方をスタンバイとする冗長構成を実現できる。

●社内から L 社クラウドサービス方向の経路設計

本事例では，「VPNa1 側をアクティブ，VPNb1 側をスタンバイとする構成」にするので，VPNa1 から広告された方を優先するように設定する。

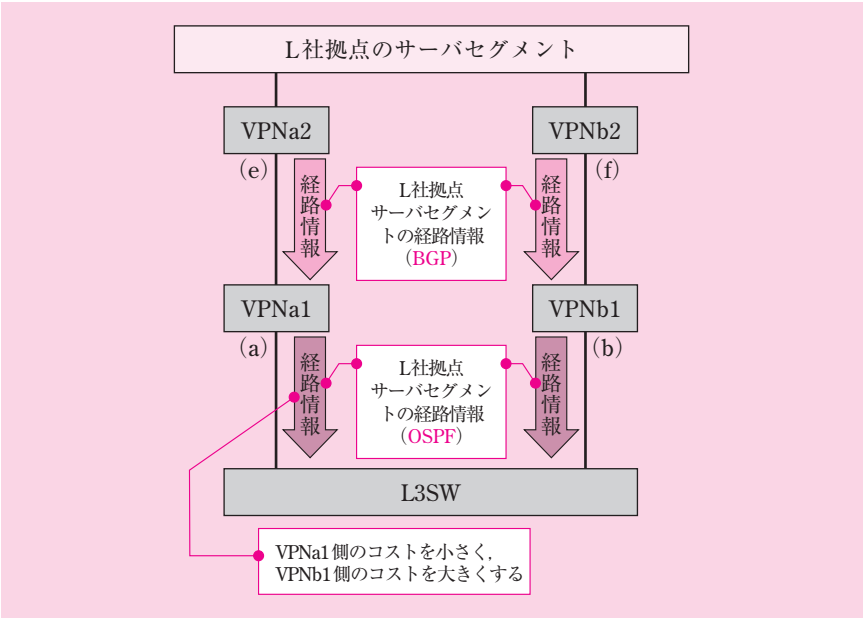
再配布の解説で述べたとおり，L3SW のルーティングテーブルには，L 社拠点のサーバセグメントの経路情報が二つある。正常時は，VPNa1 から広告された経路情報が選択される。しかし，VPNa1 側の VPN トンネルの障害発生時は，こちらの経路情報がなくなり，VPNb1 から広告された経路情報が残る。

以上により，社内から L 社クラウドサービスの方向について，VPN トンネルのフェールオーバを実現することができる。

O さんの 2 番目の発言にある，「BGP で受けた経路情報を OSPF に再配布する際に，異なるコストを付与すると転送先を選択でき（る）」という記述は，VPNa1 から広告された方を優先するための処置を指している。

OSPF は，同じネットワークに到達する経路が複数ある場合，当該経路のコストを比較して，より小さい方を選択する仕組みになっている。

そこで，BGP で受けた経路情報を OSPF に再配布する際に，VPNa1 から広告される経路情報のコストを，VPNb1 のものより小さくすればよい。



図：社内から L 社クラウドサービス方向の経路設計

●解の導出

ここまで理解できれば，正解を導くことができる。

空欄 A を含む記述は，「VPNb1 側のコストを VPNa1 側と比べて［ A ］します」とある。したがって，ここに入る字句は，「**大きく**」となる。よって，これが正解となる。

●参考：L 社クラウドサービスから社内方向の経路設計

参考までに，L 社クラウドサービスから社内方向の経路設計について簡潔に解説しよう。

I 主任の 2 番目の発言，これを受けた O さんの 3 番目の発言を要約すると，次のように整理できる。

- L 社クラウドサービスから社内の方向は，BGP のパスアトリビュート AS_PATH を使う。
- AS_PATH は，AS_PATH 長が短い方が選択される。

AS_PATH は，宛先ネットワークに至る経路（パス）を表す属性である。このパスが，「AS 番号の羅列」で記述されている。

具体例を挙げて説明しよう。

ここに，AS1，AS2，AS3 という三つの AS があるとする。

AS1 が自ネットワークを経路広告するとき，AS_PATH は「AS1」である（見やすくするために「AS1」という AS 名を記したが，本当は AS 番号である）。

AS2 がこれを受け取り，AS3 に経路広告するとしよう。このとき AS2 は，AS_PATH の先頭に「AS2」を追加してから広告する。この結果，AS2 が経路広告する，「AS1 ネットワークの経路情報」の AS_PATH は，「AS2 AS1」となる。

AS3 がこれを受け取ると，AS1 ネットワークに到達するには「AS2 → AS1」というパスを通ることが分かる。

もしかすると，AS3 は，他の AS からも AS1 ネットワークの経路情報を広告されるかもしれない。AS_PATH に基づいてベストパスを決定するときは，AP_PATH 長が短いものを選択する仕様になっている。要するに，経由する AS の合計数が少ない方を優先するわけだ。

通常，BGP は，特にパスアトリビュートの調整をしなければ，AS_PATH に基づいてベストパスを選択する。BGP が経路ベクトル方式と呼ばれる理由はここにある。

L 社クラウドサービスから社内方向の経路設計は，この仕組みを利用している。

VPNa1 は，K 社拠点のネットワーク（VPN セグメント，サーバセグメント，クライアントセグメント）の経路を VPNa2 に広告する。このとき設定する AS_PATH は，K 社の AS 番号「65505」である。

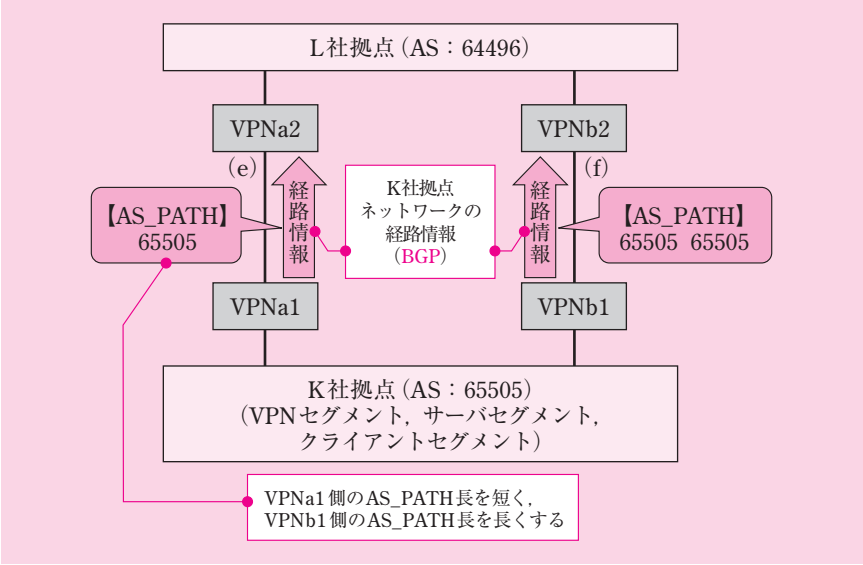
同様に，VPNb1 も，K 社拠点のネットワークの経路を VPNb2 に広告する。このとき，AS パスプリペンドと呼ばれる手法を用い，AS_PATH に，K 社の AS 番号を複数設定する。すなわち，「65505 65505」とするのである。

本事例では，「VPNa1 側をアクティブ，VPNb1 側をスタンバイとする構成」にするので，VPNa1 から広告された方を優先するように設定する必要があるからだ。

この結果，L 社拠点の VPN ルータのルーティングテーブルにおいて，正常時は，VPNa1 から広告された経路情報が選択される。しかし，VPNa1 側の VPN トンネルの障害発生時は，こちらの経路情報がなくなり，VPNb1 から広告された経路情報が残る。

以上により，L 社クラウドサービスから社内の方向について，VPN トンネルのフェールオーバを実現することができる。

設問 3 全体の解説の「●本事例における BGP の使用」で述べたとおり，K 社拠点の VPN ルータは，L 社側に経路広告しているのだ。



図：L 社クラウドサービスから社内方向の経路設計

最後に，O さんの 3 番目の発言中にある「MED」について，簡潔に説明しよう。

MED（Multi Exit Discriminator）は，本事例のケースのように，隣接する AS 間で

複数のリンクを設ける際に適用される。複数あるリンクのうち優先させたい側のMED値を小さく設定した上で，経路広告する。要するに，「こちらのリンクを優先してほしい」と隣接 AS に通知する役割を担っているわけだ。

MED に基づいてベストパスを決定するときは，MED 値が小さいものを選択する仕様になっている。

このようにBGPには様々なパスアトリビュートがある。複数の属性が設定されているときは，属性の優先順位に従ってベストパスを決定する仕組みになっている。AS_PATH と MED を比較した場合，AS_PATH の優先順位が高い。

(4)

解答例

e	B	G	P	か	ら	O	S	P	F	へ	再	配	布	さ	れ	た	経	路	を	再	び	e	B	G	P
へ	再	配	布	し	な	い	。																		

（34字）

問題文は，「本文中の下線⑤について，経路のループを防止するために必要な経路制御を……述べよ」と記述されている。

下線⑤は，〔K 社 NW と L 社クラウドサービスとの経路情報の交換の検討〕の第 10 段落，O さんの 4 番目（最後）の発言の中にある。

設問 3（3）で解説したとおり，この第 10 段落では，「VPNa1 側をアクティブ，VPNb1 側をスタンバイとする構成」を検討している。その実現方法として，社内から L 社クラウドサービス方向の経路設計では，BGP で受けた経路情報を OSPF に再配布する手法を採用しようとしている。

ここまでの話の流れを踏まえて，I 主任は，3 番目の発言の中で，「一点注意が必要です。経路情報の再配布を行うときには，経路のループを防止しなければいけません」と述べている。

これを受けて，O さんの 4 番目の発言がある。O さんは，「分かりました。⑤経路のループを防止する経路制御を行います」と述べている。

したがって，ここで問われていることは，経路情報の再配布に起因する経路のループを防止するために，どのような経路制御を行ったらよいか，という点である。

本小問は，一般的な知識から解を導くことが求められている。

そのように言える根拠は，本文の中で，経路のループ防止を具体的に検討するに足る十分な情報が記載されていないからだ。

本書の序章「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」で触れたが，試験に取り組むとき，本文に書かれていない条件を無理に加えたりしないようにしたい。事例に特化した具体的な解を導くだけの情報が読み取れなかったら，「出題者は一般的な知識を問うているに違いない」と割り切って，最も妥当な答を述べればよい。

それでは，経路情報の再配布に起因する経路のループ発生について，及び，それを防止する方法について，ごく一般的な説明を述べる。その後，字数を満たすような答を求めることにしよう。

●経路情報の再配布に起因する経路のループ発生

経路情報の再配布は，二つのダイナミックルーティングプロトコルの間で行われる。便宜的に，これらプロトコルを P1，P2 と名付けよう。

再配布をするルータでは，P1 と P2 が両方とも稼働している。今，このルータで，P1 から P2 に再配布するものとしよう。このとき，P2 の属性（例えば，OSPF のコスト等）の値を適宜付与した上で，P2 の形式に経路情報に変換する。その後，P2 が稼働しているネットワークに向けて経路広告する。

経路のループは，P1 から P2 に再配布された経路情報が，P1 に改めて再配布されることによって，つまり，再び自分に戻されることによって，発生し得る現象である。

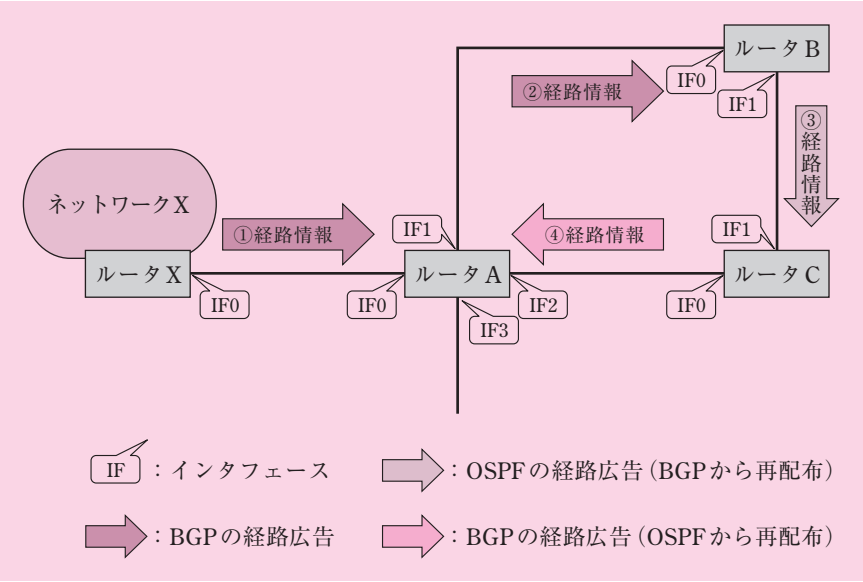
もっとも，再び自分に戻されたとしても，経路のループが必ず発生するわけではない。再び戻されたときに付与される属性の値によって，ループが発生する可能性があるのだ。

具体例を挙げて説明しよう。

次の図に示すネットワークは，BGP と OSPF の二つのダイナミックルーティングプロトコルが稼働している。なお，予めお断りしておくが，経路のループに着目するため，この図にはルータ間の経路広告がすべて記載されているわけではない（例：ルータ A→ルータ C，ルータ C→ルータ B の経路広告などを省略）。

これから説明する四つの手順（①から④）によって，ここに経路のループが生じる。

注目すべきは，ルータ A がもつ，ネットワーク X の経路情報である。



図：再配布によって経路のループが発生する手順

・手順①：ルータ A

ルータ A は，図の左側にあるネットワーク X の経路情報（BGP）を，ルータ X よりインタフェース IF0 から受け取る。

この時点で，ルータ A は次に示す経路情報をもつ。

宛先ネットワーク：ネットワーク X
ネクストホップ　：ルータ X の IF0

本来，ルータ A は，宛先 IP アドレスがネットワーク X である IP パケットを受け取ったとき，この経路情報に基づいてインタフェース IF0 に転送しなければならない。この点を念頭に置いて，続きを読んでいただきたい。

・手順②：ルータ B

ルータ B は，ネットワーク X の経路情報（BGP）を，ルータ A よりインタフェース IF0 から受け取る。

この時点で，ルータ B は次に示す経路情報をもつ。

宛先ネットワーク：ネットワーク X
ネクストホップ　：ルータ A の IF1

その後，ルータ B は，この経路情報を OSPF に再配布する。

・手順③：ルータ C

ルータ C は，ネットワーク X の経路情報（OSPF）を，ルータ B よりインタフェース IF1 から受け取る。

この時点で，ルータ C は次に示す経路情報をもつ。

宛先ネットワーク：ネットワーク X
ネクストホップ　：ルータ B の IF1

その後，ルータ C は，この経路情報を BGP に再配布する。

・手順④：再びルータ A

ルータ A は，ネットワーク X の経路情報（BGP）を，ルータ C よりインタフェース IF2 から受け取る。

この時点で，ルータ A は二つの経路情報をもつことになる。

一つは，手順①で受け取ったものである。

もう一つは，今，この手順④で受け取った，次に示す経路情報である。

宛先ネットワーク：ネットワーク X
ネクストホップ　：ルータ C の IF0

再配布では，属性の値を比較的自由に付与することができる。

もしも，手順④の経路情報の属性が，手順①のそれに比べて，高い優先度をもつ値に設定されていたならば，どうなるだろうか。

このとき，ルータ A は，手順④の経路情報に基づいて，ルーティングしてしまうのだ。

この結果，このネットワークにおいて，経路のループが発生する。

宛先 IP アドレスがネットワーク X であるパケットを，ルータ A が受け取ったとしよう。すると，このパケットは，次のように三つのルータの間を周回し続ける（TTL が 0 になるまで）。

ルータ A →ルータ C →ルータ B →ルータ A　……

●このループ発生を防止する方法

このループ発生の防止策は，幾つか考えられる。

一つ目の防止策は，「再配布したものを再び自分に再配布させないこと」である。

これは，比較的よく採られる方法だ。

前述の手順に適用してみると，手順③において，ルータ C が BGP の再配布を実施しなければ，手順④そのものが起こらないので，経路のループは発生しない。あるいは，ルータ C にルートフィルタリング（ある経路情報を広告するか否かをフィルタリングする技術）を設定しても，同様の効果が得られる。

二つ目の防止策は，「再配布したものを再び自分に再配布させるときは，属性値を慎重に付与すること」である。

これは，首尾よく成し遂げるのが結構大変な方法だ。

前述の手順に適用してみると，手順④に至ったとき，ルータ A が，手順①で受け取った経路情報の方を優先すれば，経路のループは発生しない。それゆえ，手順③のルータ C が，BGP に再配布する際に，ループが発生しないように属性値を付与すればよいわけだ。ただ，ここで例示した簡素なネットワークはいざ知らず，数多くのサブネットワークとルータから構成された，現実に存在する大規模なネットワークでは，適切な属性値を見出すのは難しい作業となる。

三つ目の防止策は，もし可能であれば，「再配布しなくてすむよう，経路制御の方法を統一すること」である。一応，方法論としてはあるので，挙げておこう。とはいえ，現実には，本事例のようにルーティングプロトコルを統一できず，再配布せざるを得ない状況が起こり得る。そのときは先の二つの解決策のどちらかを採用する。

●解の導出

本事例では，社内から L 社クラウドサービス方向の経路設計において，eBGP から OSPF に再配布する方法を採っている。これを前提に解を導く必要がある。

したがって，ループ発生の防止策として，前述の一つ目と二つ目を選ぶことになる。

本問は，BGP や OSPF の事細かな情報を本文中に与えていない。それゆえ，一般的な知識から解を導くのが適切である。

したがって，一つ目の防止策に基づいて，解答すればよい。二つ目の防止策に基づいて解を導くのは，情報が足りないため，難しいと言わざるを得ない。

よって，正解は，「**eBGP から OSPF へ再配布された経路を再び eBGP に再配布しない**」となる。

■設問 4

解答例

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

（27 字）

問題文は，「本文中の下線⑥について，二つある VPN トンネルをそれぞれ監視する目的を……述べよ」と記述されている。

下線⑥は，〔ネットワーク監視の検討〕の第 1 段落の中にある。そこには，「⑥二つある VPN トンネルがそれぞれ正常に稼働しているかを常に確認する」と記述されている。

これは一般的な知識から解を導くことができる。

本事例は，二つの拠点を接続する VPN トンネルを，アクティブ／スタンバイ方式で冗長化している。

このように冗長化した構成において，アクティブ側とスタンバイ側の双方を監視する理由は，障害発生によって冗長構成が失われたことを検出するためである。

アクティブ／スタンバイ方式を採っているため，アクティブ側の障害発生時にはフェールオーバする。スタンバイ側の障害発生時にはフェールオーバのような目立った動きは起こらない。どちらにせよ，単一障害（アクティブ又はスタンバイのいずれか一方で障害が発生すること）の発生では，業務は継続できる。フェールオーバ時の短時間の停止で済むだけだ。

このとき，単一障害のまま，放置してはならない。なぜなら，もし二重障害（アクティブ及びスタンバイの双方で障害が発生すること）に見舞われたなら，業務が継続できなくなるからである。

そのような最悪の事態に陥らないように，単一障害を確実に検出し，いち早く本格復旧しなければならない。つまり，元どおりの冗長構成を取り戻すわけだ。

その第一歩となるのが監視である。アクティブ側とスタンバイ側の双方の正常性を確認することが必要不可欠となる。

よって，正解は，「**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**」となる。