平成 30 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，社内グループウェアをクラウド上の SaaS に移行する事例が増えてきている。それに伴い，ネットワークトラフィックの流れに大きな影響が生じ，ネットワーク構成の変更をしなければならなくなることがある。特に，グループウェアの膨大なセッション数と増加するインターネットトラフィックをさばくためのプロキシサーバやファイアウォール構成は，検討が必要なポイントとなる。

また，機器設定の集中管理のために SDN（Software-Defined Networking）技術を導入する事例も増加傾向にある。

本問では，SaaS を利用する場合に密接に関連するネットワークやセキュリティの知識及び SDN の IPsec VPN への応用である SD-WAN についての知識を問う。

採点講評

問 1 では，社内グループウェアのクラウドへの移行を題材として，SaaS を利用する場合に密接に関連するネットワークやセキュリティの知識及び SDN（Software-Defined Networking）の IPsec VPN への応用である SD-WAN についての知識について出題した。

設問 2(1)は，暗号化されている HTTPS プロトコルをプロキシサーバで処理するために必要な HTTP の CONNECT メソッドについて出題したが，正答率は低かった。HTTPS の利用が増えてきた今日，CONNECT メソッドは，便利な技術である反面セキュリティホールとなる可能性のある技術であるので，よく理解しておいてほしい。

設問 3 は，SD-WAN によって SaaS へのトラフィックだけを迂回する方法について出題した。アプリケーションの通信先を制御するためには，ルーティングの変更とアプリケーションの経由先変更の両方に目を向ける必要があることに注意してほしい。

設問		解答例・解答の要点		備考
設問 1	(1)	ア	フォワード	
		イ	リバース	
	(2)	利用者 ID		
設問 2	(1)	メソッド名	CONNECT メソッド	
		対策	HTTPS 以外のポートの CONNECT を拒否する。	
	(2)	ウ	プロキシサーバのルート証明書	
設問 3	(1)	エ	コントロール	
	(2)	ネクストホップが SD-WAN ルータとなるデフォルトルート		
	(3)	オ	SD-WAN コントローラ	
	(4)	G 社 SaaS への HTTPS 通信		
	(5)	①	・社内 PC から G 社 SaaS へのアクセスがプロキシサーバを経由しなくなるから	
		②	・出張先の PC から G 社 SaaS へのアクセスが記録されるから	

本問は，本社と四つの営業所を拠点にもつネットワークにおいて，SaaS の導入に伴う性能劣化を解消するため，トラフィック経路を分散させる事例を取り上げている。

本問は，プロキシサーバについて出題している。詳しくは本書の第 8 章「8.3.2　プロキシ」を参照していただきたい。

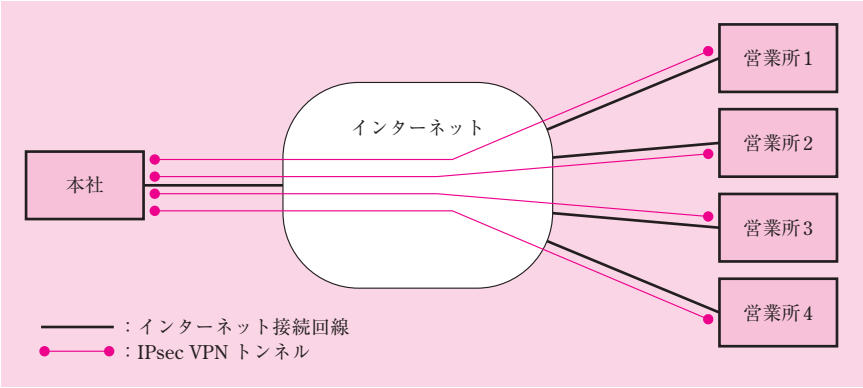
●本問の全体像

・G 社 SaaS 導入を見越した，現行ネットワーク構成

事例に登場する F 社は，本社と四つの営業所を拠点にもつ。これら拠点の接続について，序文の第 1 段落には次のように記述されている。

> 本社を中心としたハブアンドスポーク構成の IPsec VPN を使って，本社と営業所を接続している。営業所からインターネットへの通信は，全て本社を経由させている。

「本社を中心としたハブアンドスポーク構成の IPsec VPN」とは，具体的に言うと，各営業所は本社とのみ IPsec のトンネルを構築していることを表している。

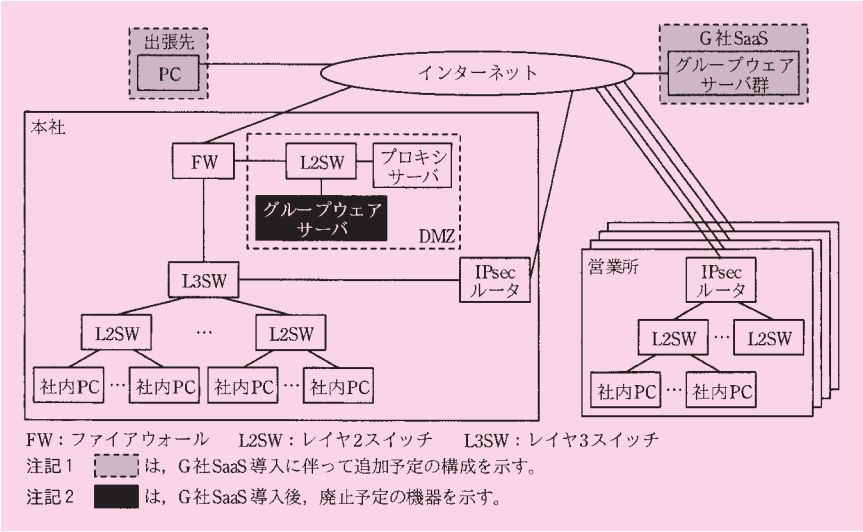


図：本社を中心としたハブアンドスポーク構成の IPsec VPN のトンネル

このたび F 社では，グループウェアサーバの老朽化に伴い，グループウェアサーバを廃止し，グループウェア機能（電子メール，スケジューラ，ファイル共有，等）をもつ G 社 SaaS を導入することにした。

SaaS にアクセスするのは，本社と営業所の社内 PC，出張先の PC である。

G 社 SaaS 導入を見越した現行ネットワーク構成は，本文の図 1 に示されている。



図：G 社 SaaS 導入を見越した現行ネットワーク構成（図 1 の抜粋）

G 社 SaaS を含むインターネットへのアクセスについて，序文の第 1 段落，及び〔F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策〕の第 1 段落の 3 番目の箇条書きの中で，次のように記述されている。

> 営業所からインターネットへの通信は，全て本社を経由させている。
> 社内 PC からインターネットへは，Web アクセスだけが許可されており，プロキシサーバを経由して通信を行っている。

社内 PC は本社と営業所にあるが，それぞれのインターネットへの通信経路は次のようになる。

［本社の PC からインターネットへの通信］
本社 PC → L3SW → FW →プロキシサーバ→ FW →インターネット
［営業所の PC からインターネットへの通信］
営業所 PC →営業所 IPsec ルータ→ IPsec トンネル（インターネット）
→本社 IPsec ルータ→ L3SW → FW →プロキシサーバ→ FW →インターネット

インターネットへの「Web アクセス」は，一般的に言って，HTTP 通信と HTTPS

通信の 2 種類がある。ただし，G 社 SaaS への通信は，HTTPS 通信に限定されている。この点について，〔F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策〕の第 3 段落，1 番目の箇条書きは次のように記されている。

・G 社 SaaS との通信は，HTTPS によって暗号化する。

さて，G 社 SaaS の本格導入に先立ち，システムの利便性と性能を確認するため，本社と一つの営業所を対象に少数ライセンスで G 社 SaaS を試用した。その結果，〔G 社 SaaS の試用〕の第 2 段落にあるとおり，性能劣化の問題が発覚した。

・G 社 SaaS にアクセスした際にプロキシサーバを通過するセッション数を実測したところ，スケジューラにアクセスする 1 人当たりのセッション数が大幅に増加した。
・複数人が同時に大容量のファイルを G 社 SaaS に転送している間，本社の FW を経由するインターネット接続回線のスループットが低下した。

このまま全社で G 社 SaaS の利用を開始すると，プロキシサーバの処理可能セッション数の超過，インターネット接続回線の帯域不足が予想された。

その問題を解決するため，SD-WAN（Software-Defined WAN）ルータを使用した，新しいネットワーク構成を採用することにした。

・SD-WAN ルータを使用したネットワーク構成

G 社 SaaS の試用で明らかになった性能劣化に対処する方法は，トラフィック経路の分散である。その点について，〔SD-WAN ルータの導入〕「(2) SD-WAN ルータを用いたときの通信」の第 1 段落には，次のように記述されている。

・社内 PC から G 社 SaaS への Web アクセスは，プロキシサーバを経由せず各 SD-WAN ルータを経由する。
・社内 PC から G 社 SaaS 以外のインターネットへの Web アクセスは，プロキシサーバを経由する。

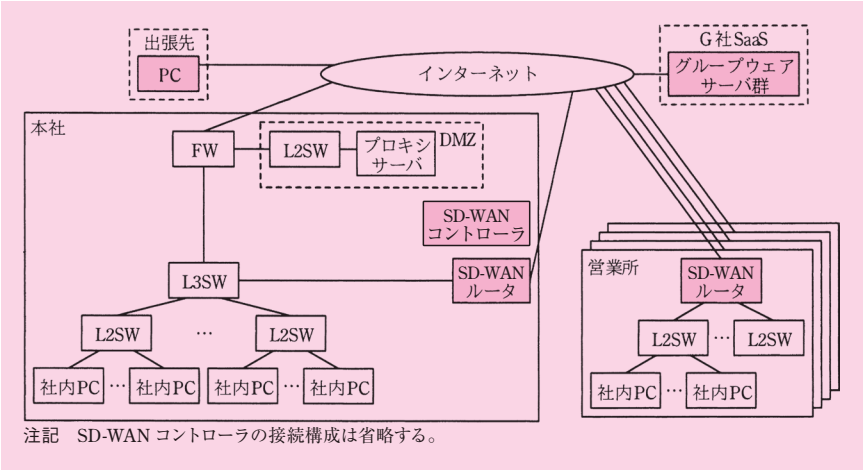
G 社 SaaS への Web アクセスは，各拠点の SD-WAN ルータからインターネットに直接出ていくようにする。このとき，SD-WAN ルータは，通常のルータとして動作する。

これに対し，G 社 SaaS 以外のインターネットへの Web アクセスは，従来どおりプ

ロキシサーバを経由する。

このようにトラフィック経路を分散した結果，プロキシのセッション超過，及び本社側インターネット接続回線の帯域不足が解消されるわけだ。

この解決策を適用した新しいネットワーク構成は，本文の図 2 に示されている。物理的な構成は，IPsec ルータが SD-WAN ルータに置き換わったこと以外に変化していないが，トラフィック経路が変化している。



図：SD-WAN ルータを使用したネットワーク構成案（図 2 の抜粋）

・G 社 SaaS の IP アドレスブロックの変更

〔SD-WAN ルータの導入〕「(3) SD-WAN ルータの運用」の第 1 段落によると，G 社 SaaS が利用している IP アドレスブロックは，随時更新される仕様になっている。

なお，本文には明記されていないが，G 社 SaaS の FQDN（ホスト名）は変化しない。よって，PC からアクセスする際は，DNS による名前解決で最新の IP アドレスを取得できる。

更新は G 社から RSS（Really Simple Syndication）により配信されるが，これに追随して通信装置のルーティングテーブルを変更するのは骨の折れる作業だ。その問題を解決するため，新しいネットワーク構成では次のような対策を講ずることにした。

［対策 1］L3SW の静的経路情報を変更し，G 社 SaaS の IP アドレスが変更された場合でもその都度 L3SW を設定しなくても済むようにする（「(2) SD-WAN ルータを用いたときの通信」の 3 番目と 5 番目の箇条書き）。
［対策 2］RSS 配信された G 社 SaaS の IP アドレスブロックを検知するツールを作成し，自動的にツールから全社の SD-WAN ルータの設定を変更する（「(3) SD-WAN ルータの運用」の第 2 段落）。

このような設定を施すと，本社のトラフィック経路は従来よりも多少複雑になる。この設定変更について設問 3 で問われているので，詳しくはそこで解説しよう。

・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
F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策	現行ネットワークの構成 図 1「F 社の現行ネットワーク構成（抜粋）」	1	(1) 空欄ア～イ
			(2)
G 社 SaaS の試用	プロキシ経由の HTTPS 通信	2	(1) ～ (2)
SD-WAN ルータの導入	SDN の知識	3	(1) 空欄エ
	L3SW の設定変更 SD-WAN の自動設定変更 プロキシの自動設定		(2) ～ (5)

それでは，設問の解説に移ろう。

■設問 1

本設問は，〔F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策〕の中から，プロキシサーバについて問うている。

（1）

解答例

ア：フォワード
イ：リバース

本小問は，本文中の空欄ア，イに入れる字句を問うている。

空欄ア，イは，〔F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策〕の第 2 段落の中にある。

そこには，まず，「一般に，プロキシには，［ア］プロキシと［イ］プロキシがある」と記述されている。

プロキシサーバは，フォワードプロキシとリバースプロキシの 2 種類がある。したがって，空欄ア，イには，両者のどちらかが当てはまるはずだ。

その点を踏まえて後続の記述を見ると，空欄の解を導くことができる。

［ア］

空欄アについて，「F 社のプロキシのように［ア］プロキシは，社内に対して，アクセス先 URL のログ取得や，外部サーバのコンテンツをキャッシュして使用帯域を削減する目的で用いられる」と記述されている。

ここで言及されている F 社のプロキシについて，第 1 段落の 3 番目の箇条書きの中で「社内 PC からインターネットへは，Web アクセスだけが許可されており，プロキシサーバを経由して通信を行っている」と記述されている。

社内 PC からインターネット上の Web サーバにアクセスする経路は，「社内 PC →プロキシ→インターネット」となる。このように，自拠点のクライアントの代理となりインターネットにアクセスするプロキシは，フォワードプロキシである。

よって，正解は「**フォワード**」となる。

［イ］

空欄イについて，「［イ］プロキシは，外部から公開サーバのオリジナルコンテンツに直接アクセスさせないことによる改ざん防止，キャッシュによる応答速度の向上，及び複数のサーバでの負荷分散を行う目的で用いられる」と記述されている。

ここに記されているように，このプロキシサーバを使用したとき，外部から自拠点の公開サーバにアクセスする経路は，「外部→プロキシ→公開サーバ」となる。

このように，自拠点の公開サーバの代理となりインターネットからのアクセスを受け付けるプロキシは，リバースプロキシである。

よって，正解は「**リバース**」となる。

(2)

解答例

利用者 ID

問題文は，「本文中の下線①について，プロキシサーバで認証を行うことによってアクセスログに付加できる情報を答えよ」と記述されている。

一般的に言って，プロキシサーバがログに記録する情報は，二つの方法で取得されたものである。

一つ目は，中継する HTTP パケットを解析することによって得られた情報である。具体例を挙げると，アクセス先 URL，送信元／宛先 IP アドレス，HTTP ステータス，HTTP ヘッダフィールド，等を記録することができる。

二つ目は，プロキシサーバが中継時に実施する処理から得られた情報である。本事例では，フォワードプロキシとして Web アクセスを中継するだけではなく，下線①にあるとおり，認証を行っている。それゆえ，中継処理に関する情報（アクセス時刻，等），認証処理に関する情報（利用者 ID，認証の成否，等）を記録することができる。

この点を踏まえ，プロキシサーバで取得するログについて見てみよう。

〔F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策〕の第 3 段落，3 番目の箇条書きには，次のように記述されている。

> - アクセス先 URL と利用者 ID

プロキシサーバのログのうち，「アクセス先 URL」は，Web サーバにアクセスする HTTP パケットに必ず格納されている。この情報は，前述のとおり，一つ目の方法（HTTP パケットの解析）によって取得したものである。

「利用者 ID」は，Web サーバの方で認証を行わない限り，これにアクセスする HTTP パケットには格納されない。一方，プロキシサーバで認証を行っているので，その処理から得ることができる。したがって，二つ目の方法で取得したものであると言える。

プロキシサーバが実施する認証は，社内 PC から社員がインターネットにアクセス

する際に実施するものなので，当該社員の真正性を確認する目的で実施している。具体的な認証方式は記されていないが，パスワード認証にせよトークン認証にせよ，利用者認証には，利用者を識別するための情報，すなわち利用者 ID が必要である。

したがって，利用者 ID は，プロキシサーバで認証を行うことによってアクセスログに付加できる情報であると言える。

よって，正解は，「**利用者 ID**」となる。

■設問 2

本設問は，〔G 社 SaaS の試用〕について問うている。

(1)

解答例

メソッド名：CONNECT メソッド

対策：H T T P S 以 外 の ポ ー ト の C O N N E C T を 拒 否 す る 。
（25 字）

問題文は，「本文中の下線②について，HTTPS でアクセスするための HTTP プロトコルのメソッド名を答えよ。また，このメソッドを用いる場合，社内に侵入したマルウェアによる通信（ただし，HTTPS 以外の通信）を遮断するためのプロキシサーバでの対策を……述べよ」と記述されている。

下線②は，〔G 社 SaaS の試用〕の第 1 段落の中にある。そこには，「プロキシサーバで HTTPS のアクセスログを確認したところ，②アクセス先のホスト名は記録されていたが，URL は記録されていなかった」と記述されている。

本小問は，大きく分けて二つのことを問うている。

一つ目は，「HTTPS でアクセスするための HTTP プロトコルのメソッド名」である。下線②によると，そのメソッドを用いたアクセスでは，ホスト名は記録されていたが，URL は記録されていなかった。

二つ目は，「このメソッドを用いる場合，社内に侵入したマルウェアによる通信（ただし，HTTPS 以外の通信）を遮断するためのプロキシサーバでの対策」である。

それでは，一つずつ解を導くことにしよう。

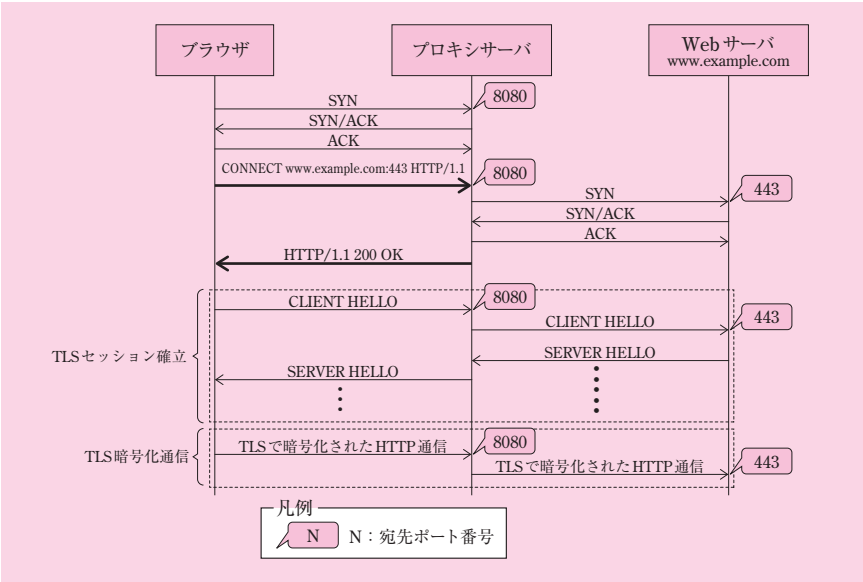
●解の導出：HTTPS でアクセスするための HTTP プロトコルのメソッド名

これは一般的な知識に基づいて解を導くことができる。

プロキシサーバを経由して，クライアントと Web サーバ間で HTTP 以外の通信を行うとき，クライアントはプロキシサーバに CONNECT メソッドを発行する。メソッドの中に，当該通信の接続先となる Web サーバが指定されている。

本事例では，プロキシサーバを経由して HTTPS 通信（TLS で暗号化された HTTP 通信）を行うため，CONNENCT メソッドを使用する必要がある。

この通信の手順を次の図に示す。この図では，接続先の Web サーバを「www.example.com」とし，プロキシサーバに接続するときの宛先ポート番号を 8080 番としている。



図：プロキシサーバを経由する HTTPS 通信の動作手順

1. クライアントのブラウザは，ポート 8080 番を指定してプロキシサーバとの間で TCP コネクションを確立する。
2. ブラウザは，CONNECT メソッドをプロキシサーバに送信する。このメソッドは，プロキシサーバに対し，接続先 Web サーバのホスト名，及び，HTTP 以外のプロトコルを使用して通信する旨を伝える。なお，プロトコルを指定する方法として，ポート番号を用いる。

   図中では，接続先 Web サーバのホスト名として「www.example.com」を，HTTP

以外のプロトコルとして「443」（HTTPS のポート番号）を，それぞれ指定している。

3. プロキシサーバは，トンネルの宛先である Web サーバとの間で TCP コネクションを確立する。

これら一連のやり取りを経た後，ブラウザと Web サーバ間で TLS セッション（HTTP 通信）を確立する。これ以降のやり取りは，接続先 Web サーバとの HTTP 通信が暗号化されている。接続先 Web サーバのコンテンツの URL は，TLS で暗号化された HTTP パケットの中に格納されている。

したがって，本文中の下線②にあるとおり，CONNECT メソッドをプロキシサーバに送信する際，「アクセス先のホスト名」は格納されているが，URL は格納されていないわけだ。

以上より，HTTPS でアクセスするための HTTP プロトコルのメソッド名は，「**CONNECT メソッド**」であることが分かる。よって，これが正解となる。

●解の導出：このメソッドを用いる場合，社内に侵入したマルウェアによる通信（ただし，HTTPS 以外の通信）を遮断するためのプロキシサーバでの対策

ここで問われていることは，CONNECT メソッドを用いる場合，HTTPS 以外の通信を遮断する方法である。

前述のとおり，CONNECT メソッドは，HTTP 以外の通信をプロキシサーバ経由で行うときに使用する。CONNECT メソッドで当該プロトコルのポート番号を格納することにより，プロキシサーバはその通信を中継する。

したがって，HTTPS 以外のポート番号を指定した CONNECT メソッドを拒否することにより，HTTPS 以外の通信をプロキシサーバで中継させないようにすることができる。

よって，正解は解答例に示したとおりとなる。

●参考：設問文中で「マルウェアによる通信」に言及されている理由

プロキシを問うこの設問で「マルウェアによる通信」を取り上げているのはなぜだろうか。

実は，侵入したマルウェアは，ハッカーが設置した C&C サーバ（Command & Control サーバ）と通信を行うことがあるからだ。

例えば，マルウェアは C&C サーバの指令を受け，サーバに侵入して機密情報を盗み出し，C&C サーバに送信するかもしれない。

マルウェアが外部のサーバと通信する際，FW で通常許可されている Web アクセス（HTTP 通信，HTTPS 通信）を利用することが多い。

このようなマルウェアによる通信への対策として，本事例では，インターネットへの Web 通信をプロキシサーバ経由で行うようにし，プロキシサーバにて

- 利用者認証
- ログ採取

を実施しているのである。

マルウェアは利用者認証に必要な情報を知らないのでこれに失敗し，C&C サーバと通信できなくなる。

さらに，この通信を試みた痕跡がログに残るため，ログを分析することでマルウェアの発見につながる。

このような，侵入したマルウェアの活動を抑えたり，その活動を発見したりする対策を「出口対策」という。言うまでもなく，そもそもマルウェアを侵入させないようにする「入口対策」も，併せて実施しておく必要がある。

参考までに，平成 26 年午後Ⅱ問 1 では標的型攻撃をテーマに，メールに添付されたマルウェアの入口対策と出口対策について，様々な角度から出題している。

良い勉強になるので，一度目を通してみることをお勧めしたい。

(2)

解答例

ウ：プロキシサーバのルート証明書（14字）

ウ

本小問は，本文中の空欄ウに入れる適切な字句を問うている。

空欄ウは，〔G 社 SaaS の試用〕の第 1 段落の中にある。そこには，「プロキシサーバで暗号化通信を一旦復号し，必要な処理を行った上で再度暗号化した。しかし，社内 PC でエラーメッセージ“証明書が信頼できない”が表示されたので，社内 PC に［ウ］をインストールして解決した」と記述されている。

本事例のプロキシサーバは，HTTPS 通信を中継する際，暗号化通信を復号し，再度暗号化している。これは，「SSL 可視化」(*)と呼ばれる技術である。

（＊）今日，「SSL」と呼ばれている通信の正体は，実際は TLS の通信である。SSL には脆弱性があるため，これを改良した TLS が RFC で標準化され，今日では TLS が用いられる。とはいえ，先に登場した SSL という名称が知れ渡っているため，TLS 通信のことを，慣用的に SSL 通信と呼称している。したがって，ここに書いた「SSL 可視化」も，本当のところは「TLS 可視化」である。

本小問を首尾よく解くには，SSL 可視化の仕組みを理解しておく必要がある。そこで，その点についてまずは簡潔に解説する。次いで，解を導こう。

● SSL 可視化装置の仕組み

社内に侵入したマルウェアが不正な通信を TLS で暗号化してしまうと，それを検知できなくなるという問題が生じる。なぜなら，通常のプロキシサーバが HTTPS 通信（TLS で暗号化された HTTP 通信）を中継する際，ただ単に HTTPS パケットを中継しているだけだからだ。その内容は TLS で暗号化されているため，プロキシサーバはこれを解読することはできない。

その対策として，HTTPS を中継するプロキシサーバで SSL 可視化を行う手法が，昨今注目を集めている。

以下，SSL 可視化の仕組みを解説するに当たり，通常のプロキシサーバと区別するため，SSL 可視化機能を装備したプロキシサーバを「SSL 可視化装置」と称することにしよう。ただし，詳細の仕様は製品依存であることを申し添えておく。

通常のプロキシサーバは，HTTPS パケットを中継するだけなので，社内 PC と接続先サーバとの間でやり取りされる TLS 通信に介入しない。

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。

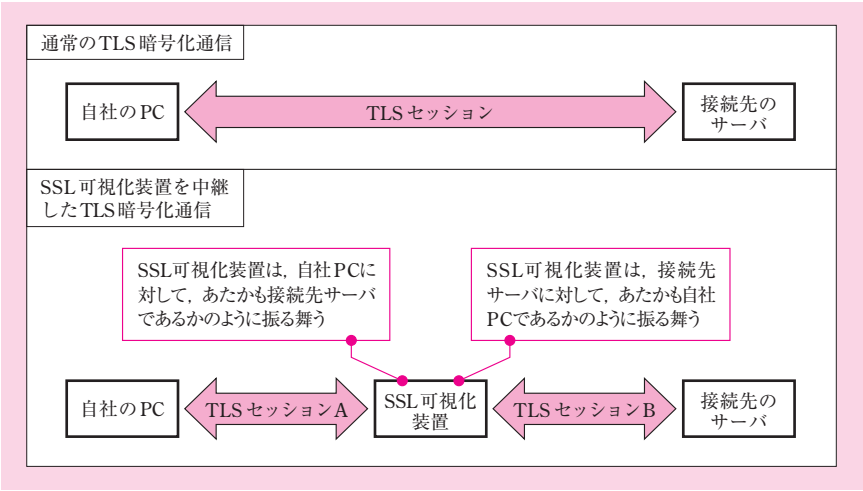
この結果，SSL 可視化装置は，二つの TLS セッション A，B のエンドポイントになる。当然ながら，それぞれの TLS セッションの共通鍵を有している。それぞれを鍵 A，鍵 B と呼ぼう。

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。

ここで，ブラウザの「信頼できる CA のリスト」にプライベート CA を加えると書いたが，その方法はいたって簡単である。プライベート CA の証明書をブラウザにインストールし，その際に「信頼できる CA のリスト」に加えるように指定すればよい。

プライベート CA はプロキシサーバに独自に設置されたものなので，プライベート CA 証明書に署名するのは自分自身となる。このような証明書をルート証明書と呼ぶ。

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。

●解の導出

SSL 可視化の仕組みが理解できれば，本小問の解を導くことができる。

改めて空欄ウを含む文章を見てみよう。それは，「プロキシサーバで暗号化通信を一旦復号し，必要な処理を行った上で再度暗号化した。しかし，社内 PC でエラーメッセージ“証明書が信頼できない”が表示されたので，社内 PC に［ ウ ］をインストールして解決した」と記述されている。

SSL 可視化を行うには，プロキシサーバに設置されたプライベート CA のルート証明書を社内 PC のブラウザにインストールし，このプライベート CA を信頼された認証局のリストに登録しておく必要がある。社内 PC とプロキシサーバ間の HTTPS 通信

は，プライベート CA によって署名された公開鍵証明書を使用しているからだ。

プライベート CA のルート証明書をインストールしないならば，ここに記されているとおり，エラーメッセージ“証明書が信頼できない”が表示されてしまう。

このエラーメッセージが表示されないようにするためにインストールしたものが，空欄ウの解となる。したがって，ここに当てはまる字句は「プロキシサーバに設置されたプライベート CA のルート証明書」となる。

とはいえ，この字数は 28 字である。問題文で指定された字数である 20 字より，8 字多い。それゆえ，解答に含めるキーワードを取捨選択しなければならない。

そこで，「ルート証明書」というキーワードを採択し，「プライベート CA」というキーワードを除外することにしよう。ルート証明書はプライベート CA を設置するときに必ず作成するものなので，このキーワードを用いることで，プライベート CA の存在を示せるからだ。

よって，正解は，「**プロキシサーバのルート証明書**」となる。

■設問 3

本設問は，〔SD-WAN ルータの導入〕について問うている。

(1)

解答例

エ：コントロール

エ

本小問は，本文中の空欄エに入れる適切な字句を問うている。

空欄エは，〔SD-WAN ルータの導入〕「(1) SD-WAN ルータの概要」の第 1 段落の中にある。そこには，「今回使用する予定の SD-WAN ルータは，SDN（Software-Defined Networking）によって制御される IPsec ルータである。SDN は，利用者の通信トラフィックを転送するデータプレーンと，通信装置を集中制御する［エ］プレーンから構成されており，［エ］プレーンのソフトウェアでデータ転送を制御する方式である」と記述されている。

本小問は SDN の専門用語を問うており，正解を得るにはその知識が欠かせない。そこで，その点についてまずは簡潔に解説する。次いで，解を導こう。

● SDN（Software-Defined Networking）

SDN とは,「通信装置の機能をソフトウェアで定義できるようにした技術や規格」である。従来のネットワーク機器を，経路制御などの管理機能を実行するコントローラと，データ転送を行う通信装置（以下，SDN 通信装置という）に分け，パケットの経路制御をコントローラが集中制御する方式を採用する。

SDN 通信装置の振る舞いは，従来の通信装置のようにハードウェアで硬直的に定まっているのではなく，ソフトウェアで自由自在に決定することができる。

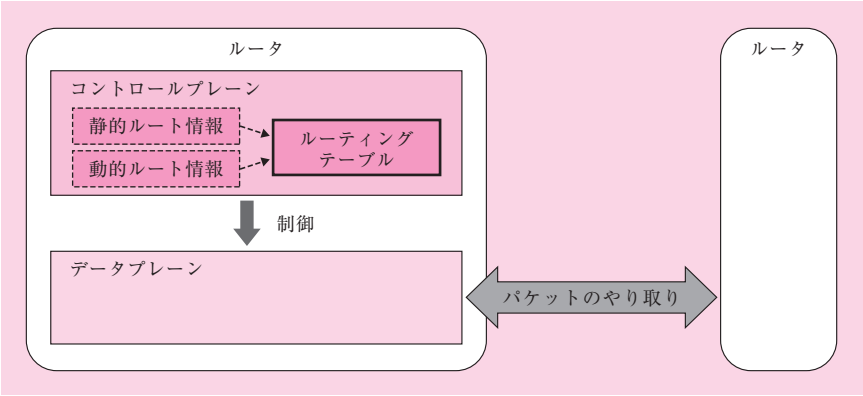
本事例では，SD-WAN ルータは，IPsec ルータとして機能するように定義されている。図 2 には，全社の SD-WAN ルータを集中制御するための SD-WAN コントローラが図示されている。

コントローラが SDN 通信装置を制御できるようにするため，両者を専用のネットワークで接続する。つまり，SDN 通信装置が利用者の通信トラフィックを転送するネットワークとは別のものにしておく。

通信トラフィックを転送するネットワークを「データプレーン」と呼び, コントローラ，及び制御用ネットワークを「コントロールプレーン」と呼ぶ。

従来の通信装置では，データプレーンとコントロールプレーンとが，装置内部に存在している。データプレーンは，ポート間のパケット転送を処理する部位（ポート間をつなぐ電子回路，等）であり，ASIC によって制御されている。コントロールプレーンは，そのパケット転送のルールを定義している部位（ルーティングテーブル，等）であり，組込みソフトウェアによって制御されている。

例として，従来のルータにおけるプレーン構成を次の図に示す。



図：従来のルータのプレーン構成

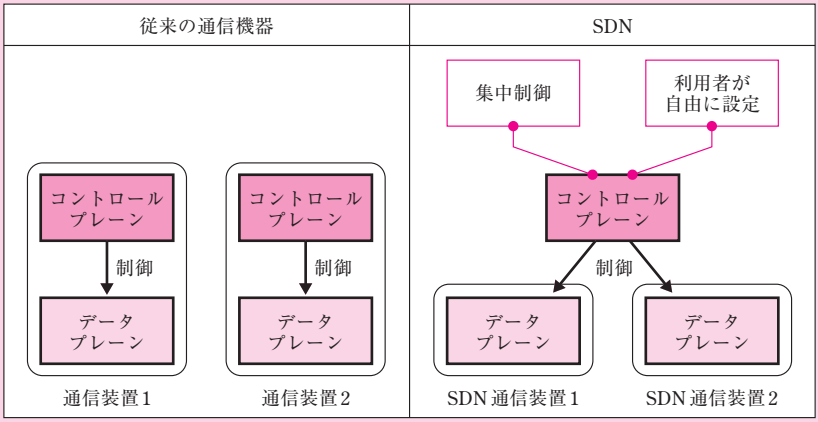
利用者は，組込みソフトウェアに読み込ませるコンフィグレーション情報（インタフェースの設定，静的ルートの設定，等）を登録することができる。しかし，組込みソフトウェアそのものを好き勝手に書き換えることはできない。例えば，ルータに組み込まれたソフトウェアを L2SW 用のものにし，L2SW に生まれ変わらせるといった芸当はできないわけだ。

これに対し SDN は，いわばコントロールプレーンを通信機器の外部に出したものだと考えればよい。これを制御する組込みソフトウェアに相当するのが SDN のコントローラであり，利用者は組込みソフトウェアそのものを自由自在に操れるのである。

このコントロールプレーンの在り様が，SDN の最たる特徴となっている。

要するに，SDN は，従来の通信機器のネットワークに比べ，次の 2 点が異なっていると言える。

- 1 台以上の通信装置から出されたコントロールプレーンを，1 台のコントローラが集中制御する構成になっている。
- コントローラに搭載するソフトウェアを，利用者が自由に設定できるようになっている。



図：プレーン構成に着目した，従来の通信装置と SDN の比較

最後に，コントローラが SDN 通信装置を制御する方法について，簡単に触れておこう。

SDN 通信装置は，データプレーン上のパケット受信を契機に，コントローラからの

指示を仰ぐために当該パケットをコントローラに転送する。その後，コントロールプレーンの制御用ネットワークを介し，コントローラは当該パケットに応じたコマンドを送り，SDN 通信装置に経路制御の動作を指示する。

それだけでなく，SDN のコントローラは，通信に先立ち，SDN 通信装置の動作の一部を登録しておくこともできる。コントロールプレーンの制御用ネットワークを介し，SDN 通信装置にコマンドを事前に送っておけばよいのである。

利用者は，このコマンドを自由自在に設定できる。望むなら，SDN 通信装置をルータとして振る舞わせたり，L2 スイッチとして振る舞わせたりすることができる。

●解の導出

SDN の仕組みが理解できれば，本小問の解を導くことができる。

改めて空欄エを含む文章を見てみよう。それは，「SDN は，利用者の通信トラフィックを転送するデータプレーンと，通信装置を集中制御する［ エ ］プレーンから構成されており，［ エ ］プレーンのソフトウェアでデータ転送を制御する方式である」と記述されている。

前述のとおり，通信装置を集中制御する部分は，コントロールプレーン（コントローラ，及び制御用ネットワーク）である。コントロールプレーンのソフトウェア（コントローラに搭載されたソフトウェア）でデータ転送を制御する。

よって，正解は，「**コントロール**」となる。

(2)

解答例

ネクストホップがSD-WANルータとなるデフォルトルート

（28字）

問題文は，「本文中の下線③について，設定変更後の静的経路情報を……答えよ」と記述されている。

下線③は，〔SD-WAN ルータの導入〕「(2) SD-WAN ルータを用いたときの通信」の 5 番目の箇条書きの中にある。この箇条書きは新しいネットワークのトラフィック経路に関わるものであり，本小問を解く上で重要な手掛かりを与えている。そこで，全ての箇条書きを掲載しておこう。

・社内 PC から G 社 SaaS への Web アクセスは，プロキシサーバを経由せず各 SD-WAN ルータを経由する。
・社内 PC から G 社 SaaS 以外のインターネットへの Web アクセスは，プロキシサーバを経由する。
・L3SW にプロキシサーバへの静的経路情報を追加する。
・営業所と本社間の通信は，SD-WAN ルータ間で IPsec によって暗号化する。
・本社の社内 PC から G 社 SaaS への通信について，③ G 社 SaaS の IP アドレスが変更された場合でもその都度 L3SW を設定しなくても済むように，L3SW の静的経路情報を設定変更する。

冒頭の「・SD-WAN ルータを使用したネットワーク構成」で解説したとおり，新しいネットワーク構成ではトラフィック経路の分散が図られている。その点が，1 番目と 2 番目の箇条書きに記されている。

さらに，冒頭の「・G 社 SaaS の IP アドレスブロックの変更」で解説したとおり，G 社 SaaS の IP アドレスブロックの更新に追随するため，次に示す対策を講じている。ポイントを再掲しよう。

［対策 1］L3SW の静的経路情報を変更し，G 社 SaaS の IP アドレスが変更された場合でもその都度 L3SW を設定しなくても済むようにする（「(2) SD-WAN ルータを用いたときの通信」の 3 番目と 5 番目の箇条書き）。
［対策 2］RSS 配信された G 社 SaaS の IP アドレスブロックを検知するツールを作成し，自動的にツールから全社の SD-WAN ルータの設定を変更する（「(3) SD-WAN ルータの運用」の第 2 段落）。

現行ネットワークにおける L3SW の静的経路情報は，デフォルトルートのネクストホップを FW に設定したものであった（〔F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策〕の第 1 段落）。

もし，デフォルトルートのネクストホップを従来のまま変更しなかったら，新しいネットワークにおけるトラフィック経路分散をどのように実現するのだろうか。

この点を考察するに当たり，前提条件として，社内 PC から送信されるパケットの宛先 IP アドレスが，次のように設定されているものとする。

［前提条件 1］G 社 SaaS への Web アクセス（HTTPS 通信）は，宛先 IP アドレスが G 社 SaaS の IP アドレスブロック内の IP アドレスである。
［前提条件 2］G 社 SaaS 以外への Web アクセス（HTTP 通信，HTTPS 通信）は，宛先 IP アドレスがプロキシサーバの IP アドレスである。

この前提条件は，トラフィック経路分散の方針に合致したものである。前提条件 2 は従来から実施されていたものである。

なお，この前提条件を満たすには，ある設定を PC のブラウザに行う必要がある。その点は設問 3（4）で問われているので，後ほど解説しよう。

さて，本社 PC から G 社 SaaS への Web アクセスは本社 SD-WAN ルータを経由させる。デフォルトルートのネクストホップを変更しないなら，次に示す静的経路情報を L3SW に追加する必要がある。

宛先ネットワーク	G 社 SaaS の IP アドレスブロック
サブネットマスク	同アドレスブロックに見合うサブネットマスク
ネクストホップ	本社 SD-WAN ルータ

ロンゲストマッチアルゴリズムに基づく経路制御により，この静的経路はデフォルトルートよりも優先されるので，経路制御上はうまくいく。

とはいえ，この設定は，**本事例が採用しているものではない**。

本小問が問うている下線③は，「③ G 社 SaaS の IP アドレスが変更された場合でもその都度 L3SW を設定しなくても済むように」と記述されている。それゆえ，これとは異なる静的経路を L3SW に設定しなければならないわけだ。

前述の［対策 2］に記したとおり，G 社 SaaS の IP アドレスブロックは，ツールにより SD-WAN ルータの静的経路情報に反映される（この点について，詳しくは設問 3（3）で解説する）。

したがって，パケットを本社 SD-WAN ルータに転送し，そちらで G 社 SaaS を宛先とするか否かを判断してもらえばよい。具体的に言うと，次に示す経路情報を L3SW に設定すればよいのだ。

・G 社 SaaS への Web アクセス（本社 SD-WAN ルータ経由）

宛先ネットワーク	0.0.0.0
サブネットマスク	0.0.0.0
ネクストホップ	本社 SD-WAN ルータ

要するに，デフォルトルートのネクストホップを，FW から本社 SD-WAN ルータに変更したわけである。

さて，この設定に従えば，あらゆるパケットは本社 SD-WAN ルータに転送されてしまう。しかし，全てのパケットを SD-WAN ルータに転送する必要はない。

G 社 SaaS 以外の Web アクセスはプロキシサーバを経由するようにブラウザに設定されているので，その宛先 IP アドレスはプロキシサーバとなる。それゆえ，次に示す経路情報を L3SW に設定することができる。

・G 社 SaaS 以外への Web アクセス（プロキシサーバ経由）

宛先ネットワーク	プロキシサーバの IP アドレス
サブネットマスク	255.255.255.255
ネクストホップ	FW

さらに，インターネットから営業所 PC へのリプライパケットを転送するため，現行ネットワークの頃から，次に示す経路情報が L3SW に設定されていたはずだ。

・営業所 PC への通信

宛先ネットワーク	営業所の IP アドレスブロック
サブネットマスク	同アドレスブロックに見合うサブネットマスク
ネクストホップ	本社 SD-WAN ルータ

なお，デフォルトルートのネクストホップを本社 SD-WAN ルータに変更したことで，この経路情報はそちらに集約されてしまう。それゆえ，削除しても差し支えない。

以上をまとめると，L3SW の静的経路情報に関し，二つの設定変更を行う必要があることが分かる。

［設定変更 1］G 社 SaaS への Web アクセス（本社 SD-WAN ルータ経由）のため，デフォルトルートのネクストホップを本社 SD-WAN ルータに変更する。

［設定変更 2］G 社 SaaS 以外への Web アクセス（プロキシサーバ経由）のための，プロキシサーバを宛先とする経路情報を追加する。

このうち，［設定変更 2］は，3 番目の箇条書きに明記されている。それゆえ，［設定変更 1］が，5 番目の箇条書きの下線③で問われているものだと推察できる。

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。

(3)

解答例

オ：SD-WAN コントローラ

オ

本小問は，本文中の空欄オに入れる適切な字句を問うている。

空欄オは，〔SD-WAN ルータの導入〕「(3) SD-WAN ルータの運用」の第 2 段落の中にある。そこには，「F 社は，RSS 配信された IP アドレスブロックを検知するツールを作成して，自動的にツールから［ オ ］に指示を行い，全社の SD-WAN ルータの設定を変更することにした」と記述されている。

設問 3 (1) で解説したとおり，SD-WAN ルータは，SD-WAN コントローラにより集中制御されている。

したがって，次のような処理を行うことにより，RSS 配信にリアルタイムに追随して，全社の SD-WAN ルータの設定を変更することができる。

1. G 社 SaaS から配信された RSS を受信する。
2. ツールは，変更すべき IP アドレスブロックを検知する。
3. ツールは，SD-WAN コントローラに対し，下記 4 を行う旨の指示を出す。
4. SD-WAN コントローラは，SD-WAN ルータに対し，「SD-WAN ルータの静的経路情報のうち，G 社 SaaS を宛先ネットワークとする経路の IP アドレスブロックを変更する」旨の指示を出す。

この処理を「(3) SD-WAN ルータの運用」の第 2 段落に当てはめてみると，「自動的にツールから［ オ ］に指示を行い」という記述は，前述の項番 3 に該当することが分かる。

よって，正解は，「**SD-WAN コントローラ**」となる。

(4)

解答例

G社SaaSへのHTTPS通信 (15字)

問題文は,「本文中の下線④について,このファイルを作成することによってプロキシから除外する通信を……答えよ」と記述されている。「プロキシから除外する通信」とは,要するに,「プロキシサーバを経由しない通信」を指している。

下線④は,〔SD-WAN ルータの導入〕「(3) SD-WAN ルータの運用」の第 2 段落の中にある。そこには,「F 社は,RSS 配信された IP アドレスブロックを検知するツールを作成して,自動的にツールから SD-WAN コントローラに指示を行い,全社の SD-WAN ルータの設定を変更することにした。さらに,社内 PC から参照する④プロキシ自動設定ファイルを作成することにした」と記述されている。

したがって,本小問が問うていることは,「社内 PC から参照するプロキシ自動設定ファイルをツールが自動的に作成することによって,プロキシサーバを経由しない通信をブラウザに登録できるが,それは何であるか」ということである。

本小問を首尾よく解くには,プロキシサーバを経由しない通信について,及び,そのような通信をブラウザに登録する技術であるプロキシ自動設定について,理解しておく必要がある。そこで,その点についてまずは解説する。次いで,解を導こう。

●プロキシサーバを経由しない通信

冒頭の解説で述べたとおり,性能劣化の問題を解決するため,インターネットへの Web アクセスを 2 種類に分け,それぞれの経路を異なるものにしている。つまり,トラフィック経路を分散することにより,性能劣化が生じないように工夫しているわけだ。

(これまでの解説で何度も言及しているが,) この点について,〔SD-WAN ルータの導入〕「(2) SD-WAN ルータを用いたときの通信」の 1 ～ 2 番目の箇条書きの中で,次のように記述されている。

- 社内 PC から G 社 SaaS への Web アクセスは,プロキシサーバを経由せず各 SD-WAN ルータを経由する。
- 社内 PC から G 社 SaaS 以外のインターネットへの Web アクセスは,プロキシサーバを経由する。

このようなトラフィックを実現するには，社内 PC が送信するパケットの宛先 IP アドレスが，次のように設定されていることが前提となる。これは，設問 3（3）の解説の中で，「前提条件」として列挙したものと同じだ。

［前提条件 1］G 社 SaaS への Web アクセス（HTTPS 通信）は，宛先 IP アドレスが G 社 SaaS の IP アドレスブロック内の IP アドレスである。
［前提条件 2］G 社 SaaS 以外への Web アクセス（HTTP 通信，HTTPS 通信）は，宛先 IP アドレスがプロキシサーバの IP アドレスである。

［前提条件 1］の「HTTPS 通信」について補足しておこう。G 社 SaaS への Web アクセスは，セキュリティ強化のために HTTPS で暗号化している。この点は，〔F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策〕の第 3 段落の 1 番目の箇条書きで言及されている。試験問題で「Web アクセス」と書いてあるときには，HTTP 通信と HTTPS 通信のどちらであるか（あるいは両方であるか），注意深く見定めるように心掛けておきたい。

さて，これら二つの前提条件を満たすには，ブラウザのプロキシ設定に関し，次のような設定を行っておく必要がある。

［設定 1］G 社 SaaS への Web アクセス（HTTPS 通信）は，プロキシサーバを経由せず，直接アクセスする。
［設定 2］G 社 SaaS 以外への Web アクセス（HTTP 通信，HTTPS 通信）は，プロキシサーバを経由する。

全社 PC に対して，このようなプロキシ設定を手動で行うのは，大変な労力が求められるし，しかも，手作業に起因するミスが懸念されるため，得策ではない。プロキシ設定を自動で行う方法を採用するのが妥当である。

実は，下線④で言及されている「プロキシ自動設定ファイル」を用意しておけば，この設定を自動的に行うことができる。

それでは，次にプロキシ自動設定について解説しよう。

●プロキシ自動設定

一般的に言って，ブラウザ上で行うプロキシ設定では，次の情報を登録することができる。

- プロキシサーバの IP アドレスとポート番号の組
- 上記プロキシサーバを経由して通信するホスト名(*1)，通信するポート番号(*2)
- 上記プロキシサーバを経由せず，直接通信するホスト名，通信するポート番号

（＊ 1）ホスト名の代わりに IP アドレスを指定することができる。
（＊ 2）通信するポート番号を省略すると，既定値の HTTP（80 番）が適用される。

こうした設定を各 PC に手動で行うのは骨の折れる作業である。そこで登場したのが，プロキシ自動設定（PAC：Proxy Auto-Configuration）という技術である。

前述の情報を記述したファイル（PAC ファイルという）を，イントラネット上の Web サーバのコンテンツとして登録しておき，そのファイルを取得するための URL をブラウザに設定しておく。ブラウザの起動時，当該 PAC ファイルを取得してプロキシ設定を読み込むことで，自動設定が行われる仕組みになっている。

●解の導出

本事例では，RSS 配信された G 社 SaaS の IP アドレスブロックを検知するツールを作成して，自動的にツールがプロキシ自動設定ファイルを作成する。

そのファイルに設定する内容は，「●プロキシサーバを経由しない通信」の［設定 1］，［設定 2］に示したものである。

本小問が問うているのは「プロキシサーバを経由しない通信」であるから，［設定 1］に則した内容を解答すればよい。

したがって，正解は，「**G 社 SaaS への HTTPS 通信**」となる。

(5)

解答例

①社内PCからG社SaaSへのアクセスがプロキシサーバを経由しなくなるから（36字）

②出張先のPCからG社SaaSへのアクセスが記録されるから（28字）

問題文は，「本文中の下線⑤について，G 社 SaaS の API 経由で取得する理由を二つ挙げ（よ）」と記述されている。

下線⑤は，〔SD-WAN ルータの導入〕「(4) G 社 SaaS アクセスログの取得」の第 1 段落にある。そこには，「G 社 SaaS へのアクセスログは，⑤プロキシサーバからではなく，G 社 SaaS の API にアクセスして取得することにした」と記述されている。

下線⑤に「プロキシサーバからではなく」とあるが，わざわざこのように書かれているのは理由がある。その点は，本事例の全体像を考察するとよく理解でき，その理由に気が付くと本小問の解を導くことができる。

当初，本事例では，図 1「F 社の現行ネットワーク構成（抜粋）」に示されたネットワーク構成で，G 社 SaaS にアクセスする予定であった。

当初の検討内容について，〔F 社の現行ネットワーク構成と G 社 SaaS 導入に合わせたセキュリティ対策〕の第 3 段落の 2 番目と 3 番目の箇条書きの中で，次のように記述されている。

> ・出張先の PC から直接 G 社 SaaS を利用できるようにする……。
> ・G 社 SaaS 導入に合わせて……，プロキシサーバで次のログを取得する。
> - アクセス先 URL と利用者 ID
> - G 社 SaaS のファイルアップロード／ダウンロードのログと利用者 ID

この記述から，G 社 SaaS へのアクセスログの取得に関し，二つのことが分かる。

一つ目は，出張先 PC からのアクセスはプロキシサーバを経由しないので，アクセスログを取得するには G 社 SaaS 側で行うしか方法がないという点である。

二つ目は，(現行ネットワークの構成では) 社内 PC からのアクセスはプロキシサーバを経由するので，そこでアクセスログを取得するつもりだったという点である。

一つ目で述べたことは，そのまま下線⑤の理由（G 社 SaaS 上で取得する理由）となる。つまり本小問の解となるわけだが，解の導出はいったん後回しにしよう。

二つ目で述べたことは，その後のストーリー展開が関わってくる。〔G 社 SaaS の試用〕で発覚した性能劣化の問題を解決する必要が生じ，図 2「SD-WAN ルータを使用したネットワーク構成案（抜粋）」で示された新しいネットワーク構成を採用するに至ったのである。この新しいネットワーク構成では，G 社 SaaS へのアクセスはプロキシサーバを経由しなくなったのである。したがって，当初の予定とは異なり，プロキシサーバでアクセスログを取得することが不可能になってしまったわけだ。

これら二つのことを念頭において，下線⑤は，「プロキシサーバからではなく」と前置きした上で，「G 社 SaaS の API にアクセスして取得することにした」と述べているのだ。

●解の導出

本事例のストーリーを振り返りつつ，G 社 SaaS へのアクセスログの取得に関して分かったことを整理すると，本小問の解を導くことができる。

まず，一つ目に分かったことは，出張先 PC からのアクセスはプロキシサーバを経由しないという点である。それゆえ，このアクセスログを取得するには G 社 SaaS 側で行うしかない。よって，正解（一つ目）は，「**出張先の PC から G 社 SaaS へのアクセスが記録されるから**」等となる。

次に，二つ目に分かったこと（及びその後の経緯も含めて分かったこと）は，社内 PC からのアクセスは，当初の予定とは異なりプロキシサーバを経由しなくなったので，そこでアクセスログを取得できなくなったという点である。このアクセスログを取得するには G 社 SaaS 側で行うしかない。よって，正解（二つ目）は，「**社内 PC から G 社 SaaS へのアクセスがプロキシサーバを経由しなくなるから**」等となる。

問 2

出題趣旨

企業ネットワークを運営する際には，要件に合わせて設計構築するだけではなく，業務が滞りなく実施できるよう，適切に運用管理を行う必要がある。運用中においては，当初想定しえなかった問題に遭遇し，改善を求められることもある。

本問では，ある企業ネットワークを想定し，VRRP（Virtual Router Redundancy Protocol）や STP（Spanning Tree Protocol）といった冗長化に用いられる基本的な技術の理解，ICMP や SYSLOG，SNMP（Simple Network Management Protocol）といった監視に利用される基本的な技術の理解，及び，ネットワーク監視の問題に対してどのように考え，改善できるか，について問う。

採点講評

問 2 では，ネットワーク監視の改善を題材として，企業ネットワークの冗長化や監視に用いられる基本的な技術の理解とネットワーク監視の問題に対してどのように考え，改善できるかについて出題した。

設問 1 のエは，SNMP の基本的な用語だが，正答率が低かった。

設問 2(2)では，VRRP についての説明を求めたが，VRRP と異なるプロトコルについて述べた解答が目立った。VRRP は冗長化設計で用いられる基本的な技術であり，正しく理解しておいてほしい。

設問 4(2)では SNMP ポーリングと SNMP トラップの特徴を踏まえての解答を期待したが，的外れな解答が目立った。監視に用いられる技術の特徴を正しく把握することは，ネットワーク監視を設計する上で非常に重要である。ネットワーク技術者として是非知っておいてもらいたい。

設問 4(3)は正答率が低かった。問題文をよく読み，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		解答例・解答の要点		備考
設問 1		ア	ICMP	
		イ	IP アドレス	
		ウ	UDP	
		エ	コミュニティ	
設問 2	(1)	デフォルトゲートウェイ		
	(2)	VRRP アドバタイズメント		
	(3)	VLAN100，VLAN200，VLAN300		
設問 3	(1)	p2		
	(2)	スパニングツリーが再構築中だったから		
設問 4	(1)	SNMP エージェント	コア SW1 **又は** コア SW2 **又は** フロア SW1 **又は** フロア SW2 **又は** フロア SW3 **又は** フロア SW4 **又は** サーバ SW	
		SNMP マネージャ	監視サーバ	
設問 4	(2)	ボーリング	5 分ごとに状態を取得するので多くの場合異常検知が遅れる。	
		トラップ	到達確認がないのでメッセージが失われる可能性がある。	
	(3)	スパニングツリーが再構築するまでインフォームの再送信を繰り返す。		

本問は，ネットワーク監視を改善する事例を取り上げている。

本問は，スパニングツリー（STP），VRRP，SNMP について出題している。詳しくは本書の次の章を参照していただきたい。

表：出題されている要素技術

要素技術	掲載箇所
STP	第 6 章「6.2.1　リンクの冗長化」「● STP」
VRRP	第 6 章「6.2.2　ルータの冗長化」「● VRRP」
SNMP	第 9 章「9.5.1　監視に用いられるプロトコル」「● SNMP」

●本問の全体像

・A 社の LAN の概要

A 社のシステム部門では，統合監視サーバ（以下，監視サーバという）を構築し，A 社のサーバや LAN の運用監視を行っている。

A 社の LAN は，VRRP と STP を用いた冗長化構成が採用されている。その点は設問 2 で取り上げられているので，そこで詳しく解説しよう。

・A 社が実施している監視の概要

監視サーバは，ping による死活監視，SYSLOG による異常検知監視を行っている。

監視対象の機器が異常を検知すると，SYSLOG メッセージを監視サーバに送信する仕組みになっている。

・監視サーバの問題と状況確認

ある日，ケーブルの断線による障害が発生した際，監視サーバで検知できなかったという問題が発生した。

調査の結果，監視対象機器は SYSLOG メッセージを送信したが，それが監視サーバに到達しなかったことが判明した。その点は設問 3 で取り上げられているので，そこで詳しく解説しよう。

・ネットワーク監視の改善策の立案

問題を解決するため，SNMP のポーリング，トラップ，インフォームについて調査を行った。

その結果，ポーリング及びトラップは解決策として不十分であることが分かり，インフォームを採用することになった。その点は設問 4 で取り上げられているので，そこで詳しく解説しよう。

・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
A 社 LAN の概要	現行ネットワークの構成 図 1「A 社 LAN の構成（抜粋）」	2	(1) ～ (3)
監視サーバの概要	VRRP による冗長化 トランクポートに設定する VLAN ID	1	空欄ア～ウ
監視サーバの問題	ネットワークの異常を監視サーバで検知できないという問題が発生	—	—
障害発生時の状況確認	ケーブル断線によるスパニングツリーの状態変化，及び，リンク状態変化を通知した SYSLOG メッセージの到達可否	3	(1) ～ (2)
ネットワーク監視の改善策の立案	SNMP の知識	1	空欄エ
	SNMP のポーリング，トラップで解決できない理由 SNMP のインフォームで解決する際のパラメタ設定	4	(1) ～ (3)

それでは，設問の解説に移ろう。

■設問 1

解答例

ア：ICMP
イ：IP アドレス
ウ：UDP
エ：コミュニティ

本設問は，空欄ア～エに入れる適切な字句を問うている。

ア

空欄アは，〔監視サーバの概要〕の第 2 段落の中にある。

そこには，「ping 監視には，RFC 792 で規定されているプロトコルである［ア］を用いている」と記述されている。

ping は，IP ノードの到達性（reachability）を監視する目的で用いられている。使用しているプロトコルは ICMP である。

監視用機器上で，監視対象機器の IP アドレスに向けて 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，空欄アを見てみよう。文脈上，ここに該当する字句は，ping コマンドが使用しているプロトコルである。

よって，正解は「**ICMP**」となる。

イ

空欄イについて，「echo request パケットの宛先として，監視対象機器には［イ］を割り当てる必要がある」と記述されている。

空欄アで解説したとおり，ping は，IP ノードの到達性を監視する目的で用いられている。それゆえ，監視対象機器には IP アドレスを割り当てておく必要がある。

よって，正解は「**IP アドレス**」となる。

さて，空欄イの解は得られたが，わざわざ「監視対象機器には IP アドレスを割り当

てる必要がある」と述べているのはなぜだろうか。

その理由は，本事例の監視対象機器にある。

監視対象機器について，〔監視サーバの概要〕の第 1 段落には，「監視対象機器は，コア SW，サーバ SW 及びフロア SW である」と記述されている。

ここに列挙されたスイッチが L3 スイッチであれば，IP アドレスが割り当てられているのは当然のことである。L3 スイッチとして機能させるにはインタフェースの設定が欠かせないが，その設定時に IP アドレスを割り当てるからだ。

一方，L2 スイッチであれば，通常の設定で IP アドレスが割り当てられることはない。それゆえ，ping 監視を行うために，IP アドレス（及びサブネットマスク，デフォルトゲートウェイ）をわざわざ設定する必要があるのだ。

監視対象のスイッチが L3 スイッチ，L2 スイッチのどちらであるのかは，図 1 の脚注を見れば明らかになる。そこを見ると，コア SW は L3 スイッチであり，サーバ SW 及びフロア SW は L2 スイッチであることが分かる。

したがって，監視対象機器に L2 スイッチが含まれていることから，「監視対象機器には IP アドレスを割り当てる必要がある」と注意喚起する一文を用意したわけだ。

もっとも，サーバ SW 及びフロア SW は，このような IP アドレスの設定ができる L2 スイッチでなければならない。本文にはその点が明記されていないが，ping 監視の対象となっていることから，この機能が装備されているものと判断できる。

ウ

空欄ウは，〔監視サーバの概要〕の第 3 段落の中にある。

そこには，「SYSLOG は，トランスポートプロトコルとして RFC 768 で規定されている［ウ］を利用する」と記述されている。

syslog は，サーバや機器が取得したログを，ネットワーク経由で別のサーバに転送する技術である。なお，自サーバの特定のディレクトリに保存することもできる。

ログの取得に際しては，取得元となるファシリティ（kernel，daemon，cron，等）を指定したり，ログの重要度により取得の要否を指定したりすることができる。

syslog は，転送に用いるトランスポート層プロトコルとして，UDP を用いる。

よって，正解は「**UDP**」となる。

エ

空欄エは，〔ネットワーク監視の改善策の立案〕の第 2 段落の中にある。

そこには，「SNMP エージェントと SNMP マネージャは，同じグループであることを示す［エ］を用いて，機器の管理情報（以下，MIB という）を共有する」と記

述されている。

ネットワーク監視システムは，監視する側（SNMP マネージャ）と監視される側（SNMP エージェント）から構成される。

SNMP はネットワーク機器を監視するための標準的なプロトコルである。SNMP を用いることで，SNMP マネージャは，SNMP エージェントが管理している情報（MIB）を取得することができる。ただし，SNMP マネージャと SNMP エージェントが同じグループに属していない限り，MIB を取得することはできない。このグループのことを「コミュニティ」という。

SNMP マネージャは，SNMP エージェントに対し MIB の取得を要求する際，自分が属するコミュニティ名を伝える。SNMP エージェントは，同じコミュニティに属しているかを検証した後，SNMP マネージャが指定した MIB を応答する仕組みになっている。

このやり取りにおけるコミュニティ名を「パスワード」に置き換えれば，SNMP エージェントが行っていることは，パスワードによる主体認証と事実上同じである。

以上より，「同じグループであることを示す［　エ　］」に当てはまる字句は，「**コミュニティ**」となる。

よって，これが正解となる。

■設問 2

本設問は，〔A 社 LAN の概要〕について問うている。

(1)

解答例

デ	フ	ォ	ル	ト	ゲ	ー	ト	ウ	ェ	イ

（11 字）

問題文は，「本文中の下線①について，PC 及びサーバに設定する情報に着目して，VRRP による冗長化対象を……答えよ」と記述されている。

下線①は，〔A 社 LAN の概要〕の第 3 段落，1 番目の箇条書きの中にある。そこには，「コア SW には，① VRRP が設定してあり」と記述されている。

したがって，本小問が問うているのは，「VRRP について，PC 及びサーバに設定する情報に着目して，VRRP による冗長化対象を答えよ」ということである。

これは，一般的な知識から解を導くことができる。

VRRP は，ルータを冗長化させる技術である。VRRP を利用すれば，同一サブネット内に存在する複数台のルータをグループ化し，仮想的な 1 台のルータのように見せかけることができる。これを仮想ルータと呼ぶ。

仮想ルータを構成するルータは，仮想 IP アドレスを共有している。仮想ルータを構成するルータのうち，優先度の最も高いルータが，この仮想 IP アドレスをもつルータとして振る舞う。これをマスタルータという。

マスタルータ以外のルータをバックアップルータという。マスタルータがダウンしたとき，バックアップルータの中から優先度が最も高いルータがマスタルータに昇格する。すなわち，仮想 IP アドレスを引き継いで仮想ルータとして振る舞う。

仮想ルータを構成する複数台のルータのどれかが稼働している限り，仮想 IP アドレスをもつ仮想ルータがネットワーク上に存在している。それゆえ，仮想 IP アドレスの稼働率は，ルータの実 IP アドレスのそれよりも高いことが分かる。

したがって，PC 及びサーバのデフォルトゲートウェイとして，ルータの実 IP アドレスではなく仮想 IP アドレスを指定することにより，デフォルトゲートウェイの稼働率を高くすることができる。

VRRP は，「PC 及びサーバに設定する情報」に着目すると，デフォルトゲートウェイを冗長化する技術であると言えるわけだ。

よって，正解は，「**デフォルトゲートウェイ**」となる。

(2)

解答例

V	R	R	P	ア	ド	バ	タ	イ	ズ	メ	ン	ト

（13字）

問題文は，「本文中の下線②について，バックアップルータはあるメッセージを受信しなくなったときにマスタルータに切り替わる。VRRP で規定されているメッセージ名を……答えよ」と記述されている。

下線②は，〔A 社 LAN の概要〕の第 3 段落，1 番目の箇条書きの中にある。そこには，「②正常時は，コア SW1 がマスタルータで，コア SW2 がバックアップルータ」と記述されている。

端的に言うと，本小問で問うているのは，「VRRP のメッセージ名」である。問題文には，そのメッセージをバックアップルータが受信しなくなるとマスタルータに切り替わるとある。この記述から，VRRP に関する知識に基づき，解を導くことができる。

下線②はマスタルータ，バックアップルータの具体的な機器名を記しているだけで，本小問を解く上で考慮する必要はない。

さて，マスタルータは，VRRP アドバタイズメント（VRRP 広告）メッセージを定期的に送信し，バックアップルータに自らの健在を通知する。

バックアップルータは，マスタルータからの VRRP アドバタイズメントを一定時間受信しなくなると，マスタルータがダウンしたと判断する。次いで，バックアップルータの中から優先度が最も高いルータ（今やダウンしたマスタルータの次に優先度が高いルータ）がマスタルータに昇格する。

したがって，問題文中の「バックアップルータはあるメッセージを受信しなくなったときにマスタルータに切り替わる」に記された「あるメッセージ」とは，VRRP アドバタイズメントを指していることが分かる。

本小問は「VRRP で規定されているメッセージ名」を問うているので，正解は「**VRRP アドバタイズメント**」となる。

(3)

解答例

VLAN100，VLAN200，VLAN300

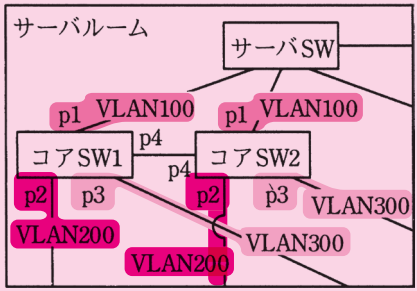
問題文は，「本文中の下線③について，p4 ポートでトランクポートに設定する VLAN ID を全て答えよ」と記述されている。

下線③は，〔A 社 LAN の概要〕の第 3 段落，3 番目の箇条書きの中にある。そこには，「コア SW の p1 ポート，p2 ポート及び p3 ポートはアクセスポートで，③ p4 ポートを IEEE 802.1Q を用いたトランクポートに設定している」と記述されている。

アクセスポートは，1 個のポートに対し 1 個の VLAN ID が割り当てられている。トランクポートは，1 個のポートに対し複数個の VLAN ID が割り当てられている。

本小問は，コア SW のトランクポートである p4 ポートに対して割り当てられた VLAN ID を問うている。

コア SW1，コア SW2 のアクセスポートに割り当てられている VLAN ID について，図 1 には次のように記されている。



図：コア SW のアクセスポートに割り当てられている VLAN ID

したがって，次のように整理できる。

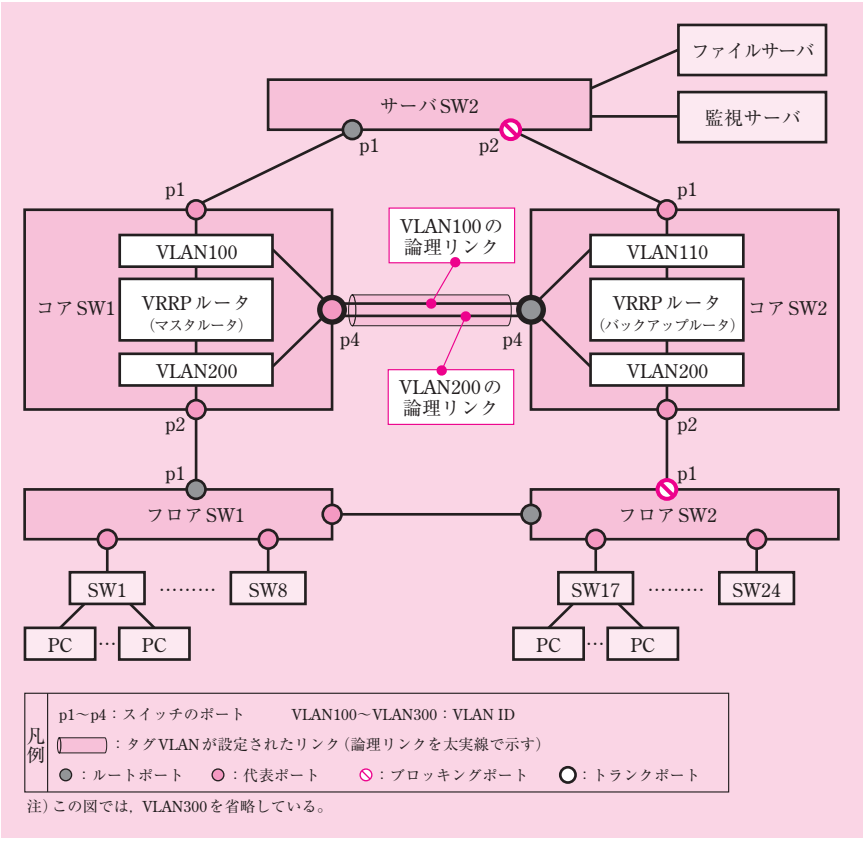
表：各スイッチに割り当てられる VLAN ID

スイッチ	p1 ポート	p2 ポート	p3 ポート
コア SW1	VLAN100	VLAN200	VLAN300
コア SW2	VLAN100	VLAN200	VLAN300

2 台のコア SW は，それぞれ VLAN100，VLAN200，VLAN300 を配下にもっている。

結論から言うと，トランクポートの役割は，2 台のコア SW にまたがって存在する各 VLAN を接続することである。トランクポートである p4 には，これら三つの VLAN が割り当てられているわけだ。その理由は，リンク障害時，トランクポートが迂回ルートになるためである。

この点を踏まえて，コア SW の内部構成を書き加えた A 社 LAN の構成は，次の図のようになっている。なお，紙面の都合により，この図では VLAN300 を省略している。コア SW 内部において VLAN200 と VLAN300 の VLAN 構成は同じなので，VLAN ID やポート番号を適宜読み替えれば理解できるはずだ。



注）この図では，VLAN300 を省略している。

図：コア SW の内部構成を書き加えた，LAN 構成

コア SW をまたがる各 VLAN がそれぞれトランクポートで接続されたことにより，各 VLAN はループ構成を含んでいる。これによりレイヤ 2 ネットワークの経路は冗長化されるが，ループを防止するために STP を設定している（〔A 社 LAN の概要〕の第 3 段落，2 番目の箇条書き）。

この図では，サーバ SW の p2，フロア SW2 の p1 がブロッキングポートであると仮定している(*)。

（＊）念のため，このように仮定した根拠を挙げておこう。
まず，〔A 社 LAN の概要〕の第 3 段落，2 番目の箇条書きから，正常時はコア SW1 がルートブリッジとなるように設定していることが分かる。
次いで，レイヤ 3 ネットワークにおいてコア SW1 のバックアップルータがコア SW2 であることに着目する。この点から，レイヤ 2 ネットワークにおいても同様であるに違いないと考えられる。つまり，コア SW2 は，コア SW1 のダウン時にルートブリッジになるように設定されているものと推察できる。そこで，その推察どおり，ブリッジプライオリティの仮定を置く。
さらに，パスコストについて，本文中に何も言及されていないのでシンプルに考えることとし，どのリンクもパスコストが等しいとの仮定を置く。
その結果，サーバ SW の p2，フロア SW2 の p1 がブロッキングポートになる。
この点と調和し，〔障害発生時の状況確認〕の第 2 段落，2 番目の箇条書きを見ると，正常時はフロア SW2 の p1 がブロッキングポートになっていることが示されている。それゆえ，この仮定に問題がないことが伺える。
なお，たとえ別のポートがブロッキングポートであったとしても，リンク障害時に迂回ルートが設定されることに変わりはないので，以下で解説する内容は実質的に変わらない。

先ほど，「結論から言うと，トランクポートの役割は，2 台のコア SW にまたがって存在する各 VLAN を接続することである。……その理由は，リンク障害時，トランクポートが迂回ルートになるためである」と解説した。

これから，その理由について解説しよう。

具体例として，VLAN200 を取り上げる。

まず，正常時の経路について考察しよう。PC からマスタルータに至る経路は，次のようになる。

［フロア SW1 配下の PC →マスタルータ］
フロア SW1 配下の PC →フロア SW1 →コア SW1 の VLAN200 →マスタルータ
［フロア SW2 配下の PC →マスタルータ］
フロア SW2 配下の PC →フロア SW2 →フロア SW1 →コア SW1 の VLAN200 →マスタルータ

次いで，リンク障害発生時の経路を幾つか考察してみよう。このとき，トランクリンクが使われていることに注目していただきたい。

コア SW1 とフロア SW1 間のリンク障害時，フロア SW2 の p1 のブロックが解除され，ルートポートになる。その結果，PC からマスタルータに至る経路は，次のようになる。

［フロア SW1 配下の PC →マスタルータ］
フロア SW1 配下の PC →フロア SW1 →フロア SW2 →コア SW2 の VLAN200
→トランクリンク→コア SW1 の VLAN200 →マスタルータ
［フロア SW2 配下の PC →マスタルータ］
フロア SW2 配下の PC →フロア SW2 →コア SW2 の VLAN200
→トランクリンク→コア SW1 の VLAN200 →マスタルータ

フロア SW1 とフロア SW2 間のリンク障害時，フロア SW2 の p1 のブロックが解除され，ルートポートになる。その結果，PC からマスタルータに至る経路は，次のようになる。

［フロア SW1 配下の PC →マスタルータ］
フロア SW1 配下の PC →フロア SW1 →コア SW1 の VLAN200 →マスタルータ
［フロア SW2 配下の PC →マスタルータ］
フロア SW2 配下の PC →フロア SW2 →コア SW2 の VLAN200
→トランクリンク→コア SW1 の VLAN200 →マスタルータ

VLAN100，VLAN300 に関する解説は，これまで述べた内容と似通っていることから，割愛しても大丈夫だろう。実際に試してみると分かるが，様々なリンク障害時にトランクポートが使われている。

このように，リンク障害時の迂回ルートを確保するため，全ての VLAN がトランクポートを必要としている。以上より，「トランクポートの役割は，2 台のコア SW にまたがって存在する各 VLAN を接続することである」との結論を導いた次第である。

ここから解を導くことができる。

本小問が問うているのは，コア SW のトランクポートである p4 ポートに対して割り当てられた VLAN ID であった。

よって，正解は，「**VLAN100，VLAN200，VLAN300**」となる。

■設問 3

本設問は，〔障害発生時の状況確認〕について問うている。

（1）

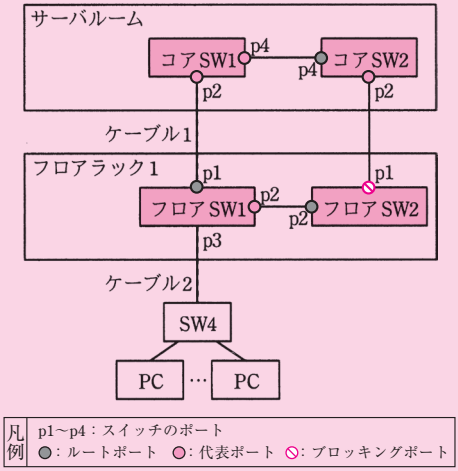
解答例

p2

問題文は，「本文中の下線④について，BPDU（Bridge Protocol Data Unit）を受信しなくなったフロア SW2 のポートを，図 2 中の字句を用いて答えよ」と記述されている。

下線④は，〔障害発生時の状況確認〕の第 2 段落，2 番目の箇条書きの中にある。そこには，本文の図 2 に基づき，「ケーブル 1 の断線によって，④フロア SW2 の p1 ポートの STP のポート状態がブロッキングから，リスニング，ラーニングを経て，フォワーディングに遷移した」と記述されている。

本文の図 2 は，VLAN200 の LAN 構成を抜粋したものとなっている。なお，図 2 はケーブルの断線を書き加えたものになっているので，正常時の構成を次の図に示そう。



図：VLAN200 の LAN 構成（図 2 より作成）

この VLAN200 は，次に示すとおりループ構成になっている。

コア SW1 － コア SW2 － フロア SW2 － フロア SW1 － コア SW1

ループを防止するため，〔A 社 LAN の概要〕の第 3 段落，2 番目の箇条書きには，「STP を用いて（いる）」と記述されている。

STP の設定について，「正常時はコア SW1 がルートブリッジとなるように設定している」と記述されている。さらに，下線④を見ると，ケーブル 1 が断線する前までは，フロア SW2 の p1 ポートはブロッキングポートであることが分かる。

この情報から，各ポートの割当てが次のように定まる。

［コア SW1］

- コア SW1 がルートブリッジであるので，コア SW1 の各ポートは代表ポートになる。

［フロア SW2］

- フロア SW2 の p1 がブロッキングポートであるので，フロア SW2 の p2 はルートポートでなければならない。さもないと，フロア SW2 に BPDU が届かなくなる。

［コア SW2］

- コア SW1 がルートブリッジであるので，コア SW2 の p4 はルートポートになる。
- フロア SW2 の p1 がブロッキングポートであるので，コア SW2 の p2 は代表ポートでなければならない。さもないと，コア SW2 とフロア SW2 間のセグメントに BPDU が届かなくなる。

［フロア SW1］

- コア SW1 がルートブリッジであるので，フロア SW1 の p1 はルートポートになる。
- フロア SW2 の p1 がブロッキングポートであるので，フロア SW2 の p2 はルートポートでなければならない。さもないと，フロア SW2 にルートポート経由で BPDU が届かなくなる。さらに，フロア SW1 とフロア SW2 間のセグメントに BPDU が届かなくなる。

フロア SW2 のルートポートは p2 なので，正常時はここから BPDU を受信する。その経路は次のとおりである。

コア SW1 の p2 ポート→フロア SW1 の p1 ポート
→フロア SW1 の p2 ポート→フロア SW2 の p2 ポート

しかし，図 2 中のケーブル 1（コア SW1 とフロア SW1 のケーブル）が断線すると，フロア SW2 の p2 ポートは，この経路から BPDU を受信できなくなる。

その代わり，下線④に記されているとおり，フロア SW2 の p1 ポートがフォワーディング状態になるので，今度はこの p1 ポートから BPDU を受信するようになる。このとき，p1 ポートはルートポートになっている。

したがって，ケーブル 1 の断線に伴い，BPDU を受信しなくなったフロア SW2 のポートは，「**p2**」である。よって，これが正解となる。

(2)

解答例

ス	パ	ニ	ン	グ	ツ	リ	ー	が	再	構	築	中	だ	っ	た	か	ら

（18字）

問題文は，「本文中の下線⑤について，フロア SW1 が送信した SYSLOG メッセージが監視サーバに到達できなかったのはなぜか。“スパニングツリー”の字句を用いて……述べよ」と記述されている。

下線⑤は，〔障害発生時の状況確認〕の第 2 段落，3 番目の箇条書きの中にある。そこには，本文の図 2 に基づき，「ケーブル 2 の断線に伴って⑤フロア SW1 が送信した，リンク状態遷移を示す SYSLOG メッセージが監視サーバに到達できなかった」と記述されている。

本小問を解くには，〔障害発生時の状況確認〕に示された，本事例の障害について全体像を把握する必要がある。そこで，まずはその点について解説する。

問題文中に「“スパニングツリー”の字句を用いて」とあるとおり，本小問を解く鍵はスパニングツリーである。具体的に言うと，障害発生時に生じるスパニングツリーの再構築について理解しておく必要がある。

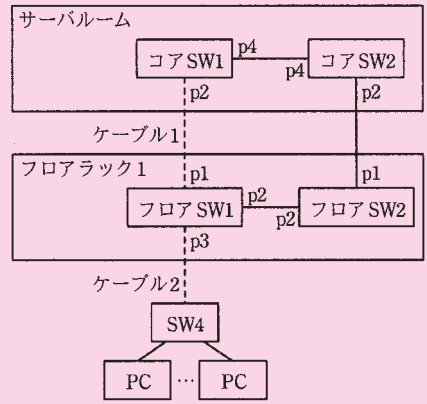
そこで，どのように再構築が行われるかについて，まずは解説する。次いで，解を導こう。

●本事例の障害

本事例の障害は，第 2 段落の三つの箇条書きの中で，次のように記されている。

まず，ケーブル 1 とケーブル 2 が同時に断線する。

・フロア SW1 の p1 ポートとコア SW1 の p2 ポートを接続するケーブル 1 が断線した。同時に，フロア SW1 の p3 ポートと SW4 を接続するケーブル 2 が断線した。

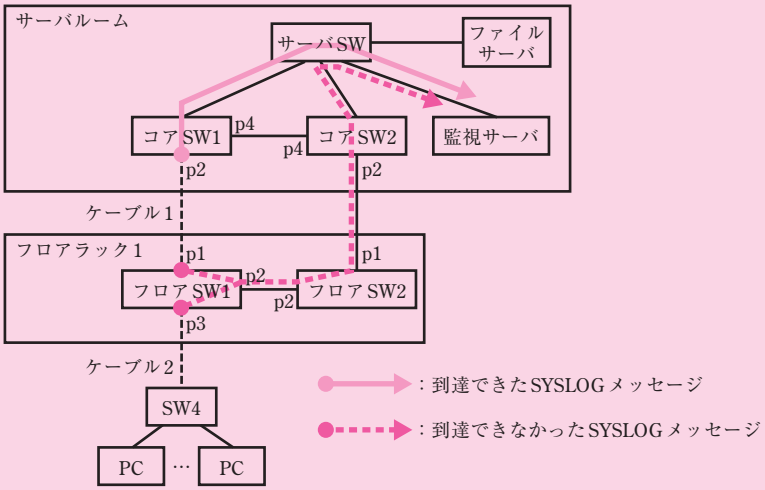


注記　破線は，断線したケーブルを示す。

図：ケーブル 1 とケーブル 2 の断線（図 2 の抜粋）

次いで，スパニングツリーの再構築，及び，ポートのリンクダウンを通知する SYSLOG メッセージが送信される。

・ケーブル 1 の断線によって，④フロア SW2 の p1 ポートの STP のポート状態がブロッキングから，リスニング，ラーニングを経て，フォワーディングに遷移した。また，監視サーバでは，SYSLOG 監視によって，ケーブル 1 が接続されているポートのリンク状態遷移が発生したことを検知した。
・ケーブル 2 の断線に伴って⑤フロア SW1 が送信した，リンク状態遷移を示す SYSLOG メッセージが監視サーバに到達できなかった。その結果，監視サーバは，ケーブル 2 が接続されているポートのリンク状態を検知できなかった。



図：SYSLOG メッセージの到達可否

ケーブル 1 の断線によって，コア SW1 は「p2 ポートのリンクダウン」を通知する SYSLOG メッセージを送信する。同様に，フロア SW1 は「p1 ポートのリンクダウン」を通知する SYSLOG メッセージを送信する。

このうち，コア SW1 が送信した SYSLOG メッセージが監視サーバに到達できる。一方，フロア SW1 が送信したものは到達できないが，その理由について，「●スパニングツリーの再構築」で解説しよう。

ケーブル 2 の断線によって，フロア SW1 は「p3 ポートのリンクダウン」を通知する SYSLOG メッセージを送信する。フロア SW1 が送信したものなので，これは到達できない。その理由についても，「●スパニングツリーの再構築」で解説しよう。

これら SYSLOG メッセージの送信と同時進行で，下線④に記されているとおり，スパニングツリーの状態遷移が生じている。それは，スパニングツリーが再構築されているからだ。

それでは，次にスパニングツリーの再構築について解説しよう。

●スパニングツリーの再構築

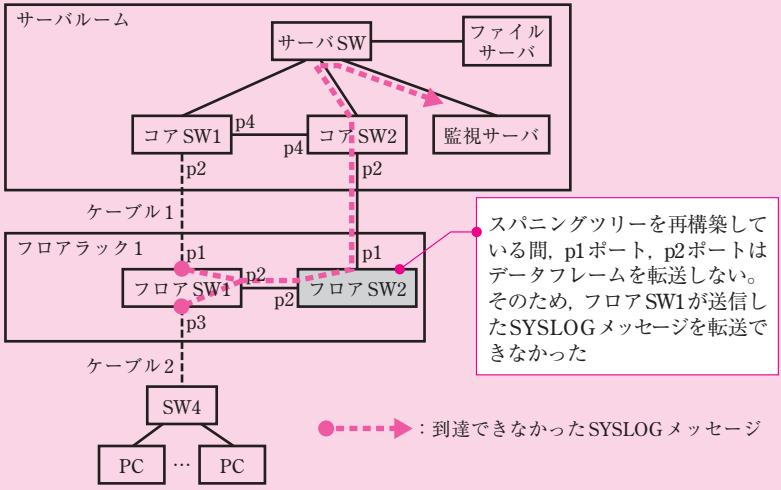
設問 3（1）で解説したとおり，ケーブルの断線によって，フロア SW2 の p2 ポートは BPDU を受信できなくなる。その結果，下線④に記された状態遷移を経て，スパニングツリーが再構築される。

STP では，スパニングツリーを再構築している間，リスニング状態，及びラーニング状態のポートは，データフレームを転送しない仕様になっている。したがって，この間，フロア SW2 の p1 ポート，p2 ポートは，データフレームを転送しない。

●解の導出

ケーブル断線の後，スパニングツリーの再構築，SYSLOG メッセージの送信が行われている。

スパニングツリーを再構築している間，フロア SW1 が SYSLOG メッセージを送信したため，経路上のフロア SW2 が SYSLOG メッセージを転送できなかった。それゆえ，監視サーバに到達できなかったことが分かる。



図：SYSLOG メッセージが到達できなかった理由

本小問が問うているのは，フロア SW1 が送信した SYSLOG メッセージが監視サーバに到達できなかった理由である。

よって，正解は，「**スパニングツリーが再構築中だったから**」となる。

■設問 4

本設問は，〔ネットワーク監視の改善策の立案〕について問うている。

（1）

解答例

SNMP エージェント：コア SW1　又は　コア SW2　又は　フロア SW1　又は
フロア SW2　又は　フロア SW3　又は　フロア SW4　又は
サーバ SW
SNMP マネージャ：監視サーバ

問題文は，「本文中の下線⑥について，SNMP エージェントと SNMP マネージャに該当する機器名を，図 1 中の機器名を用いてそれぞれ一つ答えよ」と記述されている。

下線⑥は，〔ネットワーク監視の改善策の立案〕の第 2 段落の中にある。そこには，「SNMP は機器を管理するためのプロトコルで，⑥ SNMP エージェントと SNMP マネージャで構成される」と記述されている。

これは一般的な知識から解を導く。

SNMP エージェントは監視される側であり，SNMP マネージャは監視する側である。それぞれの解を順に求めていこう。

●解の導出：SNMP エージェント

本事例における SNMP エージェントは，監視対象の機器が分かればよい。

その点について，〔監視サーバの概要〕の第 1 段落には，「監視対象機器は，コア SW，サーバ SW 及びフロア SW である」と記述されている。さらに，〔ネットワーク監視の改善策の立案〕の第 1 段落では，これらの監視対象の機器で，SNMPv2c が利用可能であると述べている。

したがって，これが SNMP エージェントとなることが分かる。

本小問は「図 1 中の機器名」を用いて答えるよう求めているので，コア SW，サーバ SW 及びフロア SW に該当する機器名を一つ答えればよい。

よって，正解は解答例に示したとおりとなる。

●解の導出：SNMP マネージャ

本事例における SNMP マネージャは，監視サーバが分かればよい。

本文中には，SNMP マネージャの機能をサポートしているサーバの存在が明記されていないが，唯一の候補と言えるのは，既存の監視サーバ（正式名称は「統合監視サーバ」）である。

この監視サーバは，ping による死活監視，SYSLOG による異常検知監視を行っている。このたび，ネットワークの異常を監視サーバで検知できなかったという問題が発生し，その改善策として，SNMPv2c を使って監視することを検討している。

したがって，SNMPv2c で検知した異常を，引き続き監視サーバで管理するのは，至極当然の流れと言えよう。それゆえ，監視サーバが SNMP マネージャとなることが分かる。

よって，正解は解答例に示したとおりとなる。

(2)

解答例

ポーリング：5分ごとに状態を取得するので多くの場合異常検知が遅れる。（28字）

トラップ：到達確認がないのでメッセージが失われる可能性がある。（26字）

問題文は，「本文中の下線⑦について，ポーリングとトラップの問題を……述べよ」と記述されている。

下線⑦は，〔ネットワーク監視の改善策の立案〕の第 4 段落の中にある。そこには，「⑦5 分間隔のポーリング，又はトラップを使用して監視しても，今回発生したネットワークの異常においてはそれぞれ問題があることが分かった」と記述されている。

今回発生したネットワークの異常は，ケーブルの断線である。そのとき問題視されたのは，その異常を監視サーバが検知できなかったことである。

これを検知できなかった理由は，設問 3（2）で解説したとおり，ケーブルの断線によるリンクダウンを SYSLOG メッセージで通知したとき，ケーブルの断線によるスパニングツリーの再構築が同時進行で行われており，再構築中のスイッチが SYSLOG メッセージを転送できなかったためである。

つまり，SNMPv2c の導入で解決すべきことは，今回発生したネットワークの異常において，スパニングツリーの再構築が行われたとしても，監視サーバが異常を検知できるようにすることである。

それでは，SNMP のポーリング，又はトラップを用いれば解決できるだろうか。下線⑦によると，それぞれ問題があることが示されている。要するに，解決策になり得ない理由があるわけだ。

本小問が問うているのは，ポーリング，トラップが抱える問題点である。その答えを見つけるには，解決策となり得ない理由を考えてみればよい。

●ポーリング

ポーリングとは，第 3 段落に記されているとおり，「SNMP マネージャが，SNMP エージェントに対して，例えば 5 分ごとといった定期的に MIB の問合せを行うことによって，機器の状態を取得」することである。

インタフェースのリンクアップ／ダウンは MIB に定義されているので，これを取得すれば今回の異常を検知することができる。

スパニングツリーの再構築に要する時間は，最大で 50 秒である。それゆえ，5 分間隔でポーリングすれば，最短で 50 秒，最長で 5 分 50 秒後にリンクダウンを検知することができる。

［最短］
- リンクダウン
- 再構築（50 秒）
- 再構築の終了直後にポーリング（異常検知に成功）

［最長］
- リンクダウン
- 再構築（50 秒）
- 再構築の終了直前にポーリング（再構築中のためポーリングの転送に失敗）
- ポーリング間隔の経過（5 分）
- ポーリング（異常検知に成功）

しかしながら，5 分ごとのポーリングは，リアルタイムに状態を検知することはできない。それゆえ，ポーリングによる異常検知は，解決策としては不十分であると言える。

よって，正解は，「**5 分ごとに状態を取得するので多くの場合異常検知が遅れる**」となる。

●トラップ

トラップとは，第 3 段落に記されているとおり，「MIB に変化が起きた際に，SNMP エージェントが直ちにメッセージを送信し，SNMP マネージャがメッセージを受信することによって，機器の状態を取得」することである。

インタフェースのリンクダウンをトラップ対象のイベントとして SNMP エージェントに登録しておくことで，今回の異常を SNMP エージェントが送信することができる。

しかし，トラップには到達確認の仕組みがないという欠点がある。

したがって，今回と同様の異常によりリンクダウンが発生し，トラップの送信が「直ちに」行われると，スパニングツリーの再構築中であるため，転送に失敗することが分かる。

SNMP エージェントはトラップを送ったつもりでいるが，SNMP マネージャはそれを受け取っていない。両者ともトラップ送信に失敗したことが分からないまま，メッセージが失われてしまう。つまり，SYSLOG メッセージを使ったときと同じ問題を抱えていることが分かる。

それゆえ，トラップによる異常検知は，解決策として全くもって不十分であると言える。

よって，正解は，「**到達確認がないのでメッセージが失われる可能性がある**」となる。

(3)

解答例

ス	パ	ニ	ン	グ	ツ	リ	ー	が	再	構	築	す	る	ま	で	イ	ン	フ	ォ	ー	ム	の	再	送
信	を	繰	り	返	す	。																		

（32字）

問題文は，「本文中の下線⑧について，SNMP エージェントが満たすべき動作の内容を……述べよ」と記述されている。

下線⑧は，〔ネットワーク監視の改善策の立案〕の第 5 段落の中にある。そこには次のように記述されている。

> SNMP のインフォームでは，MIB に変化が起きた際に，SNMP エージェントが直ちにメッセージを送信し，SNMP マネージャからの確認応答を待つ。確認応答を受信できない場合，SNMP エージェントは，SNMP マネージャがメッセージを受信しなかったと判断し，メッセージの再送信を行う。C さんは，⑧今回と同様なネットワークの異常が発生した場合に備えて，SNMP マネージャがインフォームの受信を行えるよう，SNMP エージェントの設定パラメタを考えた。

設問 4（2）のトラップの解を導くときに考察したとおり，トラップには到達確認の仕組みがない。そのため，今回と同様の異常によりリンクダウンが発生し，トラップの送信が「直ちに」行われると，スパニングツリーの再構築中であるため，転送に失敗する。

一方，SNMP のインフォームでは，SNMP エージェントはメッセージを送信した後，SNMP マネージャからの確認応答を待つ。確認応答を受信できない場合，SNMP エージェントは，SNMP マネージャがメッセージを受信しなかったと判断し，メッセージの再送信を行う。

スパニングツリーの再構築が原因で転送に失敗したならば，確認応答が受信できないため，インフォームを再送信すればよい。要は，スパニングツリーの再構築が終わるまで，再送信を繰り返せばよいのだ。

したがって，本小問が問うている「SNMP マネージャがインフォームの受信を行えるようにするための，SNMP エージェントの設定」とは，「スパニングツリーが再構築するまでインフォームの再送信を繰り返す」ことである。

よって，これが正解となる。

参考までに，具体的な設定内容の例を挙げておこう。ある製品は，インフォームの送信に関し，次に示すパラメタを設けている。

表：SNMP エージェントの設定パラメタの例

パラメタ	内容
タイムアウト	インフォームに対する確認応答の時間を設定する
再送信回数	インフォームを再送信する最大回数を設定する。確認応答がない場合，ここに設定された回数まで再送信を行う

スパニングツリーの再構築の所要時間は最大 50 秒である。その点を考慮に入れるなら，「タイムアウト時間×リトライ回数」が 50 秒を上回るように設定すれば，スパニングツリーの再構築後に再送信が行えるようになる。

問 3

出題趣旨
企業内ネットワークにおいて，複数の拠点間を接続する方法には様々な方法があるが，効率性や安定性や運用容易性，その他の様々な要件を考慮しながら，利用可能な回線サービスとネットワーク技術を組み合わせて，最適な拠点間接続構成をとることが求められている。そうした中，特定の WAN サービスを利用しながら，別の WAN サービスをバックアップ回線として利用することで，信頼性の高いネットワークを構築することが，一般的に行われている。 本問では，専用線を基本的に利用している企業内ネットワークから，IP-VPN とインターネット VPN の両方式を活用した企業内ネットワークへの再構築を通じて，複数回線サービス利用の信頼性の高いネットワークを構築する能力を問う。

採点講評
問 3 では，企業内ネットワーク再構築を題材として，IP-VPN とインターネット VPN の両方式の VPN と複数のルーティングプロトコルを利用した冗長ネットワーク構築技術について出題した。全体として，正答率は低かった。 設問 1 及び設問 2 は，主に MPLS の基本事項について出題したが，正答率は低かった。MPLS は IP-VPN サービスの中核を成す技術であり，MPLS を理解することは，VPN 技術を理解するためにも役に立つので基本は押さえておいてほしい。 設問 3(1)は，OSPF ネットワーク内の IPsec トンネル上での GRE over IPsec の利用についてその目的を出題したが，正答率は低かった。IPsec トンネル上での GRE over IPsec の利用は OSPF ネットワークでは必要な技術であるので，理解しておいてほしい。 設問 4(1)は，フルメッシュな IPsec トンネルのネットワークにおける課題を出題したが，正答率は高かった。ネットワークトポロジに関する基本的な理解がうかがわれた。

設問		解答例・解答の要点		備考
設問 1		ア	ラベル	
		イ	PE ルータ	
		ウ	ネットワーク	
		エ	IP-VPN	
		オ	インターネット VPN	
設問 2	(1)	MPLS		
	(2)	利用者ごとのトラフィックを区別するため		
設問 3	(1)	OSPF のマルチキャスト通信を通すため		
	(2)	ほかの拠点への経路情報		
	(3)	BGP4 から得られた経路を優先する。		
設問 4	(1)	新拠点追加のときに全拠点の設定変更が必要になるから		
	(2)	大阪支店の FW2 のグローバル IP アドレス		
	(3)	機器	FW2，FW3	
		設定	OSPF のプライオリティを 0 に設定する。	

本問は，本社と二つの支店（名古屋，大阪）を拠点にもつネットワークにおいて，企業内ネットワークを再構築する事例を取り上げている。

本問は，GRE over IPsec，OSPF，BGP について出題している。詳しくは本書の次の章を参照していただきたい。

表：出題されている要素技術

要素技術	掲載箇所
GRE over IPsec	第 8 章「8.4.5　IPsec」「● GRE over IPsec」
OSPF	第 3 章「3.8.5　OSPF」
BGP	第 3 章「3.8.6　BGP」

●本問の全体像

・WAN 構成の検討

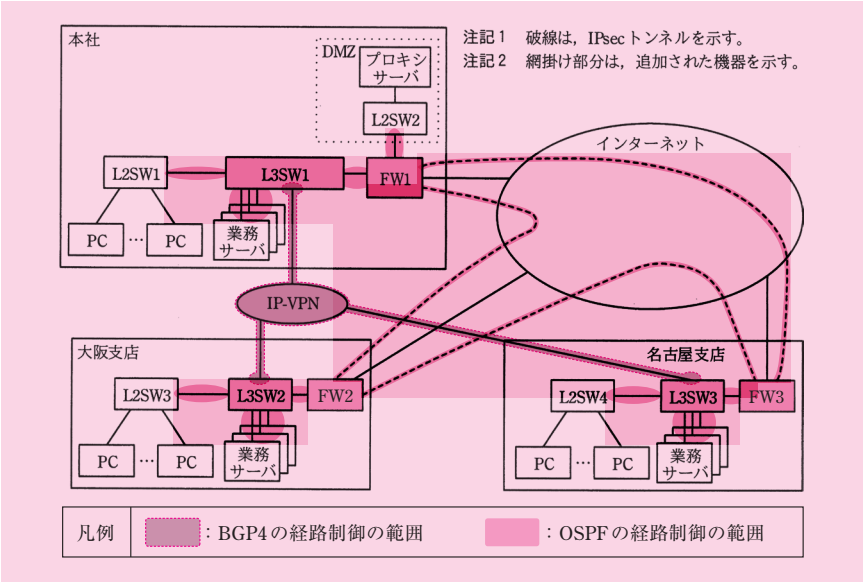
事例に登場する D 社は，東京の本社，名古屋支店及び大阪支店の 3 拠点をもっている。

このたび WAN 構成を見直すこととなり，その方針案を検討した。その点について，〔WAN 構成の検討〕「(1) WAN 構成の見直し方針案」の第 1 段落の中で，次のように記述されている。適宜抜粋して掲載しておこう。

> ・IP-VPN を利用して 3 拠点間を接続する。
> ・通常時は拠点間通信に IP-VPN を用いるが，IP-VPN の障害時にはインターネット VPN をバックアップ回線として用いる。

この検討に基づいて，図 2 に示すネットワーク構成案を策定した。

ここに登場する IP-VPN 網は，その内部が MPLS 網で構築されている。MPLS について，設問 1，2 で問われている。



図：見直し方針に基づくネットワーク構成（図 2 の抜粋）

・冗長化ルーティングの検討

通常時は拠点間通信に IP-VPN を用い，IP-VPN の障害時にはインターネット VPN をバックアップ回線として用いるため，このネットワークではダイナミックルーティングプロトコルを使用する。

その点については，〔冗長化ルーティングの検討〕の第 1 段落の中に記述されている。

要点をまとめると，次のとおりとなる。

- 各拠点間の IPsec トンネル及び各拠点内 LAN のルーティングは，OSPF を利用する（1 番目の箇条書き）。
- IP-VPN 網経由での拠点間のルーティングは，BGP4 を利用する（3 番目の箇条書き）。

2 種類のルーティングを組み合わせた方式について，設問 3 で問われている。

・自動トンネリングの検討

インターネット VPN は，本社を中心とするハブアンドスポーク構成のトンネルを固

定的に設定する。スポーク間のトンネル接続は，必要に応じて動的に生成する。

この点について，設問 4 で問われている。

・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
WAN 構成の検討	見直し方針案 IP-VPN 及び IPsec の概要 図 2「E さんが考えた D 社のネットワーク構成（抜粋）」	1	空欄ア～ウ
		2	(1) ～ (2)
冗長化ルーティングの検討	OSPF と BGP4 を組み合わせた経路制御	1	空欄エ～オ
		3	(1) ～ (3)
拠点追加の場合の IPsec トンネル接続追加の検討	フルメッシュ構成を手動設定する問題点 自動トンネリング機能の設定	4	(1) ～ (3)

● MPLS

本問の設問 1，設問 2 の中で，MPLS が登場する。複数の設問に関わるので，ここであらかじめ解説しておこう。

MPLS（Multi Protocol Label Switching）とは，ラベルと呼ばれる固定長のヘッダを IP パケットに付与してカプセル化し，パケットを高速に転送する技術である。

MPLS 対応ルータ（LSR：Label Switching Router）によって構成された IP ネットワーク（以下，MPLS 網という）では，独自のラベルを基にした転送を行う。

MPLS 網のエッジ（出入口）に位置する LSR を LER（Label Edge Router）と呼ぶ。LER は，MPLS 網へ入ってくる IP パケットにラベルを与え，MPLS 網から出てくる IP パケットからラベルを取り去る。この仕組みにより，エンド間の通信では MPLS 網の存在が透過的になっている。

・IP-VPN 網での MPLS の使用

本事例に登場する IP-VPN 網は，その内部が MPLS 網で構築されている。

IP-VPN 網の出入口となる PE（Provider Edge）ルータが，MPLS 網の LER である。

送信元拠点の CE（Customer Edge）ルータから送られた IP パケットは，入口とな

る PE ルータでラベルが付与される。MPLS 網内を転送した後，出口となる PE ルータに到着したらラベルが除去され，元の IP パケットが宛先拠点の CE ルータに送られる。

IP-VPN 網には複数の利用者が接続している。例えば本事例では D 社が利用しているが，D 社以外の企業も利用しているはずだ。

もしかすると，複数の異なる利用者の拠点において，たまたま同じネットワークアドレス（例：192.168.0.0/24 等のプライベートアドレス）が割り当てられているかもしれない。そのような場合であっても，それら利用者間でパケットが混在することがあってはならない。

つまり，IP-VPN の MPLS 網では，利用者を区別する必要があるわけだ。

これを実現するため，MPLS のラベルには，利用者ごとのトラフィックを区別する情報が格納されている。これにより，同一の利用者の拠点間でのみパケットが転送される仕組みになっている。

・MPLS による転送の仕組み

本問の範囲を超えるが，良い機会なので，MPLS による転送の仕組みについて簡潔に解説しよう。

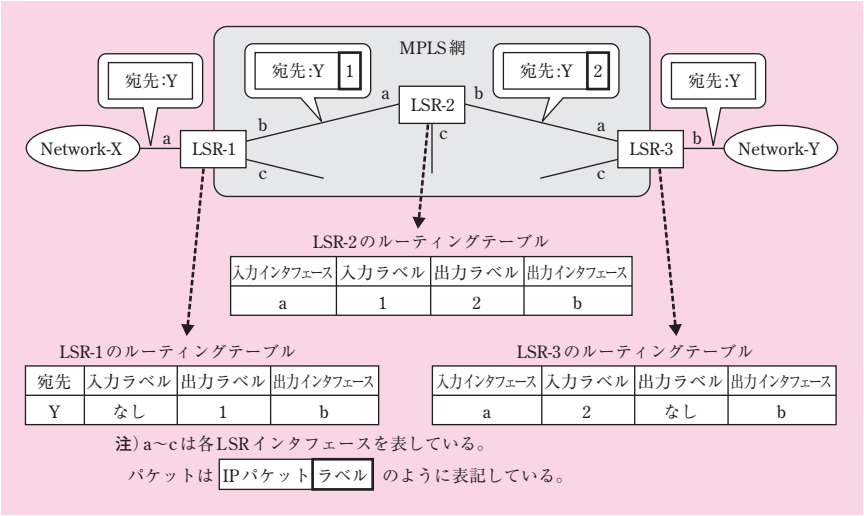
先ほど述べたとおり，MPLS 網内では，転送される IP パケットにラベルが付与されている。

このラベルは，利用者の拠点のネットワークごとに，それぞれ異なる値が割り当てられる。つまり，ラベルは，拠点のネットワークを識別する役割を果たしているわけだ。

なお，利用者の拠点が複数のサブネットワークから構成される場合，通常，これを集約したネットワークアドレスに対し，ラベルの値を割り当てる。

ラベルの値は，LSR ごとに付け替えられる。LSR 同士は LDP（Label Distribution Protocol）を用いて経路情報の交換を行っており，経路変更に伴い適切なラベル値を割り当てている。

ラベルを用いて転送経路を決定する様子を次の図に示す。図中の LSR-1，LSR-3 が LER（IP-VPN 網の PE ルータ）である。



図：ラベルを用いて転送経路を決定する様子

この図に基づき，MPLS がパケットを転送する手順を次に示す。

1. 拠点 X のホストが，拠点 Y のホストを宛先とする IP パケットを送信する。
2. この IP パケットが拠点 X の CE ルータに到着すると，拠点 X の入口となる PE ルータ，すなわち，LSR-1 に転送する。
3. この IP パケットが LSR-1 に到着すると，LSR-1 は出力インタフェースを決定するとともに，ラベルを付与する。
   今の例では，入力インタフェースが「a」，出力時点のラベルの値が「1」，出力インタフェースが「b」となる。
   その後，LSR-1 は MPLS パケットを LSR-2 に転送する。
4. この MPLS パケットが LSR-2 に到着すると，LSR-2 はラベルを付け替えるとともに，出力インタフェースを決定する。
   今の例では，入力インタフェースが「a」，入力時点のラベルの値が「1」であることを読み取り，出力インタフェースとして「b」を決定する。そして，出力する際，ラベルの値を「1」から「2」に置き換える。
   その後，LSR-2 は MPLS パケットを LSR-3 に転送する。
5. この MPLS パケットが LSR-3 に到着すると，LSR-3 は出力インタフェースを決定するとともに，ラベルを除去する。
   今の例では，入力インタフェースが「a」であり，入力時点のラベルの値が「2」

であることを読み取って，インタフェース b を選択する。

LSR-3 は，拠点 Y への出口となる PE ルータである。LSR-3 は，ラベルを除去して元の IP パケットを取り出してから，これを拠点 Y の CE ルータに転送する。

6. この IP パケットが拠点 Y の CE ルータに到着すると，宛先となるホストに転送する。
7. 拠点 Y の宛先ホストが，この IP パケットを受信する。

これまで解説したように，MPLS のルーティングでは，ラベル値に基づいて転送している。これは，ロンゲストマッチアルゴリズムに基づくルーティングより簡単な仕組みであるため，それよりも高速な転送を実現できる。

以上で MPLS の仕組みを概観できた。本問を解く準備が整ったところで，それでは，いよいよ設問の解説に移ろう。

■設問 1

解答例

ア：ラベル
イ：PE ルータ
ウ：ネットワーク
エ：IP-VPN
オ：インターネット VPN

本設問は，本文中の空欄ア～エに入れる字句を問うている。

［ア］，［イ］

空欄ア，イは，〔WAN 構成の検討〕「(2) IP-VPN 及び IPsec の概要」「(i) IP-VPN」の中にある。

冒頭の「● MPLS」で解説したとおり，IP-VPN 網は，その内部が MPLS 網で構築されている。その点を踏まえ，空欄ア，イを含む箇条書きを見てみよう。そこには次のように記述されている。

・利用者のネットワークと事業者閉域 IP 網との接続点において，利用者が設置する CE（Customer Edge）ルータから送られたパケットは，通信事業者の PE（Provider Edge）ルータで［ア］と呼ばれる短い固定長のタグ情報が付与される。
・事業者閉域 IP 網内では，②タグ情報を参照して中継され，［ア］は対向側の［イ］で取り除かれる。

送信元拠点の CE ルータから送られた IP パケットは，入口となる PE ルータに到着すると，ラベルが付与される。

よって，空欄アの正解は，「**ラベル**」となる。

ラベルが付与された MPLS パケットは，その後，MPLS 網内を転送される。最終的に，宛先拠点への出口となる PE ルータに到着すると，ラベルが除去される。

よって，空欄イの正解は，「**PE ルータ**」となる。

［ウ］

空欄ウは，〔WAN 構成の検討〕「(2) IP-VPN 及び IPsec の概要」「(ⅱ) IPsec」の中にある。そこには，「IPsec は，OSI 基本参照モデルの［ウ］レイヤで動作する」と記述されている。

IPsec は，IP パケットをカプセル化し，暗号化とメッセージ認証を行う機能を備えたプロトコルである。IP はネットワークレイヤのプロトコルであるから，空欄ウに当てはまる字句は「**ネットワーク**」となる。

よって，これが正解となる。

［エ］，［オ］

空欄エ，オは，〔冗長化ルーティングの検討〕の第 1 段落の中にある。そこには，「図 2 のネットワーク構成で拠点間通信を行う場合，正常時は［エ］を利用するが，［エ］の障害時は［オ］に切り替える必要がある」と記述されている。

現在，D 社では WAN 構成の再構築を検討している。その内容については〔WAN 構成の検討〕の中に記述されており，その検討を基に考えたネットワーク構成が図 2 である。

したがって，〔WAN 構成の検討〕を見てみれば，正常時，障害時に使用する WAN 回線が何であるかが分かるはずだ。

その点について，〔WAN 構成の検討〕「(1) WAN 構成の見直し方針案」の 3 番目の箇条書きには，次のように記述されている。

・通常時は拠点間通信に IP-VPN を用いるが，IP-VPN の障害時にはインターネット VPN をバックアップ回線として用いる。

したがって，図 2 のネットワーク構成で拠点間通信を行う場合，正常時は IP-VPN を用い，IP-VPN の障害時はインターネット VPN に切り替えることが分かる。

よって，空欄エの正解は「**IP-VPN**」となり，空欄オの正解は「**インターネット VPN**」となる。

■設問 2

本設問は，〔WAN 構成の検討〕について問うている。

本設問で出題されている MPLS について，冒頭の「● MPLS」で解説しているので，詳しくはそちらを参照していただきたい。

(1)

解答例

MPLS

問題文は，「本文中の下線①について，IP-VPN サービス提供のために事業者閉域 IP 網内で用いられるパケット転送技術を答えよ」と記述されている。

下線①は，〔WAN 構成の検討〕「(2) IP-VPN 及び IPsec の概要」「(i) IP-VPN」の 2 番目の箇条書きの中にある。そこには，「IP-VPN は，①事業者閉域 IP 網内で複数の利用者のトラフィックを中継するのに，RFC 3031 で規定された方式が用いられる」と記述されている。

これは一般的な知識から解を導く。

IP-VPN 網内で，複数の利用者のトラフィックを中継するために用いられるプロトコルは，MPLS である。これは RFC 3031「Multiprotocol Label Switching Architecture」で規定されている。

よって，正解は，「**MPLS**」となる。

(2)

解答例

利用者ごとのトラフィックを区別するため（19字）

問題文は，「本文中の下線②について，事業者閉域 IP 網内の利用者トラフィック中継処理において，タグ情報を利用する目的を……述べよ」と記述されている。

下線②は，〔WAN 構成の検討〕「(2) IP-VPN 及び IPsec の概要」「(ⅰ) IP-VPN」の中にある。下線②の前後に空欄ア，イがあるので，そこを補填した上で抜粋してみよう。

> ・利用者のネットワークと事業者閉域 IP 網との接続点において，利用者が設置する CE（Customer Edge）ルータから送られたパケットは，通信事業者の PE（Provider Edge）ルータでラベルと呼ばれる短い固定長のタグ情報が付与される。
> ・事業者閉域 IP 網内では，②タグ情報を参照して中継され，ラベルは対向側の PE ルータで取り除かれる。

下線②の「タグ情報」は，文脈から明らかなように，ラベルを指している。

冒頭の「● MPLS」で解説したとおり，IP-VPN 網は MPLS 網で構築されており，その網内は MPLS のラベルを用いて転送されている。

網内で複数の利用者のトラフィックを中継する必要があるため，ラベルには，利用者ごとのトラフィックを区別する情報が格納されている。これにより，同一の利用者の拠点間でのみパケットが転送される仕組みになっている。

したがって，ラベル（タグ情報）を利用する目的は，「**利用者ごとのトラフィックを区別するため**」となる。よって，正解は解答例に示したとおりとなる。

■設問 3

本設問は，〔冗長化ルーティングの検討〕について問うている。

（1）

解答例

O	S	P	F	の	マ	ル	チ	キ	ャ	ス	ト	通	信	を	通	す	た	め

（19字）

問題文は，「本文中の下線③について，GRE over IPsec を利用する目的を……述べよ」と記述されている。

下線③は，〔冗長化ルーティングの検討〕の第 1 段落の中にある。そこには次のように記述されている。

> ・各拠点間の IPsec トンネル及び各拠点内 LAN のルーティングは，OSPF を利用する。
> ・各拠点間の IPsec トンネル接続では，③ GRE over IPsec を利用する。

本小問は，一般的な知識から解を導くことができる。

ここに，「各拠点間の IPsec トンネル及び各拠点内 LAN のルーティングは，OSPF を利用する」とあるので，OSPF が経路制御する範囲には，IPsec トンネルが含まれていることが分かる。したがって，OSPF のリンクステート情報を交換するパケットが IPsec トンネル区間を通過する。

OSPF は，IP マルチキャストパケットを用いて，経路のリンクステート情報を交換している。

しかし，IPsec は，IP マルチキャストパケットを直接カプセル化することができない。

OSPF のマルチキャスト通信を通すため，本事例では，下線③に示されているとおり，GRE over IPsec を使用している。

よって，正解は，「**OSPF のマルチキャスト通信を通すため**」となる。

なお，IPsec が IP マルチキャストパケットをカプセル化できない技術的な理由について，詳しくは，本書の第 8 章「8.4.5　IPsec」の「● IPsec で IP マルチキャストパケットを直接カプセル化できない」を参照していただきたい。

● GRE over IPsec

さて，本小問の解は得られたが，良い機会なので，本問に登場した GRE over IPsec について解説しておこう。

ここ数年，IPsec パケットをトンネリングする技術が立て続けに出題されている。

- GRE over IPsec によるトンネリング　　平成 30 年午後Ⅰ問 3（本問）
- IP in IP による IPsec のトンネリング　　平成 29 年午後Ⅰ問 3
- GRE over IPsec によるトンネリング　　平成 28 年午後Ⅱ問 2
- L2TP over IPsec によるトンネリング　　平成 28 年午後Ⅰ問 2

本問と同様に，平成 28 年午後Ⅱ問 2 の事例においても，WAN 回線を冗長化し，ダイナミックルーティングプロトコルで経路制御しており，GRE over IPsec が OSPF のマルチキャスト通信を通すために使用されていた。

こういった出題を踏まえ，トンネリング技術について習熟しておくことをお勧めしたい。

さて，話を GRE over IPsec に戻そう。

GRE over IPsec は，トンネリングに GRE を用い，トンネル区間の暗号化に IPsec を用いる技術である。

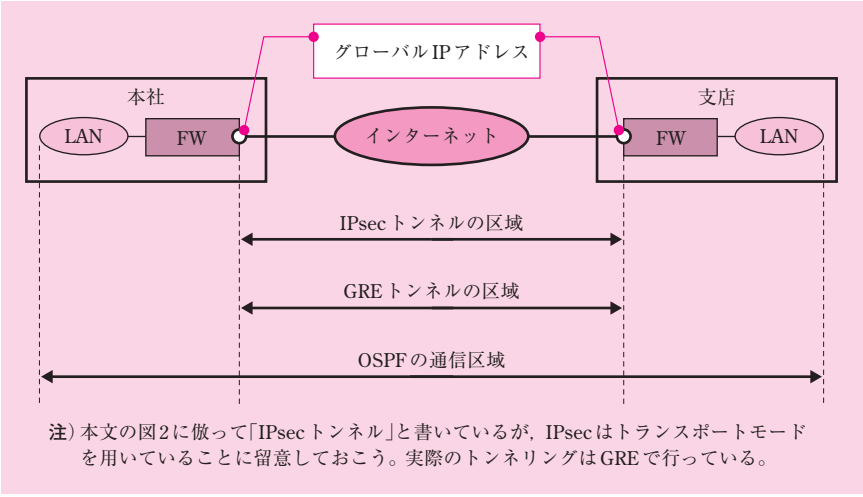
GRE でトンネリングすることによって，インターネット区間を仮想的な専用線とみなして通信することを可能にしている。この GRE のトンネル区間は，図 2 に当てはめると，本社 FW と支店 FW を両端とする区間となる。要するにインターネット区間と同じである。

そして，その GRE パケットを IPsec でカプセル化することによって，インターネット区間を通過する GRE パケットを暗号化し，セキュリティを確保している。

IPsec でカプセル化するときは，トランスポートモードを用いる。既に GRE でトンネリングしているので，IPsec で再度トンネリングする必要がないからである。

この点を考慮すると，図 2 の中に「IPsec トンネル」と書かれているが，実際には「GRE トンネル」である。あるいは，「GRE over IPsec トンネル」と言ってよいだろう。なお，本書の解説では，本文に倣って「IPsec トンネル」という表記を用いることにする。

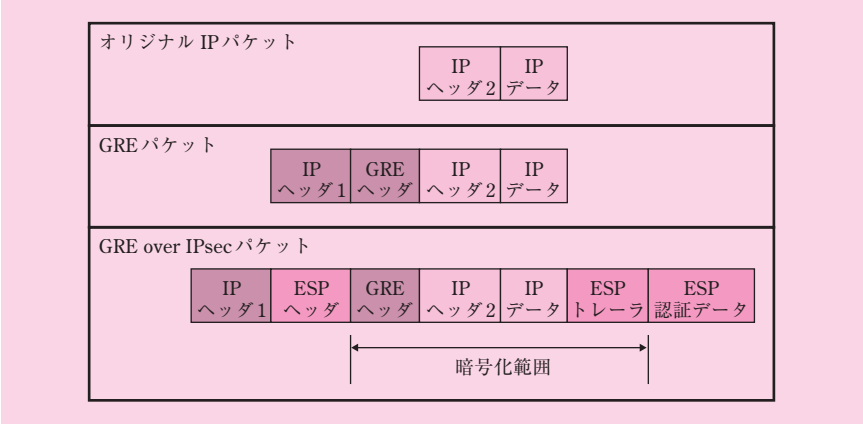
OSPF は，本文に書いてあるとおり「各拠点間の IPsec トンネル及び各拠点内 LAN のルーティング」に利用されるため，その経路制御の範囲に IPsec トンネルが含まれている。つまり，トンネル区間と OSPF 通信区間の関係を図示すると，次の図のように整理できる。



注）本文の図 2 に倣って「IPsec トンネル」と書いているが，IPsec はトランスポートモードを用いていることに留意しておこう。実際のトンネリングは GRE で行っている。

図：GRE over IPsec を稼働させたときの，トンネルの区間，OSPF 通信の区間

IPsec トンネル区間を通過する GRE over IPsec パケットのフォーマットを次の図に示す。



図：GRE over IPsec のパケットフォーマット

図中の「オリジナル IP パケット」が，本小問で問われた，OSPF のリンクステート情報交換に用いられる IP マルチキャストパケットである。つまり，IP ヘッダ 2 の宛先 IP アドレスが IP マルチキャストアドレスとなるわけだ。

これを GRE でカプセル化すると，IP ヘッダ 1 が付与される。この宛先／送信元 IP アドレスは，仮想的な専用線の区間（すなわちインターネット区間）の両端アドレスとなるから，本社又は支店の FW のグローバル IP アドレスとなる。つまり，IP ヘッダ 1 は IP ユニキャストアドレスとなるわけだ。

以上をまとめると，トンネリングプロトコルである GRE パケットで IP マルチキャストパケットをカプセル化し，それをさらに IPsec でカプセル化している。GRE は IP ユニキャストパケットなので，IPsec でカプセル化できる。

このようにして，OSPF のマルチキャスト通信が IPsec トンネルを通過できるのである。

(2)

解答例

ほ か の 拠 点 へ の 経 路 情 報 （11 字）

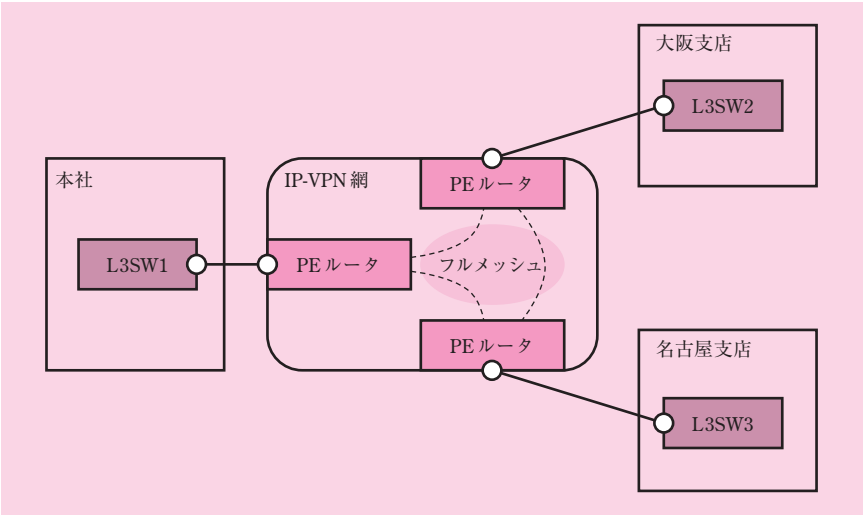
問題文は，「本文中の下線④について，各拠点の CE ルータが受信する経路情報を……答えよ」と記述されている。

下線④は，〔冗長化ルーティングの検討〕の第 1 段落の 3 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。

> ・CE ルータでもある各拠点の L3SW は，IP-VPN 側で隣接する PE ルータと BGP4 で経路交換する。具体的には，各拠点の L3SW は，自拠点の経路情報を PE ルータに広告するとともに，④ PE ルータから経路情報を受信する。

IP-VPN 網は多数の通信機器からなる事業者 IP 網であるが，利用者から直接見えるのは PE ルータである。IP 網内はブラックボックスであり，何らかの方法で PE ルータがあたかもフルメッシュで接続されているかのように見える。

つまり，本事例の図 2 のネットワーク構成において，IP-VPN 網は，次の図に示すようなイメージでとらえることができる。



図：本事例における IP-VPN 網のイメージ

この IP-VPN 網において，L3SW（すなわち CE ルータ）と PE ルータが，BGP4 を用いた経路情報の交換を行っている。この経路広告は，隣接する CE ルータと PE ルータ間，及び，PE ルータ相互間でやり取りされている（「PE ルータ相互間」でやり取りされているかのように見えるが，実際には MPLS により IP-VPN 網内で転送されている）。

その結果，ある拠点の経路情報は，次に示す手順を経て，他の拠点に経路広告される。

1. 自拠点の L3SW は，隣接する PE ルータに対し，自拠点の経路情報を広告する。
2. 自拠点の PE ルータは，他拠点の PE ルータに対し，この経路情報を広告する。
3. 他拠点の PE ルータは，隣接する L3SW に対し，この経路情報を広告する。

裏を返せば，同様に他拠点の経路情報も，自拠点に広告されているのである。

したがって，本小問で問うている，各拠点の CE ルータが受信する経路情報は，「**ほかの拠点への経路情報**」である。

よって，正解は解答例に示したとおりとなる。

なお，BGP について，詳しくは本書の第 3 章「3.8.6　BGP」を参照していただきたい。

(3)

解答例

B	G	P	4	か	ら	得	ら	れ	た	経	路	を	優	先	す	る	。

（18字）

問題文は，「本文中の下線⑤について，E さんが検討したルーティング方式において，L3SW での経路の優先選択の考え方を……述べよ」と記述されている。

下線⑤は，〔冗長化ルーティングの検討〕の第 2 段落の中にある。そこには次のように記述されている。

> この方式で，本社，名古屋支店，大阪支店の L3SW からそれぞれの別拠点への経路の冗長化を行う。各拠点の L3SW は，⑤複数のルーティングプロトコルから得た同一宛先への異なる経路情報から，適切な経路を選択する。

ここに記されている「この方式で」とは，第 1 段落に説明されている方式である。まず，第 1 段落に示された方針は次のとおりである。

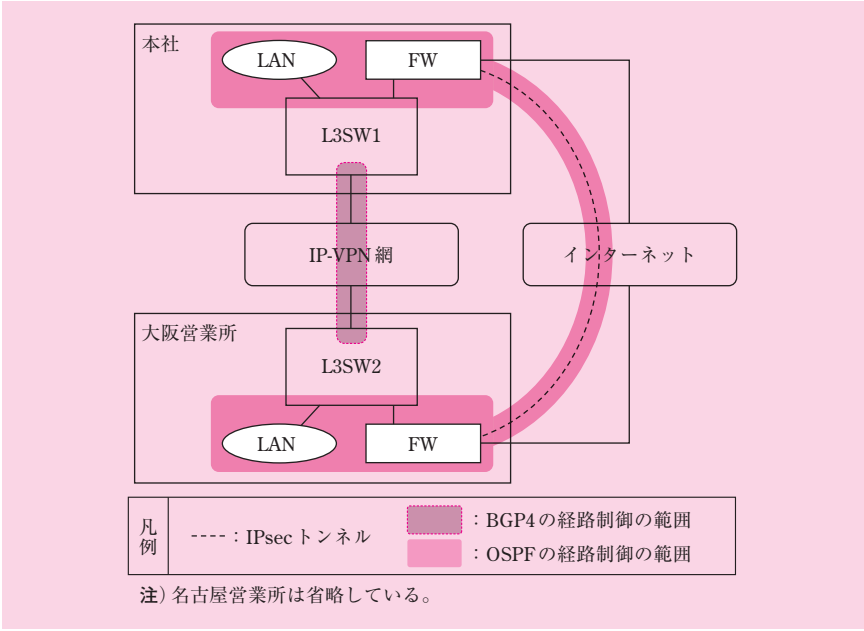
> ［方針］正常時は IP-VPN を利用し，IP-VPN の障害時はインターネット VPN を利用する（第 1 段落の本文）。

この方針に基づく方式をまとめると，次のとおりとなる。

> ［方式 1］各拠点間の IPsec トンネル及び各拠点内の LAN のルーティングは，OSPF を利用する（1 番目の箇条書き）。
> ［方式 2］IP-VPN 網経由での拠点間のルーティングは，BGP4 を利用する（3 番目の箇条書き）。

つまり，OSPF によるルーティングと，BGP4 によるルーティングの二つの経路制御を用いているわけだ。

それぞれのルーティングの経路制御の範囲を次の図に示す。



注）名古屋営業所は省略している。

図：OSPF，BGP4 の経路制御の範囲

この図を見ると，二つのルーティングの経路制御の範囲は，L3SW で重なり合っている。つまり，L3SW から見ると，自拠点から他拠点への経路情報が，OSPF 及び BGP4 から広告されているわけだ。

下線⑤に「複数のルーティングプロトコルから得た同一宛先への異なる経路情報」とあるとおり，OSPF 及び BGP4 から経路広告される拠点の経路情報は，ネットワークアドレス（IP アドレスとサブネットマスク長）の値が等しくなる。

このように，複数の異なるルーティング方式を用いる場合，同一宛先への経路情報が，それぞれルーティングテーブルにエントリされることがある。

同一宛先の経路が複数あるとき，ロンゲストマッチアルゴリズムでは，どちらか一方の経路を選択することができない。つまり，BGP4 に基づく IP-VPN 経由にすればよいか，OSPF に基づくインターネット VPN 経由にすればよいのか，判断できないのだ。

このような場合，ルーティング方式にあらかじめ優先度を付与しておくことで，どちらか一方の経路を選択させることができる。

もしも優先度の高い方の経路において障害が発生し，その経路広告が途絶えたならば，この経路情報がルーティングテーブルから消去される。その結果，優先度の低い方の経路情報だけが残されるので，今度はそちらの経路情報が選択されるのである。

このようにして，経路の冗長化を実現できる。

参考までに，この「優先度」を意味する用語の名称はベンダにより異なるが，Cisco Systems 社の場合，「アドミニストレイティブディスタンス」という。

本事例では，先ほど「方針」にまとめたとおり，正常時は IP-VPN を利用し，IP-VPN の障害時はインターネット VPN を利用する。したがって，BGP4 から経路広告された経路情報の優先度を高くすることで，この方針に沿った経路制御を実現することができる。

よって，正解は「**BGP4 から得られた経路を優先する**」となる。

■設問 4

本設問は，〔拠点追加の場合の IPsec トンネル接続追加の検討〕について問うている。

(1)

解答例

新拠点追加のときに全拠点の設定変更が必要になるから（25字）

問題文は，「本文中の下線⑥について，望ましくない理由を……述べよ」と記述されている。

下線⑥は，〔拠点追加の場合の IPsec トンネル接続追加の検討〕の第 1 段落の中にある。そこには，「E さんは，IPsec トンネル接続の追加について，今後拠点が追加になった場合を想定した検討を始めた。図 2 のような⑥フルメッシュの IPsec トンネルのネットワーク構成に，追加拠点向け IPsec トンネルを手動で追加設定するネットワーク拡張方式は望ましくないと考え（た）」と記述されている。

IPsec トンネルは仮想的な専用線である。したがって，その設定は，トンネルの両端拠点のそれぞれで行う必要がある。つまり，トンネル 1 本につき 2 個である。

ここで，具体的な状況を考察してみよう。

今，図 2 では三つの拠点が記されている。新たに拠点が一つ追加され，フルメッシュで構成させるとしよう。

このとき 3 本のトンネルを追加するので，本社，名古屋支店，大阪支店にそれぞれ 1 個（1 本分）ずつの設定を行い，新拠点に 3 個（3 本分）の設定を行う必要がある。

つまり，全拠点の設定変更が必要となることが分かる。

本小問は，このようなフルメッシュで IPsec トンネルを構成する場合，追加拠点向け IPsec トンネルの設定を手動で行う方式が望ましくない理由を問うている。したがって，先ほど述べたとおり，「新拠点を追加するたび，全拠点の設定変更が必要となる」旨を解答すればよい。

よって，正解は解答例に示したとおりとなる。

(2)

解答例

大阪支店のFW2のグローバルIPアドレス （20字）

問題文は，「本文中の下線⑦について，NHRP から得られる情報を……答えよ」と記述されている。

下線⑦は，〔拠点追加の場合の IPsec トンネル接続追加の検討〕の第 2 段落の中にある。

まず文脈を考慮してみよう。第 1 段落の中で，フルメッシュで IPsec トンネルを構成する場合，追加拠点向け IPsec トンネルの設定を手動で行う方式が望ましくないと考えた。その結果，ネットワーク機器ベンダから

> IPsec トンネルを動的に確立する機能（以下，自動トンネル機能という）

を活用した方式を提案されている。

この方式を前提として立案した設計方式が，箇条書きで次のように記述されている。

> ・本社をハブ拠点，支店の 2 拠点をスポーク拠点とするハブアンドスポーク構成とし，ハブ拠点とスポーク拠点間の IPsec トンネルを従来どおり固定的に設定する。
> ・スポーク拠点間 IPsec トンネル（以下，S-S トンネルという）については，拠点間のトラフィックの発生に応じてトンネルを動的に確立させる。
> ・S-S トンネルは，一定時間トラフィックがなければ自動的に切断するようにする。
> ・動的に S-S トンネルを確立するために，NHRP（Next Hop Resolution Protocol）を用いる。

第 2 段落は，この NHRP の仕組みについて説明している。その中に下線⑦が含まれている。そこには次のように記述されている。

> NHRP は，IPsec トンネル確立に必要な対向側 IP アドレス情報を，トンネル確立時に動的に得るのに利用される。IPsec トンネルの確立は，スポーク拠点間での通信の発生を契機にして行われる。例えば，名古屋支店内の PC から大阪支店内のサーバへの通信が行われる場合，⑦名古屋支店の FW3 は NHRP によって得られた情報を利用して S-S トンネルを確立する。このように，自動トンネル機能を利用すれば，フルメッシュ構成のトンネルを手動で設定する必要がない。

本小問で問われているのは，名古屋支店内の PC から大阪支店内のサーバへの通信が行われる場合，名古屋支店の FW3 が NHRP によって得られる情報である。

NHRP によって得られる情報について，第 2 段落の最初に「NHRP は，IPsec トンネル確立に必要な対向側 IP アドレス情報を，トンネル確立時に動的に得るのに利用される」とある。つまり，IPsec トンネルの「対向側 IP アドレス情報」を得られることが分かる。

スポーク拠点 FW は，対向側スポーク拠点 FW の IP アドレスをどのように取得するのだろうか？

第 1 段落の 1 番目の箇条書きを見てみよう。そこには，「本社をハブ拠点，支店の 2 拠点をスポーク拠点とするハブアンドスポーク構成とし，ハブ拠点とスポーク拠点間の IPsec トンネルを従来どおり固定的に設定する」と記述されている。

この記述から，ハブ拠点である本社の FW1 には，スポーク拠点の FW のグローバル IP アドレスがあらかじめ設定されていることが分かる。したがって，NHRP を利用することにより，ハブ拠点 FW の設定情報から，対向側スポーク拠点 FW の IP アドレスを取得できることが分かる。

名古屋支店の FW3 が大阪支店の FW2 との間で S-S トンネルを確立したければ，NHRP を利用して，大阪支店の FW2 のグローバル IP アドレスを取得すればよい。

つまり，ここで問われている，NHRP を利用して得られる情報とは，「**大阪支店の FW2 のグローバル IP アドレス**」である。

よって，これが正解となる。

(3)

解答例

機器：FW2，FW3
設定：OSPFのプライオリティを0に設定する。（20字）

問題文は，「本文中の下線⑧について，追加設定が必要な機器を，図 2 中の機器名で全て答えよ。また追加すべき OSPF の設定を……述べよ」と記述されている。

下線⑧は，〔拠点追加の場合の IPsec トンネル接続追加の検討〕の第 3 段落の中にある。そこには次のように記述されている。

> ネットワーク機器ベンダの技術者からは，OSPF と自動トンネル機能を組み合わせて利用する場合の留意点の指摘があった。その指摘の内容は，“スポークとなる機器が OSPF の代表ルータに選出されてしまうと，スポーク拠点間の IPsec トンネルが解放されなくなってしまうので，それを防ぐために，スポークとなる機器の OSPF に追加の設定が必要になる”というものであった。そこで，E さんは，防止策として⑧追加すべき設定内容を定めた。

本小問は二つのことを問うている。

一つ目は，ネットワーク機器ベンダの技術者の指摘に基づき，追加設定を行う必要がある機器名である。

二つ目は，その指摘に基づいて追加した設定の内容である。

●解の導出：機器名

ネットワーク機器ベンダの技術者の指摘は，「スポークとなる機器が OSPF の代表ルータに選出されてしまうと，スポーク拠点間の IPsec トンネルが解放されなくなってしまうので，それを防ぐために，スポークとなる機器の OSPF に追加の設定が必要になる」というものであった。

つまり，この技術者が指摘している機器は，スポークとなる機器である。

IPsec トンネルの端点に位置するのは FW であるから，スポークとなる機器は，スポーク拠点の FW である。

したがって，これを図 2 の名称で答えると，「**FW2，FW3**」となる。よって，これが正解となる。

●解の導出：設定

ネットワーク機器ベンダの技術者の指摘は，次のように整理できる。

表：ネットワーク機器ベンダの技術者の指摘

問題点	スポーク拠点間の IPsec トンネルが解放されなくなってしまう
原　因	スポークとなる機器が OSPF の代表ルータに選出されるため

この問題を防ぐには，原因を取り除けばよい。つまり，解決策は次のように整理できる。

表：問題の解決策

解決策	スポークとなる機器（スポーク拠点の FW）が，OSPF の代表ルータに選出されないようにする

ここまで整理できれば，あとは一般的な知識から解を導くことができる。

OSPF の仕様では，代表ルータに選ばれないようにする方法は，プライオリティを 0 に設定することである。

よって，正解は「**OSPF のプライオリティを 0 に設定する**」となる。

●参考：OSPF の代表ルータ

さて，本小問の解は得られたが，良い機会なので，本問に登場した代表ルータについて解説しておこう。

OSPF の代表ルータは，マルチアクセスネットワークにおいて，サブネットごとに選出される。その役割は，代表ルータではない OSPF ルータとの間で，OSPF のリンクステート情報を交換することである。

マルチアクセスネットワークは，3 台以上の OSPF ルータを技術的に収容し得るサブネットである（実際の収容台数は 3 台未満であってもよい）。言い換えると，ポイントツーポイントで接続されたネットワークではないことを意味している。

具体的に言うと，マルチアクセスネットワークには次の 2 種類がある。

表：マルチアクセスネットワークの種類

種類	説明
ブロードキャストマルチアクセス	イーサネットのような，ブロードキャストドメインのサブネットである。 ブロードキャストパケットやマルチキャストパケットによる 1 対多の同報通信を行うことができる
非ブロードキャストマルチアクセス （NBMA：Non Broadcast Multi Access）	本事例のようなトンネルで構成されたサブネットである。 ブロードキャストパケットやマルチキャストパケットによる 1 対多の同報通信を行うことができない

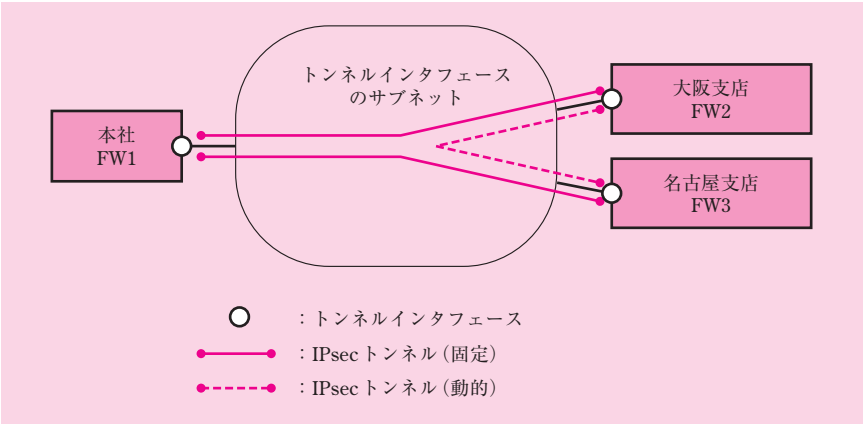
本事例に登場する，IPsec トンネルで構成されたネットワークは，NBMA である。

本文には明記されていないが，各拠点の FW は，LAN インタフェース，WAN インタフェースに加え，GRE over IPsec のトンネル用のインタフェース（以下，トンネルインタフェース）が設定されている。

このトンネルインタフェースには，WAN インタフェースのグローバル IP アドレスとは別に，プライベート IP アドレスを割り当てることができる。

この独自のプライベート IP アドレスは，FW 内でインタフェースを識別するために用いられている。GRE over IPsec パケットの IP ヘッダに格納されるわけではない。

通常，各拠点のトンネルインタフェースのプライベート IP アドレスは，共通のサブネットのアドレスブロックから払い出される。言い換えると，このサブネットに対し，各拠点のトンネルインタフェースを接続している構成となる。



図：トンネルインタフェースのサブネット

このように，複数のトンネルインタフェースを収容しているサブネットは，マルチアクセスネットワークとみなせるわけだ。

このマルチアクセスネットワークは，実際にはトンネルによって 2 拠点が接続されたものであるから，ブロードキャストパケットやマルチキャストパケットによる 1 対多の同報通信を行うことができない。それゆえ，NBMA となる。

さて，ブロードキャストマルチアクセスにせよ，NBMA にせよ，マルチアクセスネットワークである以上，複数台の OSPF ルータが収容されている。

このとき，OSPF ルータ間のリンクステート情報をどのようにやり取りしたらよいだろうか。

仮に，相互にやり取りする場合，OSPF ルータの台数が増えるにつれて，やり取りの数がどんどん増加していくことになる。仮に N 台あるとき，やり取りするペアの数は「N ×（N − 1）／ 2」，つまり O（n^2）となる。

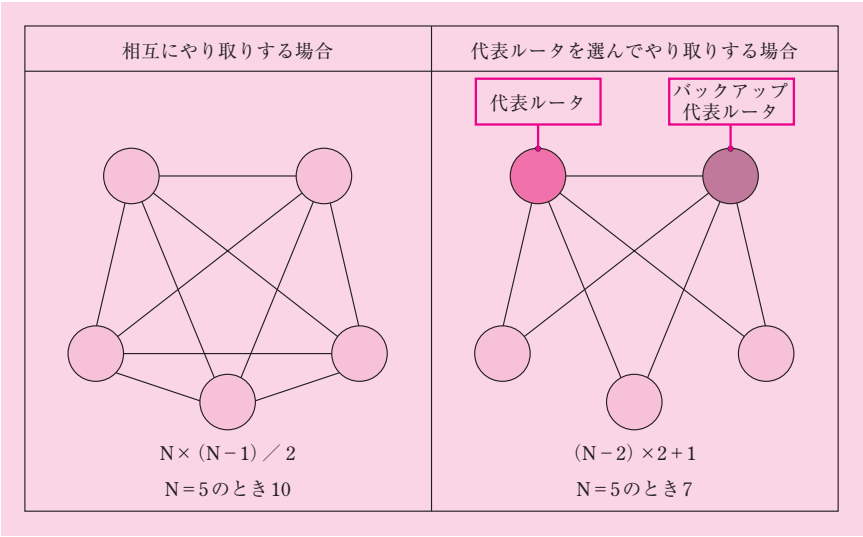
マルチアクセスネットワークでは，このやり取りを削減するため，OSPF ルータの中から 1 台を代表ルータに選ぶ。さらに，代表ルータの障害に備えて，バックアップ代表ルータも選ぶ。

代表ルータでもなくバックアップ代表ルータでもない残りのルータは，代表ルータ及びバックアップ代表ルータとの間で，リンクステート情報をやり取りする。バックアップ代表ルータは，代表ルータとの間でやり取りする。

仮に N 台あるとき，やり取りするペアの数は「（N − 2）× 2 + 1」，つまり O（n）となる。

このように，代表ルータを選んでやり取りする方式は，代表ルータを選ばずに相互にやり取りする方式に比べ，OSPF ルータ間のやり取りを削減する効果があるわけだ(*)。

（*）ブロードキャストマルチアクセスネットワークでは，マルチキャストパケットを使用することで，実際に送信するパケットの数を削減することができる。例えば，宛先マルチキャストアドレスを「224.0.0.5」に指定したパケットを 1 個送信すれば，全ての OSPF ルータがこれを受信できる。あるいは，「224.0.0.6」に指定したパケットを 1 個送信すれば，代表ルータとバックアップ代表ルータがこれを受信できる。
実は，OSPF はマルチキャストパケットだけを使用しているわけではない。ユニキャストパケットを適宜使用することもあるが，代表ルータを選ぶ方式を採用することで，ユニキャストパケットのやり取りを削減できている。

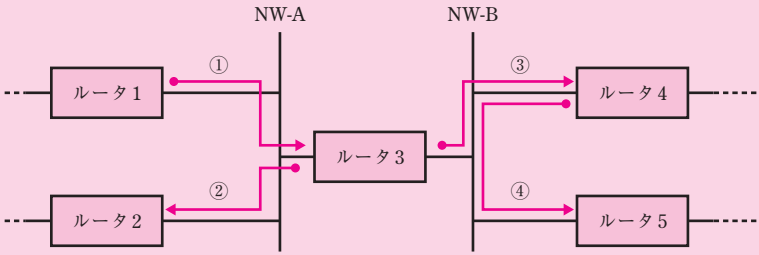


図：やり取りの比較

マルチアクセスネットワークでは，代表ルータとそれ以外のルータとの間で，リンクステート情報がやり取りされる。

例えば，ネットワーク構成が変更されたり，障害が発生したりすることによって，サブネット内のリンクステート情報が変化したとしよう。

このとき，OSPF ルータは，サブネット内の代表ルータに，変化したリンクステート情報を通知する。この代表ルータが，当該サブネットとは別のサブネットに接続している場合，次にその別のサブネットの代表ルータに向けて，変化したリンクステート情報を通知する。つまり，リンクステート情報が伝播していくわけだ。この伝播は，エリアの全域に及ぶ。



ルータ3：サブネットNW-Aの代表ルータ
ルータ4：サブネットNW-Bの代表ルータ

項番	内容
①	ルータ1がリンクステート情報の変化を検知すると，NW-3の代表ルータであるルータ3に通知する
②	ルータ3は，NW-A内の他のルータに通知する
③	ルータ3は，NW-Bの代表ルータであるルータ4に通知する
④	ルータ4は，NW-B内の他のルータに通知する

注）バックアップ代表ルータへの通知，通知を受けた旨の確認応答を省略。

図：リンクステート情報の伝播

さらには，リンクステート情報が変化しないときでも，30 分周期で各リンクステート情報がやり取りされる。

このように，代表ルータは，随時通信していることが分かる。

以上，OSPF の代表ルータについて概観した。

この点を踏まえると，ネットワーク機器ベンダの技術者が指摘した問題点が浮き彫りとなる。

自動トンネル機能は，スポーク拠点間でのユニキャスト通信の発生を契機に，IPsec トンネルの確立を行う。もしスポークとなる機器が OSPF の代表ルータに選出されたならば，リンクステート情報の通知やその確認応答をユニキャスト通信で行うとき，スポーク拠点間の IPsec トンネルが確立されるわけだ。

ひとたび確立されたトンネルは，一定時間トラフィックがなければ自動的に切断する（〔拠点追加の場合の IPsec トンネル接続追加の検討〕の第 1 段落，3 番目の箇条書き）。しかし，裏を返せば，その一定時間内にリンクステート情報を交換したならば，トンネルが解放されなくなってしまうことになる。

したがって，ネットワーク機器ベンダの技術者はこの点を問題視したことが分かる。