

平成 26 年度
秋期

午後Ⅱ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

最近、特定の企業や官公庁などを標的にして、その組織が保有する知財情報や個人情報などの重要な情報の窃取や破壊などを行う、標的型メール攻撃が増加してきた。標的型メール攻撃は、攻撃手口が巧妙なために、発見が難しく被害が増加している。

標的型メール攻撃の対策は、PC やサーバに対するセキュリティ対策だけでなく、ネットワークでの対策も欠かせない。そこで、標的型メール攻撃の対策には、セキュリティ技術者とネットワーク技術者が協力して実施策を立案することが求められている。

本問では、標的型メール攻撃の対策を題材として、セキュリティ技術者とネットワーク技術者が協力して実施策を立案する過程を記述した。その中で、ネットワーク技術者が実施すべきネットワークでの対策を取り上げ、その対策を通して、ネットワーク技術者に求められる、ネットワーク設計・構築技術とネットワークセキュリティ技術を基にした、ネットワークでのセキュリティ対策についての理解を問うた。

採点講評

問 1 では、標的型メール攻撃の対策をテーマに、ネットワークでの入口対策と出口対策を取り上げた。その中で、SPF (Sender Policy Framework)、プロキシサーバ、L3SW でのパケットフィルタリング及びログの検査に関連する記述を基に、ネットワーク技術者に求められる、ネットワーク設計・構築・運用技術とネットワークセキュリティ技術についての理解を問うた。全体として、よく理解されていた。特に、設問 5 の正答率が高かった。しかし、設問 3 (3)、設問 4 (4) では、問題の趣旨に沿わない解答が散見された。問われている内容をよく理解して、適切な記述が行えるよう努力してほしい。

設問 1 では、a、b に比して c、d、e の正答率が低かった。c は、TCP/IP 通信の基本動作に関わる問いなので、正答を導き出してほしかった。

設問 2 は、入口対策に関連した問題だったが、(2)、(3) 及び (4) の理由の正答率が低かった。(2) の誤った解答の例から、SMTP によるメール転送で、詐称が可能な情報と詐称が困難な情報が十分には理解できていないことが推測された。(3)、(4) は、本文の記述を理解すれば、SPF に関連する前提知識がなくても正答が導き出せる問いだったが、記述内容を読みこなせなかったのではないと思われる解答が散見された。

設問 3 は、SSL 関連の問題だったが、正答率は低かった。ネットワーク技術者は、業務で SSL の細部までの理解が必要とされることがなかった結果と思うが、安全で安心できるネットワークの構築のために、ネットワークセキュリティについても十分に理解し、その仕組みを適切に説明できるようにしてほしい。

設問 4 では、パケットフィルタリングについて問うたが、業務で取り組むことが多かったためか、正答率が高かった。その中で、(4) については、制御内容はおおむね理解できていても、その内容を適切に説明できていない解答が散見された。

設問 5 は、安全なネットワークを維持するための運用に関連する設問だったが、業務で直面している課題だったためか、受験者の理解度は高かった。

設問	解答例・解答の要点						備考	
設問 1	a	URL 又は 統一資源位置指定子						
	b	HTTP						
	c	IP アドレス						
	d	コンテンツフィルタリング						
	e	トンネリング						
設問 2	(1)	添付ファイルを開いたり、メールに記載されたリンク先にアクセスしたりする。						
	(2)	メール送信元の MTA の IP アドレスが所属するドメインと、送信者のメールアドレスのドメイン						
	(3)	社外に送信されるメールの送信元 IP アドレスになるから						
	(4)	サーバ名	メール中継サーバ					
	理由	社外から Y 社宛てに送信されたメールを直接受信するから						
設問 3	(1)	PC と Web サーバの間						
	(2)	プロキシサーバのルート証明書						
	(3)	プロキシサーバが、暗号化されたプリマスタシークレットを復号できないから						
設問 4	(1)	表 4	ポート A のポート ID	P3	通信の方向	IN		
		表 5	ポート B のポート ID	P5	通信の方向	OUT		
	(2)	部署 1 と本社サーバセグメント間の疎通テスト						
	(3)	動作	許可	送信元 IP アドレス	192.168.1.0/24			
		宛先 IP アドレス	192.168.11.0/24	プロトコル	UDP			
		送信元ポート番号	any	宛先ポート番号	53			
		TCP 制御ビット	any					
	(4)	部署 1 の PC から管理 PC に対して確立する TCP コネクションは禁止するが、逆方向に確立する TCP コネクションは許可する。						
	設問 5	(1)	・社外の Web サーバとの間の SSL で暗号化された通信においても、認証された利用者と通信内容が取得できる。 ・プロキシサーバの認証に連続して失敗したことが記録されたログから、マルウェアの活動と推測できる情報が取得できる。					
		(2)	①	・メールに添付されたファイルを開かない。				
		②	・メール本文に記載されたリンク先にアクセスしない。					
		③	・メールが、正しい送信者から送信されたものか確認する。 ・不審なメールの内容を、セキュリティ担当者に報告する。 ・発見した不審なメールに関する情報を、全社で共有する。					
	(3)	マルウェアの社内での活動を、早期に発見できること						

■設問 1

解答例

- a : URL 又は 統一資源位置指定子
- b : HTTP
- c : IP アドレス
- d : コンテンツフィルタリング
- e : トンネリング

著者解答例

- e : トンネル

a

空欄 a を含む文章は、[標的型メール攻撃の手法と対策案] の第 2 段落にある。第 2 段落は標的型メール攻撃について説明している。第 2 段落の前半では、標的型メール攻撃とは何かを述べている。後半では、メールに「マルウェアが埋め込まれたファイルが添付されていたり（する）」ことを述べている。続く第 3 段落では、標的型メールを通して入手したマルウェアが、バックドアを開設置して攻撃基盤を構築することについて説明している。

本文には明言されていないが、第 2 段落から第 3 段落に至る文脈から判断すると、第 2 段落の後半で言わんとしていることは、標的型メールを通してマルウェアに感染する、ということだ。

一般的に言って、メールを通してマルウェアに感染する方法は大きく分けて二つある。一つ目は、マルウェアが埋め込まれたファイルが添付されており、そのファイルを不用意に開くことにより感染することである。二つ目は、マルウェアが仕込まれた Web サイトへのリンク先を示す URL が本文に記載されており、そのリンク先に不用意にアクセスすることにより感染することである。

この点を踏まえて、空欄 a を含む文章を見てみよう。そこには、「送り付けられたメールには、悪意のあるコード、マルウェアが埋め込まれたファイルが添付されていたり、マルウェアが仕込まれた Web サイトへのリンク先を示す a が本文に記載されていたりする」と記述されている。

一つ目の感染方法は、「マルウェアが埋め込まれたファイルが添付されていたり」という記述に対応していることは明らかだ。

二つ目の感染方法は、「マルウェアが仕込まれた Web サイトへのリンク先を示す

a が本文に記載されていたりする」という記述に対応していると推論できる。

よって、空欄 a に該当する字句は、「URL」又は「統一資源位置指定子」である。

●標的型メールによるマルウェアの感染

序文の第 6 段落、S 主任の 1 番目の発言の中で、「標的型メール攻撃に対しては、マルウェアの侵入を防ぐ入口対策だけではなく、社内の LAN に侵入したマルウェアの活動を抑えたり、活動を発見しやすくしたりする対策（以下、出口対策という）も必要になっている」と記述されている。ここから、標的型メール攻撃の対策として、入口対策にせよ出口対策にせよ、どちらもマルウェアに焦点を当てていることが分かる。要するに、真の脅威となるのはマルウェアなのである。メールによる感染は、攻撃の第一歩なのだ。

先ほど、メールによる感染方法は二つあると解説した。それ自体は、特に目新しいものではない。

とはいえ、近年、標的型メール攻撃によるマルウェアの侵入が大きな被害をもたらしている。その理由は、「攻撃対象者と関係がありそうな組織、機関及び実在の人物を装ったメールを送り付けてくる」からである。いわば、ねらいを定めて悪意あるメールを送り付けてくるわけだ。この手法がまさしく「標的型」という呼び名の由来ともなっている。

標的型メールは、読み手の関係者が差出人になっているため、読み手は警戒心を抱かずにメールを開いてしまう。メールの本文は、添付ファイルを開いたりリンク先にアクセスしたりするよう巧みに促す内容であり、それに誘導されることによりマルウェアに感染してしまうのである。

●感染した後のマルウェアの活動

〔標的型メール攻撃の手法と対策案〕の第 3 段落は、マルウェアの活動について説明している。

要約すると、次のような手順を踏むことが分かる。

1. バックドアを開設して、攻撃基盤を構築する
2. 攻撃基盤を構築した後、システム内部への侵入を行い、拡散、情報の窃取、破壊などを行う

ここで、セキュリティの専門用語について補足しておこう。「攻撃基盤の構築」と

は、インターネット上の攻撃者のサーバとマルウェアとの通信路を開設することである。「バックドアの通信」とは、攻撃者のサーバとマルウェアとの間で秘密裏に行われる通信のことである。

b

空欄 b を含む文章は、「HTML で作成されたコンテンツの送受信用プロトコルである [b] 」と記述されている。HTML で作成されたコンテンツを送受信するプロトコルは、HTTP である。よって、空欄 b に該当する字句は、「HTTP」である。

c

空欄 c を含む文章は、「SMTP では、送信者が、…… (略) ……、送信元の MTA 又は MUA が稼働するサーバ又は PC に設定されている [c] を書き換えることは困難である」と記述されている。

MTA (Mail Transfer Agent) とは、電子メールを配送するソフトウェアを指し、いわゆるメールサーバのことである。MUA (Mail User Agent) とは、利用者がメールを送受信するソフトウェアを指し、いわゆるメーラのことである。

送信者による詐称が困難なもののうち、「送信元の MTA 又は MUA が稼働するサーバ又は PC に設定されているもの」に該当するものは何であろうか。

この文は「又は」の係受けがやや分かりづらい。MTA と MUA はソフトウェアであり、サーバと PC はマシンであることに着目すると、次のように考えられる。

送信元のソフトウェア (MTA 又は MUA) が稼働するマシン (サーバ又は PC) に設定されているもの

したがって、ここで問われているのは、「送信元のマシンに設定されているもので、送信者による詐称が困難なもの」である。文脈からして、これは電子メールの送受信に登場する情報である。そして、詐称して受信者を欺こうとしている以上、受信側者から見える送信元マシンの情報であり、それゆえネットワーク層以上の情報であると推論できる。

このように考えると、解答の候補はだいぶ絞られた。思いつくものと言えば、ホスト名、ドメイン名、IP アドレスであろう。

攻撃者は、送信元のマシンのホスト名やドメイン名を詐称できるだろうか。SMTP の仕様では、MTA が稼働するマシンのホスト名はエンベロープに記載され、ドメイン名はメールアドレスの @ マークより後に記載される。これらはいずれも、送信者が書

き換えたとしても、メールは相手に送信されてしまう。つまり、詐称が可能である。

それでは、送信元のマシンの IP アドレスを詐称できるだろうか。SMTP はトランスポート層プロトコルに TCP を使用する。コネクション型の TCP では、SMTP の通信に先立って TCP のコネクションを確立する。このとき、もしも送信元 IP アドレスが詐称されていたら、コネクション確立フェーズのやり取りに失敗するので、データ通信フェーズに遷移しない。

SMTP の通信において、送信者と受信者のやり取りが行われるコネクションは、送信元の MTA が稼働しているメールサーバと、宛先の MTA が稼働しているメールサーバの間に確立される。つまり、受信者側から見えるマシンとは送信元の MTA のメールサーバであり、詐称が困難なネットワーク層以上の情報とは IP アドレスである。

以上をまとめると、(少なくとも、送信元の MTA の) IP アドレスは、詐称が困難であることが分かる。よって、正解は、「IP アドレス」となる。

参考までに、送信元の MUA が稼働している PC については、IP アドレスの詐称は困難であると言えるだろうか。

もしもこの PC からインターネット上のサーバに直接アクセスする場合(つまり、グローバル IP アドレスをもつ場合)には、コネクション型の通信を行う限り、IP アドレスの詐称は困難である。

しかし、インターネット上のサーバにアクセスせず、送信元の MTA との間でコネクションを確立するだけであれば、IP アドレスを自由に割り振ることは可能だ。とはいえ、宛先の MTA との間でコネクションを確立しないのであれば、IP アドレスを改ざんしたところで、受信者に実害が及ぶわけではない。

d

空欄 d を含む文章は、「復号機能によって、SSL/TLS (以下、SSL という) 通信でも、受信したデータ中に不適切な言葉や文字列などが含まれていたとき、その通信を遮断する d や、…… (略) ……などの、セキュリティ対策が行えるようになる」と記述されている。

SSL 通信を復号することで、アプリケーション層プロトコルのやり取りを解析できるようになる。したがって、空欄 d で言及された対策とは、アプリケーションの通信を監視し、「不適切な言葉や文字列などが含まれていたとき、その通信を遮断する」というものだ。したがって、これは「コンテンツフィルタリング」である。よって、これが空欄 d に該当する字句となる。

e

空欄 e を含む文章は、〔プロキシサーバの復号機能の実現方法〕の第 2 段落にある。第 2 段落は、プロキシサーバ経由で PC と Web サーバとの間で SSL 通信を行うときに connect 要求を使用することについて説明している。そこには、「プロキシサーバは PC に connect 応答を送信して、それ以降に受信した TCP データをそのまま接続先に転送する、e 処理の準備が整ったことを知らせる」と記述されている。

これは一般的な知識から解を導く。

本文にある「connect 要求」とは、HTTP の CONNECT メソッドのことである。HTTP 1.1 の仕様を定めている RFC7231「Hypertext Transfer Protocol (HTTP/1.1)」の「4.3.6. CONNECT」では、次のように述べている（少し意識している）。

CONNECT メソッドは、これを受け取ったホストが、接続先サーバとの間でトンネルを確立することを要求する。この接続先サーバは、当メソッドの中で指定されている。

ここで言う「CONNECT メソッドを受け取ったホスト」は、本事例のプロキシサーバに相当する。

続いて同文書は、このホストは、トンネルを確立した後、受信したパケットをそのまま接続先に転送すると述べている。

したがって、本文の「受信した TCP データをそのまま接続先に転送する」という処理に該当する字句は、「トンネリング」であると言える。よって、これが正解となる。

試験センターの解は、RFC の表記に合わせたものである。技術用語を覚えるときは、できるだけ規格に従うよう心掛けたい。

読者は、普段から、何かを調べるために雑誌やネットの記事に当たっていることだろう。では、どこかで時間を取って、技術の仕様を定めた RFC や ISO などの原本にも当たっているだろうか。

腰を落ち着けて規格文書を読むことは大切だと著者は考えている。雑誌やネットの記事で得た知識の裏付けとなり、その土台をしっかりと正確に固めることができる。更には、断片的な知識を体系的に整理するのにも役立つからである。

■設問 2

(1)

解答例

添	付	フ	ァ	イ	ル	を	開	い	た	り	,	メ	ー	ル	に	記	載	さ	れ	た	リ	ン	ク	先
に	ア	ク	セ	ス	し	た	り	す	る	。														

(36字)

本問は、「下線（ア）のメールによって、メール送信者が誘導しようとする受信者の行動」を問うている。

下線（ア）は、「標的型メール攻撃の手法と対策案」の第2段落にある。そこには、「標的型メール攻撃の多くは、ソーシャルエンジニアリング手法で収集した攻撃対象者の情報を基に、（ア）攻撃対象者と関係がありそうな組織、機関及び実在の人物を装ったメールを送り付けてくる手法をとる」と記述されている。したがって、下線（ア）のメールとは、標的型メール攻撃で用いられるメールである。

設問1の空欄aで解説したとおり、標的型メール攻撃の第一歩は、メールによるマルウェアの感染である。メール送信者が受信者に行わせたいこととは、端的に言うなら、攻撃者が準備したとおりの手順を踏んで、マルウェアに感染することだ。本問は、受信者のその行動を具体的に解答することを求めている。

第2段落には、「メール送信者が誘導しようとする受信者の行動」は書かれていない。それが本問の解そのものだからだ。その代わり、その解を導くための手掛かりが与えられている。そこには、「送り付けられたメールには、悪意のあるコード、マルウェアが埋め込まれたファイルが添付されていたり、マルウェアが仕込まれた Web サイトへのリンク先を示す URL が本文に記載されていたりする」と記述されている（空欄aを補填）。つまり、感染を企てて準備した事柄が述べられている。

したがって、このメールの本文で誘導していることは、「添付ファイルを開いたり、メールに記載されたリンク先にアクセスしたりすること」である。よって、正解は解答例に示したとおりとなる。

(2)

解答例

メ	ー	ル	送	信	元	の	M	T	A	の	I	P	ア	ド	レ	ス	が	所	属	す	る	ド	メ	イ	
ン	と	,	送	信	者	の	メ	ー	ル	ア	ド	レ	ス	の	ド	メ	イ	ン							

(44字)

本問は、「下線（イ）で、比較する二つのドメイン」を問うている。

下線（イ）は、「標的型メール攻撃の手法と対策案」の第4段落にある。そこには、「SMTPでは、送信者が、自分自身のメールアドレスを容易に詐称することができる。しかし、送信元のMTA又はMUAが稼働するサーバ又はPCに設定されているIPアドレスを書き換えることは困難である。そこで、（イ）ドメインを比較するだけでも、送信者のメールアドレスが詐称されているかどうか、ある程度判別できる」と記述されている（空欄cを補填）。したがって、ここで問われているのは、送信者のメールアドレスが詐称されているかどうかを判別するために、どのドメインを比較するか、ということである。

この段落には、送信者がメールアドレスを詐称できること、及び、送信元のマシンのIPアドレスは詐称が困難であることが述べられている。具体的に言うと、IPアドレスの詐称が困難であるマシンとは、設問1の空欄cで解説したとおり、送信元のMTAが稼働しているマシンである。なぜなら、これは宛先のMTAとTCP通信を行うからだ。

そこで、詐称が容易であるメールアドレスのドメインと、詐称が困難である送信元のMTAのIPアドレスが所属するドメインとを比較し、両者が一致するかどうかで判別できるに違いない。もしも一致すれば、メールアドレスは詐称されていないと判定できる。

よって、正解は、解答例に示したとおりとなる。

(3)

解答例

社	外	に	送	信	さ	れ	る	メ	ー	ル	の	送	信	元	I	P	ア	ド	レ	ス	に	な	る	か	ら
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

(26字)

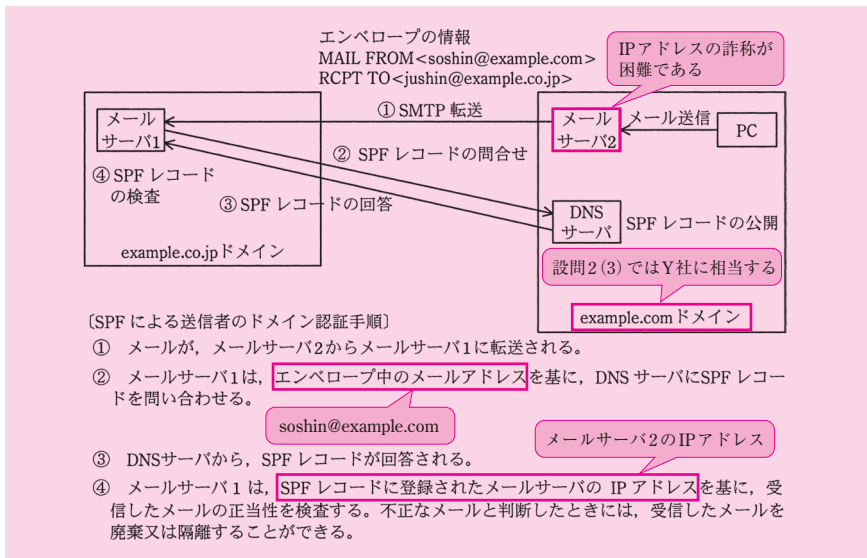
本問は、「下線（ウ）」について、Y社には3台のメールサーバがあるが、その中でメール中継サーバのIPアドレスを記述する理由」を問うている。

下線（ウ）は、「標的型メール攻撃の手法と対策案」の第6段落にある。そこには、「Y社でSPFを導入するときは、DMZの社外向けDNSサーバに、（ウ）メール中継サーバのIPアドレスを記述したSPFレコードを追加することになる」と記述されている。したがって、ここで問われているのは、Y社のDNSサーバのSPFレコードに、なぜメール中継サーバのIPアドレスを登録するのか、ということである。

本問を解くには、SPFによる認証処理に関する一般的な知識が必要である。そこで、まずはその点について解説する。それを踏まえて、解を導こう。

● SPF による認証処理

SPFによる認証処理は、本文の図2「SPFによる認証処理の概要」に記されている。ただし、設問の都合上、SPFレコードに登録する内容を具体的に説明していない。そこで、特にその点を掘り下げて解説しよう。



図：SPFによる認証処理の概要（図2から作成）

図2の手順②には、「メールサーバ1は、エンベロープ中のメールアドレスを基に、DNSサーバにSPFレコードを問い合わせる」と記述されている。メールサーバ1が受信したメールのエンベロープ中にある送信元メールアドレスは、「soshin@example.com」。

com」である。このメールアドレスの @ マークに続くドメイン名に基づき、example.com の DNS サーバに問い合わせている。

この送信元メールアドレスはエンベロープ From と呼ばれ、メールサーバ 2 とメールサーバ 1 が SMTP 通信を行っている間、送信側（メールサーバ 2）から MAIL FROM コマンドで通知される。

図 2 の手順④には、「メールサーバ 1 は、SPF レコードに登録されたメールサーバの IP アドレスを基に、受信したメールの正当性を検査する」と記述されている。メールサーバ 1 から見て、SMTP 通信の送信元の MTA が稼働しているサーバは、メールサーバ 2 である。

設問 1 の空欄 c で解説したとおり、送信元のマシンの IP アドレスを詐称することは困難であるため、メールサーバ 1 は、メールサーバ 2 の IP アドレスは本物であると考ええる。

設問 2 (2) で解説したとおり、受信メールのメールアドレスのドメインと、メールサーバ 2 の IP アドレスが所属するドメインが一致していた場合、受信メールのメールアドレスが詐称されていないと判別できる。したがって、手順②で問い合わせた DNS サーバの SPF レコードに、本物であると考えられるメールサーバ 2 の IP アドレスが登録されていれば、メールサーバ 1 は、受信したメールの正当性（送信元メールアドレスが詐称されていないこと）を確認できるわけだ。

以上より、SPF レコードに登録するメールサーバは、図のメールサーバ 2 のように、社外にメールを送信するメールサーバである。

●解の導出

本問において、Y 社は DNS サーバに SPF レコードに登録する側に当たる。それゆえ、図 2 において、「example.com」に相当する。

Y 社に 3 台あるメールサーバのうち、図 2 中のメールサーバ 2 と同じように、社外にメールを送信する役割を担っているものが、SPF レコードに登録するサーバである。

表 1「メールの転送経路」を見ると、宛先が社外となっている転送経路は、メール中継サーバから社外に転送されている。次の図の赤枠で示す。

宛先が社外となっている転送経路は、メール中継サーバから社外に転送されている

送信元	宛先	転送経路
本社，営業所	本社，営業所	PC → 本社メールサーバ
	工場	PC → 本社メールサーバ → 工場メールサーバ
	社外	PC → 本社メールサーバ → メール中継サーバ → 社外
工場	本社，営業所	PC → 工場メールサーバ → 本社メールサーバ
	工場	PC → 工場メールサーバ
	社外	PC → 工場メールサーバ → 本社メールサーバ → メール中継サーバ → 社外
社外	本社，営業所	社外 → メール中継サーバ → 本社メールサーバ
	工場	社外 → メール中継サーバ → 本社メールサーバ → 工場メールサーバ

図：メールの転送経路（表 1 から作成）

したがって、Y 社の DNS サーバの SPF レコードに登録するメールサーバは、メール中継サーバである。

問題文で問われているのは、Y 社の DNS サーバの SPF レコードにメール中継サーバの IP アドレスを登録するのはなぜか、ということであった。よって、正解は、「社外に送信されるメールの送信元 IP アドレスになるから」となる。

(4)

解答例

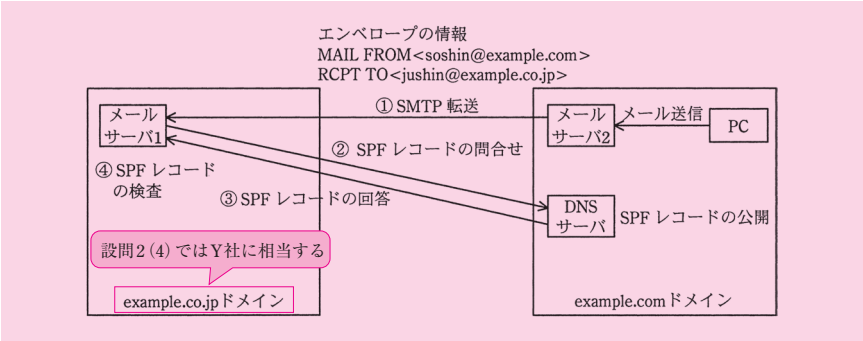
サーバ名：メール中継サーバ

理由：社外から Y 社宛てに送信されたメールを直接受信するから

(26 字)

本問は、「SPF による認証処理を実施させるサーバ名」及び「認証処理を正しく行うには、そのサーバでなければならない理由」を問うている。

今度は、Y 社は SPF による認証処理を実施する側に当たる。それゆえ、図 2 において、「example.co.jp」に相当する。



図：SPFによる認証処理の概要（図2から作成）

Y社に3台あるメールサーバのうち、図2のメールサーバ1と同じように、社外からY社宛てのメールを直接受信する役割を担っているものが、認証処理を実施させるサーバとなる。

表1「メールの転送経路」を見ると、送信元が社外となっている転送経路は、メール中継サーバ宛てに転送されている。次の図の赤枠で示す。

送信元	宛先	転送経路
本社、営業所	本社、営業所	PC → 本社メールサーバ
	工場	PC → 本社メールサーバ → 工場メールサーバ
	社外	PC → 本社メールサーバ → メール中継サーバ → 社外
工場	本社、営業所	PC → 工場メールサーバ → 本社メールサーバ
	工場	PC → 工場メールサーバ
	社外	PC → 工場メールサーバ → 本社メールサーバ → メール中継サーバ → 社外
社外	本社、営業所	社外 → メール中継サーバ → 本社メールサーバ
	工場	社外 → メール中継サーバ → 本社メールサーバ → 工場メールサーバ

送信元が社外となっている転送経路は、メール中継サーバ宛てに転送されている

図：メールの転送経路（表1から作成）

したがって、SPFによる認証処理を実施させるサーバは、メール中継サーバとなる。その理由は、社外からY社宛てに送信されたメールを直接受信するからである。よって、正解は解答例に示したとおりとなる。

■設問 3

(1)

解答例

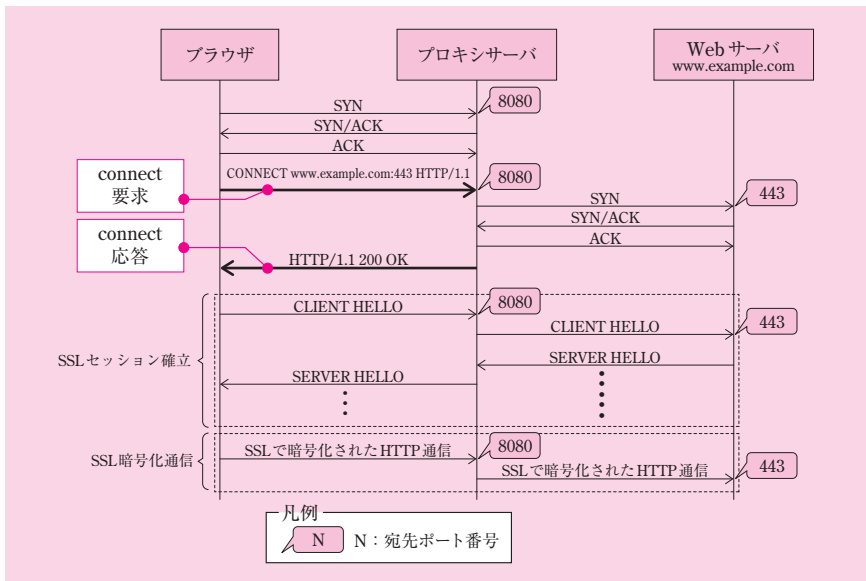
PC と Web サーバの間

問題文は、「既設のプロキシサーバの場合、SSL セッションはどの機器間で開設されるか」と記述されている。既設のプロキシサーバは、SSL の復号機能をもたない、標準的なプロキシサーバである。

本問を解くには、CONNECT メソッドを用いた、プロキシサーバ経由の SSL 通信に関する一般的な知識が必要である。そこで、まずはその点について解説する。それを踏まえて、解を導こう。

●プロキシサーバ経由の SSL 通信

この通信の手順を次の図に示そう。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 SSL 通信の動作手順

まず、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。

次いで、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、PC と接続先サーバとの間でトンネルを確立することを要求している。当メソッドの中で、接続先サーバのホスト名「www.example.com」とトンネル通信のポート番号「443」を伝えている。問題本文は、この要求を「connect 要求」と表記している。

次いで、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。そして、CONNECT メソッドの要求に対する応答を PC に送信する。問題本文は、この応答を「connect 応答」と表記している。

その後、ブラウザと Web サーバ間で SSL セッションを確立する。ブラウザと Web サーバ間の通信は暗号化されており、プロキシサーバは TCP データ（暗号化されたデータ）をそのまま転送しているだけである。つまり、SSL のやり取りには一切関与しない。

●解の導出

先ほどの解説から明らかとなおり、プロキシサーバ経由の SSL 通信において、SSL セッションを確立するのは、ブラウザと Web サーバ間となる。プロキシサーバは、暗号化されたデータをそのまま転送しているに過ぎない。

本問は、「SSL セッションはどの機器間で開設されるか」を問うているので、図 3 中の機器名で解答する。よって、正解は、「PC と Web サーバの間」となる。

(2)

解答例

プロキシサーバのルート証明書 (14字)

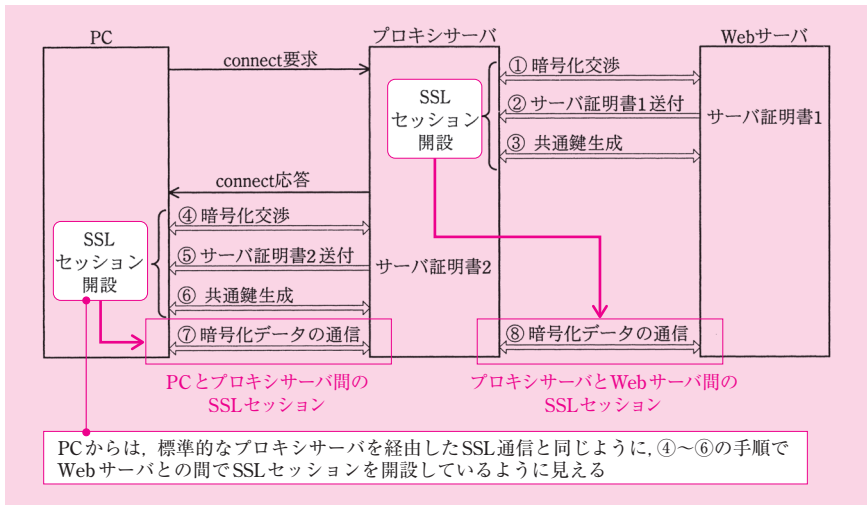
本問は、下線 (エ) の情報は何かを問うている。下線 (エ) は、「プロキシサーバの復号機能の実現方法」の第 5 段落にある。そこには、「PC がサーバ証明書 2 を正当なものとして判断してプロキシサーバを認証するためには、PC に、(エ) サーバ証明書 2 を検証するのに必要な情報を保有させる必要がある」と記述されている。

復号機能をもつプロキシサーバの動作手順は、図 3 及び第 5 段落に説明されている。PC と接続先サーバ間の通信は、プロキシサーバを経由する。このとき、プロキシ

サーバは、二つの SSL セッションを開設する。一つ目は、「①～③の手順で Web サーバとの間で SSL セッションを開設（する）」とあるとおり、プロキシサーバと接続先サーバ間である。二つ目は、「更に PC との間でも、④～⑥の手順で SSL セッションを開設する」とあるとおり、PC とプロキシサーバ間である。

図 3 の⑦は、PC からプロキシサーバへパケットを転送する手順である。この区間は、PC とプロキシサーバ間に開設された SSL セッションで、暗号化されている。プロキシサーバは、この SSL 通信を復号し、接続先サーバに転送する。

図 3 の⑧は、プロキシサーバから接続先サーバへパケットを転送する手順である。この区間は、プロキシサーバと接続先サーバ間に開設された SSL セッションで、暗号化されている。接続先サーバは、この SSL 通信を復号し、パケットを受信する。



図：復号機能をもつプロキシサーバの動作手順の概要（図 3 から作成）

⑤の手順で、プロキシサーバはサーバ証明書 2 を生成する。この点について、「⑤で、プロキシサーバは、サブジェクト (Subject) に含まれるコモン名 (CN:Common Name) に、サーバ証明書 1 と同じ情報をもたせたサーバ証明書 2 を生成して、PC 宛てに送信する」と記述されている。それゆえ、サーバ証明書 2 のコモン名は、接続先である Web サーバになっている。

このサーバ証明書 2 が、PC とプロキシサーバ間の SSL セッションで用いられる。

したがって、PC から見ると、サーバ証明書 2 は、あたかも接続先である Web サーバから、サーバ証明書が送られたかのように見える。要するに、PC からは、標準的な

プロキシサーバを経由した SSL 通信と同じように、④～⑥の手順で Web サーバとの間で SSL セッションを開設しているように見えるわけだ。

ブラウザは Web サーバとの間で SSL セッションを開設する際、Web サーバから送信されたサーバ証明書を検証する。ブラウザには、信頼できる第三者機関の認証局のルート証明書があらかじめ登録されている。最終的にこのルート証明書によってサーバ証明書が認証されたときだけ、SSL セッションを開設できる。第三者認証と電子証明書について、詳しくは本書の第 8 章「8.2.2 認証方式」を参照されたい。

さて、⑤の手順で生成されたサーバ証明書 2 は、信頼できる第三者機関の認証局が発行したものではない。それゆえ、サーバ証明書 2 を認証するルート証明書がブラウザに登録されていない限り、SSL セッションは開設されない。

したがって、図 3 の動作手順がうまくいくためには、プロキシサーバが生成するサーバ証明書を認証するためのルート証明書を、Y 社の PC のブラウザにあらかじめ登録しておく必要がある。

よって、正解は、「**プロキシサーバのルート証明書**」となる。

(3)

解答例

プ	ロ	キ	シ	サ	ー	バ	が	，	暗	号	化	さ	れ	た	プ	リ	マ	ス	タ	シ	ー	ク	レ	ッ
ト	を	復	号	で	き	な	い	か	ら	(35字)														

本問は、「下線 (オ) について、失敗する理由」を問うている。下線 (オ) は、「[プロキシサーバの復号機能の実現方法] の第 6 段落にある。そこには、「仮に、図 3 中の⑤で、プロキシサーバが Web サーバから取得したサーバ証明書 1 を PC に送信した場合、PC によるプロキシサーバの認証は成功する。しかし、(オ) ⑥において、プリマスタシークレット (Premaster Secret) の共有に失敗するので、このような方法で SSL セッションを開設することはできない」と記述されている。

⑥の手順は、「共通鍵生成」である。SSL の開設に先立ち、SSL のハンドシェイクプロトコルのやり取りを通して共通鍵を生成する。クライアント側は、サーバ証明書を検証した後、共通鍵の基となるプリマスタシークレットをサーバ側に送付する。プリマスタシークレットは、サーバ証明書から取得したサーバの公開鍵を使って、暗号化されている。これを復号できるのはサーバの公開鍵の対となる秘密鍵だけである。SSL のハンドシェイクプロトコルについて、詳しくは本書の第 8 章「8.4.6 SSL, TLS」を

参照されたい。

さて、問題文にあるとおり、図 3 中の⑤で、プロキシサーバが Web サーバから取得したサーバ証明書 1 を PC に送信すると、どうなるだろうか。

サーバ証明書 1 は、信頼できる第三者機関の認証局が発行したものであるため、問題文にあるとおり、サーバ証明書 1 の認証処理は成功する。この状態で⑥の手順に入ると、PC からプロキシサーバに送信されるプリマスタシークレットは、サーバ証明書 1 から取得した、Web サーバの公開鍵で暗号化される。この公開鍵の対となる秘密鍵は、Web サーバだけが保有している。つまり、プロキシサーバはこれを復号することができない。それゆえ、⑥の手順に失敗してしまう。

よって、正解は、「プロキシサーバが、暗号化されたプリマスタシークレットを復号できないから」となる。

■設問 4

(1)

解答例

[表 4] ポート A のポート ID : P3, 通信の方向 : IN

[表 5] ポート B のポート ID : P5, 通信の方向 : OUT

表 4、表 5 は、いずれも図 1 中の L3SW1 に設定されたパケットフィルタリングルールである。

本問は、これらの表が、L3SW1 のどのポートに適用されるものであるか、L3SW1 から見た通信の方向はどちらであるか (IN 又は OUT)、を問うている。

●表 4

表 4 は、送信元 IP アドレスはすべて「192.168.1.0/24」であり、これは本社部署 1 セグメントである。これに対し、宛先 IP アドレスは様々である。

したがって、L3SW1 のポートでこれに合致するのは、本社部署 1 セグメントの収容ポートである「P3」である。L3SW1 から見た方向は「IN」である。

よって、これが正解となる。

●表 5

表 5 は、送信元 IP アドレスは様々である。これに対し、宛先 IP アドレスは

「192.168.51.128/25」と「192.168.48.0/21」である。「192.168.51.128/25」は工場である。「192.168.48.0/21」は、本社から見て広域イーサ網の向こう側（工場、営業所1～3）の集約アドレスである。

したがって、L3SW1のポートでこれに合致するのは、広域イーサ網側のポートである「P5」である。L3SW1から見た方向は「OUT」である。

よって、これが正解となる。

(2)

解答例

部署1と本社サーバセグメント間の疎通テスト（21字）

本問は、表4中の項番2のパケットフィルタリングルールの目的を問うている。設問4(1)で解説したとおり、表4は、本社部署1セグメントの収容ポートP3のIN方向に適用されるルールである。

パケットフィルタリングルールは、どの情報に基づいて作成されたのだろうか。〔パケットフィルタリングの検討〕の第1～3段落を見ると、

- サーバの用途とアクセス元の情報を表2～表3にまとめる
- 表2～表3を基に、図4「パケットフィルタリングポリシー」をまとめる
- 図4を基にパケットフィルタリングルールを検討する

というフローで作成していることが分かる。したがって、表2～表3及び図4の情報から、パケットフィルタリングルールの目的を探り、本問の解を導くことができる。

表4の項番2は、宛先IPアドレスが本社サーバセグメント「192.168.11.0/24」であり、プロトコルが「ICMP」である。その点を踏まえて、DMZ以外で稼働しているサーバを対象にした表3、図4を見てみよう。

項番	動作	送信元 IP アドレス	宛先 IP アドレス	プロトコル	送信元 ポート番号	宛先 ポート番号	TCP 制御ビット
1	許可	192.168.1.0/24	192.168.11.0/24	TCP	any	any	any
2	許可	192.168.1.0/24	192.168.11.0/24	ICMP	any	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 パケットフィルタリングルールは、項番の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。

図：表 4（項番 1, 2 を抜粋）

表 3 DMZ 以外で稼働しているサーバの用途とアクセス元

設置場所	サーバ名	用途	アクセス元
本社サーバ セグメント	本社メールサーバ	本社社員と営業所員のメールボックスの保持	本社と営業所の PC ^① メール中継サーバ 工場メールサーバ
	業務サーバ	全社員向けの各種業務処理サービスの提供	全社の PC
	ファイルサーバ	本社社員と営業所員向けのファイルサービスの提供	本社と営業所の PC ^① 全社の PC
	社内向け DNS サーバ	全社の PC 及びメールサーバからの名前解決要求への応答	メール中継サーバ 本社メールサーバ 工場メールサーバ
工場サーバ セグメント	工場メールサーバ	工場社員のメールボックスの保持	工場の PC 本社メールサーバ
	ファイルサーバ	工場社員向けのファイルサービスの提供	工場の PC
各営業所	ファイルサーバ	営業所員向けのファイルサービスの提供	当該営業所の PC

注^① 本社と営業所の PC は、管理 PC を含んでいる。

- ① PC からサーバへの業務用通信及びサーバ間の業務用通信を、表 2, 3 どちらでも許可する。
 ② 上記①に加え、業務用通信区間における疎通テストのための通信を許可する。
 ③ 管理 PC については、上記①、②の他に、他のセグメントの PC 及びサーバへのリモート接続と疎通テストのための通信を許可する。
 ④ 上記①～③以外の通信を禁止する。

図 4 パケットフィルタリングポリシー

図：表 3, 図 4 の中で、表 4 の項番 2 が関係している箇所

本社部署 1 セグメントの PC をアクセス元とし、本社サーバセグメントを宛先とする通信は、表 3 の中に含まれている。なお、表 3 のアクセス元を調べるときは、本社部署 1 セグメントの PC が「本社と営業所の PC」「全社 PC」に含まれていることに留意する。

したがって、この通信は、図 4 の項番①のポリシー「PC からサーバへの業務用通信……を、表 2, 3 どちらでも許可する」に該当する。このルールは、表 4 の項番 1 である（ただし、項番 1 のプロトコルは TCP のみである。社内向け DNS サーバを宛先とする通信は、項番 1 だけでは不十分である。この点は、次の設問 4 (3) で取り上げられる）。

図 4 の項番②のポリシーは「業務用通信区間における疎通テストのための通信を許可する」とあるので、本社部署 1 セグメントをアクセス元とし、本社サーバセグメント

を宛先とする ICMP を許可することが分かる。このルールが、表 4 の項番 2 である。

これでほぼ正解が得られたわけだが、ここで改めて問題文を見てみよう。そこには、「目的を……述べよ」と記述されている。「目的」とあるので、この点を踏まえ、図 4 のパケットフィルタリングポリシーをしてみる。すると、項番②には、「業務用通信区間における疎通テストのための通信」と記述されている。「疎通テストのため」とあるので、この部分を引用することで目的を明確に示すことができる。

よって、正解は、「部署 1 と本社サーバセグメント間の疎通テスト」となる。

(3)

解答例

動作：許可

送信元 IP アドレス：192.168.1.0/24

宛先 IP アドレス：192.168.11.0/24

プロトコル：UDP

送信元ポート番号：any

宛先ポート番号：53

TCP 制御ビット：any

本問は、本文中の下線（カ）で指摘された、表 4 へ追加するパケットフィルタリングルールを問うている。下線（カ）は「パケットフィルタリングの検討」の第 5 段落にあり、そこには「（カ）表 4 にルールの漏れが一つあるので、項番 1, 2 の間に追加する」と記述されている。

わざわざ「項番 1, 2 の間」とあるので、解を導くための手掛かりが与えられていると考えてよいだろう。項番 1, 2 は、いずれも宛先 IP アドレスが本社サーバセグメント「192.168.11.0/24」である。したがって、本社サーバセグメントにあるサーバを宛先とする通信に着目しながら、解を導くことにしよう。

本社サーバセグメントには社内向け DNS サーバが設置されている。表 3 を見ると、このサーバには全社の PC がアクセスしている。したがって、表 4 の中に、本社部署 1 セグメントを送信元とし、社内 DNS サーバを宛先とする、名前解決の通信を許可するルールが登録されていなければならない。このプロトコルは「UDP」と「TCP」である^(*)。なお、TCP については項番 1 に含まれているので、この通信のために新たにルールを追加する必要はない。ポート番号は、宛先が DNS サーバであることから、宛

先ポート番号は「53」である。

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

よって、正解は解答例に示したとおりとなる。

(4)

解答例

部	署	1	の	P	C	か	ら	管	理	P	C	に	対	し	て	確	立	す	る	T	C	P	コ	ネ
ク	シ	ョ	ン	は	禁	止	す	る	が	、	逆	方	向	に	確	立	す	る	T	C	P	コ	ネ	
シ	ョ	ン	は	許	可	す	る	。																

(59 字)

本問は、表 4 の項番 3, 4 の二つのパケットフィルタリングルールによって制御される通信の内容を問うている。一つずつ考察して、解を導こう。

●項番 3

表 4 の項番 3 は、宛先 IP アドレスが管理セグメント「192.168.10.0/24」、プロトコルが「TCP」、TCP 制御ビットが「SYN = 1, ACK = 0」である。興味深いことに、動作が「禁止」となっている。

したがって、項番 3 が禁止している通信は、「本社部署 1 セグメントの PC から管理セグメントの PC に対して確立する、TCP コネクション」である。

図 4 「パケットフィルタリングポリシー」に照らし合わせてみると、禁止されている理由を理解することができる。この通信は、項番①～③のいずれにも該当せず、項番④の「上記①～③以外の通信を禁止する」に該当するからである。

●項番 4

表 4 の項番 4 は、宛先 IP アドレスが管理セグメント「192.168.10.0/24」、プロトコルが「TCP」、TCP 制御ビットが「any」である。図 4 の中で、管理セグメントに言及しているのは、項番③である。そこには「管理 PC については、……他のセグメントの PC 及びサーバへのリモート接続……のための通信を許可する」と記述されている。

「他のセグメントの PC」とあるので、本社部署 1 の PC が含まれている。リモート接続のプロトコルは具体的に示されていないので、ここは仮説検証型アプローチで打開してみよう。トランスポート層プロトコルが TCP であるとの仮説を立て、項番 4 のパケットフィルタリングルールと合致していることを検証できたとする。このとき、仮説は正しいものとみなして解を導くのである。

表 4 は、本社部署 1 セグメントの収容ポートの IN 方向に適用されるルールである。したがって、このリモート接続通信のリプライパケットを許可するルールが表 4 に登録されていなければならない。そのルールとは、送信元 IP アドレスは本社部署 1 セグメント、宛先 IP アドレスは管理セグメント、プロトコルは「TCP」、送信元／宛先ポート番号は「any」、TCP 制御ビットは「any」となるはずだ。これは、項番 4 と合致する。ゆえに、先ほど立てた仮説は正しいと考える。

したがって、項番 4 が許可している通信は、「管理セグメントの PC から本社部署 1 セグメントの PC へのリモート接続のうち、TCP の通信の逆方向（戻り方向）」である、と推論できる。

●解の導出

本問では、項番 3, 4 の二つのパケットフィルタリングルールによって制御される通信の内容を問うている。ここまで考察した内容をまとめると、次のようになる。

- 項番 3 で禁止する通信は、本社部署 1 セグメントの PC から管理セグメントの PC に対して確立する、TCP コネクション
- 項番 4 で許可する通信は、管理セグメントの PC から本社部署 1 セグメントの PC へのリモート接続のうち、トランスポート層が TCP である通信の逆方向（戻り方向）

この内容を、指定字数 70 字に収まるようにまとめればよいのだが、字数の制限がけっこう厳しい。そこで、本問では「通信の内容」が問われていることを踏まえ、「送信元」「宛先」「TCP コネクション」など、通信内容を表すキーワードを重視して作文してみる。このようにして、解答例に示したような正解に至る。

■設問 5

(1)

解答例

社	外	の	W	e	b	サ	ー	バ	と	の	間	の	S	S	L	で	暗	号	化	さ	れ	た	通	信	に
お	い	て	も	,	認	証	さ	れ	た	利	用	者	と	通	信	内	容	が	取	得	で	き	る	。	

(51字)

又は

プ	ロ	キ	シ	サ	ー	バ	の	認	証	に	連	続	し	て	失	敗	し	た	こ	と	が	記	録	さ	れ
た	ロ	グ	か	ら	,	マ	ル	ウ	ェ	ア	の	活	動	と	推	測	で	き	る	情	報	が	取	得	で
き	る	。																							

(55字)

本問は、プロキシサーバの交換によって、新たにログとして取得できる情報を問うている。

プロキシサーバの交換によって、どのような機能が加わったのだろうか。この点について、〔標的型メール攻撃の手法と対策案〕の第 10 段落には、「既設のプロキシサーバを、認証機能と、HTTPS で暗号化されたデータを復号する機能とをもつ機種に変換する」と記述されている。

二つの機能があることが分かったので、それぞれの機能の追加によって、新たにログとして取得できる情報が増えたのか、一つずつ考察してみよう。

●認証機能の追加による、新たにログとして取得できる情報

認証機能については、〔入口対策と出口対策の実施項目〕の第 1 段落、S 主任の 2 番目の発言の中で、より詳しい説明がなされている。そこには、「プロキシサーバで利用者認証を行えば、マルウェアによるバックドアの通信路の開設を困難にできだけでなく、バックドアの通信が発見しやすくなる」と記述されている。要するに、認証機能とは「利用者認証」のことだ。

表 2 を見ると、全社の PC から社外の Web サイトにアクセスするときは、プロキシサーバを経由することが定められている。プロキシサーバで利用者認証を行うことにより、認証に成功した PC の利用者だけが、社外の Web サイトにアクセスできるようになる。なお、問題本文には認証方法が具体的に述べられていないが、一般的にはパスワード認証が採用されることが多い。

社内に侵入したマルウェアは、インターネット上の攻撃者のサーバと通信する（〔標的型メール攻撃の手法と対策案〕の第 3 段落）。認証機能をもつプロキシサーバを設置

することにより、このマルウェアの通信は認証に失敗する。したがって、「マルウェアによるバックドアの通信路の開設を困難にできる」という S 主任の発言は正しいと言える。

それでは、「バックドアの通信が発見しやすくなる」という発言についてはどうだろうか。これが発見するには、利用者認証の成否をログに残し、ログを検査する必要がある。もちろん、人間は誤りを犯すので一度や二度の失敗は起こり得る。とはいえ、何度も連続して失敗したログがあれば、マルウェアの活動であると推測できる。

したがって、新たにログとして取得できる情報は、「プロキシサーバの認証に連続して失敗したことが記録されたログから、マルウェアの活動と推測できる情報が取得できる」となる。

よって、これが正解となる。

●復号機能の追加による、新たにログとして取得できる情報

既に正解は得られたが、念のため、復号機能についても考察してみる。結論から言うと、実はこの機能からもう一つの解を導くことができる（本問では、どちらも正解である）。

復号機能については、[プロキシサーバの復号機能の実現方法]の中で、より詳しい説明がなされている。既に設問 3 で解説しているので、ここの本論である「新たにログとして取得できる情報」にただちに入ることしよう。

設問 3 (2) で解説したとおり、復号機能をもつプロキシサーバ経由の SSL 通信では、二つの SSL セッションが開設される。プロキシサーバは二つの SSL セッションの終端であるため、プロキシが転送する通信は、プロキシサーバ上で復号されている。したがって、復号した通信の内容（送信元、宛先、プロトコルなど）をログに残すことができる。

既設のプロキシサーバでは、暗号化された通信を転送していた。それゆえ、ログに残すことができるのは、SSL 通信の内容（送信元、宛先、プロトコルは SSL）である。

したがって、新たにログとして取得できる情報は、社外の Web サーバとの間の SSL セッションを復号した通信の内容である。

交換したプロキシサーバでは認証機能も追加されるため、利用者認証に成功したときだけ、SSL セッションが開設される。この点を考え合わせるなら、「認証された利用者が誰であるか」「その利用者はどのような通信をしているのか」という情報を新たに取得できることが分かる。

よって、正解は、「社外の Web サーバとの間の SSL で暗号化された通信において、認証された利用者と通信内容が取得できる」となる。

●補足：認証に成功したログの活用方法について

プロキシサーバの認証機能はマルウェアによる通信路の開設を困難にするとはいえず、これで万全であるとは言えない。

例えば、標的型メールを受信した利用者は、本文に誘導されるまま Web サイトのリンク先にアクセスし、マルウェアをダウンロードするかもしれない。標的型メール攻撃を受けている疑いがあるときは、ダウンロードの記録を調べる必要があるだろう。このとき、たとえそのダウンロードが SSL で暗号化されていたとしても、復号した通信内容がログに残っているのだから、検査できるようになるわけだ。このように考えると、認証に成功した通信のログは役に立つことが分かる。

〔標的型メール攻撃の手法と対策案〕の第 10 段落には、コンテンツフィルタリングやウイルスチェックなどのセキュリティ対策を行える、と述べられている。(本文にはそれ以上詳しく書かれていないが、)コンテンツフィルタリング処理やウイルスチェック処理のログを、プロキシサーバの通信ログと照らし合わせることで、多角的に検査することもできる。

更に言えば、サイバー攻撃の脅威は、何も標的型メール攻撃だけではない。復号機能をもつプロキシサーバが SSL 通信を復号して通信内容をログに残すことで、従来は SSL 通信の暗号化により隠蔽されていたかもしれない、様々なサイバー攻撃についても検査しやすくなるはずだ。

(2)

解答例

(以下のうち三つ)

- ・メールに添付されたファイルを開かない。(19字)
- ・メール本文に記載されたリンク先にアクセスしない。(24字)
- ・メールが、正しい送信者から送信されたものか確認する。(26字)
- ・不審なメールの内容を、セキュリティ担当者に報告する。(26字)
- ・発見した不審なメールに関する情報を、全社で共有する。(26字)

本問は、本文中の下線(キ)で定めるべき規程の内容を三つ問うている。下線(キ)は〔入口対策と出口対策の実施項目〕の第2段落、5番目の箇条書きにある。そこには「(キ) 利用者が不審メールを発見したときの対応に関する規程を定め、運用規程に

組み入れる」と記述されている。

設問 1 の空欄 a で、標的型メール攻撃の特徴について解説した。このメールは、攻撃対象者と関係がありそうな組織、機関及び実在の人物を装って、送られてくる。そして、その本文は、添付ファイルを開いたりリンク先にアクセスしたりするよう巧みに促す内容である。

したがって、メールの差出人が関係者であったとしても、内容が不審であるならば、添付されたファイルを開くことや、リンク先にアクセスすることを控えなければならない。この点は規程に定めておくに値する。

よって、不審なメールを発見したときの対応として、次に示す二つの解を導くことができる。

- ①メールに添付されたファイルを開かない
- ②メール本文に記載されたリンク先にアクセスしない

次にできることは、メールの差出人になっている本人に対し、メールや電話などで確認を取ることである。本人が送ったものであることが確認できれば、不審なメールではないことが明らかになるからだ。よって、次に示す解を導くことができる。

- ③メールが、正しい送信者から送信されたものか確認する

本人に確認を取り、その本人が送信したメールではないことが判明したならば、どのように対応したらよいだろうか。標的型メール攻撃を受けている可能性があるので、不審なメールの内容をセキュリティ担当者に報告したり、全社で共有したりする必要がある。よって、次に示す二つの解を導くことができる。

- ④不審なメールの内容を、セキュリティ担当者に報告する。
- ⑤発見した不審なメールの情報を、全社で共有する。

(3)

解答例

マルウェアの社内での活動を，早期に発見できること (24字)

本問は、本文中の下線（ク）によって期待される効果を問うている。下線（ク）は〔入口対策と出口対策の実施項目〕の第 2 段落，6 番目の箇条書きにある。そこには「（ク） ログの検査間隔を可能な限り短縮して，定期的に検査を行う」と記述されている。

設問 5（1）で解説したとおり，マルウェアの活動は，プロキシサーバのログに記録される。とはいえ，ログを検査しない限り，その活動を実際に発見することはできない。したがって，ログの検査間隔を可能な限り短くして，定期的に検査することにより，マルウェアの社内での活動を，早期に発見できるようになる。

よって，正解は解答例に示したとおりとなる。

問 2

出題趣旨

サーバ仮想化技術の発展とともに、仮想化環境でシステムを構築する際に、従来と異なる課題が発生してくる。また、ネットワーク機器についても、最近、仮想サーバ上で動作させる試みも出てきている。

このような流れが進むと、サーバ、ネットワークの IT プラットフォームが仮想サーバという汎用的なプラットフォーム（サーバ）上に集約され、各種機能は仮想サーバで動作するソフトウェアに変わっていくことになる。このことによって、システム構築のスピードアップ、柔軟性や運用性の向上が期待される。

しかし、このような状況になっても、発生する新しい課題に対して、既存技術を活用して適切な対処をしていくためには、課題となる現象の基礎的・根本的な理解が不可欠である。本問では、その拡張性から応用範囲が広い SIP を取り上げ、SIP ベースのコミュニケーションシステムをネットワークも含め、仮想サーバ上に構築していくという状況を設定し、その構築過程で発生する課題とその解決を題材とした。

特に、仮想化が進んだシステム構築の中で、従来とは異なる課題が発生することの認識と、課題への対応といった観点で、基礎的理解に基づく状況把握力や技術応用力を問うた。

採点講評

問 2 では、SIP ベースのコミュニケーションシステムを、サービス用システムとして仮想環境上に構築する場合を取り上げ、SIP の基本的な技術的特徴・応用面での拡張性、仮想環境との間で各種の特徴をもつフレームをやり取りする場合に発生する課題と対処、また、ネットワーク機能を仮想サーバ上で実現する取組みなどへの理解を問うた。

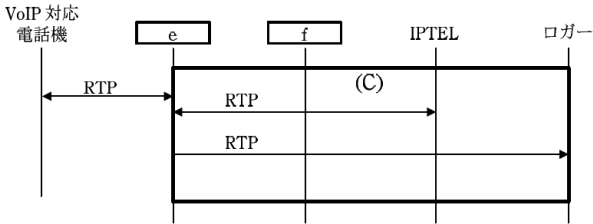
設問 2 は、SIP の拡張性を実現するセッション生成の仕組みに伴うアドレス解決の課題を問うた。(2) では、SIP メッセージ内の情報の書換えの必要性を問うたが、正答率は低かった。メッセージ内容がセッション生成に、どのように使われるかの理解を深めてほしい。

設問 3 は、スイッチのミラーポートの出力フレームを、トランクインタフェースを使って仮想環境のサーバに取り込む方法を問う問題で、正答率は低かった。ミラーポートの出力フレームの特徴として、宛先 MAC アドレスが別のフレームでは送信元 MAC アドレスになる場合が発生し、受け取るポートで、MAC アドレスの学習をすると、受け取ったフレーム宛先ポートが同一ポートになってしまうということに気が付かない受験者が多かった。ミラーポートの出力フレームの送信元 MAC アドレスが、出力したポートの MAC アドレスと誤解している解答も散見された。ブリッジの動作原理に関して再度理解を確認してほしい。

設問 4 は、音声パケットを複製し、別サーバ宛に転送する場合、SIP による専用のセッションを使う方法に関する問題で、正答率は高かった。(4) では、通話する相手間で交わされる SIP メッセージと、ログサーバとの間で交わされる SIP メッセージが同一と誤解している解答も見られた。シーケンス図の表面的なメッセージ名だけでなく、具体的にやり取りされるメッセージの内容にも注意してほしい。

設問 5 では、ネットワーク機能を仮想サーバで実現する取組みに関する問題で、正答率は高かった。(3) では、ハードウェア障害に対応するための冗長化構成のコストメリットを問うたのに対し、一般論の解答が散見された。設問の趣旨に添って明確に解答するよう心掛けてほしい。

全体として、比較的下位の層におけるネットワーク動作の理解が十分でない印象を受けた。新しい技術を用いたネットワークで発生する問題の解決にも、基本的な動作原理の理解が必要になることもあるので、基本的理解に基づく応用力を高めることを心掛けてほしい。

設問	解答例・解答の要点		備考
設問 1	(1)	a インスタントメッセージ 又は チャット	
		b RTP 又は RTP と RTCP	
		c UDP	
		d テキスト	
	(2)	URI から相手の IP アドレスを求め、相手に INVITE メッセージを送る。	
設問 2	(1)	公衆 IP 電話網の SIP サーバ、IP-PBX	
	(2)	アドレス変換対象外の SIP メッセージ内に送信者のプライベート IP アドレスが含まれている。	
	(3)	SIP メッセージ内の IP アドレス情報を送信元である VoIP-GW のグローバルアドレスに書き換える。	
設問 3	(1)	仮想スイッチのポートに該当する VLAN の全てのフレームを出力し、仮想 NIC 側でそれらを全て取り込む動作	
	(2)	状態 流入するフレームの宛先 MAC アドレスが既にポート 3 側に存在するとして登録されている。	
	対応策	MAC アドレス学習機能を抑止できる SW を使用し、通過するポート 3 で学習を抑止する。	
設問 4	(1)	音声パケットを中継しないから	
	(2)	e VoIP-GW	
		f IP-PBX	
	(3)		
	(4)	VoIP-GW には呼制御に関する SIP セッション情報も送られてくるから	
	(5)	ミラーポート出力フレームの転送用設定が不要だから	
設問 5	(1)	ア IP01	
		イ Any	
		ウ Any	
		エ 443	
	(2)	サービス提供用内部 LAN のネットワークに属する IP アドレス	
	(3)	ネットワーク機器ごとに異なるハードウェアを用意せずに済むから	

本事例は VoIP 対応電話システム（以下、IPT システムという）が登場し、解を導くには SIP に関する一般的な知識が必要となる。SIP については、〔サービス用 IPT システムの構成〕の第 6～9 段落で説明がなされているが、若干の補足を加えて解説しよう。

なお、SIP の用語やシーケンスについて理解している読者は、ここを読み飛ばして設問の解説から入っていただいても構わない。

ここで述べることは、あくまで本事例を理解するために役立つ知識だけに留めている。SIP の詳細な仕様を網羅してはいないので、あらかじめご了承ください。

● SIP

SIP（Session Initiation Protocol）は、端末間で、セッションの生成、変更、転送、切断などを行うプロトコルである。SIP では、端末のことをユーザエージェント（以下、UA という）と呼ぶ。

SIP で規定されているのは、主にセッションを制御する機能である。セッション上でやり取りされるデータそのものについて規定されていない。セッションを生成した後、リアルタイムデータ（音声、映像）の転送には、別のプロトコルが用いられる。一般的に言って、リアルタイムデータの転送に使用されるプロトコルは、RTP である。

SIP の基本的な機能であるセッション制御に関する規格は、RFC3261 で規定されている。その後、機能の追加や拡張が行われており、インスタントメッセージを交換する機能、イベントを通知する機能なども規定されている。

インスタントメッセージ機能は、RFC3428 で規定されている。これは、チャットのように、利用者間でテキスト情報を交換する機能である。

イベント通知機能は、RFC6665 で規定されている。これは、イベントを通知する側とそのイベントを購読する側とを事前に登録しておき、通知側 UA でイベントが発生する都度、購読側 UA にそのイベントが通知される機能である。よく利用されるイベント情報として、「利用者が今どんな状況にあるか」（「在席中」「離席中」「休憩中」など）といったプレゼンスに関する情報がある。

表：SIP で規定されている機能

機能	主な内容
セッション制御	セッションの生成を要求する セッションを変更する 別の UA にセッションを転送する セッションを切断する
インスタントメッセージ	インスタントメッセージを送信する

（表は次ページに続く）

機能	主な内容
イベント通知	プレゼンス情報の購読をサーバに申し込む プレゼンス情報をサーバに送信する サーバから購読者にプレゼンス情報を通知する

● SDP

リアルタイムデータの通信を始める前に、上位アプリケーション間で、どのような通信を行うかについて、情報を交換しておく必要がある。その情報とは、具体的に言うと、

- UA の IP アドレス
- リアルタイムデータ転送用プロトコルが使用するポート番号
- 音声や映像といったメディアの種別、及び、そのメディアで用いられる符号化方式

などである。

この情報の記述方法を規定したものが、SDP (Session Description Protocol) である。

この情報交換は、SIP がセッションを生成している間に行われる仕組みになっている。これをネゴシエーションという。ネゴシエーションについては、「SIP のシーケンス (基本)」で後述する。

なお、ここで言う「メディア」とは、UA 間で送受信される音声や映像などのデータのことである。SIP は、一つのセッションの中で、複数のメディアを同時に送受信することができる。例えば、音声通話のセッションを生成したり、音声と映像を組み合わせたビデオ会議のセッションを生成したりすることができる。

● SIP の構成要素

SIP を構成する要素は、UA、SIP サーバである。

・ UA

UA の識別には、SIP URI が用いられる。その書式は、「sip: 利用者識別子 @ ドメイン名」という URI 形式である。「利用者識別子」の部分には、電話番号を入れることができる。同一ドメイン内の通信であれば、「@ ドメイン名」を省略してもよい。

・ SIP サーバ

UA で電話をかけるとき、発呼する側は、着呼する側の電話番号や利用者識別子を知っている。

このとき、もしも着呼側 UA の IP アドレスを知っていれば（発呼側 UA に登録されていれば）、UA 間で SIP 通信を直接やり取りし、セッションを生成することができる。この場合、SIP サーバは不要である。

それでは、もしも着呼側 UA の IP アドレスを知らない場合、どうしたらよいだろうか。実際、相手の UA の IP アドレスまでは知らないことが多いのではないだろうか。このとき、UA 間のセッション生成を仲介するために、SIP サーバが必要となる。

SIP サーバを用いる場合、UA は、自分の利用者識別子、自分の IP アドレスを含む登録メッセージを、SIP サーバに事前に送信しておく。SIP サーバは、これを受信し、自分が仲介する全ての UA について、SIP URI と IP アドレスの対応付けを登録しておく。

通話するとき、UA は SIP サーバにセッションの生成を要求し、その要求メッセージの中で、着呼側の SIP URI を指定する。SIP サーバは、指定された SIP URI から IP アドレスを割り出すことができるので、セッション生成を仲介することができる。

SIP サーバを用いた SIP のメッセージシーケンスについては、「SIP のシーケンス (SIP サーバを用いる場合)」で後述する。

● SIP のメッセージ

SIP のメッセージの種類には、発呼側 UA から着呼側 UA に送信するリクエストと、着呼側 UA から発呼側 UA に返信するレスポンスがある。

・ リクエスト

主なリクエストメッセージは、次のとおりである。

差し当たって、本事例を理解するためには、この四つを押さえておけばよいだろう。

表：主なリクエストメッセージ

リクエスト	機能	主な内容
INVITE	セッション制御	セッションの生成を要求する
ACK	セッション制御	セッション生成を確認する
BYE	セッション制御	セッションを切断する
MESSAGE	インスタントメッセージ	インスタントメッセージの通知

※本事例を理解するのに直接関係がないもの（イベント通知機能等）は割愛している。

問題文の図 2, 図 5 に掲載されているシーケンスには, セッション制御機能のメッセージである, INVITE, ACK, BYE が登場する。最後の MESSAGE は, 設問 1 の空欄アでインスタントメッセージが問われているので, 参考までにここに掲載しておいた。

・レスポンス

レスポンスメッセージには, 次に示す 3 桁のレスポンスコードが含まれている。1 桁目の値によって六つのクラスに分類される。

差し当たって, 本事例を理解するためには, 成功応答を意味する 200 OK を押さえておけばよいだろう。

表：レスポンスコード

タイプ	クラス	意味		
Provisional (暫定応答)	1XX	100	Trying	処理中
		180	Ringin	着呼側を呼出し中
Final (最終応答)	2XX	200	OK	成功
	3XX	リダイレクション, フォワーディング		
	4XX	クライアント起因によるリクエスト失敗		
	5XX	サーバエラー		
	6XX	一般的なエラー (ビジー, 拒否など)		

※クラスの 2 桁目, 3 桁目の XX には, 0～9 の数値が入る。

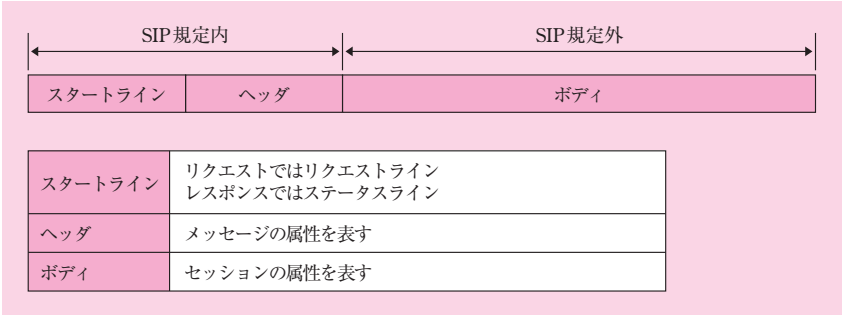
・メッセージフォーマット

SIP メッセージは, 次の図に示すとおり, スタートライン (先頭行), ヘッダ, ボディからなる。なお, ボディは必要に応じて追加されるものであり, ボディをもたないメッセージがある。

ボディは MIME 形式で記述することが定められている。とはいえ, 記述内容に関する規格は, SIP では規定されていない。

セッション制御機能の INVITE や ACK などのリクエストでは, ボディにセッションの属性が記述される。「SDP」で解説したとおり, その記述に用いられるのが SDP である。

インスタントメッセージ機能の MESSAGE リクエストでは, ボディにテキストの内容が記述される。



図：SIP のメッセージフォーマット

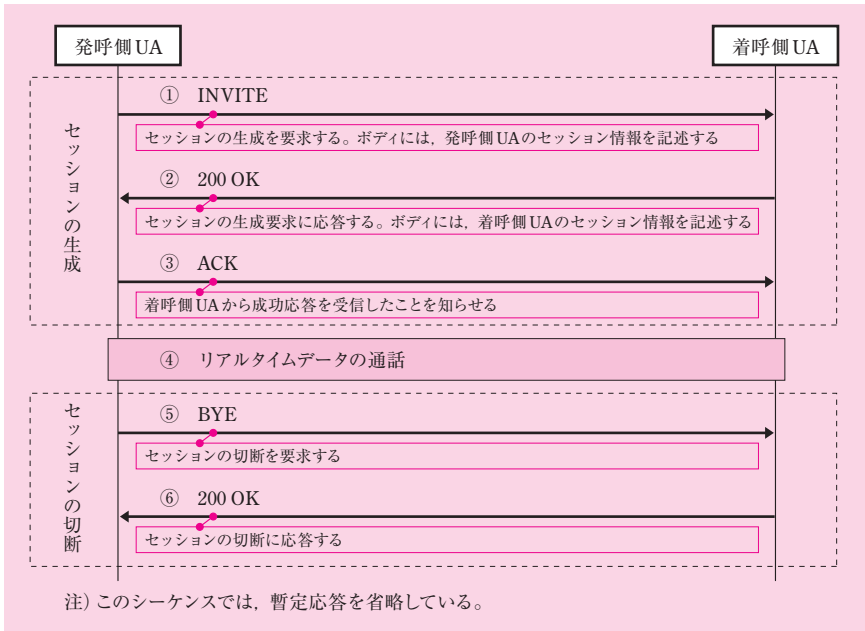
なお、本事例を理解するために、メッセージフォーマットの仕様を詳細に知っておく必要はないだろう。

問題文の図 3「INVITE リクエストの内容例（抜粋）」が掲載され、設問 2（2）で図 3 が取り上げられているが、問題文や図 3 の中に重要な手掛かりが与えられている。SIP そのものの知識がなくても解答できるよう、十分に配慮されている。

● SIP のシーケンス（基本）

SIP でセッションを生成するときの基本となるメッセージは、INVITE リクエスト、200 OK レスポンス、ACK リクエストの 1 往復半からなるやり取りである。SIP の規格を定めた RFC は、これをスリーウェイハンドシェークと呼んでいる（RFC3261, 15 ページ）。

SIP の基本的なシーケンスを次の図に示す。なお、この図では暫定応答を省略している。



図：SIP の基本的なシーケンス

- ①発呼側は、セッションの生成を要求するため、INVITE リクエストを送信する
このボディには、発呼側のセッション情報を記述する。
- ②着呼側は、セッション生成要求に应答するため、200 OK（成功応答）レスポンスを送信する
このボディには、着呼側のセッション情報を記述する。
着呼側は、INVITE リクエストの SIP メッセージに記載された情報から、発呼側の IP アドレス、通話に使用するポート番号、などのセッション情報を知ることができる。
着呼側が 200 OK を返信したことは、これら発呼側のセッション情報を受け付けたことを意味している。
- ③発呼側は、着呼側から成功応答を受信したことを知らせるため、ACK リクエストを送信する
発呼側は、200 OK レスポンスの SIP メッセージに記載された情報から、着呼側の IP アドレス、通話に使用するポート番号、などのセッション情報を知ることができる。
発呼側が ACK を送信したことは、これら着呼側のセッション情報を受け付け

たことを意味している。③が終了した時点で、セッションが生成される。

④リアルタイムデータの通話を行う

通話に用いるプロトコルは、①～②のセッション情報交換で決めたものである。通常、音声や映像などのリアルタイムデータの通話には、RTP が用いられる。

通話に用いる IP アドレスは、①～②のセッション情報交換で決めたものである。

⑤セッションの切断を要求するため、BYE リクエストを送信する

切断の要求は、発呼側、着呼側のどちらから送信してもよい。

⑥切断要求に応答するため、200 OK (成功応答) レスポンスを送信する

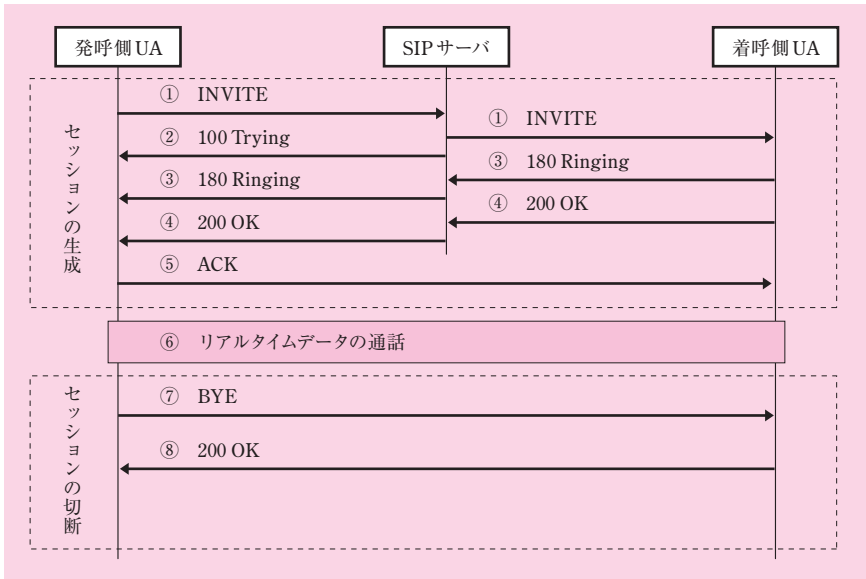
セッション生成時のスリーウェイハンドシェークを通し、発呼側と着呼側はセッション情報を交換し、かつ、双方が合意した属性でセッションを生成する。「SDP」でも触れたが、このやり取りのことを、ネゴシエーションと呼んでいる。このネゴシエーションを経て、リアルタイムデータの通信に移ることができる。

ネゴシエーションについて補足すると、発呼側が INVITE を送信する際、複数のセッション情報の候補を列挙することができる。このとき、着呼側は、その中から一つを選んで成功応答を返信する。あるいは、発呼側が INVITE を送信する際、セッション情報を一切記載しないこともできる。このとき、着呼側はセッション情報を自由に指定して成功応答を返信する。

● SIP のシーケンス (SIP サーバを用いる場合)

「SIP の構成要素」で触れたが、UA が互いの IP アドレスを把握していない場合、SIP サーバを仲介してセッションを生成する。各 UA は、SIP URI と IP アドレスの対応付けを SIP サーバに初期登録しておく。

SIP サーバを使用した場合のシーケンスを次の図に示す。この図では暫定応答も記している。



図：SIP サーバを仲介した場合のシーケンス

①発呼側は、SIP サーバに INVITE メッセージを送信する

SIP サーバは、INVITE リクエスト中の着呼側 SIP URI から IP アドレスを割り出し、着呼側にこれを転送する。

②SIP サーバは、INVITE リクエストの転送を知らせるため、発呼側に 100 Trying (処理中) レスポンスを送信する

③着呼側は、INVITE メッセージを受信すると、利用者を呼び出す（電話であれば、呼出し音を鳴らす）

呼出し中であることを知らせるため、着呼側は SIP サーバに、SIP サーバは発呼側に、180 Ringing (呼出し中) レスポンスを送信する。

④着呼側は、セッション生成要求に応答するため、200 OK (成功応答) レスポンスを SIP サーバに送信する

SIP サーバは、発呼側にこれを転送する。

⑤発呼側は、着呼側から成功応答を受信したことを知らせるため、ACK リクエストを送信する

「SIP のシーケンス (基本)」で述べたとおり、発呼側は、200 OK (成功応答) レスポンスを受信することで、着呼側の IP アドレスを知ることができる。そのため、ACK リクエストは、SIP サーバを介さずに直接相手に送信することがで

きる（SIP サーバを経由して ACK を送信してもよい）。

- ⑥リアルタイムデータの通話を行う
- ⑦セッションの切断を要求するため、BYE リクエストを送信する
- ⑧切断要求に応答するため、200 OK（成功応答）のレスポンスを送信する

以上、SIP に関する一般的な知識について略述したが、試験では、ここで述べた知識を応用した、システムの構築について出題されている。その具体的な内容については、以降の解説の中で、順次掘り下げていくことにする。

■設問 1

(1)

解答例

- a：インスタントメッセージ 又は チャット
- b：RTP 又は RTP と RTCP
- c：UDP
- d：テキスト

a

空欄 a を含む文章は、「サービス用 IPT システムの構成」の第 6 段落にある。第 6 段落は SIP について説明している。そこには、「SIP によって制御されたセッションでデータをやり取りする場合、音声だけなら電話、テキストだけなら a、音声と動画を組み合わせることでビデオ会議、というように、幅広い応用の余地がある」と記述されている。

空欄 a は、SIP でテキストデータをやり取りすることについて述べている。冒頭の「SIP」で解説したとおり、SIP は、チャットのように利用者間でテキスト情報を交換する機能をもつ。これは、「インスタントメッセージ」と呼ばれている。

よって、空欄 a に該当する字句は、「インスタントメッセージ」である。なお、この機能を「チャット」と呼ぶこともあるので、これも正解である。

b

c

空欄 b, c を含む文章は、「音声データを転送する場合の一般的なプロトコルは、RFC 3550 で規定された b」であり、そのトランスポート層のプロトコルには、リア

リアルタイム性を重視し、再送制御を行わない c が使われる」と記述されている。

RFC3550「RTP: A Transport Protocol for Real-Time Applications」で規定された、リアルタイムデータの転送プロトコルは、RTP である。よって、空欄 b に該当する字句は、「RTP」である。

RTP のトランスポート層のプロトコルには、UDP が使用される。その理由は、問題文に記述されているとおり、リアルタイム性を重視しているためである。よって、空欄 c に該当する字句は、「UDP」である。

d

空欄 d を含む文章は、「SIP で使われるメッセージは、d 形式で記述されるので、判読しやすい」と記述されている。結論から言うと、空欄 d に該当する字句は「テキスト」となる。これは仕様であるがゆえ別解の余地はない。

ただし、解答テクニックという観点から補足すると、この空欄については、問題文の中でヒントが与えられるので、正解を導けるはずだ。

まず、空欄 d の直後に「判読しやすい」と書かれているので、「テキスト」形式ではないかと推論できる。そして、極めつけは、図 3「INVITE リクエストの内容例」である。SIP メッセージが「テキスト」形式であることは一目瞭然だからだ。このように、試験では手がかりが与えられていることもあるので前後の記述もチェックしてみよう。

参考までに、SIP メッセージのボディ部分だけが問われていたなら、ボディ部分はマルチパートの MIME 形式を記述できるので、「MIME」形式も正解と言える。とはいえ、問題文は「SIP メッセージ」と記述されており、ヘッダ部分も含まれているため、「テキスト」形式が正解となる。

(2)

解答例

U	R	I	から	相手	の	I	P	アド	レス	を	求	め	,	相手	に	I	N	V	I
T	E	メ	ッ	セ	ー	ジ	を	送	る	。	(36字)								

本問は、下線①の動作を問うている。

下線①は、「サービス用 IPT システムの構成」の第 8 段落にある。そこには、「セッションは、通信を行う UA 間で直接やり取りして生成することもできるが、規模の大きな組織の場合は利用者が多く、URI の登録に手間が掛かるので、①セッションの生

成を仲介するサーバを設置する。このサーバは SIP サーバと呼ばれ(る)」と記述されている。「セッションの生成を仲介する」サーバとは、ここに述べられているとおり、「SIP サーバ」のことである。したがって、下線①の動作とは、SIP サーバが行う、セッションの生成を仲介する動作を指している。

ただし、問題文に「具体的に述べよ」とある点に留意しなければならない。それゆえ、本文から表面的に読み取れることなく、技術的な内容を掘り下げた内容を解答することが求められている（付録 PDF「午後問題の解答テクニック」の「0.3.5 問題を解く①：重要テクニック」の「2. 本文より一歩掘り下げて、できるだけ具体的に解答する」を参照されたい）。

それでは、出題の意図を探るため、下線①の文脈を見てみよう。下線①のすぐ前の文章は、「セッションは、通信を行う UA 間で直接やり取りして生成することもできるが、規模の大きな組織の場合は利用者が多く、URI の登録に手間が掛かる」と記述されている。それを受けて下線①が続いており、「(URI の登録に手間が掛かるので、) ① セッションの生成を仲介するサーバを設置する」と記述されている。

この文脈から、掘り下げるべき点が明らかになった。出題者が問いたいのは、「UA 間で直接セッションを生成すると URI を登録する手間が掛かるので、その代わりに、セッション生成のために SIP サーバが行っていること」であるに違いない。

SIP サーバの役割については、冒頭の「SIP の構成要素」で解説している。SIP サーバを用いる場合、UA は、自分の利用者識別子、自分の IP アドレスを含む登録メッセージを、SIP サーバに事前に送信しておく。SIP サーバは、これを受信し、自分が仲介する全ての UA について、SIP URI と IP アドレスの対応付けを登録しておく。

通話するとき、UA は SIP サーバにセッションの生成を要求し、その要求メッセージの中で、着呼側の SIP URI を指定する。SIP サーバは、指定された SIP URI から IP アドレスを割り出すことができるので、セッション生成を仲介することができる。

セッション生成の具体的なシーケンスについては、冒頭の「SIP のシーケンス (SIP サーバを用いる場合)」で解説している。

セッションの生成を要求するメッセージは、INVITE リクエストである。SIP サーバは、発呼側 UA から INVITE メッセージを受信する。INVITE リクエストで指定された着呼側 UA の SIP URI から、IP アドレスを割り出す。その後、着呼側 UA に INVITE リクエストを転送する。このように、SIP サーバはセッション生成を仲介している。

以上をまとめると、次に示す内容を含めるようにして、解答を作文すればよい。

- SIP サーバは、INVITE リクエスト中の着呼側 UA の SIP URI から、IP アドレスを割り出す

- SIP サーバは、着呼側 UA に INVITE リクエストを送信する

よって、正解は、「URI から相手の IP アドレスを求め、相手に INVITE メッセージを送る」などとなる。

■設問 2

(1)

解答例

公衆 IP 電話網の SIP サーバ、IP-PBX

本問は、下線②の B2BUA がその役割を果たすために、UA として初期登録する必要がある登録先を問うている。

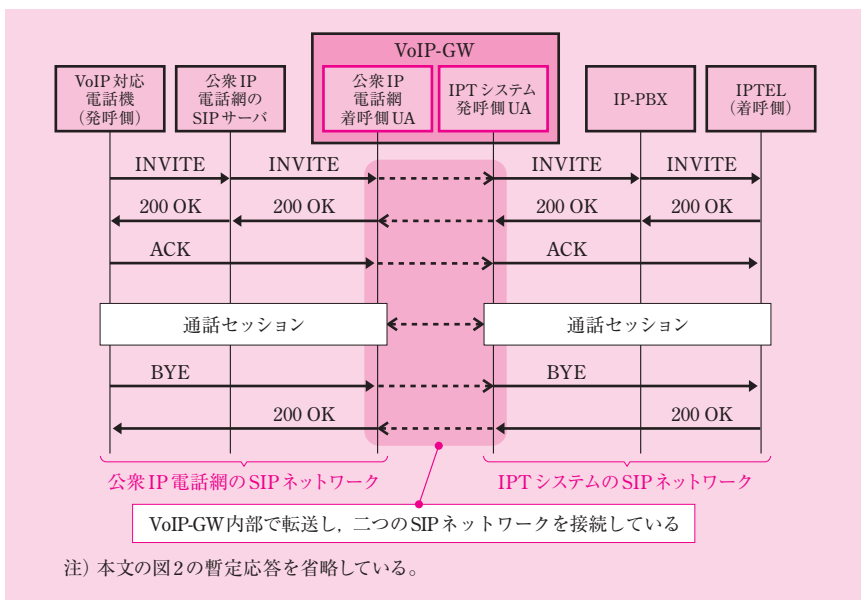
下線②は、「IPT システムの概要」の第 3 段落にある。そこには、「IP-PBX 配下の IPTEL を識別するための 050 電話番号は、公衆 IP 電話網の通信事業者から割り当てられる。通信事業者の公衆 IP 電話網の中にも SIP サーバが存在するので、VoIP-GW は、②両方の SIP ネットワークに対して UA として振る舞う特殊な UA である B2BUA (Back-to-Back User Agent) になる」と記述されている。

したがって、B2BUA は、一方の SIP ネットワーク側では着呼側、他方の SIP ネットワーク側では発呼側として振る舞うことが分かる。

本事例では、VoIP-GW は B2BUA となる。VoIP-GW は、公衆 IP 電話網と IPT システムの二つの SIP ネットワークの境界に位置しており、これら二つの SIP ネットワークに属している。

この点を理解するため、図 2 の例に当てはめて考察してみよう。

VoIP-GW は、公衆網 IP 電話網においては、着呼側の UA として振る舞う。IPT システムにおいては、発呼側の UA として振る舞う。そのようにして、二つの SIP ネットワークを接続する役割を、VoIP-GW は果たしている。



図：本文の図 2 における VoIP-GW の役割

問題文には「UA として初期登録する」とあるが、初期登録とは一体何を意味しているのだろうか。初期登録について、第 2 段落には、「IPT システムでは、UA は起動後、自分の利用者識別子、自分の IP アドレスを含む登録メッセージを SIP サーバに送信し、初期登録をする」と記述されている。つまり、初期登録とは、SIP URI と IP アドレスの対応付けを SIP サーバに事前に登録しておくことを指している。

B2BUA は「UA として振る舞う」とあるので、ここに説明されているように、「自分の利用者識別子、自分の IP アドレス」を SIP サーバに初期登録するに違いない。もちろん、第 2 段落は IPT システムの UA に関する記述であり、B2BUA に同じように当てはまるという保証はない。とはいえ、これは試験問題なので、「初期登録」という語句が一貫して用いられていると考えてよいだろう。

ここで、これまで考察した内容を、具体例に当てはめてみよう。その例として、公衆 IP 電話網の VoIP 対応電話機から、A 社の IPTEL に電話をかける場面を取り上げる。

電話をかける以上、公衆 IP 電話網の利用者は、着呼する相手の 050 電話番号を知っている。この電話番号は通信事業者が A 社に払い出したものなので、通信事業者は、公衆 IP 電話網経由で A 社の SIP ネットワークに接続すればよいことを把握している。

とはいえ、実際に接続するには、接続先となる A 社から、VoIP-GW の IP アドレスを事前に知らされていなければならない。それゆえ、公衆 IP 電話網の SIP サーバに

は、A 社の利用者識別子と VoIP-GW の IP アドレスが対応付けられて、事前に登録されていることが分かる。要するに、これが「初期登録」である。

初期登録の結果、公衆 IP 電話網から見ると、A 社に払い出した 050 電話番号の UA は、VoIP-GW になっている。

この点を踏まえて、今度は図 2 のシーケンスを見てみる。この図は、つい先ほど考慮した、VoIP 対応電話機から IPTEL に電話をかけるときの動作シーケンスを示している。

公衆 IP 電話網の SIP サーバから VoIP-GW に INVITE メッセージを送信している。通信できているということは、公衆 IP 電話網の SIP サーバが VoIP-GW の IP アドレスを知っていることを意味している。この点、図 2 の注記には「初期登録は、事前に完了している」と記されている。したがって、これまでの推論と符合していることが分かる。

A 社の IPTEL から社外に電話をかけるときは、逆方向にして考えればよい。IPT システムから見ると、社外に電話をかけるときの UA は、VoIP-GW になっている。そのためには、IPT の SIP サーバに対し、VoIP-GW を UA として初期登録しておかなければならない。

以上をまとめると、本事例の VoIP-GW は、B2BUA である。VoIP-GW は、「公衆 IP 電話網」と「IPT システム」という二つの SIP ネットワークの境界に位置し、これら二つの SIP ネットワークにおいて UA になっている。UA として振る舞うために、VoIP-GW は、それぞれの SIP ネットワークの SIP サーバに対し、初期登録を行う必要がある。したがって、これら二つの SIP サーバを解答すればよい。

公衆 IP 電話網の SIP サーバは、図 2 に「公衆 IP 電話網の SIP サーバ」とあるので、これをそのまま解答する。

IPT システムの SIP サーバは、[サービス用 IPT システムの構成]の第 8 段落に「サービス用 IPT システムでは、IP-PBX がその役割を果たしている」とあるので、「IP-PBX」を解答する。

よって、正解は、「公衆 IP 電話網の SIP サーバ、IP-PBX」となる。

(2)

解答例

ア	ド	レ	ス	変	換	対	象	外	の	S	I	P	メ	ッ	セ	ー	ジ	内	に	送	信	者	の	プ	
ラ	イ	ベ	ー	ト	I	P	ア	ド	レ	ス	が	含	ま	れ	て	い	る	。							

(44 字)

本問は、下線③に示す問題の原因を問うている。解答に際し、図 3 を参考にできる。

下線③は、〔IPT システムの概要〕の第 5 段落にある。そこには、「インターネット網を経由して、SIP を使った通話を行う場合、企業内のプライベート IP アドレスの UA と外部とを接続するために、アドレス変換を行う必要がある。このときに、③標準的な NAT 装置では、通話セッションが生成できないという問題が発生する」と記述されている。

本問を解くには、通話セッションで用いられる IP アドレスに関する一般的な知識が必要である。そこで、まずはその点について解説する。それを踏まえて、解を導こう。

●通話セッションで用いられる IP アドレス

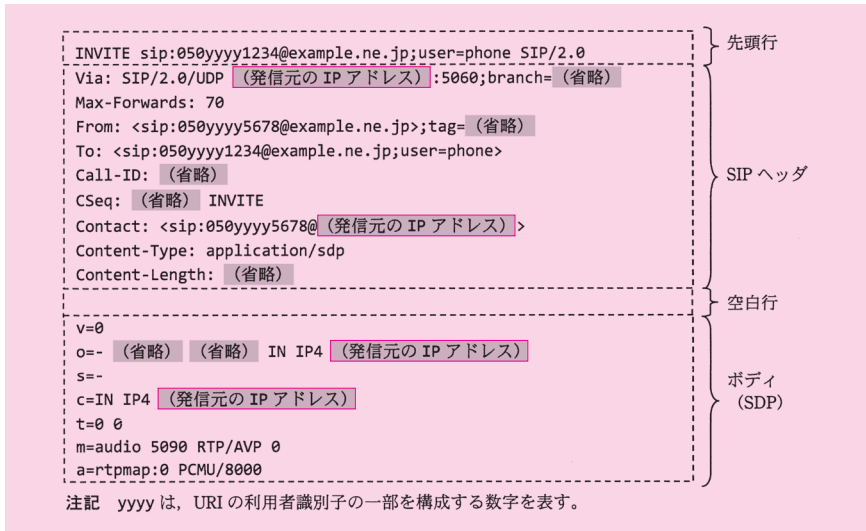
冒頭の「SIP のシーケンス (SIP サーバを用いる場合)」で解説したとおり、着呼側 UA は、INVITE リクエストを受信する。その SIP メッセージに記載された発信元 IP アドレスの情報から、発呼側 UA の IP アドレスを知ることができる。

発呼側 UA は、200 OK レスポンスを受信する。その SIP メッセージに記載された発信元 IP アドレスの情報から、着呼側 UA の IP アドレスを知ることができる。

通話セッションで用いる IP アドレスは、このときに通知し合った発信元 IP アドレスである。

本文の図 3 は、セッション生成開始時に使われる INVITE リクエストの内容例を示したものである。この図から、セッションの生成時に発信元 IP アドレスが通知されていることを見取れる。

この図を見ると、SIP メッセージのヘッダとボディの随所に、発信元の IP アドレスが記載されていることが分かる。通話セッションに入ると、着呼側が送信する RTP パケットの宛先 IP アドレスは、この INVITE リクエストに記載された発信元 IP アドレスとなる。



図：INVITE リクエストに記載されている発信元 IP アドレス（図 3 から作成）

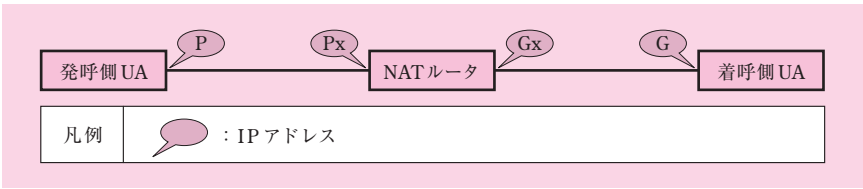
●解の導出

それでは、ここまで解説した内容を踏まえて、問題文の示す状況に照らし合わせて解を導こう。

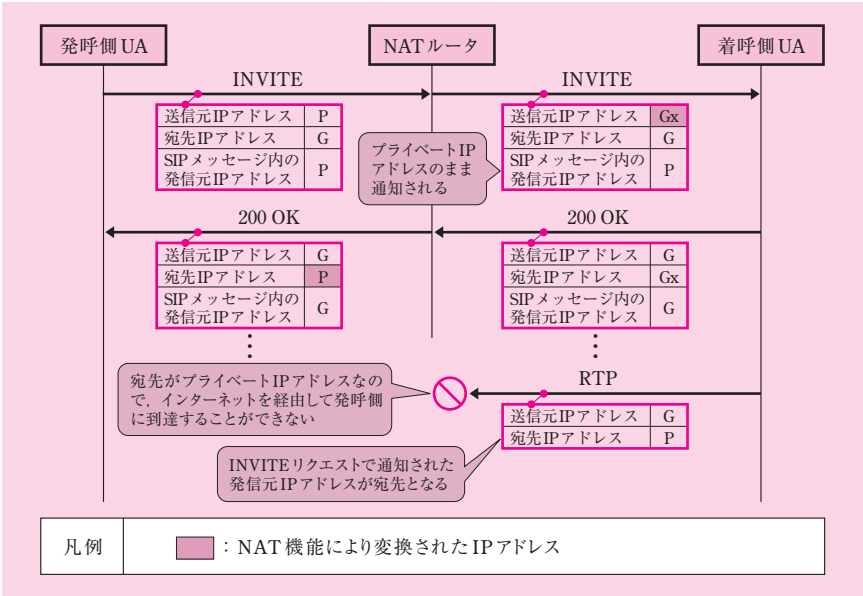
まず、この問題は、本事例の IPT システムを念頭に置いたものではないことに留意しよう。そう言える理由は、「インターネット網を経由して、SIP を使った通話を行う」と述べているものの、どのような機器を経路でアクセスしてくるのか、具体的な事柄について特に触れていないからだ。したがって、ここでは一般的な話題を取り上げているだけと考えるべきである。

では、発呼側 UA がプライベート IP アドレスをもち、着呼側 UA がグローバル IP アドレスをもつものとして、SIP のセッション生成、RTP の通話のシーケンスを考察してみる。

NAT 機能をもつルータ（以下、NAT ルータという）を経由した通信を、次の図に示す。構成図に IP アドレスを割り振っているの、これと対応させながらシーケンスを見ていただきたい。なお、この図では暫定応答は省略している。



図：NAT ルータを経由した通信の構成図



図：NAT ルータを経由した通信の動作シーケンス

この図では、シーケンスを分かりやすく示すため、SIPサーバを仲介せず、発呼側 UA は着呼側 UA の IP アドレスを知っているものとする（SIP サーバを用いる場合でも、シーケンスの本質は同じである。発呼側 UA から送信された SIP パケットは、最終的に着呼側 UA に到達する。両者の間に SIP サーバが介在しているが、そのことに変わりはないからだ）。

発呼側 UA から送信されたパケットが NAT ルータを通過すると、送信元 IP アドレスがグローバル IP アドレスに変換される。

しかし、SIP メッセージに記載された発信元 IP アドレスは、NAT ルータのアドレス変換の対象ではない。したがって、発呼側 UA のプライベート IP アドレスのまま、着呼側 UA に通知されてしまう。

通話セッションで用いる IP アドレスは、セッションの生成時に通知し合った発信元 IP アドレスである。したがって、着呼側 UA から見ると、通話セッションの相手の IP アドレスは、発呼側 UA のプライベート IP アドレスとなる。それゆえ、着呼側 UA から送信した RTP パケットは、宛先がプライベート IP アドレスなので、インターネットを経由して発呼側 UA に到達することができない。

よって、正解は、「アドレス変換対象外の SIP メッセージ内に送信者のプライベート IP アドレスが含まれている」となる。

(3)

解答例

S	I	P	メ	ッ	セ	ー	ジ	内	の	I	P	ア	ド	レ	ス	情	報	を	送	信	元	で	あ	る
V	o	I	P	-	G	W	の	グ	ロ	ー	バ	ル	ア	ド	レ	ス	に	書	き	換	え	る	。	

(49字)

本問は、下線④について、図 2 の電話接続シーケンス例の場合に、SBC が行うアドレス変換の内容を問うている。

下線④は、「IPT システムの概要」の第 5 段落、下線③のすぐ後にある。そこには、「インターネット網を経由して、SIP を使った通話を行う場合、企業内のプライベート IP アドレスの UA と外部とを接続するために、アドレス変換を行う必要がある。このときに、標準的な NAT 装置では、通話セッションが生成できないという問題が発生する。K 君によれば、④この問題への対応機能をもつ SBC があるということであった」と記述されている。

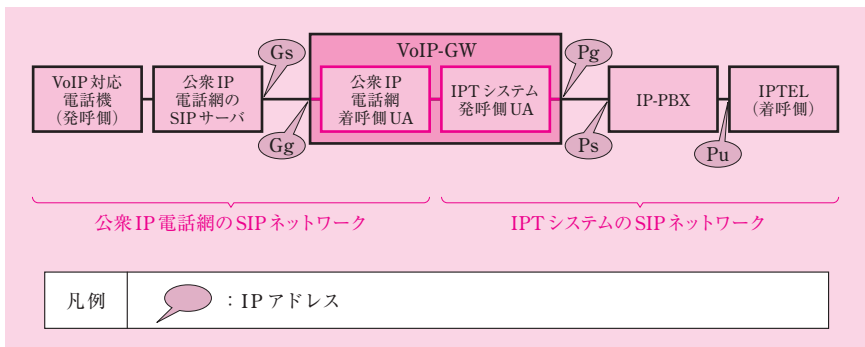
「この問題」とは、通話セッションが生成できないということである。その原因は、設問 2 (2) で解説したとおり、SIP メッセージ内の発信元 IP アドレスが変換されないためであった。したがって、SBC がこの問題に対応できるということは、SIP メッセージ内の発信元 IP アドレスを、適切なアドレスへ変換できることを意味している。本問で問われているのは、その具体的な変換の内容である。

SBC について、第 3 段落には、「VoIP-GW は、両方の SIP ネットワークに対して UA として振る舞う特殊な UA である B2BUA (Back-to-Back User Agent) になる。VoIP-GW は、SIP ネットワークの境界に存在してセッション生成を仲介するとともに RTP パケットの中継も行う Session Border Controller (以下、SBC という) と呼ばれる機能をもつ」と記述されている。したがって、本問の SBC とは、B2BUA である VoIP-GW を指していることが分かる。

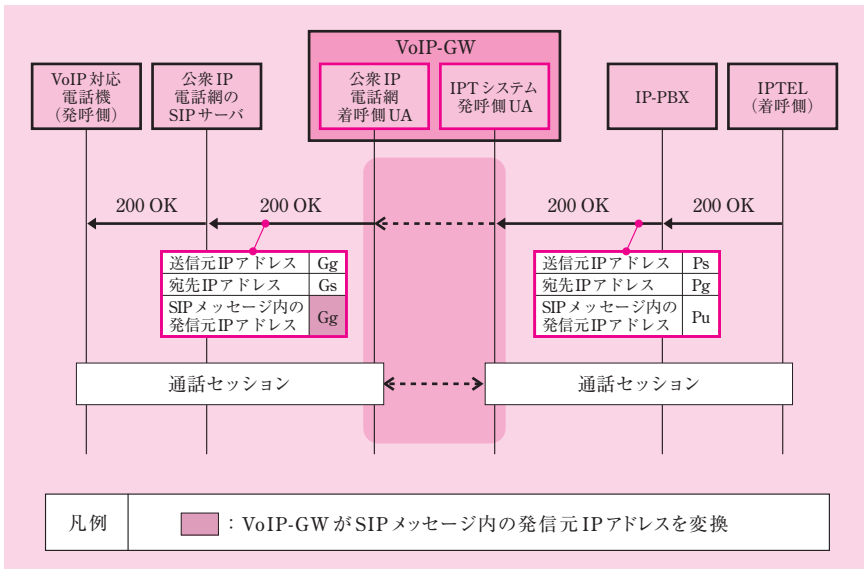
B2BUA は、設問 2 (1) で解説したとおり、二つの SIP ネットワークの境界に位置し、発呼側の SIP ネットワークから見ると着呼側 UA として振る舞い、着呼側の SIP ネットワークから見ると発呼側 UA として振る舞う。本問で問われている図 2 のネットワークにおいては、公衆 IP 電話網が発呼側であり、IPT システムが着呼側である。

本文の図 2、設問 2 (1) の解説中の図「本文の図 2 における VoIP-GW の役割」から分かるとおり、B2BUA は、通話セッションを中継している。これは、セッション生成時に、UA 間で発信元 IP アドレスの情報を適切に交換できたことを示している。すなわち、公衆 IP 電話網の側においては着呼側 UA として振る舞い、自分自身のグローバル IP アドレスを、200 OK レスポンスのメッセージ内で発呼側 UA (VoIP 対応電話機) に通知している。

VoIP-GW を経由した通信を、次の図に示す。構成図に IP アドレスを割り振っているので、これと対応させながらシーケンスを見ていただきたい。なお、この図では暫定応答は省略している。



図：VoIP-GW を経由した通信の構成図



図：VoIP-GW を経由した通信の動作シーケンス

VoIP-GW は、IPT システムの側から受け取った 200 OK レスポンスの SIP メッセージを、そのまま転送しているのではない。そこに記載された発信元 IP アドレスは、IPT システムの着呼側 UA (IPTEL) のアドレスなので、プライベート IP アドレスになっている。このまま転送するなら、設問 2 (2) で問われたとおり、通話セッションに失敗してしまう。そこで、200 OK レスポンスの SIP メッセージ内の発信元 IP アドレスを、自分自身のグローバル IP アドレスに変換する。このアドレスは、公衆 IP 電話網の側からは着呼側 UA のアドレスになっているので、通話セッションに成功する。

IPT システムにおいて、VoIP-GW は発呼側 UA として振る舞う。今度は、自分自身のプライベート IP アドレスを、INVITE リクエストのメッセージ内で着呼側 UA に通知している。詳しいシーケンスは省略する。

VoIP-GW が SIP メッセージの変換も行うことで、二つの SIP ネットワークにおいて、通話セッションを成立させている。この通話データを中継することで、公衆 IP 電話から IPTEL に電話をかけることができるわけだ。

さて、本問は、図 2 の電話接続シーケンス例における、SBC が行うアドレス変換の内容を問うていた。変換には、発呼側から着呼側に転送するときの書換えと、着呼側から発呼側に転送するときの書換えの 2 種類がある。字数制限があるので、どちらかを取り上げて解答する。

直前の設問 2 (2) は、下線③を出題しており、プライベート IP アドレスが NAT ルータで変換されないことを問うている。ここ設問 2 (3) は、下線③の直後にある下線④を出題しており、この問題に対応する SBC の機能を問うている。この文脈を考慮するなら、着呼側から発呼側への書換え、すなわち、公衆 IP 電話網の発呼側 UA に 200 OK レスポンスを転送するときに実施する、グローバル IP アドレスへの書換えを解答するのが適切である。

よって、正解は、「SIP メッセージ内の IP アドレス情報を送信元である VoIP-GW のグローバルアドレスに書き換える」となる。

●参考：SBC が実施する変換について

セッションを生成するとき、発呼側 UA と着呼側 UA の間で交換する情報は、通話セッションで用いる IP アドレスに加えて、リアルタイムデータを転送するプロトコル（つまり、ポート番号）もある。

したがって、SBC (Session Border Controller) が二つの SIP ネットワークの間で SIP メッセージを転送するときは、IP アドレスだけでなくポート番号も変換する。

■設問 3

設問 3 は、〔パッシブ方式による音声パケットの収集〕について出題している。

パッシブ方式とは、音声の通信経路にある L2SW にミラーポートを設定し、ミラーフレームをログの仮想 NIC で直接受ける方式を指している。

パッシブ方式については、〔パッシブ方式による音声パケットの収集〕の本文の中で、詳しい説明がなされている。ここでは、とりわけトラフィック経路に着目して、若干の補足を加えて解説しよう。音声パケットとそのミラーポート出力フレームの流れを理解することが、この設問を解く鍵となるからだ。

なお、解説を分かりやすくするため、ここでは利用企業 1 の音声トラフィックを主に取り上げる。

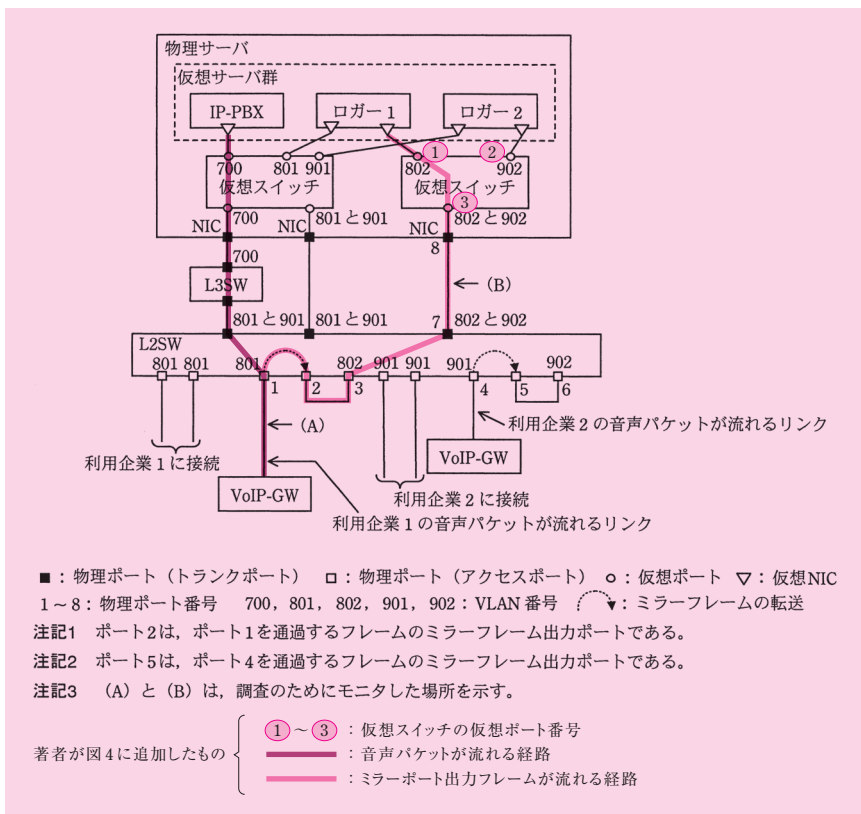
●パッシブ方式におけるパケットの流れ

VoIP-GW と IP-PBX の間を流れる音声トラフィックの経路上に、L2SW がある。この音声パケットのトラフィックは、双方向である。すなわち、IP-PBX を宛先とする音声パケットと、VoIP-GW を宛先とする音声パケットがある。

L2SW のポート 1 はミラーフレーム出力ポートに設定しており、ポート 1 を通過するフレームはすべてミラーリングされてポート 2 に転送される。ポート 2 とポート 3 をケーブル接続しているので、ミラーポート出力フレームはポート 3 から L2SW に

入って来る。このトラフィックは、片方向である。すなわち、すべてのミラーポート出力フレームは、ロガー 1 の仮想 NIC に取り込まなければならない。

このトラフィックを図示したのが、次の図である。



図：パッシブ方式におけるトラフィック経路（図4から作成）

ここで、ミラーポート出力フレームのトラフィックについて考察してみよう。

これは音声トラフィックをミラーリングしたものである。したがって、イーサネットフレームの宛先は、ロガー 1 の仮想 NIC ではない。具体的には、次に示すものになっている。

表：イーサネットフレームの宛先

イーサネットフレームの種類	宛先
IP-PBX 宛での音声パケットを上位層にもつイーサネットフレーム	L3SW ^(*)
VoIP-GW 宛での音声パケットを上位層にもつイーサネットフレーム	VoIP-GW

(*) IP-PBX は L3SW を経由して L2SW と接続している。したがって、宛先は L3SW となる。

先ほど、ミラーポート出力フレームのトラフィックは片方向であると述べた。このトラフィックを実現するために、L2SW、仮想スイッチ、ロガー 1 の仮想 NIC は、通常とは異なる動作が求められる。利用企業によって VLAN 及びポート番号が異なることに留意すると、次のようになる。

表：各機器の利用企業ごとの動作

機器	利用企業の種類 (VLAN)	動作
L2SW	利用企業 1 (802)	ポート 3 に入って来たフレームを、ポート 7 から送り出す
	利用企業 2 (902)	ポート 6 に入って来たフレームを、ポート 7 から送り出す
仮想スイッチ	利用企業 1 (802)	仮想ポート 3 に入って来たフレームを、仮想ポート 1 から送り出す
	利用企業 2 (902)	仮想ポート 3 に入って来たフレームを、仮想ポート 2 から送り出す
ロガーの仮想 NIC	利用企業 1, 2 共通	到達したフレームをすべて取り込む

注) 仮想ポートの番号は、図「パッシブ方式におけるトラフィック経路 (図 4 から作成)」による。

実を言うと、この仮想スイッチとロガーの仮想 NIC の動作について、設問 3 (1) で問われている。L2SW の動作について、設問 3 (2) で問われている。詳しくは、それぞれの小問で解説する。

ここまで理解できれば、設問 3 を解く準備は整った。それでは小問の解説に移ろう。

(1)

解答例

仮	想	ス	イ	ッ	チ	の	ポ	ー	ト	に	該	当	す	る	V	L	A	N	の	全	て	の	フ	レ	ー
ム	を	出	力	し	、	仮	想	N	I	C	側	で	そ	れ	ら	を	全	て	取	り	込	む	動	作	

(51 字)

本問は、下線⑤について、適切な動作の内容を問うている。

下線⑤は、[パッシブ方式による音声パケットの収集]の第6段落にある。そこには、「ミラーポート出力フレームを取り込むために、仮想スイッチに接続する⑤ロガーの仮想 NIC と仮想スイッチの接続ポート間で、適切な動作をさせる」と記述されている。

設問3の冒頭で解説したとおり、ミラーポート出力フレームのトラフィックは、片方向である。これを実現するために、仮想スイッチ、仮想 NIC とともに、通常とは異なる動作が求められている。

では、本問の求めに従い、それぞれの具体的な動作について、順番に考察してみよう。

●仮想スイッチ

第6段落には「接続する仮想サーバの MAC アドレスは仮想化のための仕組みで把握しているので、通過するフレームによる MAC アドレスの学習を行わない」とある。それゆえ、仮想スイッチは、仮想ポート1の先にはロガー1が存在すること、仮想ポート2の先にはロガー2が存在することを知っている。

仮想ポート3は、物理サーバのポート8に接続している。ポート8は、二つの VLAN に所属している。一つ目は、利用企業1のためのもので、VLAN 番号は802である。二つ目は、利用企業2のためのもので、VLAN 番号は902である。

仮想ポート3は二つの VLAN に所属しているので、図4の中で、「トランクポート」に設定されている。対向側の L2SW のポート7も同じくトランクポートに設定されており、同じ二つの VLAN に所属している。したがって、ポート7からフレームが出て行くとき、所属する VLAN 番号を格納した VLAN タグが挿入される。

このフレームが仮想スイッチの仮想ポート3から入って来ると、VLAN タグが除去され、その VLAN 番号が評価される。

なお、ここまでは通常のスイッチの動作と変わるところがない。

通常と異なるのは、VLAN 番号を評価した後の動作である。

設問3の冒頭で解説したが、ミラーポート出力フレームの宛先は、L3SW と VoIP-GW の2種類である。このフレームを、仮想サーバ（ロガー）に転送する必要がある。

VLAN 番号を評価した後、通常であれば、VLAN ごとに存在する MAC アドレステーブルに基づき、フレームを転送するはずだ。しかし、ミラーポート出力フレームの宛先である L3SW、VoIP-GW は、どちらも仮想スイッチには接続されていないので、MAC アドレステーブルには存在していない。それにもかかわらず、仮想スイッチは、該当する VLAN のフレームを、ロガーの収容ポートから送り出さなければならない。

すなわち、VLAN 番号を評価した後、その値が802であれば、仮想ポート1からフレームを送り出す。その値が902であれば、仮想ポート2から送り出す。

したがって、これが本問の求める解（仮想スイッチの動作に関する解）となる。

●ロガーの仮想 NIC

先ほど述べたとおり、ミラーポート出力フレームの宛先は、L3SW と VoIP-GW の 2 種類である。

通常の NIC は、自分を宛先としないユニキャストフレームを破棄する仕様になっている。しかし、本事例のロガーのように、ミラーポート出力フレームを取り込む必要がある場合、自分を宛先としないユニキャストフレームを受信するように動作させる必要がある。

このような NIC の動作を、プロミスキューモードという。

したがって、これが本問の求める解（仮想 NIC の動作に関する解）となる。

●解の導出

これまで解説した内容を整理する。

- 仮想スイッチは、入って来た全てのフレームを、VLAN に基づいて、該当する収容ポートから送り出す
- ロガーの仮想 NIC は、全てのフレームを取り込む

この内容を、指定字数に収まるようにまとめればよい。よって、正解は解答例に示したとおりとなる。

(2)

解答例

状態：流入するフレームの宛先 MAC アドレスが既にポート 3 側に存在するとして登録されている。(42 字)

対応策：MAC アドレス学習機能を抑止できる SW を使用し、通過するポート 3 で学習を抑止する。(41 字)

問題文は、「下線⑥について、MAC アドレステーブルがどのような状態になっていたことが原因だったと考えられるか。……また、T 君の示した対応策を、……述べよ」と記述されている。

下線⑥は、[パッシブ方式による音声パケットの収集] の第 9 段落にある。第 8～9 段落は、図 4 の構成で実験したとき、期待するフレームがロガーに転送されていない

という不具合について述べている。図 4 の (A) と (B) の位置で、サーバと L2SW 間のフレームをモニタして調べたところ、

- (A) の位置では、VoIP-GW が送受信したフレームを確認できた
- (B) の位置では、ミラーリングしたそれらのフレームを確認できなかった

という事実が判明した。

L2SW の MAC アドレステーブルがどのような状態であるかを調べたところ、原因が判明した。これを突き止めた T 君は、「⑥ L2SW のポート 3 に流入するフレームの送信元 MAC アドレスと宛先 MAC アドレスの組合せに着目して原因を説明し、対応策を示した」と記述されている。

本問は、この下線⑥について、二つのことを問うている。

一つ目は、「MAC アドレステーブルがどのような状態になっていたことが原因だったと考えられるか」ということである。二つ目は、「T 君の示した対応策」である。

それでは、一つずつ解いていこう。

● MAC アドレステーブルの状態

フレームのモニタ結果から明らかになった点がある。それは、VoIP-GW が送受信したフレームがポート 1 を通過しているにもかかわらず、ミラーリングしたフレームはポート 7 から送り出されていないことである。これより、問題の原因は、次の五つの候補に絞られる。

- ポート 1 からポート 2 にミラーフレームが転送されていない
- ポート 2 とポート 3 間のリンクが切断している
- ポート 2、ポート 3 が故障している
- ポート 3 から入って来たフレームが、ポート 7 に転送されない
- ポート 7 が故障している

上記の 1～3 番目が原因であったならば、802 番の VLAN の MAC アドレステーブルには、VoIP-GW が送受信したフレームが一切登録されていないはずである。しかし、下線⑥には「ポート 3 に流入するフレームの送信元 MAC アドレスと宛先 MAC アドレスの組合せに着目して原因を説明し (た)」とあるので、少なくとも、ポート 3 からフレームが入っていることが示されている。それゆえ、1～3 番目は候補から外す。

最後の 5 番目が原因であったならば、ポートの LED ランプの消灯などから原因を突

き止めるのが自然であるため、下線⑥の記述と合わない。それゆえ、5 番目も候補から外す。

消去法で考えると 4 番目となるわけだが、それでは、ポート 3 でフレームを受け取ったにもかかわらず、ポート 7 に転送しないのはなぜだろうか。そして、そのことと MAC アドレステーブルの状態とはどのような関係があるのだろうか。

下線⑥には「送信元 MAC アドレスと宛先 MAC アドレスの組合せに着目して」とあるので、ポート 3 から入って来るミラーポート出力フレームの、送信元と宛先に着目してみる。

設問 3 の冒頭で解説したとおり、このフレームは VoIP-GW が送受信した音声トラフィックであるため、フレームの宛先は、L3SW、VoIP-GW の 2 種類である。音声トラフィックは双方向なので、送信元も L3SW、VoIP-GW の 2 種類である。

ここで、レイヤ 2 スイッチのアドレス学習機能と転送機能を思い起こそう。

レイヤ 2 スイッチは、MAC フレームの受信を契機に、受信したポートの先に、送信元 MAC アドレスをもつノードが存在していることを学習する。このとき学習した内容（受信ポートと送信元 MAC アドレスの対応付け）を、MAC アドレステーブルに登録する。これがアドレス学習機能である。

レイヤ 2 スイッチは、MAC フレームを受信すると、宛先 MAC アドレスをもつノードがどのポートの先に存在しているかを MAC アドレステーブルから判定し、そのポートからフレームを送り出す。これが転送機能である。

図 4 の構成において、ポート 3 に入って来るミラーポート出力フレームは、送信元が L3SW 又は VoIP-GW である。したがって、アドレス学習機能により、ポート 3 の先にこれらノードが存在していることを学習し、MAC アドレステーブルにこれらを登録する。

MAC アドレステーブルがこの状態になっているときに、宛先が L3SW 又は VoIP-GW であるミラーポート出力フレームをポート 3 で受け取ることになる。MAC アドレステーブルから判定すると、送り出すポートはポート 3 となる^(*)。したがって、ミラーポート出力フレームをポート 7 に転送しないことが分かる。

(*) フレームが入って来たポートとフレームを送り出すポートが一致しているので、レイヤ 2 スイッチは、経路がループしていると誤って判断してしまう。このときの振舞いについては、ループ防止機能の仕様や設定により異なるため、いろいろと考えられるが、本文には記されていない。もちろん、本問を解く上では、「ミラーポート出力フレームをポート 7 に転送しない」ということが突き止められれば、それで十分である。

原因がはっきり分かったので、本問が問うている「MAC アドレステーブルがどのよ

うな状態になっていたことが原因だったと考えられるか」について、解を導くことができる。

MAC アドレステーブルは、「流入するフレームの宛先 MAC アドレスが既にポート 3 側に存在するとして登録されている」という状態になっている。それが原因でポート 7 には転送されなかったわけだ。よって、この状態を解答すればよいので、正解は解答例に示したとおりとなる。

●対応策

アドレス学習機能が動作している限り、ミラーポート出力フレームはポート 7 に転送されることはない。したがって、ポート 7 に転送するには、ミラーポート出力フレームのトラフィックが流れる VLAN で、アドレス学習機能を停止すればよい。

アドレス学習機能がなくなると、MAC アドレステーブルには、ポートと MAC アドレスの対応付けが登録されなくなる。この状態でフレームを受信すると、受信ポート以外のポートから一斉にフレームを送り出す。この動作をフラッドイングという。

図 4 の構成において、802 番の VLAN に所属するポートで、アドレス学習機能を停止したらどうなるだろうか。このとき、ポート 3 に入って来たフレームは、802 番の VLAN に所属する全てのポート（ポート 3 を除く）から送り出される。そのポートとは、ポート 7 である。したがって、この対応策によって、障害が取り除かれることが分かる。

よって、この対応策を解答すればよいので、正解は解答例に示したとおりとなる。

■設問 4

設問 4 は、〔アクティブ方式による音声パケットの収集〕について出題している。

アクティブ方式とは、録音機能をもつ端末を用意し、通話セッションをその端末を経由させる方式を指している。

アクティブ方式については、〔アクティブ方式による音声パケットの収集〕の本文の中で、詳しい説明がなされている。ここでは、とりわけセッションに着目して、若干の補足を加えて解説しよう。複数のセッションの役割を理解することが、この設問を解く鍵となるからだ。

●アクティブ方式におけるセッション

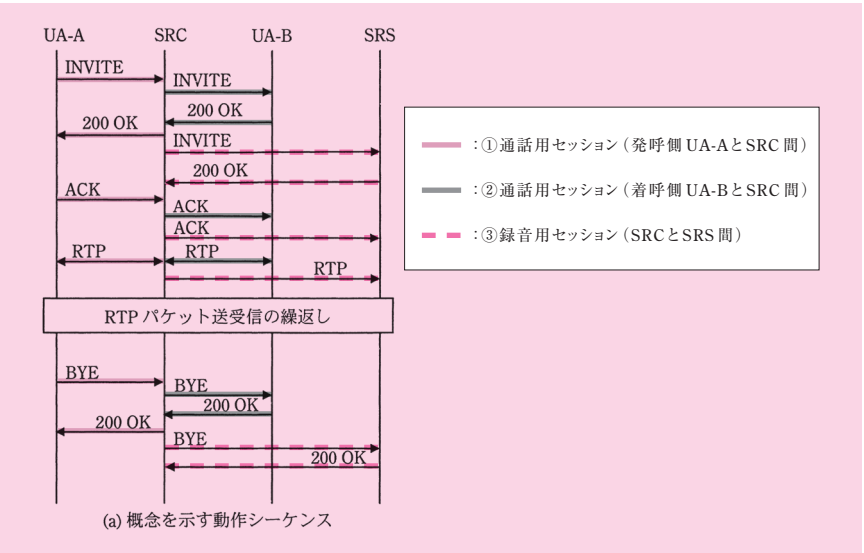
アクティブ方式については、第 2 段落と図 5 (a) に詳しい説明がなされている。第 2 段落には次のように記述されている。

アクティブ方式では、音声 packets を中継する機器上に、録音したい音声 packets をコピーして転送する機能を実装し、録音クライアント（以下、SRC という）とする。SRC は、音声 packets を受け取って録音する役割の録音サーバ（以下、SRS という）との間に SIP を用いて録音用セッションを生成し、コピーした音声 packets を、そのセッションを用いて転送する。また、音声 packets 以外に、音声 packets に関係した通話の属性情報も、通知できる。

図 5 (a) は、発呼側の UA-A と着呼側の UA-B との間の通話を収集する例を取り上げ、その動作シーケンスの概念を示した図である。この図では暫定応答は省略している。この図を見ると、セッションが 3 種類あることに着目できる。

表：セッションの種類

項番	セッションの種類	セッションの区間
①	通話用セッション	発呼側 UA-A と SRC 間
②	通話用セッション	着呼側 UA-B と SRC 間
③	録音用セッション	SRC と SRS 間



図：アクティブ方式の動作シーケンスとセッション（図 5 から作成）

・通話用セッション

まず、項番①と②の通話用セッションに着目しよう。

RTP の通信を行っているということは、通信のエンドポイントは UA であり、UA 間でセッションを生成したことを物語っている。要するに、SRC は UA として振る舞っていることになる。

表：通話用セッションにおける SRC の振舞い

項番	セッションの区間	SRC の振舞い
①	発呼側 UA-A と SRC 間	着呼側 UA
②	着呼側 UA-B と SRC 間	発呼側 UA

つまり、SRC は次のように振る舞っている。

- ①の通話セッションと、②の通話セッションに対して、UA として振る舞う
- 二つの通話セッションの境界に存在して、SIP メッセージと RTP パケットを中継している

第 4 段落の「図 5 (a) 中の SRC は、音声パケットの中継だけでなく、UA-A と UA-B 間の通話用セッションの生成にも関与している」という記述は、この SRC 振舞いを説明したものだ。

・録音用セッション

次に、項番③の録音用セッションに着目しよう。

ここでは、SRC から SRS 宛てに、コピーした音声パケットが転送される。

表：録音用セッションにおける SRC と SRS の振舞い

項番	セッションの区間	SRC の振舞い	SRS の振舞い
③	SRC と SRS 間	発呼側 UA	着呼側 UA

録音用セッションの音声トラフィックの流れは、片方向である。すなわち、送信元が SRC であり、宛先が SRS である。図 5 (a) では、RTP パケットの矢印の向きが、SRC から SRS へ向かっている（右方向の矢印）。

ここまで理解できれば、設問 4 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

音声バケットを中継しないから (14字)

本問は、下線⑦について、IP-PBX は選択できない理由を問うている。

下線⑦は、「アクティブ方式による音声バケットの収集」の第 5 段落にある。そこには、「図 5 (a) に示すシーケンスを参考に、⑦図 1 において SRC を実装する機器を選択し、図 5 (a) に対応した図 1 におけるシーケンスとして図 5 (b) を作成した」と記述されている。

第 2 段落に「音声バケットを中継する機器上に、録音したい音声バケットをコピーして転送する機能を実装し、録音クライアント (SRC) とする」とある。設問 4 の冒頭で解説したとおり、SRC は、UA として振る舞う。

しかし、IP-PBX は SIP サーバであるため、音声バケットを中継しない。したがって、IP-PBX は SRC を実装する機器にすることができない。

よって、正解は、「音声バケットを中継しないから」となる。

(2)

解答例

e : VoIP-GW

f : IP-PBX

本問は、図 5 中の e、f に入れる適切な機器名を問うている。空欄 e, f は、図 5 (b) の動作シーケンス中の機器である。これは、第 5 段落にあるとおり、図 5 (a) に示すシーケンスを参考に作成されたものである。空欄には、図 1 の機器が当てはまる。

まず、図 5 の (a) と (b) を見比べて、どのように機器が対応しているかを考察してみる。すぐに分かるのは次の 3 点である。

表：図 5 の (a) と (b) における機器の対応

(a)	(b)	共通点
SRS	ロガー	音声パケットを収集する
UA-A	VoIP 対応電話機	発呼側 UA は、INVITE リクエストを最初に送信する
UA-B	IPTTEL	着呼側 UA は、INVITE リクエストを最後に受信する

それを踏まえて、二つの空欄を順番に解いていこう。

e

(a) の SRC と (b) の e とを見比べると、両者には共通点がある。

表：(a) の SRC と (b) の e

(a) の SRC	(b) の e
<u>SRS</u> との間でセッションを生成している	<u>ロガー</u> との間でセッションを生成している

したがって、SRC は e に対応していることが分かる。ここから、更に三つのセッションの対応も分かる。

表：セッションの対応

項番	セッションの種類	セッションの区間	
		(a)	(b)
①	通話用セッション	発呼側 <u>UA-A</u> と SRC 間	<u>VoIP 対応電話機</u> と e の間
②	通話用セッション	着呼側 <u>UA-B</u> と SRC 間	<u>IPTTEL</u> と e の間
③	録音用セッション	SRC と <u>SRS</u> 間	e と <u>ロガー</u> の間

設問 4 の冒頭で解説したとおり、SRC は、①と②の二つのセッションに対して、UA として振る舞う。二つのセッションの境界に存在して、SIP メッセージと RTP パケット を中継している。

図 1 でこの役割を担っている機器は何であろうか。結論から言うと、それは VoIP-GW である。この点について、[IPT システムの概要] の第 3 段落には、次のように記述されている。

IP-PBX 配下の IPTEL を識別するための 050 電話番号は、公衆 IP 電話網の通信事業者から割り当てられる。通信事業者の公衆 IP 電話網の中にも SIP サーバが存在するので、VoIP-GW は、両方の SIP ネットワークに対して UA として振る舞う特殊な UA である B2BUA (Back-to-Back User Agent) になる。また、VoIP-GW は、SIP ネットワークの境界に存在してセッション生成を仲介するとともに RTP パケットの中継も行う Session Border Controller (以下、SBC という) と呼ばれる機能をもつ。

このように見比べると、SRC の振舞いと、VoIP-GW の B2BUA としての振舞いとが、一致している。したがって、(a) の SRC に対応する (b) の機器は、VoIP-GW である。よって、空欄 e には「VoIP-GW」が該当する。

f

(b) の f は、VoIP-GW (空欄 e) と IPTEL の間にある。それゆえ、空欄 f に該当する機器は、IPT システムに存在することが分かる。その点を踏まえて、図 2「SIP による電話接続シーケンス例」を見てみよう。

図 5 (b) の f と図 2 の IP-PBX とを見比べると、両者には共通点がある。

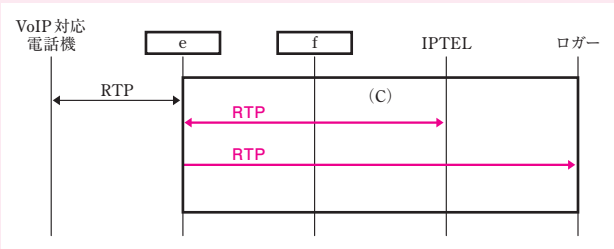
表：図 5 (b) の f と図 2 の IP-PBX

図 5 (b) の f	図 2 の IP-PBX
VoIP-GW (空欄 e) から INVITE リクエストを受信し、これを IPTEL に転送している	VoIP-GW から INVITE リクエストを受信し、これを IPTEL に転送している
IPTEL から 200 OK レスポンスを受信し、これを VoIP-GW (空欄 e) に転送している	IPTEL から 200 OK レスポンスを受信し、これを VoIP-GW に転送している
それより後の SIP メッセージ (ACK リクエスト, BYE リクエスト, 200 OK) については、 <u>中継に関わっていない</u>	それより後の SIP メッセージ (ACK リクエスト, BYE リクエスト, 200 OK) については、 <u>中継に関わっていない</u>

よって、空欄 f には「IP-PBX」が該当する。

(3)

解答例



本問は、図 5 中の (C) に処理シーケンスを追加することを求めている。

(C) は、図 5 (b) の中にある。これは図 5 (a) のどの部分に相当するだろうか。

(a) と (b) を見比べれば判明する。

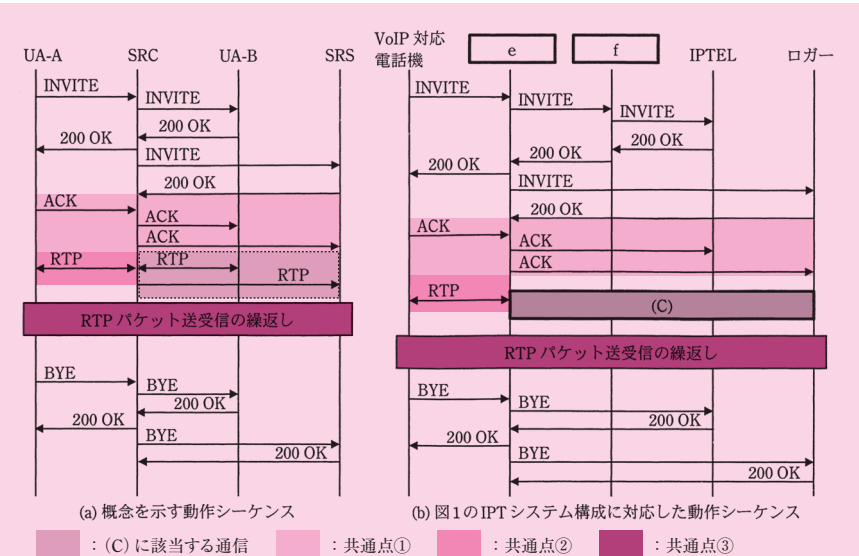


図 5 (a) の「(C) に該当する通信」と、図 5 (b) の「(C)」には、次の共通点がある。

共通点①	ACK リクエストのやり取りの直後に位置する
共通点②	VoIP 対応電話機と VoIP-GW 間の RTP パケットの送受信と同じタイミングに位置する
共通点③	「RTP パケット送受信の繰返し」と書かれた帯の直前に位置する

図 5 (a) 中の (C) に該当する部分には, 2 個のパケットのやり取りが記されている。

- SRC と UA-B 間の RTP パケットの送受信 (両方向の矢印)
- SRC から SRS 宛ての RTP パケットの送信 (右方向の矢印)

これを (b) の機器に当てはめるなら,

- VoIP-GW (空欄 e) と IPTEL 間の RTP パケットの送受信 (両方向の矢印)
- VoIP-GW (空欄 e) から ロガー宛ての RTP パケットの送信 (右方向の矢印)

となる。これが, (C) に該当するやり取りとなる。

よって, 正解は解答例に示したとおりとなる。解答に際しては, 矢印の向きにも留意しよう。

(4)

解答例

V	o	I	P	-	G	W	に	は	呼	制	御	に	関	す	r	S	I	P	セ	ッ	シ	ョ	ン	情
報	も	送	ら	れ	て	く	る	か	ら	(35字)														

問題文は, 「図 1 の構成で, 図 5 (b) の方式を使用した場合, 呼情報も録音用セッションを介して取得できる。その理由を……述べよ」と記述されている。

設問 4 (2) の空欄 e で解説したとおり, 図 1 の構成で図 5 (b) の方式を使用した場合, SRC に該当する機器は, VoIP-GW となる。

SRC は, VoIP-GW の B2BUA 機能をもつ。VoIP-GW は, 公衆 IP 電話網の SIP ネットワークと, IPT システムの SIP ネットワークの境界に位置し, 両者の間で SIP パケットと RTP パケットを中継している。

したがって, SIP パケットを中継する以上, SRC は呼制御に関する情報を把握できる立場にある。それゆえ, SRC と SRS 間に生成した録音用セッションを用い, この情報を SRS に送信して記録できるはずだ。

よって, 正解は, 「VoIP-GW には呼制御に関する SIP セッション情報も送られてくるから」となる。

(5)

解答例

ミラーポート出力フレームの転送用設定が不要だから (24字)

本問は、「パッシブ方式に比べてアクティブ方式の方が有利な点」を問うている。

本来、物事を比較するときは、何かの基準に照らして優劣を判断する。例えば、機能性であったり、信頼性であったり、経済性であったりする。

とはいえ、問題文には、判断する基準が明示されていない。

比較しようと思えば様々な観点からできそうに思われるが、まずは、本文の記述を注意深く見てみよう。解を導くのに必要な前提条件が欠けているように感じたなら、「出題者が用意しているヒントを見落としているはずだ」と考えてみよう（付録 PDF 「午後問題の解答テクニック」の「0.3.6 問題を解く②:応用テクニック 5.条件を読み落としたり、自分勝手に条件を加えたりしない」を参照されたい）。

本文や設問にヒントがないときに限り、一般的な知識から解を導くようにする。

そのようにして本文を読み返すと、二つの方式を比較している記述を見出すことができる。

〔パッシブ方式による音声パケットの収集〕の第 10 段落には、パッシブ方式について、「苦労して音声パケットの収集ができるようにはなったものの、音声パケットを収集するためのネットワークを構成する作業が大変だった」と記述されている。

対案として浮上したのが、アクティブ方式である。その点について、〔アクティブ方式による音声パケットの収集〕の第 1 段落には、「ミラーポート出力を使わない音声パケットの収集方式について調査した。その結果、アクティブ方式と呼ぶ収集方式があることが分かった」とある。最終的には、このアクティブ方式が採用された。

したがって、この文脈を考慮するなら、本事例における判断基準は、「ネットワークを構成する作業が大変であるか否か」ということだ。作業が複雑であるなら、構築やテストに関わる作業負荷が高まるし、設定ミスに起因する不具合が起きるかもしれない（現に、設問 3 (2) で取り上げられたように、不具合を目の当たりにしている）。今後、IPT システムのサービスが事業化して利用企業が増えていくことを考慮するなら、導入容易性は重要であると言える。

そこで、この観点から比較して解を導くことができる。

これまでの内容をまとめると、アクティブ方式はパッシブ方式よりも「ネットワークを構成する作業が容易である」と言うことができる。ただし、この表現のまま解答

してはならない。これでは「パッシブ方式による音声パケットの収集」の第 10 段落を転記しただけに過ぎず、しかも、どのような点で容易であるのかが漠然としているからだ。解答に際しては、できるだけ具体的に述べるように心掛けたい（付録 PDF「午後問題の解答テクニック」の「0.3.5 問題を解く①：重要テクニック」の「2. 本文より一步掘り下げて、できるだけ具体的に解答する」を参照されたい）。

先ほど、「アクティブ方式による音声パケットの収集」の第 1 段落の記述を確認した。そこには、「ミラーポート出力を使わない音声パケットの収集方式について調査した」とあった。この記述から、パッシブ方式で特に懸念されていたのは、ミラーポート出力の転送設定に関わる作業であることが分かる。

この考えに沿って具体化してみると、「ミラーポート出力フレームの転送用設定が不要だから」などと作文することができる。このようにして、解答例に示したような正解に至る。

●参考：内線通話の録音方法

本文のアクティブ方式の説明は、社外の VoIP 対応電話機と IPTEL との通話を対象にしている。それでは、利用企業の内線通話、すなわち、IPTEL 同士の通話を録音する場合、どのようにすればよいだろうか。本文では触れられていないので、以下に述べることは、あくまで推測の域を出ないことをお断りしておく。

この考察に当たって、まず、内線通話の通信経路を確認しておこう。

SIP でセッションを生成するときの通信経路は、次のとおりである。

発呼側 IPTEL ⇔ IP-PBX ⇔ 着呼側 IPTEL

RTP で通信するときとセッションを切断するときの通信経路は、次のとおりである。

発呼側 IPTEL ⇔ 着呼側 IPTEL

したがって、内線通話は VoIP-GW を経由しない。

さて、アクティブ方式では、SRC は、音声パケットを中継する機器上に実装しなければならない。設問 4 (2) で解説したとおり、本事例ではその機器として VoIP-GW を選択している。

これを踏まえると、内線通話を録音するときも、同様に VoIP-GW を使用してもよいだろう。ただし、このときの内線通話の経路は、VoIP-GW を経由するように変更しなければならない。

以上、参考までに、内線電話の録音方法について考察してみた。これは、本文中で一切言及されていない話である。したがって、設問の解を導くときは、内線通話の録音を考慮する必要はない。

■設問 5 (1)

解答例

ア：IP01

イ：Any

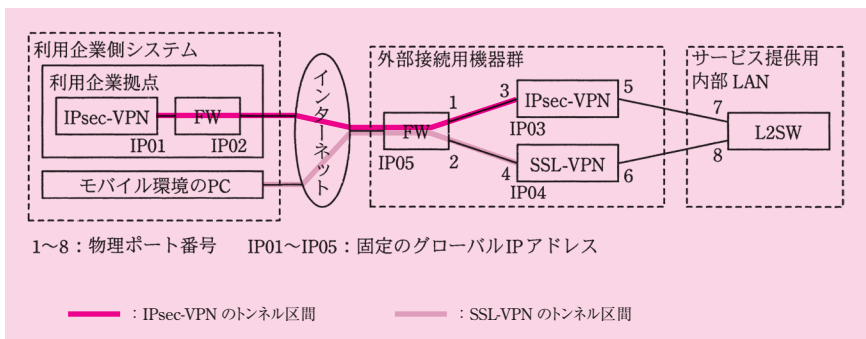
ウ：Any

エ：443

本問は、図 6 に示した外部接続用機器の構成における、A 社側の FW のフィルタリングルールの設定を問うている。

結論から言うと、図 6 の構成図では、2 種類の VPN のトンネルが形成される。

一つ目は、IPsec-VPN のトンネルである。二つ目は、SSL-VPN のトンネルである。



図：外部接続用機器の構成図における、二つの VPN のトンネル区間（図 6 から作成）

それでは、この結論がどのように導かれるのかを解説しよう。その上で、解を導くことにする。

● IPsec-VPN のトンネル

本文中には、IPsec-VPN に言及している文は見当たらない。手掛かりとなるのは、図 1 と図 6 である。図 6 は、図 1 の中から外部接続用機器の構成に関わる部分を抜粋し、そこに IP アドレスやポート番号を割り振ったものである。

図 1 及び図 6 の利用企業側システムには、利用企業拠点と呼ばれる LAN がある。図 1 を見ると、ここに IPTTEL が設置されている。〔サービス用 IPT システムの構成〕の第 2 段落を見ると、「(利用企業の) 内部ネットワークは、……プライベート IP アドレスを使用している」と述べられている。

IPTTEL は、A 社センタの IP-PBX との間で SIP 通信を行う。IP-PBX はサービス提供用内部 LAN にある。図 6 を見ると、内部 LAN には固定のグローバル IP アドレスは割り振られない。それゆえ、IP-PBX はプライベート IP アドレスをもつことが分かる。

プライベート IP アドレスが割り当てられた二つの LAN の間で、インターネットを経由して通信を行うためには、VPN が必要となる。この VPN に求められる条件は、

- 特定のアプリケーション層プロトコルに依存せずに、カプセル化できる。具体的に言うと、SIP パケット、RTP パケットをカプセル化できる
- 通信経路の一部だけをトンネル化できる。具体的に言うと、IPTTEL と IP-PBX 間の通信経路のうち、グローバル IP アドレスをもつ区間を対象にしてトンネル化できる

である。

VPN の観点から、改めて図 1 を見てみよう。すると、利用企業拠点と A 社センタには、それぞれ IPsec-VPN 装置が設置されていることに着目できる。したがって、拠点間で、IPsec 通信が行われていることが分かる。

先ほど VPN に求められる条件を考慮したが、IPsec-VPN を使用すれば全て満たすことができる。

一つ目については、IPsec ではアプリケーション層プロトコルに依存せずに IP パケットをカプセル化できるからである。

二つ目については、IPsec のトンネルモードで満たすことができる。トンネルモードでは、両側の LAN の各々に VPN 装置を設置し、VPN 装置にグローバル IP アドレスを割り当てる。形成されるトンネルの区間は、これら VPN 装置の間となる。本事例では、利用企業拠点の IPsec-VPN 装置と、A 社センタの IPsec-VPN 装置の間である。

こうして、前述したとおり、IPsec-VPN のトンネルが形成されるとの結論が導かれた。

なお、IPsec について、詳しくは本書の第 8 章「8.4.5 IPsec」を参照されたい。

● SSL-VPN のトンネル

図 1 及び図 6 の A 社センタ内の外部接続用機器群を見ると、ここに SSL-VPN 装置が設置されている。

SSL-VPN について、〔外部接続用機器群の検討〕の第 1 段落には、「モバイル環境の PC は、A 社センタへ接続するために HTTPS を使用する」と記述されている。それゆえ、モバイル環境の PC とこの SSL-VPN 装置間で、SSL 通信を行うことが分かる。

更に、第 3 段落には、SSL-VPN 装置で PC の利用者認証を行っていること、そして、認証された PC は「新たな仮想 NIC を生成し、レイヤ 2 のトンネルを通して、サービス提供用内部 LAN との通信が可能になる」と記述されている。

したがって、モバイル環境の利用者から見ると、PC はサービス提供用内部 LAN に接続しており、その状態で業務用の通信を行っている。モバイル環境の PC と SSL-VPN 装置間で確立される SSL セッションは、業務用の通信をインターネット経由で実現するための、VPN 用トンネルの役割を果たしているわけだ。

こうして、前述したとおり、SSL-VPN のトンネルが形成されるとの結論が導かれた。

なお、この SSL-VPN 通信については、設問 5 (2) で取り上げられているので、詳しくはそこで解説する。

●表 1 に記載されているフィルタリングルール

第 2 段落には「FW のポート 1 とポート 2 のアウトバウンドでは、表 1 に示すフィルタリングルール（許可条件）を適用する予定である」とある。それゆえ、表 1 に記載されているのは、インターネットから内部 LAN 宛でのトラフィックを許可するルールである。

●解の導出 (,)

FW 物理ポート 1 は、IPsec-VPN 装置に接続している。「IPsec-VPN のトンネル」で解説したとおり、IPsec-VPN のトンネルは、利用企業拠点の IPsec-VPN 装置と、A 社センタの IPsec-VPN 装置の間に形成される。FW 物理ポート 1 は、このトンネル区間の経路上にある。したがって、このポートでは、IPsec の通信を許可するルールが必要となる。

IPsec では、トンネルのことを正式には SA (Security Association) と呼ぶ。SA には、VPN 通信用のトンネルである IPsec SA と、これを生成するためのトンネルである IKE SA の 2 種類がある。二つの SA は異なるプロトコルを使用しているため、それぞれの通信を許可する必要がある。

IPsec SA は、IP の上位層プロトコルが ESP 又は AH である。インターネット経由の

VPN 通信は暗号化するのが通例であり、暗号化機能をもつ ESP が通常用いられる。ESP、AH は、ヘッダにポート番号をもたない。

IKE SA は、IP の上位層プロトコルが UDP であり、宛先ポート番号と送信元ポート番号はどちらも 500 番である。

それらを踏まえて、表 1 の FW 物理ポート 1 のフィルタリングルールを見てみよう。

空欄アは、送信元 IP アドレスの設定である。IPsec-VPN のトンネルは、利用企業拠点の IPsec-VPN 装置と、A 社センタの IPsec-VPN 装置の間に形成される。表 1 はアウトバウンドのルールであるから、このトンネル区間を通過する IPsec-VPN のパケットは、送信元が利用企業拠点の VPN 装置となる。

よって、空欄アの正解は「IP01」となる。

空欄ウは、ESP を許可するルールにおける、ポート番号の設定である。ESP はポート番号をもたないため、FW でチェックしない。表 1 の注記に「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」とあるので、ポート番号に「any」を設定すればよい。

よって、空欄ウの正解は「any」となる。

IPsec-VPNのトンネルは、利用企業拠点のIPsec-VPN装置と、A社センタのIPsec-VPN装置の間に形成される

ESPを許可するルール

FW 物理ポート	送信元 IP アドレス	宛先 IP アドレス	ポート番号	プロトコル番号
1	ア	IP03	500	17 (UDP)
			ウ	50 (ESP)

ESP : Encapsulating Security Payload

注記 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。

図：FW 物理ポート 1 のフィルタリングルール

●解の導出 (イ , エ)

FW 物理ポート 2 は、SSL-VPN 装置に接続している。「SSL-VPN のトンネル」で解説したとおり、SSL-VPN のトンネルは、モバイル環境の PC と、A 社センタの SSL-VPN 装置の間に形成される。FW 物理ポート 2 は、このトンネル区間の経路上にある。したがって、このポートでは、SSL の通信を許可するルールが必要となる。

それらを踏まえて、表 1 の FW 物理ポート 2 のフィルタリングルールを見てみよう。

空欄イは、送信元 IP アドレスの設定である。モバイル環境の PC は、インターネット

トにアクセスする際、プロバイダから IP アドレスが払い出される。その IP アドレスは固定ではない。

図 6 を見ると、IP01 ～ IP05 が固定のグローバル IP アドレスであることが明記された上で、モバイル環境の PC には IP01 ～ IP05 のどれも割り当てられていない。それゆえ、モバイル PC は固定のグローバル IP アドレスをもっていないことが分かる。

よって、空欄イの正解は「any」となる。

空欄エは、ポート番号の設定である。許可する通信は SSL なので、宛先ポート番号は「443」となる。通常、FW のフィルタリングルールでは、宛先ポート番号を設定する。それゆえ、表 1 のポート番号は宛先であると考えられる。

よって、空欄エの正解は「443」となる。

SSL-VPNのトンネルは、モバイル環境のPCと、A社センタのSSL-VPN装置の間に形成される

SSLを許可するルール

FW 物理ポート	送信元 IP アドレス	宛先 IP アドレス	ポート番号	プロトコル番号
2	イ	IP04	エ	any

注記 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。

図：FW 物理ポート 2 のフィルタリングルール

(2)

解答例

サービス提供用内部 LAN のネットワークに属する IP アドレス
(29 字)

本問は、下線⑧において、生成された仮想 NIC に対してどのような IP アドレスが付与される必要があるかを問うている。

下線⑧は、〔外部接続用機器群の検討〕の第 3 段落にある。そこには、「SSL-VPN 装置では、モバイル環境の PC からのアクセスに対し、トークンを利用した利用者認証を行っている。認証された PC は、⑧新たな仮想 NIC を生成し、レイヤ 2 のトンネルを通して、サービス提供用内部 LAN との通信が可能になる」と記述されている。

本問を解くには、この通信方式の仕組みについて理解する必要がある。そこで、ま

ずはその点について解説する。それを踏まえて、解を導こう。

なお、この通信方式は、ベンダ独自のものである。本文には特に名称が与えられていないので、本解説では「レイヤ 2 方式の SSL-VPN 通信」と呼ぶことにする。

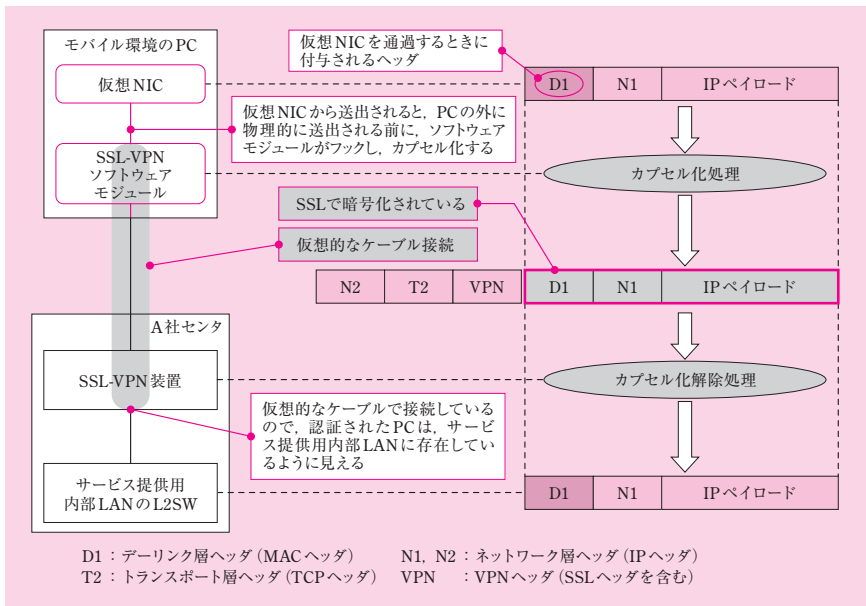
●レイヤ 2 方式の SSL-VPN 通信の仕組み

第 3 段落に「レイヤ 2 のトンネル」とあるので、イーサネットフレームがカプセル化されていることが分かる。トンネルは、仮想的な通信路である。その通信路の中を、イーサネットフレームが通ると考えればよい。つまり、「レイヤ 2 のトンネル」は、仮想的なケーブル接続の役割を果たしているわけだ。

「新たな仮想 NIC を生成し、レイヤ 2 のトンネルを通して、サービス提供用内部 LAN との通信が可能になる」ということは、要するに、仮想 NIC とサービス提供用内部 LAN が、仮想的なケーブルで接続されていることを意味している。

仮想的なケーブルで接続しているので、認証された PC は、サービス提供用内部 LAN に存在しているように見える。

この様子を示したのが次の図である。



図：レイヤ 2 方式の SSL-VPN 通信

まず、PC がサービス提供用内部 LAN のサーバ宛てに IP パケットを送信する。

PC には仮想 NIC が生成されているので、この IP パケットは、仮想 NIC を通過して送出される。仮想 NIC を通過するときに、MAC ヘッダの D1 が付与される。

このフレームが PC の外に物理的に送出される前に、PC 内部にある SSL-VPN ソフトウェアモジュールが、このフレームをフックする。そして、これを SSL でカプセル化する。

SSL でカプセル化するとき、VPN ヘッダが付与される。この VPN ヘッダには、SSL ヘッダが含まれている。なお、レイヤ 2 方式の SSL-VPN 通信はベンダ独自の技術であるため、独自のヘッダ情報を付与しているかもしれない。その点を踏まえ、VPN ヘッダと表記している。なお、本問を解く上では、VPN ヘッダの詳細を考慮に入れる必要はない。

SSL でカプセル化したのち、TCP ヘッダの T2、IP ヘッダの N2 が付与される。T2 の宛先ポート番号は、443 番である。N2 の送信元 IP アドレスは、プロバイダが付与したグローバル IP アドレスである。N2 の宛先 IP アドレスは、IP04（A 社センタの SSL-VPN 装置）である。この後、PC の外に物理的に送出される。すなわち、インターネットに出て行く。

A 社センタの SSL-VPN 装置は、このパケットを受信すると、カプセル化を解除する。そして、中身のフレーム（PC の仮想 NIC から送出された時点のフレーム）を取り出し、これをサービス提供用内部 LAN 側のポートから送出する。

この図では内部 LAN の L2SW まで記しているが、この L2SW の先に内部 LAN のサーバが存在している。L2SW の先に L3SW があって、その向こう側にサーバが存在していてもよい。

PC と内部 LAN のサーバ間でやり取りされるパケットは、IP ヘッダの N1 をもつ。

N1 の宛先 IP アドレスは、内部 LAN のサーバのアドレスである。

N1 の送信元 IP アドレスは、PC の IP アドレスである。この IP アドレスは、仮想 NIC を生成したとき、SSL-VPN 装置から払い出されたものである。これは、内部 LAN と同じネットワークに属するプライベート IP アドレスである。

●解の導出

レイヤ 2 方式の SSL-VPN 通信について分かったところで、いよいよ解を導こう。

本問で問われているのは、仮想 NIC に付与される IP アドレスであった。

先ほど解説したとおり、仮想 NIC とサービス提供用内部 LAN は、あたかも仮想的なケーブルで接続されている。認証された PC は、サービス提供用内部 LAN に存在しているように見える。

したがって、仮想 NIC に付与された IP アドレスは、「サービス提供用内部 LAN の

ネットワークに属する IP アドレス」である。

よって、これが正解となる。

(3)

解答例

ネ	ッ	ト	ワ	ー	ク	機	器	ご	と	に	異	な	る	ハ	ー	ド	ウ	ェ	ア	を	用	意	せ	ず
に	済	む	か	ら	(30字)																			

本問は、下線⑨において、コスト面での利点が得られると考えた理由を問うている。

下線⑨は、〔外部接続用機器群の検討〕の第6段落にある。第5～6段落は、ネットワーク機器の仮想化による利点を幾つか取り上げている。その文脈で下線⑨の文章がある。そこには、「保守・運用管理上、FW や VPN 装置などの⑨ネットワーク機器が仮想化されている場合、ハードウェア障害に備えた冗長化を実現する上で、コスト面での利点もある」と記述されている。

ここで、ネットワーク機器の仮想化とは、第5段落にあるとおり、「ネットワーク機器の機能が仮想サーバで動作するソフトウェアとして提供されること」を意味している。

下線⑨には「冗長化を実現する上で、コスト面での利点」があると述べられている。したがって、本問を解くには、物理的にハードウェアを冗長化する場合と、ネットワーク機器を仮想化してから冗長化する場合をコスト面から比較すればよい。仮想化する方に利点があると言える理由が見つかれば、それが本問の解となる。

本問は一般的な知識から解を導く。

図6「外部接続用機器の構成図」の外部接続用機器群のハードウェアを例に取り上げてみる。

図6の構成には、FW、IPsec-VPN 装置、SSL-VPN 装置の3台の機器がある。これを仮想化する場合、「外部接続用機器群」の点線枠が、そのまま1台のサーバに置き換わる。FW、IPsec-VPN 装置、SSL-VPN 装置は、いずれもソフトウェアとして提供される。

では、ここで二つの冗長構成を比較してみよう。

一つ目は、図6のハードウェア機器を単純に冗長化する方法を採る。二つ目は、ネットワークを仮想化した上で、サーバを冗長化する方法を採る。なお、ここで言う「冗長化」とは、二重化を意味するものとする。つまり、ハードウェア機器の台数を2倍

にし、主系と待機系の 2 系統にする。

一つ目の方法では、3 台のハードウェア機器を 2 倍にするので、合計 6 台の機器が必要になる。一方、二つ目の方法では、2 台のサーバが必要になる。

したがって、物理的にハードウェアを冗長化すると 6 台となるが、いったん仮想化してから冗長化すると 2 台で済むわけだ。

利用企業 1 社だけでなく、何社もまとめて仮想化すると、台数の開きは更に大きくなる。

このように考えると、台数に着目してコストを比較するなら、仮想化してから冗長化した方が安くなると言える。

よって、正解は解答例に示したとおりとなる。

もちろん、現実的に言うと、台数だけでコストを比較できるほど、そう単純な話ではない。ネットワークの仮想化は、コスト面で有利な点もあれば、不利な点もあることを留意すべきである。

あくまで一般論であるが、ネットワークの仮想化がコスト面で有利になる点を挙げてみよう。まず、電源系統やケーブル接続部など共有化できるコンポーネントがあるので、仮想化対象の機器の台数が増えるに従って、コストメリットが大きくなる。更には、その種の共有化により、電気代などのランニングコストが安くなる可能性も出てくる。

一方で、ネットワーク仮想化がコスト面で不利になる点も挙げてみよう。まず、仮想化には相応のハードウェアスペックが求められるので、サーバ 1 台の単価が高くなる。更には、仮想化ソフトウェアのライセンス費用が別途必要となることも見逃せない。

ネットワークの仮想化には、コスト面のメリットだけでなく、「新たな利用者への機能提供の迅速化、構成変更への柔軟性」など、考慮に値する着眼点が様々ある。これらを総合的に比較衡量した上で、導入を決定すべきである。