

平成 28 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

電子メールシステムにおいて、不正な電子メールが送信されることを防いだり、受信した電子メールが不正に送信された電子メールではないことを確認する手段を提供したりすることは、不正のない電子メール利用のために必須となっている。また、このような電子メールの安全性・信頼性を上げるための技術は、ネットワーク技術者を応用したものとなっており、ネットワーク技術者として押さえておくべき技術の一つと考えられる。

本問では、企業での安全な電子メールシステム活用を目指したシステム構築を通じて、ネットワーク技術者として必要となる能力を問う。

## 採点講評

問 1 では、電子メールシステムを用いたサポート業務を第三者に業務委託する場面を題材として、OP25B (ISP ネットワークにおける不正メール配信防止のための対策) 実施配下環境でのメール構築や、SPF による電子メールの信頼性向上の技術について出題した。全体として、正答率は高かった。

設問 2 は、よくある電子メール要件に応じたネットワーク構成に関連する問題であるが、(4) の正答率が低かった。電子メール送信のための 2 種類のポートの使い分けや、その意味については必須の技術と思われるので、SMTP-AUTH と併せて、基本をしっかりと理解してほしい。また、(5) は STARTTLS 方式で TLS 暗号化通信を行う場合のポート番号を問う問題であるが、STARTTLS 方式ではない TLS 暗号化通信の場合のポート番号を答えてしまう誤答が散見された。STARTTLS 方式の解説は本文中に書いてあるので、よく読めば正答を導けるはずである。

設問 3 は、メールサーバの認証を行う SPF に関して出題したが、正答率は低かった。特に(1)の正答率が低かった。SMTP プロトコルにおける基本的なシーケンスの理解は、メールシステム構築時の動作確認を行う上での必要事項なので、是非とも理解をしておいてほしい。

設問	解答例・解答の要点		備考
設問 1	ア	MX	
	イ	MSV3	
	ウ	MSV2	
	エ	SMTP-AUTH	
設問 2	(1)	不正メールの踏み台にされてしまうリスク	
	(2)	ルータ 4	
	(3)	オ TCP	
		カ a.b.0.0/20	
		キ 25	
	(4)	サブミッションポート	
	(5)	① ・ 110	
		② ・ 587	

(表は次ページに続く)

設問	解答例・解答の要点		備考
設問 3	(1)	MAIL FROM	
	(2)	送信元メールサーバの IP アドレス	

本問は、電子メールシステムの不正利用を防止する技術として、SMTP-AUTH、OP25B（Outbound Port 25 Blocking）、SPF 等を取り上げている。それらの技術の仕組み、及び、それらの技術を活用した安全な電子メールシステムの構築について問うている。

### ●本問の全体像

事例に登場する A 社は、一般消費者向けの自社製品のサポート業務を B 社に委託する方針である。このサポート業務での購入者とのやり取りに、電子メールを活用することを検討している。

サポート業務の電子メールシステムを構築するに当たって、次の設定が必要となる。

#### [1] 電子メールの転送

B 社がサポート業務を行うときは、B 社 PC で A 社のメールアドレスを用いる。このメールの送受信には A 社のメールサーバを使用する。

A 社と B 社は、それぞれ異なる ISP を利用してインターネットに接続している。A 社の ISP は P 社であり、B 社のそれは Q 社である。

それぞれの ISP は、OP25B のポリシーでメールシステムを運用している。そのため、サポート業務の運用を実現するための設定が必要となる。

#### [2] メール送受信の暗号化

サポート業務のために B 社の PC でメールを送受信する際、STARTTLS 方式で通信を暗号化する。そのため、A 社側のファイアウォール（以下、FW という）の設定変更が必要となる。

#### [3] SPF の導入

A 社ドメインを偽る迷惑メールの防止、及び、ドメイン偽装メールの受信拒否を実現するため、A 社は SPF を導入することにした。そのため、A 社の DNS サーバとメールサーバの設定が必要となる。

これら 3 点を踏まえて本問の構成を概観すると、次のように整理できる。

表：本問の構成

見出し	主な内容	主に対応する出題箇所	
		設問	小問
なし（序文）	現在（委託前）のメール転送	1	ア, イ
ネットワークの概要			
A 社のメール転送の概要			
サポート業務委託時の メール運用の検討	[1] 電子メールの転送	2	(2), (3), (4)
	[2] メール送受信の暗号化	2	(5)
SPF の導入	[3] SPF の導入	3	(1), (2)

それでは、設問の解説に移ろう。

## ■設問 1

### 解答例

ア：MX  
イ：MSV3  
ウ：MSV2  
エ：SMTP-AUTH

ア, イ

空欄ア、イを含む文章は、[A 社のメール転送の概要] の第 1 段落、1 番目の箇条書き「・外部からの A 社へのメール」の中にある。そこには、「外部のメールサーバは、DNS3 に設定された資源レコードのうち、ア レコードの情報に従って、A 社ドメイン宛てのメールをイ に転送する」と記述されている。

第 1 段落の冒頭に「現在、A 社のメール転送は次のとおり行われている」と記述されていることから、ここで問われているメール転送は、B 社にサポート業務を委託する前のものである。

このときのネットワーク構成は、[ネットワークの概要] の中で説明されている。

A 社のメールサーバについて、6 番目の箇条書きで、「A 社は、社内利用のための MSV3 を社内に立ち上げ、自社ドメイン（a-sha.co.jp）でメールシステムを運用している」と記述されている。したがって、外部のメールサーバが A 社ドメイン宛てにメールを送信する際、転送先となる A 社のメールサーバは、MSV3 である。

A 社の権威 DNS サーバについて、7 番目の箇条書きで、「DNS3 は、a-sha.co.jp ドメインの権威 DNS サーバである」と記述されている。したがって、外部のメールサーバが A 社ドメイン宛てにメールを送信する際、転送先メールサーバのホスト名を取得するために、DNS3 の MX レコードを問い合わせる。

よって、空欄アに該当する字句は「MX」となり、空欄イに該当する字句は「MSV3」となる。

## ウ

空欄ウを含む文章は、「サポート業務委託時のメール運用の検討」の第 1 段落、Y さんの 1 番目の発言の中にある。

そこには、「各社員の PC にインストールしたメールクライアントから、ウに SMTPS (SMTP over TLS) でメールを送信しています。受信については、同じサーバに POP3S (POP3 over TLS) でアクセスしています」と記述されている。

会話の場面は、第 1 段落の冒頭にあるとおり、サポート業務委託時のメールシステムの実現方法について検討しているところである。

Y さんは B 社のエンジニアで、A 社のエンジニアである X さんと話している。空欄ウを含むこの発言は、X さんから受けた、「B 社ではどのようにメールの送受信をしていますか」という質問に対する回答である。つまり、ここで問われているのは、B 社にサポート業務を委託する前のものだ。

このときのネットワーク構成は、「ネットワークの概要」の中で説明されている。

B 社のメールサーバについて、9 番目の箇条書きで、「B 社は、社内にメールサーバをもたず、Q 社のメールサービスを利用している」と記述されている。Q 社は、B 社が利用している ISP である（序文第 1 段落）。

Q 社のメールサーバについて、2 番目の箇条書きで、「Q 社は、……MSV2 を……用いて、顧客にメールサービスを提供している」と記述されている。したがって、B 社のメールサーバは MSV2 であることが分かる。

よって、空欄ウに該当する字句は「MSV2」となる。

## エ

空欄エを含む文章は、「サポート業務委託時のメール運用の検討」の第 3 段落、2 番目の箇条書きの中にある。

そこには、「SMTP プロトコル上でユーザ認証を行う方式であるエ」と記述されている。

SMTP のユーザ認証は、認証に成功したユーザからのみメール送信を受け付けるた

め、メールサーバが実施する。ユーザ認証の方式として、SMTP-AUTH と POP before SMTP の 2 種類がある。

### ● SMTP-AUTH

一つ目の方式は、SMTP-AUTH である。SMTP-AUTH は、SMTP プロトコル上でユーザ認証を行い、認証に成功したユーザにのみメール送信を許可する仕組みになっている。

メールクライアントがメールサーバに接続すると、メール送信に先立ってユーザ認証が行われる。メールクライアントは、メールソフトに登録されたユーザ ID とパスワードをメールサーバに送信し、これを用いてメールサーバがユーザ認証を行う。

なお、メールクライアントがメールサーバにパスワードを送信するとき、通信経路上でパスワードが盗聴されるのを防ぐため、チャレンジレスポンス方式を用いるのが一般的である。すなわち、サーバから送付されたチャレンジコードとパスワードとを組み合わせてハッシュ化したものを送信する。

### ● POP before SMTP

二つ目の方式は、POP before SMTP である。POP はユーザ認証の仕組みをもっているため、POP before SMTP は、この認証結果に基づいてメール送信を許可する仕組みになっている。つまり、SMTP プロトコル上でユーザ認証を行っているわけではない。

POP before SMTP の仕組みを略述すると、次のようになっている。

メールクライアントは、メール送信に先立ち、POP を用いてメールサーバからメールを受信する。メールサーバは、この受信に成功（POP の認証に成功）したメールクライアントの IP アドレスを記録しておき、同 IP アドレスを送信元とするメール送信を許可するのである。

なお、メールクライアントの IP アドレスは変化し得るため、メール送信を許可する IP アドレスを記録する期間は数分程度に制限するのが一般的である。

### ● 解の導出

以上を踏まえ、空欄エが指すユーザ認証方式に関する、本文の記述を確認してみよう。空欄エのすぐ前に、「SMTP プロトコル上でユーザ認証を行う」と記されているので、この認証方式は SMTP-AUTH であることが分かる。

よって、空欄エに該当する字句は「SMTP-AUTH」となる。

## ■設問 2

### (1)

#### 解答例

不正メールの踏み台にされてしまうリスク (19字)

問題文は、「本文中の下線①について、この設定がないことによって生じる情報セキュリティ上のリスクを……答えよ」と記述されている。

下線①は、[サポート業務委託時のメール運用の検討] の第 1 段落、X さんの 2 番目の発言の中にある。そこには、「①たとえ B 社の PC から MSV3 へ SMTP によるメール送信ができたとしても、MSV3 は、a-sha.co.jp ドメイン以外への宛先へは、そのメールを転送しない設定になっています」と記述されている。

MSV3 は、設問 1 の空欄イで解説したとおり、A 社のメールサーバである。B 社 PC がインターネット経由で MSV3 に接続するとき、メールサーバから見た端末の IP アドレスは、自社以外 (A 社以外) のグローバル IP アドレスとなる。

それゆえ、下線①の前半部分にある「B 社の PC から MSV3 へ SMTP によるメール送信」という記述は、「自社以外のグローバル IP アドレスをもつ端末からメールサーバへ SMTP によるメール送信」と読み替えることができる。

このような外部端末がメールサーバに接続したとき、自社以外のドメインを宛先とするメールの送信を許容するなら、どのような問題が生じるだろうか。

この外部端末を操作する差出人が、迷惑メールを大量に送り付ける意図をもった第三者であったならば、このメールサーバを踏み台にして、メールを不正に送り付けることが可能となってしまう。

このような事態を未然に防ぐため、下線①の後半部分にあるとおり MSV3 に設定が施されている。すなわち、外部端末から MSV3 へメールの送信が行われたとしても、「a-sha.co.jp ドメイン以外への宛先へは、そのメールを転送しない設定になっている」。A 社は、不正メールの踏み台となるような脆弱な状態を「リスク」と考え、それに付け込まれて問題が具現化することがないように設定することで、リスク対策を講じているわけだ。

したがって、下線①の設定がないことによって生じる「情報セキュリティ上のリスク」とは、不正メールの踏み台にされることだと結論できる。よって、正解は解答例に示したとおりとなる。

## (2)

## 解答例

## ルータ 4

問題文は、「本文中の下線②のルータ名を答えよ」と記述されている。

下線②は、「サポート業務委託時のメール運用の検討」の第2段落にある。そこには、「B 社 PC から MSV3 に向けた SMTP によるメール送信が不可能となっているのは、②図 1 中のあるルータにおいて、表 1 に示す OP25B のためのアクセスリストが設定されているからである」と記述されている。

本問の解を導くには、OP25B を理解しておく必要がある。そこで、この技術について概要をまず解説する。それを踏まえて、解を導こう。

## ● OP25B (Outbound Port 25 Blocking)

OP25B について、「ネットワークの概要」の3番目の箇条書きで、次のように説明している。

- ・ (ISP) は、迷惑メールの送信を防止する対策として、OP25B のポリシーでメールシステムを運用している。具体的には、自社が動的に割り当てた IP アドレスのホストから、自社のサービスネットワーク外のホストへの宛先ポート番号 25 の SMTP 通信を許可しないという運用上のルールを適用している。

ここに述べられているとおり、OP25B は、メールを送信するときに ISP 指定のメールサーバを用いるよう規制を加える仕組みである。この規制対象となるクライアントは、ISP から IP アドレスの動的な割当てを受けるものである。それは主に、個人や小規模な組織の利用者のホストだ。

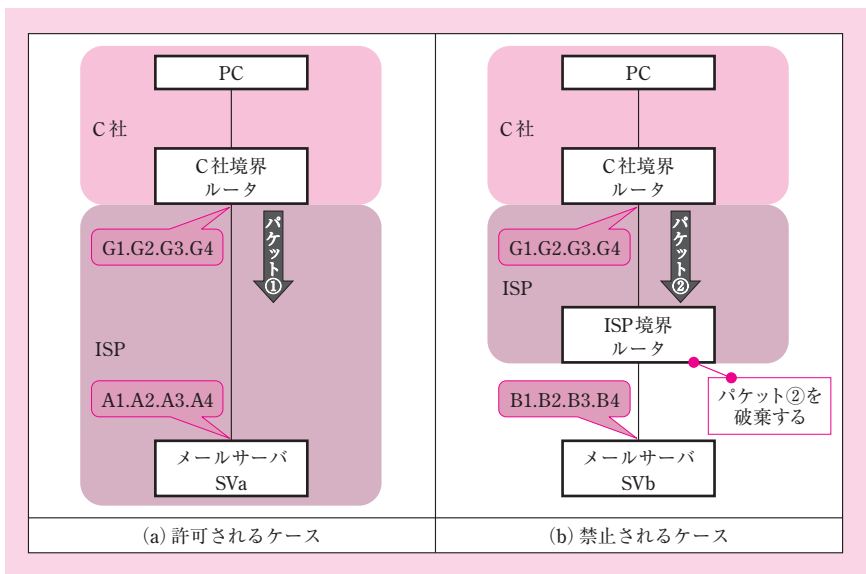
この OP25B を実現するため、ISP とインターネットとの境界に位置するルータ（又は FW）で、ISP は SMTP 通信をフィルタリングしている。これまでの解説から明らかとなっており、次に示す二つの条件に合致するパケットは OP25B のポリシーに反するため、この境界ルータで破棄される。

- [1] ISP からクライアントに割り当てられるグローバル IP アドレスが、動的なものである。

[2] ISP 指定外のメールサーバと TCP の 25 番ポートでコネクションを確立し、同サーバを用いてメールを送信する。

これが迷惑メール送信を防止する対策となる理由は、多くの迷惑メール（ウイルスに感染した端末から送信されたメールを含む）が、ISP 指定のメールサーバを経由せずに送信されているからだ。この対策を実施することで、この種の迷惑メールを撲滅できる。

次の図は、ISP が実施する OP25B によって、パケット通信が許可されるケース（a）と禁止されるケース（b）とを比較している。



図：ISP が実施する OP25B において、パケット通信が許可されるケース(a)、禁止されるケース(b)

図中の C 社は、ISP の利用者である。C 社 PC は、SMTP 通信を行うことを意図し、メールサーバとの間で TCP コネクションを確立する SYN パケットを送信している。

C 社は、ISP からグローバル IP アドレスを動的に割り当てられて、インターネットにアクセスする。

図の左側（a）は、パケット通信が許可されるケースである。このメールサーバ SVa は、プロバイダの内側に存在し、プロバイダが指定したメールサーバである。このケースでは、SYN パケットは SVa に到達する。



図の右側 (b) は、パケット通信が禁止されるケースである。このメールサーバ SVb は、プロバイダの外側に存在し、プロバイダが指定していないメールサーバである。このケースでは、SYN パケットは ISP の境界ルータで破棄され、SVb には到達しない。

図中のパケット①、②は、宛先ポート番号が 25 (SMTP) の SYN パケットである。これに IP アドレスを具体的に当てはめてみよう。

C 社が ISP から動的に割り当てられるグローバル IP アドレスを G1.G2.G3.G4 とする。これは C 社境界ルータに割り当てられ、同ルータからインターネットに出ていく際、NAPT によって送信元 IP アドレスとなる。

パケット通信が許可されるケース (a) において、メールサーバ SVa のグローバル IP アドレスを A1.A2.A3.A4 とする。C 社境界ルータからサーバ SVa に転送されるパケット①は、送信元 IP アドレスが G1.G2.G3.G4 となり、宛先 IP アドレスが A1.A2.A3.A4 となっている。

パケット通信が禁止されるケース (b) において、メールサーバ SVb のグローバル IP アドレスを B1.B2.B3.B4 とする。C 社境界ルータからサーバ SVb に転送されるパケット②は、送信元 IP アドレスが G1.G2.G3.G4 となり、宛先 IP アドレスが B1.B2.B3.B4 となっている。

表：前図のパケットを比較 (IP アドレス、宛先ポート番号等)

項目	(a) 許可されるケース	(b) 禁止されるケース
パケット	パケット①	パケット②
送信元 IP アドレス	G1.G2.G3.G4	G1.G2.G3.G4
宛先 IP アドレス	A1.A2.A3.A4	B1.B2.B3.B4
宛先ポート番号	25	同左
パケットの内容	TCP の SYN パケット (コネクション確立要求)	

この図では、前述の OP25B の規制対象となる条件 [1] をどちらも満たしている。両者の違いは、条件 [2] の宛先 IP アドレスだけだ。禁止されるケース (b) のパケット②は、宛先が ISP 指定外のメールサーバであるため ISP 境界ルータで破棄される。

### ●解の導出

B 社の ISP である Q 社は、[ネットワークの概要] の 3 番目の箇条書きに記述されているとおり、「OP25B のポリシーでメールシステムを運用している」。

したがって、B 社 PC が外部にメールを送信するとき、次に示す二つの条件を満たすならば、OP25B のポリシーに反してしまう。

- [1] Q 社から B 社に割り当てられるグローバル IP アドレスが、動的なものである。
- [2] B 社 PC が、Q 社指定外のメールサーバと TCP の 25 番ポートでコネクションを確立し、同サーバを用いてメールを送信する。

条件 [1] について、8 番目の箇条書きで、「B 社は、Q 社の動的 IP アドレス割当てブロック (a.b.0.0/20) から割当てを受けたグローバル IP ドレスを、ルータ 6 の NAPT に使用することで Q 社のサービスネットワークに接続している」と記述されている。それゆえ、条件 [1] を満たしている。

条件 [2] について、下線②を含む文には、「B 社 PC から MSV3 に向けた SMTP によるメール送信」と記されている。A 社の ISP は P 社なので、A 社のメールサーバ MSV3 は、Q 社から見ると外部に位置している。それゆえ、このメール送信は、条件 [2] を満たしている。

したがって、B 社 PC をメールクライアントとし、A 社 MSV3 をメールサーバとする SMTP 通信は、Q 社の OP25B のポリシーに反していることが分かる。この通信は、Q 社とインターネットの境界に位置するルータで遮断されてしまう。

ここで問われているのは、図 1 中のどのルータがこれに該当するか、である。図 1 を見ると、それは「ルータ 4」である。

よって、正解は「ルータ 4」となる。

### (3)

#### 解答例

オ：TCP  
カ：a.b.0.0/20  
キ：25

本問は、表 1「OP25B のためのアクセスリスト」中の空欄オ～キに入る字句を問うている。

表 1 は、[サポート業務委託時のメール運用の検討] の第 2 段落にある。これは、設問 2 (2) で問われた Q 社のルータ 4 に登録された、OP25B のためのアクセスリストである。

空欄オ～キはいずれも、OP25B のポリシーにより通信を禁止する動作のエントリに含

まれており、空欄オがプロトコル（TCP/UDP/IP の区別）、空欄カが送信元 IP アドレス、空欄キが宛先ポート番号となっている。

設問2(2)の「● OP25B」で解説したとおり、OP25Bによって破棄されるパケットは、送信元 IP アドレスが動的 IP アドレスであり、宛先 IP アドレスが ISP 指定のメールサーバではない SMTP パケットである。

したがって、プロトコルの種類（空欄オ）は、「TCP」となる。送信元 IP アドレス（空欄カ）は、Q 社の動的 IP アドレス割当てブロックである「a.b.0.0/20」となる。宛先ポート番号（空欄キ）は、SMTP 通信の「25」となる。

よって、正解は解答例に示したとおりとなる。

## (4)

### 解答例

#### サブミッションポート

本問は、下線③のポート番号の名称を問うている。

下線③は、〔サポート業務委託時のメール運用の検討〕の第3段落、2番目の箇条書きの中にある。そこには、「MSV3は、SMTPプロトコル上でユーザ認証を行う方式であるSMTP-AUTHを導入し、③TCPの587番ポートで接続を受け付ける」（空欄エを補填）と記述されている。

第3段落の冒頭に、「次の方式でB社のPCからサポート業務メールが送受信できることが確認された」と記述されている。つまり、OP25Bの規制を受けているにもかかわらず、B社PCがA社MSV3を用いてメールを送受信する方式が確認されたわけだ。

第3段落の箇条書きは、これを実現する方式として「MSV3は……TCPの587番ポートで接続を受け付ける」と述べている。ここで問われているのは、このポート番号の名称である。

結論から言うと、その答えは「サブミッションポート」(Submission port)である。

本問の解を導くには、サブミッションポートを理解しておく必要がある。そこで、この技術について概要を解説する。それを踏まえて、解を導こう。

#### ● OP25B のサブミッションポート

ISPがOP25Bを導入することにより、ISPにとっては、自ISP内の動的IPアドレスを送信元とする迷惑メールを防止するというメリットがもたらされる。OP25Bを採用

する ISP が増えることにより、社会全体として迷惑メールの削減に寄与できる。

とはいえ、個人や小規模な組織など、動的な IP アドレスの割当てを受ける利用者にとっては、メールを送信できなくなるケースが生じ得る。例えば、次に示す条件に合致するときに、これに該当する。

- [1] 他 ISP の利用者が、外出先でインターネットにアクセスするため、自 ISP の拠点に PC を接続する。この拠点は、自 ISP から動的 IP アドレスを割り当てられている。
- [2] 同利用者が、同拠点で、他 ISP のメールサーバ（利用者から見て、常時使用しているメールサーバ）と TCP の 25 番ポートでコネクションを確立し、同サーバを用いてメールを送信する。

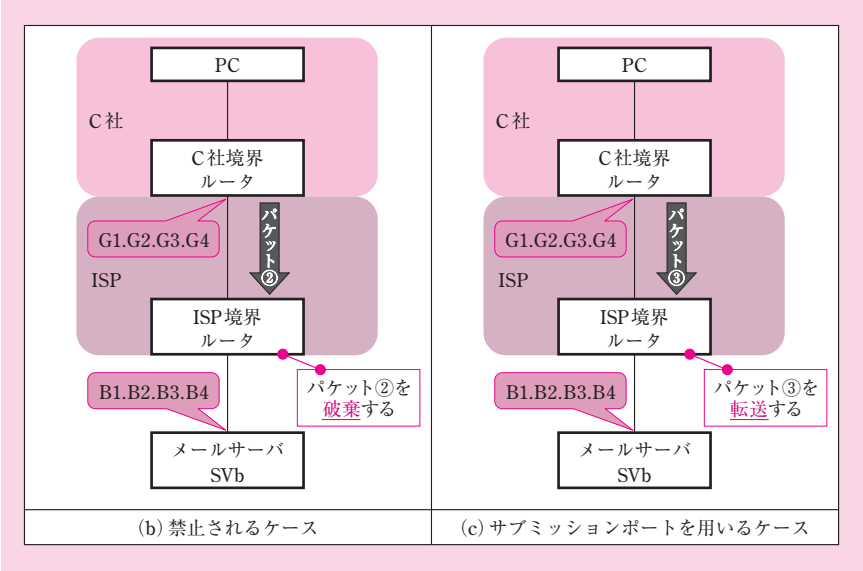
「自 ISP の拠点」が、個人や小規模な組織のものであるならば、動的 IP アドレスの割当てを受けるのが一般的なので、条件 [1] に合致してしまう。この拠点で、利用者がいつもどおり SMTP によるメール送信を行うと、条件 [2] に合致してしまう。この拠点は、利用者の仕事先であったり宿泊先であったりするかもしれないが、こういった外出先でメールを送信できないのは大変不便である。

この問題を解消するため、OP25B を採用している ISP は、TCP の 587 番ポート（サブミッションポート）を用いたメール送信を、OP25B の規制から外している。

他 ISP の利用者は、常時使用しているメールサーバ（他 ISP のメールサーバ）を用いてメールを送信したいときは、同サーバとサブミッションポートで TCP コネクションを確立すればよいわけだ。

設問 2 (2) の解説の中で、ISP が実施する OP25B によって、パケット通信が禁止されるケース (b) を図に示した。このケースにおいて、PC がメールサーバに対してコネクションを確立する宛先ポート番号を、サブミッションポートに変更すれば、コネクション確立に成功してメール送信を行うことができる。

比較のために、このサブミッションポートを用いるケース (c) を、先のケース (b) と一緒に示してみる。両者のネットワーク構成に変化は見られない。異なっているのは、宛先ポート番号だけであることに留意しよう。



図：ISPが実施するOP25Bにおいて、パケット通信が禁止されるケース(b)、サブミッションポートを用いるケース (c)

表：前図のパケットを比較（IP アドレス、宛先ポート番号等）

項目	(b) 禁止されるケース	(c) サブミッションポートを用いるケース
パケット	パケット②	パケット③
送信元 IP アドレス	G1.G2.G3.G4	G1.G2.G3.G4
宛先 IP アドレス	B1.B2.B3.B4	B1.B2.B3.B4
宛先ポート番号	25	587
パケットの内容	TCP の SYN パケット (コネクション確立要求)	TCP の SYN パケット (コネクション確立要求)

なお、サブミッションポートで接続を受けるメールサーバは、通常、ユーザ認証を行う。なぜなら、この設定を行わないならば、このメールサーバを踏み台にして、迷惑メールを不正に送り付けることが可能となってしまうからだ。つまり、設問 2（1）で解説したのと同様の問題が生じてしまう。

一般的には、このユーザ認証の方式として SMTP-AUTH が採用されている。

### ●解の導出

先ほど解説したとおり、TCP の 587 番ポートに接続すれば、OP25B の規制を受けることなく、他 ISP のメールサーバを用いることができる。

TCP の 587 番ポートの名称は、「サブミッションポート」(Submission port)である。本問が問うているのはこの名称であるから、これが求める解となる。

設問 2 (2) で解説したとおり、B 社の PC が A 社の MSV3 を用いてメール送信を行うとき、Q 社が実施している OP25B の規制を受けてしまう。その理由は、次に示す二つの条件を満たすからであった。

[1] Q 社から B 社に割り当てられるグローバル IP アドレスが、動的なものである。

[2] B 社 PC が、Q 社指定外のメールサーバと TCP の 25 番ポートでコネクションを確立し、同サーバを用いてメールを送信する。

しかし、A 社の MSV3 に対して、TCP の 587 番ポートでコネクションを確立するならば、条件 [2] を満たさないため OP25B の規制を受けなくなる。こうして、同サーバを用いてメールを送信することができるわけだ。

なお、MSV3 がサブミッションポートで接続を受け付けるように設定したことに伴い、二つの設定変更も同時に行っていることに着目できる。

一つ目は、2 番目の箇条書きに記述されているとおり、SMTP-AUTH (空欄エ) を用いたユーザ認証を行うように設定している。これは、踏み台対策のために必要なものである。

二つ目は、3 番目の箇条書きに記述されているとおり、このユーザ認証に成功したとき「A 社ドメイン以外の宛先への転送」を許可するように設定している。これは、B 社 PC からサポート業務メールを送信するために必要なものである。

## (5)

### 解答例

① 110

② 587

問題文は、「本文中の下線④について、2 種類の通信の宛先ポート番号を、それぞれ

答えよ」と記述されている。

下線④は、〔サポート業務委託時のメール運用の検討〕の第3段落、7番目の箇条書きの中にある。解を導くための手掛かりが、すぐ前の6番目の箇条書きに記述されている。少々長いが、一緒に確認してみよう。

- ・メール送受信の通信の暗号化は、STARTTLS 方式（接続時に平文で通信を開始して、途中で暗号化通信に切り替える方式）を採用し、メールクライアントからの STARTTLS コマンドに応じて TLS 暗号化を開始するよう、MSV3 を設定変更する。
- ・④外部から DMZ への 2 種類の通信を許可するために、FW を設定変更する。

この第3段落は、B社PCがA社MSV3を用いてメールを送受信する方式を説明している。したがって、メール送受信を行うメールクライアントは、B社PCである。

このメール送受信を実現するために、A社のFWを設定変更する必要性が生じている。その点について、下線④は「外部からDMZへの2種類の通信を許可する」と述べている。MSV3はDMZ上に設置されているので、この許可する通信とは、送信元がB社PCであり、宛先がMSV3である。もっとも、B社PCにはQ社から動的IPアドレスが割り当てられているため、FWの設定上は「外部」として扱われる。

暗号化について、6番目の箇条書きで「接続時に平文で通信を開始して、途中で暗号化通信に切り替える方式」を採用していると述べられている。したがって、メールの送信、受信のいずれにおいても、接続時は平文のプロトコルを用い、途中から暗号化プロトコルのTLSを用いていることが分かる。

### ●メール送信

2番目の箇条書きの下線③にあるとおり、メールを送信するときは、TCPの587ポートで接続する。ポート番号が異なるものの、通信の中身は通常のSMTPと同じである。すなわち、平文でやり取りされている。

このメール送信は、B社にサポート業務を委託するために新たに設定するものである。したがって、この通信を許可するためにFWの設定変更が必要となる。

### ●メール受信

4番目の箇条書きの中で、「受信については、POP3をTLSで暗号化して用いる」と記述されている。6番目の箇条書きにある「STARTTLS方式」の説明と照らし合わせるなら、メールを受信するために接続するときはPOP3を用い、途中からTLSを用い

て暗号化することが分かる。

この POP3 によるメール受信は、B 社にサポート業務を委託するために新たに設定するものであろうか。サポート業務を委託する前のメール転送については、「A 社のメール転送の概要」の記述から確認できる。「・外部からの A 社へのメール」を見ると、MSV3 に対して POP3 でメールを受信しているのは、「A 社内 PC」のみである。

したがって、A 社の外部である B 社 PC から、MSV3 に対して POP3 でメールを受信する通信は、サポート業務を委託するために新たに設定するものであることが分かる。したがって、この通信を許可するために FW の設定変更が必要となる。

### ●解の導出

本問が問うているのは、FW で新たに許可する宛先ポート番号である。

メール送信については、外部から 587 番ポートを宛先とする通信を許可する必要がある。よって、一つ目の解は、「587」となる。

メール受信については、外部から POP3 通信を許可する必要がある。POP3 のポート番号は「110」なので、これが二つ目の解となる。

### ● TLS の許可について

STARTTLS 方式を用いているため、メール送受信のやり取りは、途中から TLS に切り替わる。この TLS (443 番ポート) を、FW の設定で許可しておく必要はないのだろうか。

もしも、アプリケーション層を解析して動的にポートを開閉する機能を、FW が有しているならば、明示的に TLS を許可する必要がない。STARTTLS のやり取りに追随して、TLS の通信を動的に許可するからだ。

もっとも、このような機能を FW が有していることについて、本文は明確に述べていない。それゆえ、判断に迷った受験者がいたかもしれない。

## ■設問 3

### (1)

#### 解答例

MAIL FROM

本問は、「本文中の下線⑤について、送信元ドメインが得られる SMTP プロトコル



のコマンド」を問うている。

下線⑤は、[SPF の導入] の第 1 段落、2 番目の箇条書きの (1) にある。そこには、  
「⑤ “SMTP 通信中にやり取りされる送信元ドメイン名” を得る」と記述されている。

これは、一般的な知識から解を導くことができる。

一般的に言って、SMTP 通信は、拡張 SMTP と呼ばれる仕様に従って行われる。これは主に次のステップからなる。

なお、次に述べる「接続元」と「接続先」は、メールの転送経路上のホスト間に張られた TCP コネクションの両端を指している。この TCP コネクションの終端は、転送経路上にあるメール中継サーバであってもよいことに留意しよう。

### 1. 接続元から接続先への EHLO コマンドの送出、及び、接続先からの応答

まず、接続元は、自ホストの FQDN 又は IP アドレスを送信する。

次いで、接続先は、自分が対応している拡張 SMTP のコマンドの一覧を応答する。

これらコマンドの中に、設問 1 に登場したユーザ認証 (AUTH コマンド)、設問 2 (5) に登場した TLS 暗号化 (STARTTLS コマンド) 等がある。

### 2. 接続元から接続先への MAIL コマンドの送出

接続元は、メールの「送信元」(差出人) のメールアドレスを送信する。

このメールアドレスを、エンベロープ From アドレスと呼ぶ。

### 3. 接続元から接続先への RCPT コマンドの送出

接続元は、メールの「宛先」(受取人) のメールアドレスを送信する。

このメールアドレスを、エンベロープ To アドレスと呼ぶ。

### 4. 接続元から接続先への DATA コマンドの送出

接続元は、メールデータ (メールのヘッダとボディ) を送信する。

### 5. 接続元から接続先への QUIT コマンドの送出

接続元は、メール転送の完了を通知する。

本問が問うている「送信元」(差出人) のドメイン名は、項番 2 で送信される MAIL コマンドのエンベロープ From アドレスに含まれている (アドレスの「@」以降に記述されている)。

よって、正解は「MAIL」となる。

なお、試験センターの解答例は「MAIL FROM」である。MAIL コマンドは、「MAIL FROM:」という文字列の後にエンベロープ From アドレスを指定する書式になっているため、「MAIL FROM」コマンドという通称で広く知られている。おそらく、試験セ

ンターはそのような現状を踏まえて、この解答例を公表したものと考えられる。

念のため、SMTP の仕様を定めている RFC(執筆時点の最新版は 5321)では、「MAIL」コマンドとなっていることを覚えておこう。

## (2)

### 解答例

送信元メールサーバの IP アドレス (16 字)

問題文は、「本文中の下線⑥で行われる処理内容について、SPF レコードと照合される情報を……述べて」と記述されている。

下線⑥は、「SPF の導入」の第 1 段落、2 番目の箇条書きの (3) にある。そこには、「得られた⑥ SPF レコードを用いて送信元ドメインの認証を行う」と記述されている。

本問の解を導くには、SPF を理解しておく必要がある。SPF について本文中でも説明されているので、その記述を参考にしながら、この技術について概要を解説する。それを踏まえて、解を導こう。

### ● SPF

「SPF の導入」の第 1 段落には、SPF の概要が説明されている。

そこでは、次のように述べられている。

SPF は、送信メールサーバの正当性（当該ドメインの真正のメールサーバであることを）、受信メールサーバで確認する方式である。

SPF を導入するには、送信側と受信側の双方が、これに対応している必要がある。送信側について、1 番目の箇条書きに次のように述べられている。

・送信側のドメイン所有者は、あらかじめ、当該ドメインのメールサーバのグローバル IP アドレスを、SPF レコードとして DNS に登録しておく。

図 2 には、送信側の立場で A 社が設定した SPF レコードが示されている。このレコードの内容は、「a-sha.co.jp ドメインの真正のメールサーバは、IPv4 アドレスが x.y.z.1 である」というものだ。

```
a-sha.co.jp.      IN TXT "v=spf1 +ip4:x.y.z.1 -all"
```

注記 x.y.z.1 は、MSV3 の IP アドレスである。

図：A 社ドメインの SPF レコードの設定（抜粋）（本文の図 2）

受信側について、2 番目の箇条書きに次のように述べられている。

- ・受信側のメールサーバは、メール受信時に、次の手順で送信ドメインを認証する。
  - (1) “SMTP 通信中にやり取りされる送信元ドメイン名” を得る。
  - (2) 送信元ドメイン名に対する SPF レコードを、DNS に問い合わせる。
  - (3) 得られた⑥ SPF レコードを用いて送信元ドメインの認証を行う。

まず、受信側メールサーバは、設問 3 (1) で解説したとおり、MAIL コマンドで与えられたエンベロープ From アドレスからドメインを抽出する。この文脈では、得られた送信元ドメインが、A 社の「a-sha.co.jp」となる。

次いで、このドメイン名に基づき、A 社の DNS サーバに対し、SPF レコードを問い合わせる。その結果、図 2 に示された、「a-sha.co.jp ドメインの真正のメールサーバは、IPv4 アドレスが x.y.z.1 である」という情報を取得する。

最後に、受信側メールサーバは、自ホストに TCP コネクションを接続してきた送信側メールサーバの IP アドレスと、SPF レコードに示された「x.y.z.1」とを照合する。

両者が一致するならば、エンベロープ From アドレスの所属先ドメインの SPF レコードによって、送信側メールサーバの真正性が確認されたことになる。これにより、送信元ドメインの認証に成功する。

認証に成功した後、送信側メールサーバからのメールを受信する。

### ●解の導出

下線⑥は、受信側メールサーバが行う送信ドメイン認証の、3 番目のステップである。このとき、SPF レコード中の IP アドレスと照合されるのは、送信側メールサーバの IP アドレスである。

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

近年、企業においてスマートフォンやタブレットといったモバイル端末の業務利用が進んでいる。モバイル端末を用いた業務システムを設計する際には、業務要件を満たすとともに、セキュリティ脅威についても考慮する必要がある。セキュリティ脅威に対する対策は、様々な方法を組み合わせる場合が多い。

本問では、ある企業のモバイルネットワークを想定し、これを構成する無線 LAN 接続、LTE 回線を用いたインターネット接続、VPN 接続、プロキシサーバの各要素について、ネットワーク上のセキュリティ脅威を想定し、取るべき対策を考えられるか、及び不正が行われた際の影響を最小限にする設計を考えられるかを問う。

## 採点講評

問 2 では、業務システムを設計する際に、ネットワーク上のセキュリティ脅威を想定し、取るべき対策を考えられるか、及び不正が行われた際の影響を、最小限にする設計を考えられるかについて出題した。全体として、正答率は低かった。

設問 2(1)では、誤って、無線ネットワークの一覧に SSID が表示されないなど、ステルス機能によって無線 LAN クライアント側にみられる効果を解答したものが見られた。(2)では、無線 LAN は電波を利用するため通信内容を容易に傍受されうことは理解できているものの、SSID や MAC アドレスは暗号化できないために容易に取得されうことを理解している解答は少なかった。無線 LAN は広く普及した技術であり、ネットワーク技術者として正確に理解をし、身に付けてほしい。

設問 3(2)は、正答率は低くなかったが、本文中に示されている条件を見落としたと思われる解答が見られた。限られた時間の中ではあるが、本文や図表から、ネットワーク構成を正しく読み解けるようになってほしい。

設問 4 は、(1)の正答率は低かった。プロキシを通すだけでなく、利用者認証による利用者情報を含めたログ取得を行うことによって、セキュリティ脅威に対して業務システムをより堅牢にできる点について理解を深めてほしい。また、(2)の正答率は、比較的高かった。セキュリティ脅威を想定する上で、取得できるログの内容が重要であることはよく理解されていることがうかがえた。

設問	解答例・解答の要点		備考
設問 1	ア	AES	
	イ	事前共有鍵	
	ウ	SIM カード	
	エ	APN	
	オ	NAPT	
	カ	CONNECT	
設問 2	(1)	定期的に送信するビーコン信号を停止する。	
	(2)	SSID や MAC アドレスは暗号化できず、傍受されるから	
	(3)	E	
設問 3	(1)	VPN 接続の利用者 ID を停止する。	
	(2)	プロキシサーバと内部 DNS サーバへの通信	

(表は次ページに続く)

設問	解答例・解答の要点			備考
設問 4	(1)	機能名	プロキシ認証	
		設定内容	営業員ごとに利用者 ID を登録する。	
	(2)	①	・接続先ホスト名	
		②	・接続先ポート番号	

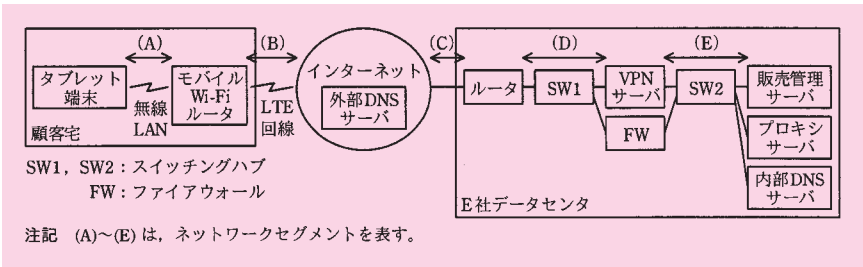
本問は、タブレット端末からモバイル Wi-Fi ルータを経由してインターネットに接続し、インターネットから社内サーバに VPN 接続するモバイルネットワークの構築を出題している。

本問は、無線 LAN 接続のセキュリティ機能、VPN 接続の設計、及び、プロキシサーバを経由させることで取得できる通信ログなどについて問うている。

### ●本問の全体像

事例に登場する運送業者の E 社は、販売管理システムを導入する予定である。本システムでは、顧客宅を訪問した営業員が、支給されたタブレット端末とモバイル Wi-Fi ルータを用いて、プレゼンテーション、見積、車両手配等の営業活動を行う。

システムで使用するモバイルネットワーク構成案は、本文の図 1 に示されている。



図：モバイルネットワーク構成案（本文の図 1）

モバイルネットワークを構築するに当たって、次の検討が必要となる。

#### [1] 無線 LAN 接続のセキュリティ対策

タブレット端末からモバイル Wi-Fi ルータに接続する際、次に示すセキュリティ対策を実施する。

1. モバイル Wi-Fi ルータのアクセスポイント保護
2. WPA2 を用いた通信の暗号化

## [2] VPN 接続の設計

VPN 接続に用いるプロトコルは、L2TP over IPsec である。L2TP トンネルは、タブレット端末と VPN 装置間に生成される。

VPN サーバへの不正アクセスを防止するため、VPN サーバ接続時に、ハードウェアトークンを用いた認証を行う。

タブレット端末、モバイル Wi-Fi ルータ、及び、ハードウェアトークンの紛失時の運用ルールを策定する。

## [3] プロキシサーバの設置

タブレット端末の通信ログを取得するため、プロキシサーバを設置する。

## [4] アクセス範囲の限定

VPN 接続に成功した後、タブレット端末が販売管理サーバ及びインターネット上のサーバと通信する場合、プロキシサーバを経由する。

タブレット端末が直接インターネットに接続することがないようにするため、モバイル Wi-Fi ルータを経由してインターネットに接続する範囲を、VPN サーバとその名前解決に用いる外部 DNS サーバに限定する。

## [5] アドレスの設計

図 1 中のネットワークセグメント (A) において、タブレット端末のプライベート IP アドレスは、モバイル Wi-Fi ルータから DHCP で配布される。

図 1 中のネットワークセグメント (B) において、モバイル Wi-Fi ルータのグローバル IP アドレスは、インターネット接続時に通信事業者から割り当てられる。タブレット端末がインターネットに接続する際、モバイル Wi-Fi ルータで NATP によるアドレスとポート番号の変換処理が行われる。

タブレット端末が VPN 接続を行うと、VPN サーバからタブレット端末に対し、図 1 中のネットワークセグメント (E) のプライベート IP アドレスが割り当てられる。

これら 5 点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。

見出し	主な内容	主に対応する出題箇所	
		設問	小問
なし（序文）	販売システムの モバイルネットワークの構成	—	—
モバイルネットワークの検討	[3] プロキシサーバの設置		

(表は次ページに続く)

見出し	主な内容	主に対応する出題箇所	
		設問	小問
無線 LAN 接続の検討	[1] 無線 LAN 接続のセキュリティ対策	2	(1), (2)
	[5] アドレスの設計	2	(3)
LTE 回線を用いたインターネット接続の検討	[5] アドレスの設計	1	オ
	[4] アクセス範囲の限定		
VPN 接続の検討	[2] VPN 接続の設計	3	(1), (2)
プロキシサーバの検討	[3] プロキシサーバの設置	4	(1), (2)

本問を首尾よく解くに当たって、VPN 接続に用いる L2TP over IPsec の知識が助けになる。もっとも、この要素技術に関する知識が細かく問われているわけではない。「[2] VPN 接続の設計」, 「[5] アドレスの設計」を理解できる程度まで、概要を押さえておこう。

### ● L2TP over IPsec

L2TP (Layer 2 Tunneling Protocol) は、データリンク層の PPP フレームをトンネリングする技術である。L2TP は UDP の上位層として規格化されており、IP ネットワーク内を通信できる。

PPP (Point to Point Protocol) は、専用線などで結ばれた 2 点間の通信に用いられる、データリンク層のプロトコルである。L2TP は、ここで言う「専用線」を仮想的に生成する技術である。

つまり、L2TP は、IP (レイヤ 3) のネットワーク上に、専用線の役割を果たすトンネルを設けることで、PPP (レイヤ 2) の通信を実現しているわけだ。本問の事例に登場する VPN 接続において、このトンネルは、タブレット端末と VPN サーバ間に生成されている。

本問の事例のようにインターネットを経由して VPN 接続を行う場合、次に示すセキュリティ対策が必要となる。

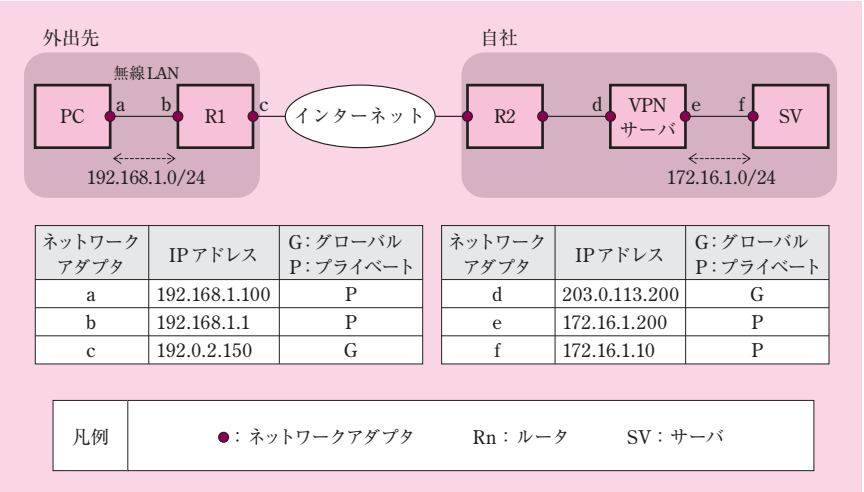
1. トンネル区間 (端末と VPN サーバ間) の暗号化
2. VPN サーバに接続する際の利用者認証

一つ目のトンネル区間の暗号化には、IPsec を用いる。IPsec について、詳しくは第 4 章「4.4.4 IPsec」を参照していただきたい。

二つ目の VPN サーバ接続時の利用者認証には、PPP が備えるパスワード認証方式である CHAP などを用いる。CHAP について、詳しくは第 4 章「4.4.1 認証プロトコル」を参照していただきたい。

● L2TP over IPsec を用いた VPN 接続の仕組み

ここで、本問の事例よりも若干シンプルなネットワーク構成例を使って、L2TP over IPsec を用いた VPN 接続の仕組みについて解説しよう。



図：VPN 接続のネットワーク構成

ここでは、本問の事例と同じように、PC とモバイル Wi-Fi ルータ（R1）を携えて外出している状況を想定している。なお、PC の OS は Windows にしている（Windows は多くの読者に馴染みがあると思われるため）。

外出先の PC から自社内のサーバ SV にアクセスする際、一般的には次の 4 段階の手順を踏む。

1. PC の利用者は、VPN 接続用ネットワークアダプタを用い、VPN サーバに手動で接続する。
2. VPN サーバは、利用者認証を行う。
3. VPN サーバは、自社 LAN のプライベート IP アドレスを、PC の VPN 接続用ネットワークアダプタに割り当てる。
4. PC の利用者は、SV に接続する。



手順 1 は、Windows の場合、VPN 接続用ネットワークアダプタを手動で選択した上で、「接続」の操作を行う。

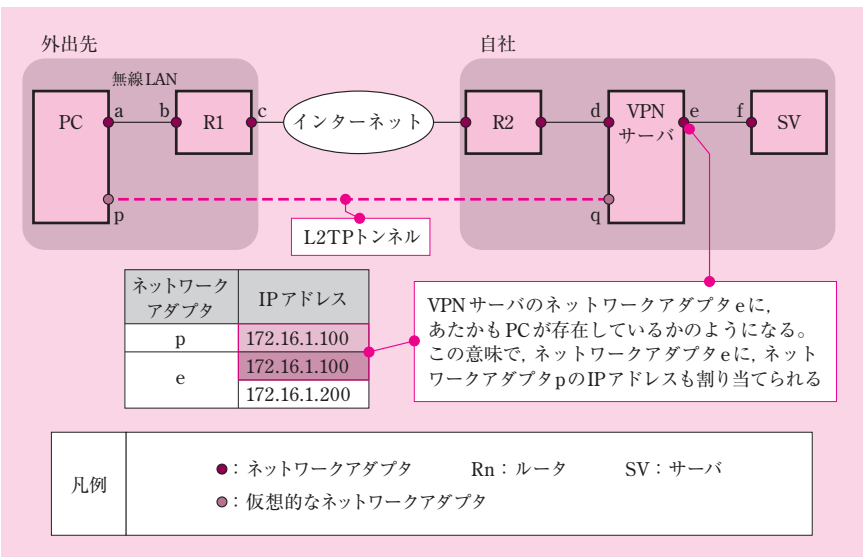
手順 2 で行われる利用者認証の方式やパラメータは、VPN 接続用ネットワークアダプタにあらかじめ設定しておく。

手順 3 で割り当てる IP アドレスの範囲は、VPN サーバにあらかじめ設定しておく。参考までに、手順 3 では、IPCP (IP Control Protocol) のやり取りが行われている。IPCP とは、PPP フレーム上の IP パケット伝送を準備する目的で、IP 通信に先立って自動的に実施されるものだ。この IPCP によって、PC に対し、接続先ネットワークの IP アドレスが割り当てられる。

これら一連の手順に成功すると、PC と VPN サーバ間に L2TP トンネルが生成され、PC はあたかも社内 LAN に存在しているかようになる。前述のとおり、このトンネルは、PC と VPN サーバ間を仮想的につなぐ専用線の役割を果たす。このトンネルの中を、IP パケットを格納した PPP フレームが流れる仕組みになっている。

手順 4 の時点で、PC は仮想的に自社 LAN に存在している。この段階では、ただ単に PC から社内 LAN の SV に IP パケットを直接送信するだけだ。

次の図は、VPN 接続によって生成される L2TP トンネルを示している。PC の VPN 接続用ネットワークアダプタは、図中のネットワークアダプタ p に該当する。





図：VPN 接続によって生成される L2TP トンネル

VPN 接続に成功すると、PC には二つのネットワークアダプタが「接続」状態となる。

参考までに、二つのネットワークアダプタについて、Windows のコントロールパネルの表示例、設定例（ipconfig コマンドの出力結果）を示しておこう。

表：PC のネットワークアダプタの表示例（Windows の場合）

ネットワークアダプタ	Windows のコントロールパネルに表示される ネットワークアダプタのアイコンイメージ
a	 Wi-Fi Wireless-... ..
p	 VPN 接続 WAN Miniport (L2TP)

<div>Wi-Fi</div> <div>Wireless LAN adapter Wi-Fi: 接続固有の DNS サフィックス ..... : 説明 ..... : <input type="checkbox"/> 物理アドレス ..... : <input type="checkbox"/>-<input type="checkbox"/>-<input type="checkbox"/>-<input type="checkbox"/>-<input type="checkbox"/>-<input type="checkbox"/> DHCP 有効 ..... : はい 自動構成有効 ..... : はい リンクローカル IPv6 アドレス ..... : fe80::<input type="checkbox"/>:<input type="checkbox"/>:<input type="checkbox"/>:<input type="checkbox"/>%9 (優先) IPv4 アドレス ..... : 192.168.1.100 (優先) ● サブネット マスク ..... : 255.255.255.0 リース取得 ..... : <input type="checkbox"/> リースの有効期限 ..... : <input type="checkbox"/> デフォルト ゲートウェイ ..... : 192.168.1.1 DHCP サーバー ..... : 192.168.1.1 DHCPv6 IAID ..... : <input type="checkbox"/> DHCPv6 クライアント DUID ..... : <input type="checkbox"/> DNS サーバー ..... : 192.168.1.1 NetBIOS over TCP/IP ..... : 有効</div>	● ネットワーク アダプタ a の IP アドレス
<div>VPN 接続 (L2TP トンネル生成時の状態)</div> <div>PPP アダプター VPN: 接続固有の DNS サフィックス ..... : 説明 ..... : VPN 接続 物理アドレス ..... : DHCP 有効 ..... : いいえ 自動構成有効 ..... : はい IPv4 アドレス ..... : 172.16.1.100 (優先) ● サブネット マスク ..... : 255.255.255.255 デフォルト ゲートウェイ ..... : 0.0.0.0 DNS サーバー ..... : <input type="checkbox"/>.<input type="checkbox"/>.<input type="checkbox"/>.<input type="checkbox"/> NetBIOS over TCP/IP ..... : 有効</div>	● ネットワーク アダプタ p の IP アドレス

図：PC のネットワークアダプタの設定例（Windows の場合）

およその概要がつかめたところで、IP アドレスの設定とパケットフォーマットについて解説しよう。

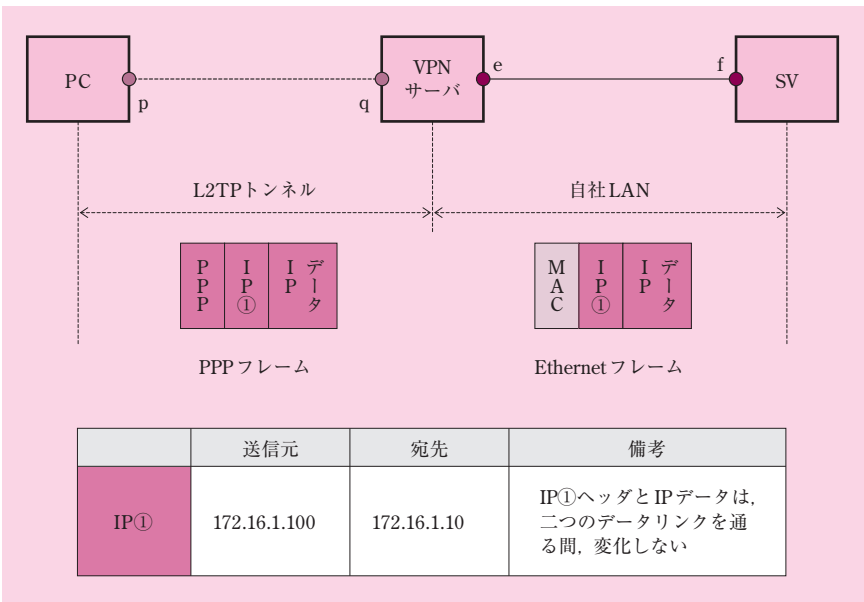
PC のネットワークアダプタ a は、Wi-Fi 接続である。R1 の DHCP 機能により、プライベート IP アドレス 172.16.8.100 が PC に割り当てられている。

PC からインターネットにアクセスする際、R1 の NAT 機能により、IP パケットの送信元 IP アドレスが、PC のプライベート IP アドレスから R1 のネットワークアダプタ c のグローバル IP アドレスに変換される。

VPN 接続に成功すると、PC のネットワークアダプタ p に、プライベート IP アドレス 172.16.8.100 が割り当てられる。同時に、VPN サーバのネットワークアダプタ e にも、172.16.8.100 が割り当てられているかのように振る舞う。こうして、ネットワークアダプタ e に、あたかも PC が存在しているかようになる。

仮想的には、PC と VPN サーバ間は L2TP トンネル（仮想的な専用線）で、VPN サーバ間と SV はイーサネット、それぞれ接続されている。つまり、PC と SV 間の IP パケットは、L2TP トンネル、イーサネットという 2 種類のデータリンクを通して、伝送されているわけだ。

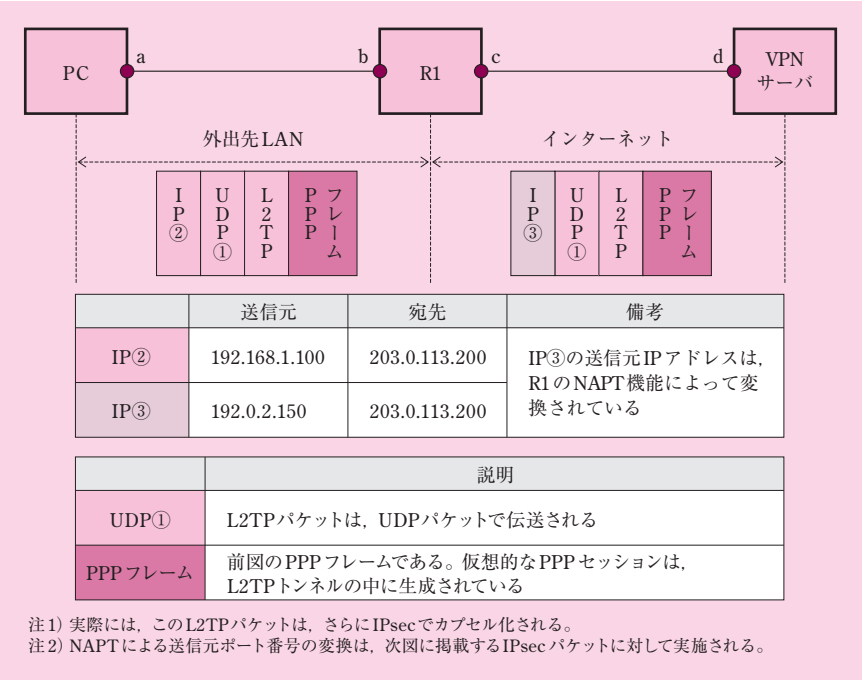
次の図は、L2TP トンネルを通信する PPP フレームと自社 LAN を通信する Ethernet フレームを示している。通信の方向は、PC から SV である。



図：L2TP トンネルを通信する PPP フレームと自社 LAN を通信する Ethernet フレーム

実際には、L2TP トンネルを流れる PPP フレームは、L2TP でカプセル化して、インターネット経由で VPN サーバに送信している。

次の図は、PPP フレームを L2TP でカプセル化した L2TP パケットを示している。通信の方向は、前図と同じだ。

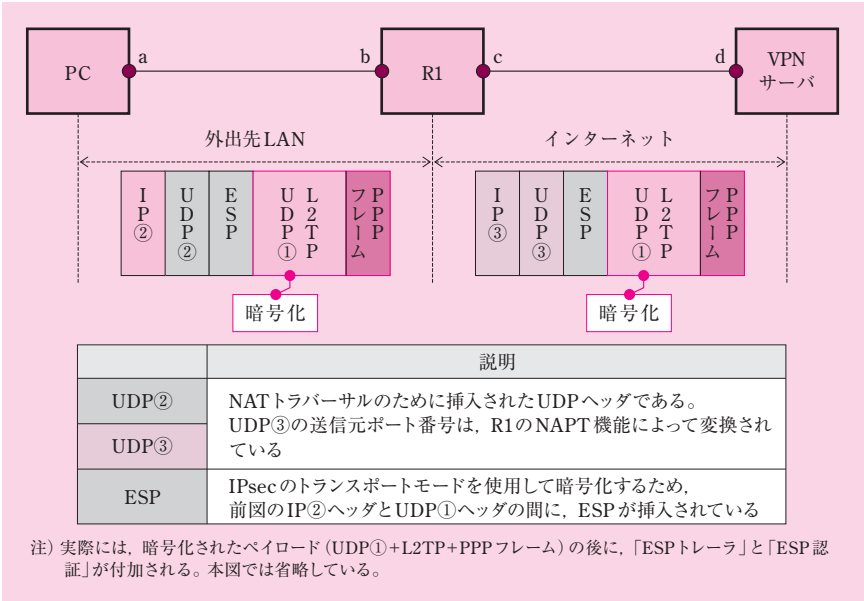


図：PPP フレームを L2TP でカプセル化した L2TP パケット

さらに続けると、実際には、この L2TP パケットは、IPsec でカプセル化し、暗号化してから、インターネット経由で VPN サーバに送信している。IPsec の暗号化区間は L2TP のトンネル区間と等しくなるため、暗号化にはトランスポートモードを用いる。

NAPT 機能を有するモバイル Wi-Fi ルータ R1 を越えるため、この IPsec パケットの伝送には NAT トラバーサルが必要である。NAT トラバーサルについて、詳しくは第 4 章「4.4.4 IPsec」を参照していただきたい。

次の図は、L2TP パケットを IPsec でカプセル化し、暗号化した IP パケットを示している。通信の方向は、前図と同じだ。



図：L2TP パケットを IPsec でカプセル化し、暗号化した IP パケット

● VPN 接続時のルーティングテーブル

次の図は、VPN 接続時の PC のルーティングテーブルを示している。

ネットワーク宛先	ネットマスク	ゲートウェイ	インタフェース	メトリック
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.100	4270
0.0.0.0	0.0.0.0	リンク上	172.16.1.100	26
172.16.1.0	255.255.255.0	リンク上	172.16.1.100	26
192.168.1.0	255.255.255.0	リンク上	192.168.1.100	4526
203.0.113.200	255.255.255.255	192.168.1.1	192.168.1.100	4271

1 行目と 2 行目は、ロングストマッチアルゴリズムでは同等となる。このときは、メトリックの値が小さい 2 行目が選ばれる

図：VPN 接続時のルーティングテーブル設定例の抜粋（Windows の場合）

まず、1 行目と 2 行目のエントリに着目しよう。これらはどちらもデフォルトゲートウェイのエントリである。ロングストマッチアルゴリズムではどちらも同等となるので、メトリックの値が小さい 2 行目を選ばれる。つまり、デフォルトゲートウェイは、VPN 接続の「リンク上」となる。

このリンクは、インタフェースが「172.16.1.100」であることから、L2TP トンネルにつながっていることが分かる。このリンクの対向側には VPN サーバしかない。したがって、デフォルトゲートウェイは、事実上、VPN サーバとなる。

次に 5 行目のエントリに着目しよう。これは、宛先が VPN サーバである。VPN サーバ宛てのパケット（IPsec でカプセル化された L2TP パケット）は、元からある Wi-Fi のアダプタ（ネットワークアダプタ a）から出ていく。

この 2 行目と 5 行目を踏まえると、PC がインターネット上のサーバに接続するとき、次のように動作して、デフォルトゲートウェイの VPN サーバに到達することが分かる。

- 仮想的には、L2TP トンネルの先にある VPN サーバに向かう（2 行目のエントリ）。
- 実際には、このパケットは L2TP、IPsec の順にカプセル化されるので、Wi-Fi のアダプタからインターネット上の VPN サーバに向かう（5 行目のエントリ）。

VPN サーバにパケットが到達してカプセル化が解除されると、接続先ネットワークを経由して、そこからインターネット上のサーバに向かうことになる。

3 行目と 4 行目は、PC に直接接続されたネットワークのエントリである。3 行目は、VPN の接続先ネットワークであり、4 行目は元から接続していた Wi-Fi の自ネットワークだ。

L2TP over IPsec、及び、これを用いた VPN 接続の概要を理解できたので、いよいよ設問の解説に移ろう。

## ■設問 1

## 解答例

ア：AES  
イ：事前共有鍵  
ウ：SIM カード  
エ：APN  
オ：NAPT  
カ：CONNECT

ア

空欄アを含む文章は、〔無線 LAN 接続の検討〕の第 2 段落の中にある。そこには、「WPA2 は、無線 LAN の暗号化アルゴリズムとして  が初めて採用された方式である」と記述されている。

WPA2 は、暗号化アルゴリズムとして AES を採用している。WPA2 より前の無線 LAN 規格では、AES を採用していない。例えば、WPA2 の一世代前の規格である WPA では、暗号化アルゴリズムとして TKIP を採用していた。

よって、空欄アに該当する字句は「AES」となる。

イ

空欄イを含む文章は、〔無線 LAN 接続の検討〕の第 2 段落の中にある。そこには、「(WPA2 の) 認証方式には、あらかじめタブレット端末とモバイル Wi-Fi ルータに同じパスフレーズを設定する  認証を用いる」と記述されている。

WPA2 は、無線 LAN 端末の認証方式を二つ規定している。

一つ目は、IEEE802.1X を用いた方法である。この方式では、RADIUS サーバを設置し、RADIUS サーバが無線 LAN 端末を認証する。IEEE802.1X について、詳しくは第 4 章「4.4.3 IEEE802.1X」を参照していただきたい。

二つ目は、PSK (Pre-shared Key: 事前共有鍵) を用いた方法である。PSK とは、アクセスポイントと無線 LAN 端末の間で、事前に共有するパスフレーズである。同じ PSK を共有していることに基づき、アクセスポイントは無線 LAN 端末を認証し、自アクセスポイントを使用した無線 LAN 通信を許可する。

この点を踏まえて本文を確認してみよう。問われている認証方式について、空欄イの直前に、「あらかじめタブレット端末とモバイル Wi-Fi ルータに同じパスフレーズを

設定する」と記述されている。本問のモバイルネットワーク構成では、Wi-Fi ルータはアクセスポイントを兼ねている。したがって、ここで問われている認証方式は、PSK 認証（事前共有鍵認証）であることが分かる。

よって、空欄イに該当する字句は「事前共有鍵」又は「PSK」となる。

ウ

空欄ウを含む文章は、〔LTE 回線を用いたインターネット接続の検討〕の第 1 段落の中にある。そこには、「モバイル Wi-Fi ルータには、通信事業者が契約者を識別する情報が記録されている [ウ] が挿入されている」と記述されている。

結論から言うと、空欄ウに該当する字句は「SIM カード」である。

SIM カード（Subscriber Identity Module Card）とは、通信事業者が契約者を識別する情報が記録されたカードである。

SIM カードは、フィーチャーフォン、スマートフォン、モバイル Wi-Fi ルータなど、LTE 回線に接続する機器に装着する。これを使って LTE 回線に接続する際、SIM カードを読み取り、契約者の電話番号や契約種別を識別する。正規の契約者であることを認証できたら、LTE 回線を使用することができる。

エ

空欄エを含む文章は、〔LTE 回線を用いたインターネット接続の検討〕の第 1 段落の中にある。そこには、「モバイル Wi-Fi ルータには、……LTE 回線からインターネットのようなネットワークへのゲートウェイの指定を意味する、[エ] の情報を設定する」と記述されている。

結論から言うと、空欄エに該当する字句は「APN」である。

APN（Access Point Name：アクセスポイント名）とは、携帯端末からインターネットに接続してデータ通信を行う際に指定する、アクセスポイントである。技術的に見ると、このアクセスポイントは、LTE 回線とインターネットをつなぐゲートウェイである。

通信事業者は契約者に APN の登録情報を開示しており、契約者は携帯端末の購入時に APN を設定することで、データ通信が可能になる。

オ

空欄オを含む文章は、〔LTE 回線を用いたインターネット接続の検討〕の第 2 段落の中にある。そこには、「モバイル Wi-Fi ルータは、電源投入時に自動的にインターネット接続を開始し、グローバル IP アドレスが割り当てられる。タブレット端末がイ



インターネット上のサーバと通信を行う際に、モバイル Wi-Fi ルータでは「オ」による IP アドレスとポート番号の変換処理が行われる」と記述されている。

タブレット端末の IP アドレスについて、〔無線 LAN 接続の検討〕の第 3 段落の中で「タブレット端末が無線 LAN に接続すると、モバイル Wi-Fi ルータは、DHCP によってプライベート IP アドレスの配布を行う」と記述されている。したがって、タブレット端末はプライベート IP アドレスをもつことが分かる。

このタブレット端末がインターネット上のサーバと通信を行うには、モバイル Wi-Fi ルータで NATP による変換を施す必要がある。タブレット端末がインターネット上のサーバに IP パケットを送信すると、NAPT により、送信元 IP アドレスがタブレット端末のプライベート IP アドレスからモバイル Wi-Fi ルータのグローバル IP アドレスに変換される。それと同時に送信元ポート番号も変換され、モバイル Wi-Fi ルータの配下にある複数のタブレット端末が、一つのグローバル IP アドレスを共有できるようにしている。

よって、空欄オに該当する字句は「NAPT」である。

#### カ

空欄カを含む文章は、〔プロキシサーバの検討〕の第 1 段落の中にある。そこには、「HTTPS プロキシの場合、プロキシサーバは、タブレット端末からの「カ」要求によって HTTPS サーバへの TLS トンネルを中継し、その後のリクエストは、TLS トンネルの中をそのまま転送する」と記述されている。

プロキシサーバを経由して、クライアント端末とサーバ間で HTTPS 通信（TLS 通信）を行うとき、クライアント端末のブラウザは、プロキシサーバに CONNECT メソッドを発行する。このメソッドの中で、HTTPS 通信の接続先ホスト名と接続先ポート番号を指定する。

このメソッドは、プロキシサーバに対し、クライアント端末と接続先サーバとの間で TLS トンネルを確立することを要求している。トンネルが確立されると、プロキシサーバは、クライアント端末とサーバ間の TLS パケットを中継する。

よって、空欄カに該当する字句は「CONNECT」である。

プロキシサーバが行う TLS 通信のトンネル処理について、詳しくは第 4 章「4.3.2 プロキシ」の「● TLS 通信のトンネル処理」を参照していただきたい。

## ■設問 2

### (1)

#### 解答例

定期的に送信するビーコン信号を停止する。(20字)

問題文は、「本文中の下線①について、ステルス機能の動作を……述べよ」と記述されている。

下線①は、「無線 LAN 接続の検討」の第 1 段落の中にある。そこには「アクセスポイント保護のために次のセキュリティ対策機能が搭載されている」とあり、2 番目の箇条書きに「SSID を隠ぺいする①ステルス機能」と記述されている。

これは一般的な知識から解を導く。

アクセスポイントは、ビーコン信号を定期的に送信して、自分の SSID を周囲に通知する機能をもつ。無線 LAN を利用したければ、端末が検出した SSID のの中から接続先をただ選択すればよいだけだ。その後、PSK 認証など、アクセスポイントに設定された認証の手続きに成功すれば、同アクセスポイントを経由して通信することができる。

このように、無線 LAN 端末が SSID を受動的に入手する方法を、パッシブスキャンと呼ぶ。通常、この方法が用いられる。

しかし、SSID を隠ぺいして特定の利用者にだけ接続させたい場合、ビーコン信号のブロードキャストを止めることができる。この結果、SSID が通知されなくなるので、利用者が無線 LAN 端末上の操作<sup>(\*)</sup>により SSID を指定しない限り、アクセスポイントに接続することができなくなる。

(\*) Windows 10 の場合、「ワイヤレスネットワークに手動で接続する」の設定画面で、ステルスされた SSID を登録し、「ネットワークがブロードキャストしていない場合でも接続する」をチェックする。

この「ネットワークがブロードキャストしていない……」という記述は、前述の解説に照らせば、「アクセスポイントがビーコン信号を送信していない……」と読み替えることができる。これをチェックすると、SSID を格納したブロードキャスト信号を送信する。

無線 LAN 端末上で SSID を明示的に指定すると、SSID を格納したブロードキャスト信号を送信するので、同じ SSID をもつアクセスポイントはこれに応答する。この結果、無線 LAN 端末は SSID を検出することができる。その後は、パッシブスキャンと同じく、

しかるべき認証の手続きに成功すれば、アクセスポイントを経由して通信することができる。

このように、無線 LAN 端末が SSID を明示的に指定する方法を、アクティブスキャンと呼ぶ。この方法を採用するには、下線①の「ステルス機能」を有効にすればよい。

さて、本問で問われているのは、「ステルス機能の動作」である。よって、「**定期的**に送信するビーコン信号を停止する」旨を解答すればよい。

## (2)

### 解答例

SSIDやMACアドレスは暗号化できず、傍受されるから  
(27字)

問題文は、「本文中の下線②について、SSID や MAC アドレスは容易に取得される危険性がある。その理由を、電波を用いて通信を行う無線 LAN の特性に着目して……述べよ」と記述されている。

下線②は、「無線 LAN 接続の検討」の第2段落にある。そこには、「②ステルス機能と MAC アドレスフィルタリング機能を用いたセキュリティ対策だけでは不十分なので、無線 LAN 通信の暗号化を行う」と記述されている。

これは一般的な知識から解を導く。

#### ● SSID の取得が可能であることについて

アクセスポイントのステルス機能を用いてビーコン信号を停止したとしても、無線 LAN 端末から送信されるプローブ信号を傍受すれば、SSID を取得することができる。

この点、Windows をはじめとする一部の OS は、登録した SSID に対して「自動的に接続」するように設定すると、PC 起動時にプローブ信号を送信して SSID の検出を試みる仕組みになっている。たとえアクセスポイントのステルス機能で SSID を隠しても、これでは意味をなさない（それどころか、至るところで起動時に SSID を触れ回っている）。

#### ● MAC アドレスの取得が可能であることについて

MAC フィルタリング機能を用い、特定の MAC アドレスをもつ無線 LAN 端末のみ接続を許可したとしても、無線 LAN フレームを傍受すれば MAC アドレスを取得する

ことができる。

取得した MAC アドレスを用いて詐称すれば、MAC フィルタリング機能を無力化できてしまう。

### ●暗号化すれば秘匿できるだろうか

ここで、改めて下線②を含む文章を読み返してみると、「②ステルス機能と MAC アドレスフィルタリング機能を用いたセキュリティ対策だけでは不十分なので、無線 LAN 通信の暗号化を行う」と記述されている。

ここで暗号化について言及されているが、一般的に言って、第三者に何かを秘匿したいときは暗号化という手段を講ずることができる。それでは、SSID と MAC アドレスは、無線 LAN の暗号化によって、取得されないように保護できるのだろうか。

その答えは「否」である。

まず、SSID について解説しよう。無線 LAN の仕様では、ビーコン信号とプローブ信号は、暗号化されない。SSID を通知する重要な役割を担う信号なので、これは当然のことだ。

次いで、MAC アドレスについて解説しよう。無線 LAN の仕様では、暗号化はあくまでフレームのデータ部分に対して実施されるのであり、ヘッダは対象外である。

よくよく考えてみれば、宛先 MAC アドレスが暗号化されてしまうと相手は受信しようがないし、送信元 MAC アドレスが暗号化されてしまうと相手は返信しようがないので、これは当然のことだ。

したがって、たとえ暗号化したとしても、SSID と MAC アドレスの取得は可能であると考えなければならない。

### ●解の導出

これまで解説したとおり、SSID と MAC アドレスの取得は可能である。暗号化をはじめいかなる手段を講じて、無線 LAN の仕様上、これは不可避である。

よって、正解は解答例に示したとおりとなる。

## (3)

### 解答例

E

問題文は、「本文中の下線③について、重複してはいけないセグメントを、図 1 中の (A) ～ (E) から選べ」と記述されている。

下線③は、「無線 LAN 接続の検討」の第 3 段落にある。そこには、「タブレット端末が無線 LAN に接続すると、モバイル Wi-Fi ルータは、DHCP によってプライベート IP アドレスの配布を行う。③このプライベート IP アドレスは他のネットワークと重複しないように設計する」と記述されている。

モバイル Wi-Fi ルータが DHCP によって配布するアドレスは、図 1 中の (A) のセグメントである。したがって、ここで問われているのは、(A) が重複してはならないネットワークアドレスをもつセグメントである。

それでは、答えるべきセグメントが複数ある可能性を考慮しつつ、一つずつ検討してみよう。

### ●セグメント (A)

問題文を見ると、解答の候補の中に (A) 自体が挙げられている。

一見すると、(A) は解答から除外してもよいように見える。しかし、顧客宅に外出する営業員が複数いることを考えるなら、早とちりして (A) を排除すべきではない。仮に「複数の顧客宅ネットワーク間で重複してはいけない」という解が導けたとしたら、答えるべきセグメント名は (A) になるからだ。

結論から言うと、「複数の顧客宅ネットワーク間で重複」しても問題はないのだが、その裏付けを得て初めて (A) を排除できる。

複数の顧客宅ネットワークから VPN サーバに接続したとき、モバイル Wi-Fi ルータのグローバル IP アドレスはそれぞれ異なっている。つまり、VPN サーバは、接続元である顧客宅ネットワークを各々識別できる。そして、セグメント (E) のプライベート IP アドレスを、それぞれに割り当ててのるのだ。

つまり、VPN 接続の成立に当たって、顧客宅のプライベート IP アドレスが何らかの役割を果たすことはない。それゆえ、複数の顧客宅ネットワーク間でプライベート IP アドレスが重複していたとしても、何ら問題はないのである。

したがって、(A) は解答の候補から外す。

### ●セグメント (B) ～ (D)

下線③には、モバイル Wi-Fi ルータが配布する IP アドレスは、「プライベート IP アドレス」と記述されている。

これを前提に解を導くため、グローバル IP アドレスをもつセグメントは、解答の候補から外す必要がある。

セグメント (B) のアドレスについて、[LTE 回線を用いたインターネット接続の検討] の第 2 段落には、「モバイル Wi-Fi ルータは、電源投入時に自動的にインターネット接続を開始し、グローバル IP アドレスが割り当てられる」とある。それゆえ、グローバル IP アドレスをもつことが分かる。

セグメント (C)、(D) のアドレスについて、[VPN 接続の検討] の第 1 段落には、「E 社データセンタの VPN サーバには、グローバル IP アドレスを割り当てる」とある。それゆえ、セグメント (D) はグローバル IP アドレスをもつことが分かる。そこから、セグメント (D) とインターネットの間に位置するセグメント (C) も、グローバル IP アドレスをもつことが分かる。

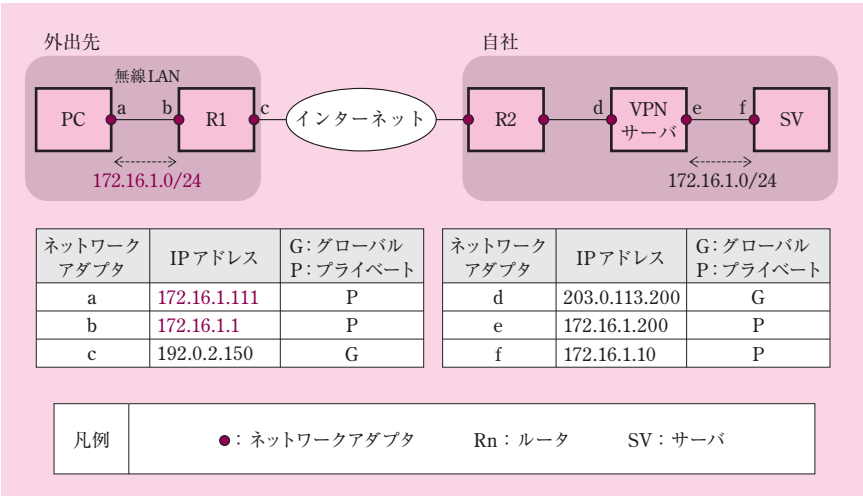
したがって、(B)～(D) は解答の候補から外す。

●セグメント (E)

冒頭の「● L2TP over IPsec を用いた VPN 接続の仕組み」「● VPN 接続時のルーティングテーブル」で解説したとおり、VPN 接続時には、PC は二つのネットワークアダプタが接続状態になるので、二つのネットワークに収容される。一つ目は元からあった自ネットワークであり、二つ目は VPN の接続先ネットワークである。

それでは、自ネットワークと、VPN の接続先のネットワークのアドレスが重複していたら、状況はどのように変化するだろうか。

ネットワーク構成は冒頭の解説と同じものとし、自ネットワーク(外出先ネットワーク)の IP アドレスだけ変化させてみよう。



図：自ネットワークと、VPN の接続先ネットワークのアドレスが重複した構成

仮に、PCの利用者が、VPNの接続先ネットワーク上のサーバに接続することを意図して、通信を開始したとしよう。

このとき、利用者の意図に反し、技術的観点からは、自ネットワーク上のサーバに接続していることになる。直接接続されたサーバを宛先に指定したものと解釈されるため、L2TP over IPsecによるVPN接続は行われない。

それゆえ、自ネットワークのアドレスと、VPNの接続先ネットワークのアドレスは、重複してはならないことが分かる。

したがって、(E)は解答の候補となる。

### ●解の導出

これまで解説したとおり、セグメント(A)のネットワークアドレスと重複してはならないのは、VPNの接続先となるセグメント(E)のみである。

よって、正解は「E」となる。

## ■設問3

### (1)

#### 解答例

V P N 接 続 の 利 用 者 I D を 停 止 す る 。 (17字)

問題文は、「本文中の下線④について、報告を受けたモバイルネットワーク管理者が取るべき行動を、紛失したVPN接続の利用者IDに着目して……述べよ」と記述されている。

下線④は、「VPN接続の検討」の第4段落にある。そこには、「訪問した顧客宅での利用が前提となるタブレット端末、モバイルWi-Fiルータ及びハードウェアトークンは、紛失する可能性がある。④営業員が、これらを紛失した際には、直ちにモバイルネットワーク管理者に報告するという運用ルールを策定する」と記述されている。

ここで問われているのは、タブレット端末、モバイルWi-Fiルータ及びハードウェアトークンを紛失した際、「紛失したVPN接続の利用者ID」に関して実施する運用ルールである。

その運用ルールの目的は、文脈から推論できる。第2段落の冒頭に、「VPNサーバへの不正アクセスを防止」とあり、下線④に続く文章も「不正アクセスが行われた際の影響を最小限にとどめる……」とある。したがって、「VPNサーバへの不正アクセ

スの防止」を目的として、紛失の報告を受けた後にネットワーク管理者が行うことを定めたルールであると推論できる。

さて、問題文には「紛失した VPN 接続の利用者 ID」とあるが、これは具体的に何を指しているのだろうか。「紛失した」とあるので、紛失した三つの機器のどれかに関係する利用者 ID であると推論できる。

そこで、まずは利用者 ID の観点から機器を一つ一つ検討してみよう。次いで解を導こう。

### ●ハードウェアトークン

問題文に列挙された機器の順序では最後にあるが、実際に試験問題を解くとき、ハードウェアトークンにまず着目できる。

なぜなら、今は「VPN サーバへの不正アクセスの防止」という観点で解いているからだ。そのために最初に確認すべきことは、VPN サーバの認証機能に関する記述である。(この後すぐに解説するが、) この認証機能にハードウェアトークンが用いられることが分かり、そこから利用者 ID との関連性を推論して、解を導くことができる。

VPN サーバの認証機能について、[VPN 接続の検討] の第 2 段落には、次のように記述されている。

VPN サーバへの不正アクセスを防止するためのセキュリティ対策を行う。例えば、利用者 ID、固定パスワードを用いて利用者認証を行う場合、これらが漏えいすると、直ちにインターネットから不正アクセスが可能となり、危険である。その対策として、ハードウェアトークンを利用する。ハードウェアトークンでは、一定時間ごとに変化する数字が表示されるので、これをワンタイムパスワードとして利用する。

「利用者 ID、固定パスワード」を用いた利用者認証は、これらが漏えいすると不正アクセスの危険性がある。それゆえ、ハードウェアトークンを利用したワンタイムパスワード認証を行うことが分かる。

ここで、本文を読み解く際に注意深さが求められている。利用者 ID と固定パスワードを用いた利用者認証については、「採用しない」とは述べていないのだ。固定パスワードの認証を「危険である」と述べているに過ぎない。それだけでは危険であるから、ハードウェアトークンを用いたワンタイムパスワード認証も併せて行う、と推論しなければならない(このように推論できる理由は、後述するハードウェアトークンを用いた認証の仕組みから明らかになる)。



要するに、VPN サーバでは、2 種類の認証方式を組み合わせているわけだ。これを二要素認証と呼ぶ。

一つ目の方式は、利用者 ID、固定パスワードを用いた、いわゆるパスワード認証である。これは、認証される相手だけが「知っていること」に基づくものだ。

二つ目の方式は、ハードウェアトークンを用いた認証である。認証される相手だけが「持っているもの」に基づくものだ。

ハードウェアトークンは、「一定時間ごとに変化する数字」、すなわち、ワンタイムパスワード（以下、OTP と称する）を発行する。さらに、本文には明記されていないが、この OTP は、同じ時刻であっても個体ごとに異なっている。

通常、ハードウェアトークンを用いた認証では、ベンダ固有の認証システムを用いる。VPN サーバには認証システムの本体をインストールし、タブレット端末には認証システムの専用アプリをインストールする。

ハードウェアトークンは、ベンダが提供するものを用いる。ベンダは、ハードウェアトークンに個体ごとにシリアル番号を割り当てている。

このシリアル番号と時刻から、VPN サーバの認証システム本体で、発行される OTP を照合できる仕組みになっている。

この仕様を踏まえ、ハードウェアトークンを用いた認証は、一般的に次のように行われている。なお、この説明では、話を簡単にするため、認証時の通信が暗号化されており盗聴のリスクはないものとする。

#### ● 事前登録

VPN サーバに、二要素認証を行う利用者 ID、固定パスワード、シリアル番号を登録する。

#### ● 認証時の手順

1. タブレット端末は、パスワード認証のための利用者 ID、固定パスワードを送信する。
2. VPN サーバは、送信された利用者 ID、固定パスワードを照合し、パスワード認証を行う（一つ目の認証方式）。
3. タブレット端末は、ハードウェアトークン認証のための OTP を送信する。
4. VPN サーバは、手順 1 で送信された利用者 ID からシリアル番号を取得し、送信された OTP と時刻を照合し、ハードウェアトークン認証を行う（二つ目の認証方式）。

この説明から、ハードウェアトークンを用いた認証では、利用者 ID が重要な役割を果たしていることを理解できるはずだ。

この点を踏まえると、〔VPN 接続の検討〕の第 2 段落の中で、固定パスワードを用いた利用者認証の危険性に言及しているものの、この文脈では二要素認証を採用していると推論すべきことが分かるだろう。

それでは、VPN サーバが実施している、ハードウェアトークンを用いた認証の仕組みが理解できたので、いよいよ解を導こう。

ハードウェアトークンが紛失し、これが第三者に悪用されるとどうなるだろうか。

当然ながら、二要素認証の一つ「持っているもの」に基づく認証が、用をなさなくなってしまう。もう一つの頼みの綱は、「知っていること」に基づく認証であるが、固定パスワードがクラッキングされるのは時間の問題だ。

したがって、ハードウェアトークンの紛失時に、その連絡を受けたネットワーク管理者が直ちに行うことは、VPN サーバの認証システム本体で、紛失した利用者 ID を停止することである。

よって、その旨を解答すればよい。

さて、既に正解は得られたが、念のため、他の紛失した機器の利用者 ID についても確認しておこう。もしかしたら、他にも行うべきことがあるかもしれないからだ。

ただ、あらかじめ断っておくと、他に考慮することは何もないという結論に至る。

## ●タブレット端末

本文は、タブレット端末の OS やアプリについて特に何も述べていない。利用者 ID が登録されていることを示唆する記述もない。

仮に、タブレット端末の OS がスマートフォンと同じものであれば、利用者用のアカウントは端末ごとに一つであり、そもそも「利用者 ID」を端末に登録しない。

タブレット端末からインターネットへの接続はモバイル Wi-Fi ルータを用いているため、タブレット端末には SIM が装着されていないことが分かる。したがって、SIM カードの契約者 ID を端末に関連付けて考察する必要もない。

一般的に言って、タブレット端末には VPN 接続の登録情報があるので、タブレット端末の紛失時に不正利用を防止することは、VPN サーバの不正アクセスの防止に寄与する。通常、そのために端末起動時にパスワード認証や生体認証を実施していると考えられる。とはいえ、これは、紛失前にあらかじめ設定するものである。

したがって、いろいろな角度から考察してみたものの、本問の解を導くに当たって、タブレット端末は考慮しなくてよいことが分かる。

### ●モバイル Wi-Fi ルータ

モバイル Wi-Fi ルータの利用者 ID について、[LTE 回線を用いたインターネット接続の検討] の第 1 段落の中に、「モバイル Wi-Fi ルータには、通信事業者が契約者を識別する情報が記録されている SIM カードが挿入されている。モバイル Wi-Fi ルータには、利用者 ID やパスワードといった認証情報に加えて、……APN の情報を設定する」という記述がある（空欄ウ、エを補填）。

「利用者 ID……を設定する」とあるので、SIM カードに記録された契約者の ID とは別のものを指している。契約者の情報は SIM カードに記録済みであり、モバイル Wi-Fi ルータにわざわざ設定するものではないからだ。

「利用者 ID やパスワードといった認証情報」とあるので、モバイル Wi-Fi ルータの設定を行うために Web ブラウザからログイン認証するとき求められる、ID とパスワードを指していると考えられる。それゆえ、「VPN サーバへの不正アクセスの防止」とは無関係である。なお、製品依存の話であるが、この ID は固定値でありパスワードだけで認証している製品が多いようだ。

一般的に言って、モバイル Wi-Fi ルータを紛失したとき、管理者が行うべきことがある。それは、「モバイル Wi-Fi ルータの不正利用の防止」である。そのために講ずる有効な手段は、遠隔ロックである。すなわち、紛失時に通信事業者に連絡し、SIM カードを利用停止にすることで、当該 SIM カードを装着したモバイル Wi-Fi ルータから LTE 回線に接続できないようにするわけだ。

とはいえ、ここで問われているのは「VPN サーバへの不正アクセスの防止」であるから、論点がずれている。さらに、前述のとおり、本文中の「利用者 ID」は、SIM カードの契約者情報とは異なるものと考えられる。したがって、遠隔ロックという観点からは、解を導くことはできない。

そもそも、VPN サーバの IP アドレスを割り出すことさえできれば、紛失したモバイル Wi-Fi ルータを使わずとも、VPN サーバに接続することまでは行える。それゆえ、VPN サーバの不正アクセス防止という目的に照らすと、紛失した時点で、モバイル Wi-Fi ルータに対し有効な手段を講ずる余地はない。

したがって、本問の解を導くに当たって、モバイル Wi-Fi ルータは考慮しなくてよいことが分かる。本文中にモバイル Wi-Fi ルータの利用者 ID に関する記述はあったものの、本問とは無関係だ。

### ●解の導出

ハードウェアトークンの解説で述べたとおり、紛失した利用者 ID についてネットワーク管理者が行うことは、VPN サーバの利用者 ID を停止することである。この措

置を講ずることによって、VPN サーバへの不正アクセスを防止することができる。  
よって、正解は「VPN 接続の利用者 ID を停止する」となる。

## (2)

## 解答例

プロキシサーバと内部 DNS サーバへの通信 (20 字)

問題文は、「本文中の下線⑤について、許可するとしている通信を、図 1 中の字句を用いて……答えよ」と記述されている。

下線⑤は、「VPN 接続の検討」の第 4 段落にある。そこには、「不正アクセスが行われた際の影響を最小限にとどめるために、⑤ VPN 接続で許可する通信を必要最小限に設定する」と記述されている。

タブレット端末の VPN 接続時の通信について、「モバイルネットワークの検討」の第 2 段落、4 番目と 5 番目の箇条書きに、次のように記述されている。

- ・タブレット端末は、VPN サーバと VPN 接続を行い、VPN 接続後の名前解決は、内部 DNS サーバを用いて行う。
- ・タブレット端末から販売管理サーバ及びインターネット上のサーバへの通信は、VPN 接続を通して、プロキシサーバ経由で行う。

4 番目の箇条書きから、VPN 接続後の名前解決のために、内部 DNS サーバとの通信を許可することが分かる。

5 番目の箇条書きから、VPN 接続後に販売管理サーバ及びインターネット上のサーバにアクセスするために、プロキシサーバとの通信を許可することが分かる。

よって、正解は「プロキシサーバと内部 DNS サーバへの通信」となる。

## ■設問 4

### (1)

#### 解答例

機能名： 

プ	ロ	キ	シ	認	証
---	---	---	---	---	---

 (6字)

設定内容： 

営	業	員	ご	と	に	利	用	者	I	D	を	登	録	す	る	。
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

 (17字)

問題文は、「本文中の下線⑥について、プロキシサーバに必要な機能名を……答えよ。また、営業員を特定するために必要な設定内容を……述べよ」と記述されている。

下線⑥は、「プロキシサーバの検討」の第1段落にある。そこには、「プロキシサーバは、タブレット端末の通信ログを取得する目的で利用し、⑥プロキシサーバのログから各営業員を特定できるようにする」と記述されている。

したがって、ここで問われていることは、プロキシサーバの通信ログから営業員を特定するための機能名及び設定内容である。

プロキシサーバを経由する通信は、図1中のセグメント(E)内で行われている。タブレット端末のIPアドレスは、VPN接続時にVPNサーバから動的に割り当てられたものである。したがって、このIPアドレスから営業員を特定することはできない。

ここまで考察したところで、あとは一般的な知識から解を導く。

プロキシサーバの中には、認証機能をもつ製品がある。この機能を用いることで、プロキシサーバを経由した通信を行う際、正規の利用者にだけ通信を許可し、その通信ログを取得することができる。その通信ログを見れば、いつ誰がどのような通信を行ったかが分かる。

したがって、営業員ごとに利用者IDをプロキシサーバに登録し、利用者認証を実施することにより、下線⑥にある「プロキシサーバのログから各営業員を特定」することが可能となる。

よって、正解は、プロキシサーバに必要な機能名が「プロキシ認証」となり、設定内容が「営業員ごとに利用者IDを登録する」となる。

## (2)

## 解答例

① 接続先ホスト名 (7字)

② 接続先ポート番号 (8字)

問題文は、「本文中の下線⑦について、HTTPS の Request-URI から取得できるログの内容を二つ挙げ（よ）」と記述されている。

下線⑦は、「プロキシサーバの検討」の第 1 段落にある。そこには、「⑦ HTTPS の場合は、HTTP と比較して取得できるログの内容が限られる」と記述されている。

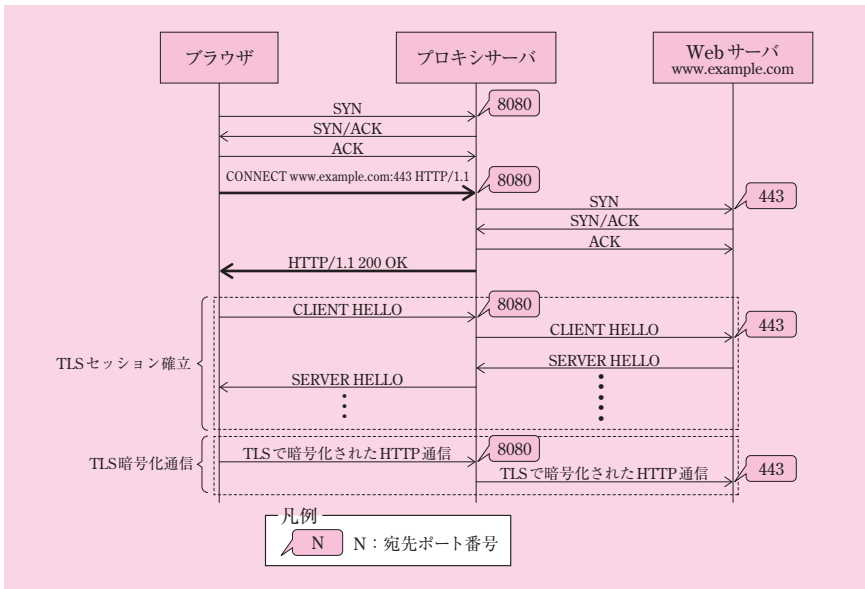
同段落の中で、このたび導入を検討しているプロキシサーバについて、「プロキシサーバは、HTTP プロキシと HTTPS プロキシの各機能をもつ」とある。

したがって、ここで問われていることは、HTTPS プロキシとして動作しているとき、HTTPS 通信のログから取得できる内容であり、そのうち、Request-URI から取得できるものである。

Request-URI とは、HTTP 通信のリクエストラインの中で、メソッド名に続いて指定されるものである。簡単に言うと、メソッドのパラメータだ。

設問 1 の空欄カで解説したとおり、プロキシサーバを経由して、クライアント端末とサーバ間で HTTPS 通信（TLS 通信）を行うとき、クライアント端末のブラウザは、プロキシサーバに CONNECT メソッドを発行する。このメソッドの中で、HTTPS 通信の接続先ホスト名と接続先ポート番号を指定する。

例えば、接続先の Web サーバを「www.example.com」とし、HTTPS 通信（TCP の 443 番ポート）をプロキシサーバ経由で行うときの動作手順は、次のとおりとなる。ここで、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

CONNECT メソッドのパラメータ「www.example.com:443」が、ここで問うている Request-URI となる。このやり取りは HTTPS 通信の開始前に行われており、暗号化されていないので、ログに平文で記録されている。

ここから取得できる内容は、「接続先ホスト名」「接続先ポート番号」である。よって、正解は解答例に示したとおりとなる。

参考までに、本文の下線⑦の直後に「システム運用上問題はない」とあるが、これは何を意味しているのだろうか。

この CONNECT メソッドのやり取りは、設問 4 (1) で解説したとおり、プロキシサーバの認証機能によって許可されている。そして、認証した利用者 ID とともに、ログに平文で記録されている。したがって、下線⑥の「プロキシサーバの通信ログから各営業員を特定する」ことは達成できているので、「問題はない」と述べているのだろう。

## 問 3

## 出題趣旨

電子メールサービスを支えるインフラ技術は、性能、信頼性、コスト、セキュリティ対策など、様々な面で、大きく発展してきた。また、電子メールは古くから利用されているサービスであり、相当に古い設備のまま運用し続けてきて、更改が必要な時期になっている企業は多いと思われる。電子メールが利用され続ける限り、メールサーバの更改や移行は、重要なテーマと考えられる。

メールサーバの更改・移行は、情報システム部門だけでなく、利用者の負担も大きく、容易ではない。標準といえる方法や手順があるわけでもなく、個々の状況や制約に応じて、計画し実行することが必要である。

本問では、メールサーバ更改を題材として、電子メールサービスを支える各種技術に対する基礎的な理解及び応用力と、利用者を含めたサービス全体を把握して、移行や運用の手順を設計・実施できる能力を問う。

## 採点講評

問 3 では、メールサーバの移行において行う、アカウント収容替えの設計、移行手順の設計、利用者への影響などに関して出題した。また、それらを行う基礎として、各種の要素技術に関しても出題した。全体として、正答率は低かった。

設問 1 の (2)、(3) は、DNS のプライマリとセカンダリの通信に関する設問である。DNS は、IP ネットワークではほぼ必ず使用される根幹の機能なので、基礎的なことは正確に理解しておいてほしい。(4) は、正答率が低かった。DNS キャッシュの影響に言及できた解答はあったが、負荷が偏りやすくなる条件を答えられた解答は少なかった。(4) の対象である MGW から MSV への通信と異なり、PC から MSV への通信では DNS ラウンドロビンを用いて負荷分散をしている。後者の通信でも DNS キャッシュが介在するが、それを理由とした負荷の偏りは生じない。この対比に気付いてほしい。

設問 2 は、VRRP と DNS の名前解決に関する基礎知識があれば、本問のような構成に初めて触れた人でも正答を導けるはずである。正答に至らなかった受験者は、よく復習してほしい。また、VRRP と DNS ラウンドロビンによる Act-Act 冗長構成は、応用の範囲が広いので、是非知っておいてもらいたい。

設問 3 は、(1) の正答率が高かったが、誤答の中には、設問文の条件に合致していない解答や、勝手な仮定に基づいたと思われる解答が多く見られた。また、(2)、(3) の正答率は低かった。この 2 問は、移行工程における、未変更社員、メール送受信サーバの変更を実施済みの社員、社外の三者間のメール転送経路を、本文に従って図 3 に書き込めば、正答にたどり着くことができる。この 2 問を正しく解答できた受験者は、他の設問の正答率も高い傾向があり、問題全体を正しく読み解いた人が多かったと推測される。

設問		解答例・解答の要点		備考
設問 1	(1)	a	ゾーン転送	
		b	SMTP	
	(2)	c	DNS1	
	(3)	公開ゾーン情報の更新通知		
	(4)	条件	送信元が少数の場合	
		理由	送信元は、DNS のキャッシュが生存している間、宛先を変えないから	

(表は次ページに続く)



設問		解答例・解答の要点		備考					
設問 2	(1)	d	新 MSV1						
		e	新 MSV2						
	(2)	<table><tr><th>ホスト名</th><th>IP アドレス</th></tr><tr><td>msvc</td><td>VIP1</td></tr><tr><td>msvc</td><td>VIP2</td></tr></table>		ホスト名	IP アドレス	msvc	VIP1	msvc	VIP2
ホスト名	IP アドレス								
msvc	VIP1								
msvc	VIP2								
設問 3	(1)	機器名	FW						
		設定変更内容	新 MSV と MGW との間の SMTP 通信を、双方向とも許可する。						
	(2)	送信元	メール送受信サーバの変更を実施済みの社員 又は 社外						
		宛先	未変更社員						
	(3)	(A)	新 MSV → 旧 MSV						
		(B)	旧 MSV						
	(4)	申請者のメールアドレスに対応するメールサーバが、新 MSV に変更される。							

本問は、メールサーバの更改に伴い、従来とは異なる方法でメールを転送することとし、その設計と移行を出題している。

本問は、現行ネットワーク（以下、現行 NW という）の構成、更改後のネットワーク（以下、更改後 NW という）の構成、及び、移行の工程などについて問うている。

### ●本問の全体像

事例に登場する D 社は、メールサーバ（以下、MSV という）の更改を計画している。

メールサーバの更改に当たって、次の検討が必要となる。

#### [1] 新 MSV の負荷分散の設計

新 MSV を 2 台導入する。VRRP と DNS ラウンドロビンを併用した負荷分散を実現する。

現行 NW では、社員のメールボックス（以下、MBOX という）は、MSV に分散収容していた。更改後 NW では、2 台の新 MSV でストレージを共有し、同ストレージに MBOX を配置する。

#### [2] 移行によるネットワークの変更

現行 NW から継続して使用する DNS サーバ、メールゲートウェイ（以下、

MGW という), FW について, 設定変更が必要となる。

現行 NW では, 社員の MBOX 収容先である MSV を検索するため, LDAP を用いていた。移行完了後, 更改後 NW では LDAP が不要になる。

### [3] 移行の工程

社員は, 移行期間中の任意の日時に, メール送受信サーバを新 MSV に変更する。

移行工程の計画立案に際しては, 移行期間中に, この変更を実施済みの社員(実施済み社員)と未実施の社員(未変更社員)が混在することを考慮に入れる必要がある。

これら 3 点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。

見出し	主な内容	主に対応する出題箇所	
		設問	小問
なし (序文)	現行 NW の仕様 (DNS サーバ, MGW, 旧 MSV, LDAP, FW)	1	(1) ~ (4)
現行 NW の仕様			
新メールサーバの 負荷分散の仕様	[1] 新 MSV の負荷分散の設計	2	(1), (2)
MSV の移行	[2] 移行によるネットワークの変更	3	(1), (3)
	[3] 移行の工程	3	(2), (4)

## ■設問 1

### (1)

#### 解答例

a : ゾーン転送

b : SMTP

a

空欄 a を含む文章は, [現行 NW の仕様] の (1) の中にある。そこには, 「ゾーン情報の更新時には, プライマリ DNS がセカンダリ DNS へ更新通知 (NOTIFY メッセージ) を送信する。これを契機として, a が行われる」と記述されている。

結論から言うと, 空欄 a に該当する字句は「ゾーン転送」である。

ゾーン転送とは、セカンダリ DNS がプライマリ DNS からゾーン情報を取得することである。その契機は2種類ある。

一つ目は、SOA レコードに登録されたゾーン転送のリフレッシュ期間が満了することである。この期間満了を契機に、セカンダリ DNS はゾーン転送の取得を要求する。

二つ目は、プライマリ DNS からセカンダリ DNS への更新通知である。更新通知を受信したことを契機に、セカンダリ DNS はゾーン転送の取得を要求する。空欄 a は、この二つ目のケースに該当している。

ゾーン転送は、セカンダリ DNS よりもプライマリ DNS のゾーン情報のバージョンが新しい場合にのみ行われる。そのバージョンは、SOA レコードのシリアル番号に登録されている。2種類あるゾーン転送の契機のいずれにおいても、セカンダリ DNS は、ゾーン転送に先立ってこれをチェックしている。

b

空欄 b は、〔現行 NW の仕様〕の表1「DMZ 上の機器と MSV 及び DNS との間で許可されている通信」の項番1, 2のルールにある。そのプロトコルが空欄 b である。

項番1は、送信元が「MGW1, 2」であり、宛先が「MSV1」である。

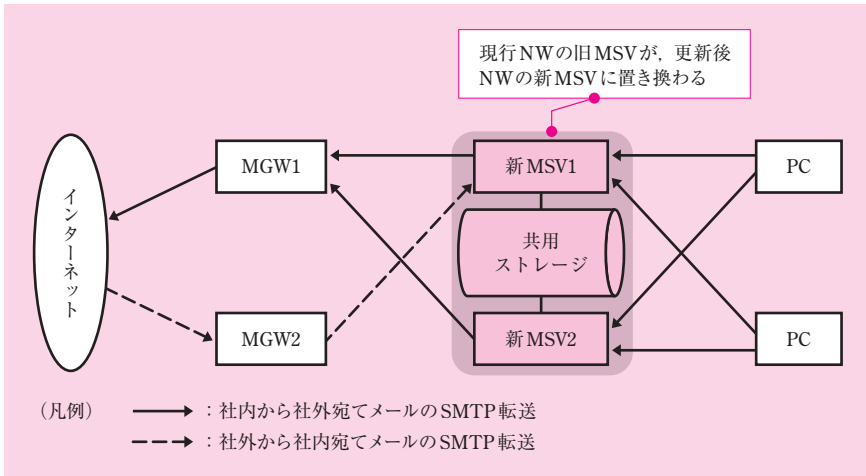
項番2は、送信元が「MSV1～3」であり、宛先が「MGW1, 2」である。

そのどちらも、通信する機器がメールサーバ（旧 MSV）又は中継メールサーバ（MGW）である。それゆえ、現行 NW のメール転送に関する記述が、解を導く鍵となるはずだ。

### ●現行 NW のメール転送経路

現行 NW のメール転送経路を探る上での重要なヒントが、図2「社内-社外間の正常時のメール転送経路」である。

この図は、更新後 NW のメール転送経路を示している。ここに登場するのは新 MSV であるが、これは旧 MSV から置き換わったものであるため、現行 NW の転送経路を推論する手掛かりを与えてくれるはずだ。



図：更新後 NW における、社内 - 社外間の正常時のメール転送経路（本文の図 2）

この図を踏まえ、現行 NW、及び、現行 NW から更新後 NW への変化に関する記述を幾つか確認してみよう。

まず、現行 NW のメール転送について、〔現行 NW の仕様〕の (3) の中に「MGW の転送先は MSV1 に固定している」、(4) の中に「社内から社外へのメールは MGW1 が、社外から社内へのメールは MGW2 が中継先として選択される。一方の MGW が停止しているときは、他方の MGW が……中継先として選択される」と記述されている。

次いで、更新後 NW のメール転送について、〔新メールサーバの負荷分散の仕様〕の (4) の中で、「メールの転送方向に応じた MGW の選択方法は、〔現行 NW の仕様〕の (4) から変更しない」と記述されている。

したがって、図 2 の新 MSV を旧 MSV に置き換えて考えたとき、MGW の前後の転送経路は変化しないことが分かる。つまり、図 2 を踏まえると、次のように推論できる。

- 社外から社内宛て：インターネット → MGW2 → MSV1
- 社内から社外宛て：旧 MSV (MSV1 ~ 3 の 3 台) → MGW1 → インターネット

さて、設問 1 (1) の解説としてはここまで分かれば十分であるが、他の設問を解くための準備も兼ねて、現行 NW の転送経路を完成させよう。残るは、PC と旧 MSV の経路である。

そのためには、現行 NW における、PC のメールソフトに設定されている送受信メールサーバを確認すればよい。

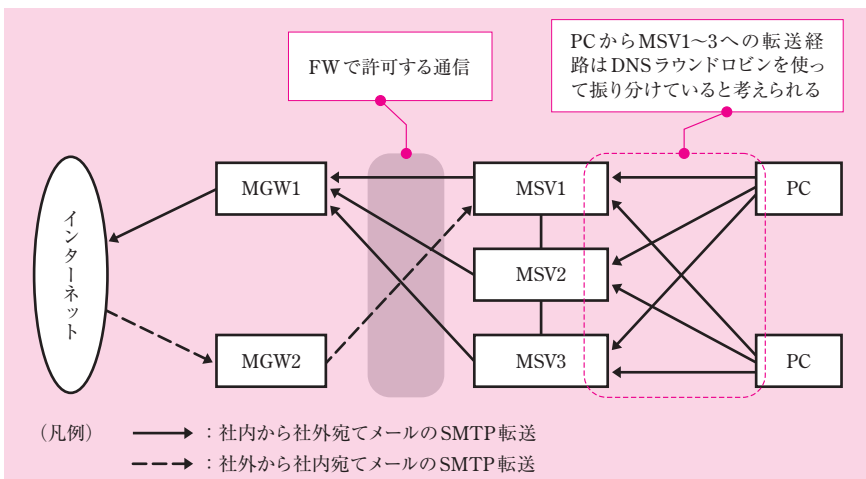
表 2「MSV 移行工程の概要」の「移行工程」の中で、「PC と新 MSV の間でメール送受信を行えるように、PC のメールソフトのメール送受信サーバ設定に、新 MSV を追加する。また、旧 MSV の使用も継続できるように、旧 MSV の設定は残す」と記述されている。さらに、「終了工程」の中で、「各社員は、PC のメールソフトのメール送受信サーバ設定から、旧 MSV の定義を削除する」とも記述されている。

したがって、現行 NW において、PC のメールソフトに設定されている送受信メールサーバに設定されているのは、旧 MSV であることが分かる。

PC から旧 MSV (MSV1 ~ 3) への転送経路は、本文に明記されていないが、DNS ラウンドロビンを使って振り分けていると考えられる。なぜなら、[現行 NW の仕様]の(2)の中に、MSV1 ~ 3 がメールを「受信」し、次いで「メールルーティング」するとあるからだ。MGW2 は MSV1 に送信する以上、PC が MSV1 ~ 3 のどれか 1 台に送信していることになる。

- 社外から社内宛て：インターネット → MGW2 → MSV1
- 社内から社外宛て：PC → 旧 MSV (MSV1 ~ 3 のどれか 1 台) → MGW1 → インターネット

これまでの考察を踏まえ、現行 NW における、社内 - 社外間の正常時の転送経路を示す。



図：現行 NW における、社内 - 社外間の正常時のメール転送経路

### ●解の導出

現行 NW のメール転送経路について理解できたので、いよいよ解を導こう。

FW は、前図の MGW と MSV の間にある。

正常時のメール転送が成立するには、MGW と MSV の間の SMTP 通信を許可する必要がある。表 1 の表記に従うと、FW のフィルタリングルールを次のように記述できる。

表：正常時の許可すべき SMTP 通信

転送の方向	送信元	宛先	プロトコル
社外から社内宛て	MGW2	MSV1	SMTP
社内から社外宛て	MSV1 ～ 3	MGW1	SMTP

それでは、MGW が停止した場合はどうなるだろうか。先ほど引用した「現行 NW の仕様」の (4) の中に「社内から社外へのメールは MGW1 が、社外から社内へのメールは MGW2 が中継先として選択される。一方の MGW が停止しているときは、他方の MGW が……中継先として選択される」と記述されている。

FW のフィルタリングルールは停止時にも対応している必要がある。それゆえ、MGW1 に許可すべき通信は MGW2 にも許可する必要がある、その逆も然りである。

したがって、正常時と停止時の両方に対応するには、フィルタリングルールを次のように改めることになる。書き加えた部分を網掛けで示す。

表：正常時及び停止時の許可すべき SMTP 通信

転送の方向	送信元	宛先	プロトコル
社外から社内宛て	<u>MGW1</u> , MGW2	MSV1	SMTP
社内から社外宛て	MSV1 ～ 3	MGW1, <u>MGW2</u>	SMTP

表 1 の項番 1, 2 を、この表と見比べてみよう。

すると、項番 1 は「社外から社内宛て」のルールと一致し、項番 2 は「社内から社外宛て」のルールと一致することが分かる。

このメール転送に使われているプロトコルが、空欄 b の解となる。当然ながら、それは SMTP である。

よって、空欄 b に該当する字句は「SMTP」となる。

## (2)

## 解答例

c : DNS1

c

空欄 c は、〔現行 NW の仕様〕の表 1「DMZ 上の機器と MSV 及び DNS との間で許可されている通信」の項番 3 のルールにある。

項番 3 は、送信元が「DNS3」であり、宛先が空欄 c である。プロトコルが「DNS プロトコル」である。

現行 NW の DNS について、〔現行 NW の仕様〕の (1) の中に「プライマリ DNS は DNS1 である。……DNS3 は公開ゾーン情報だけを保有するセカンダリ DNS である。プライマリ DNS はセカンダリ DNS とだけ通信を行う」と記述されている。

表 1 の表題から分かるとおり、通信の一方が DMZ 上の機器であるならば、もう一方は「MSV」又は「DNS」となる。それゆえ、項番 3 の送信元が DNS3 であるので、宛先は「MSV」又は「DNS」である。

項番 3 のプロトコルは、DNS である。DNS3 は公開ゾーン情報用のセカンダリ DNS であるが、これを送信元とする DNS 通信として、何が考えられるだろうか。設問 1 (1) 空欄 a で解説したとおり、これはゾーン転送である。ゾーン転送は、送信元がセカンダリ DNS であり、宛先がプライマリ DNS だからだ。

前述のとおり、現行 NW では、プライマリ DNS は DNS1 である。したがって、これが項番 3 の宛先となる。

よって、空欄 c に該当する字句は「DNS1」となる。

## (3)

## 解答例

公開ゾーン情報の更新通知 (12字)

本問は、「表 1 中の項番 4 で許可されている通信では、どのような情報が送信されるか」を問うている。

項番 4 は、送信元が「DNS1」であり、宛先が「DNS3」であり、プロトコルが「DNS

プロトコル」である。

〔現行 NW の仕様〕の (1) の中にあるとおり、DNS1 はプライマリ DNS であり、DNS3 は公開ゾーン情報用のセカンダリ DNS である。

設問 1 (1) 空欄 a で解説したとおり、本事例では、プライマリ DNS がセカンダリ DNS へ更新通知を送信することを契機として、ゾーン転送が行われる。この通信は、まさしく項番 4 に符合している。

よって、正解は「公開ゾーン情報の更新通知」となる。

試験では、事例に特化した具体的な記述があるならば、その点に着目し、その具体的な内容を踏まえて解を導く必要がある。本問の場合、DNS3 が「公開ゾーン情報だけ」を保有するセカンダリ DNS であることを見落とさないように気をつける必要がある。

## (4)

### 解答例

条件：送信元が少数の場合 (9字)

理由：送信元は、DNS のキャッシュが生存している間、宛先を変えないから (32字)

問題文は、「本文中の下線①は、送信元によって選択される宛先に偏りが生じやすく、その偏りが長時間継続しやすいからである。宛先に偏りが生じやすくなる条件を……述べよ。また、その偏りが継続しやすい理由を……述べよ」と記述されている。

下線①は、〔現行 NW の仕様〕の (3) の中にある。そこには「① MGW から MSV へのメール転送は、DNS ラウンドロビンを用いても、負荷の偏りが生じやすい」と記述されている。

したがって、ここで問われていることは、次の二つである。

一つ目は、DNS ラウンドロビンを用いたとしても、「送信元によって選択される宛先に偏りが生じやすくなる条件」である。

二つ目は、その偏りが「長時間継続しやすい理由」である。

### ● DNS ラウンドロビンを用い、どの経路を負荷分散するか

DNS ラウンドロビンとは、一つのホスト名に対して複数個の A レコードを事前に登録しておき、当該ホスト名の名前解決の問合せに対し、登録した A レコードの IP ア



ドレスを順繰りに回答していく方式である。

DNS ラウンドロビンを用いると、名前解決後にクライアントがアクセスする IP アドレスが順次異なっているため、アクセス経路の負荷分散を実現することができる。

本問を解くためには、下線①の中で「DNS ラウンドロビンを用いても」と述べられている、その適用箇所を見定める必要がある。「MGW から MSV へのメール転送」の経路上のどの部分に DNS ラウンドロビンを用い、負荷分散しようと考えたのだろうか。

その考えに沿って検討したところ、ある事情（本問の解）が判明し、「DNS ラウンドロビンを用いても、負荷に偏りが生じる」（下線①）という結論に至る。その検討結果に基づき、現行 NW において、MGW から MSV へのメール転送経路は、負荷分散していないのである。

その転送経路は、設問 1 (1) 空欄 b の解説中の図「現行 NW における、社内-社外間の正常時のメール転送経路」に示している。MGW から MSV へのメール転送は、次のとおりである。

インターネット → MGW2 → MSV1

DNS ラウンドロビンを用いて負荷分散できる経路として、二つの候補がある。これらを、経路 A、B と呼ぶことにしよう。

[経路 A] MGW1 ～ 2 → MSV1

現行 NW では、外部に公開している MX レコードのホスト名（仮に MGW とする）に対し、1 個の A レコードを対応付けている。その A レコードに指定した IP アドレスは、MGW2 である。

このホスト名 MGW に DNS ラウンドロビンを適用し、2 個の A レコードを対応付ける。1 個目の A レコードに MGW1 の IP アドレスを、2 個目の A レコードに MGW2 の IP アドレスを、それぞれ指定しておく。

この結果、社外から社内宛でのメール転送経路は、次に示す 2 パターンとなる。つまり、二つの経路に分散させてメールを転送できる。

- インターネット → MGW1 → MSV1
- インターネット → MGW2 → MSV1

[経路 B] MGW2 → MSV1 ～ 3

現行 NW では、旧 MSV（MSV1 ～ MSV3）のホスト名に対し、それぞれ 1 個

ずつ、A レコードを対応付けている。

ホスト名 MSV を新たに設け、これに DNS ラウンドロビンを適用し、3 個の A レコードを対応付ける。1 個目の A レコードに MSV1 の IP アドレスを、2 個目の A レコードに MSV2 の IP アドレスを、3 個目の A レコードに MSV3 の IP アドレスを、それぞれ指定しておく。

この結果、社外から社内宛てのメール転送経路は次に示す 3 パターンとなる。つまり、三つの経路に分散させてメールを転送できる。

- インターネット → MGW2 → MSV1
- インターネット → MGW2 → MSV2
- インターネット → MGW2 → MSV3

繰り返すが、本問を解くためには、「経路 A、B のどちらを負荷分散するか、あるいは両方とも負荷分散するか」を見定める必要がある。しかしながら、そのためのヒントが、本文にも問題文にも見出せないのだ。

実は、試験センターの公表した解答例を見ると、本問では経路 A のみ負荷分散することを想定していることが分かる。今ここを読んでいる皆さんは、試験センターの解答をどのように導出するかを知りたいと思っておられることだろう。

そこで、本書としては、ヒントが足りない点を過度に問題視せず、試験センターの出題趣旨に沿って、経路 A という想定でこのまま解説を続けることにする。

なお、不十分ながら、経路 A を示唆する記述が本文に存在している。その点は、「●参考：試験センターの用意したヒント」の中で、後ほど取り上げることにしよう。

### ●なぜ偏りが生じるのか

本問では、前述のとおり、外部に公開している MX レコードのホスト名 (MGW) の名前解決に、DNS ラウンドロビンを適用すると想定している。このホスト名の名前解決に対し、DNS サーバは、MGW1、MGW2 の IP アドレスを交互に繰り返して回答することになる。

問題文に「送信元によって選択される宛先に偏りが生じやすく」とあるが、この送信元は社外メールサーバであり、宛先は MGW1 又は MGW2 である。

もしも、社外メールサーバが D 社にメールを転送するたびに、その宛先となる MGW の名前解決が行われるならば、MGW1、MGW2 に向けて送信されるメールの数は、それぞれ同じ数になるはずだ。つまり、均等に負荷分散されることになる。

ここで、「社外メールサーバが D 社にメールを送信するたびに、その宛先となる MGW の名前解決が行われるならば」という前提を置いたことに、注目していただき

たい。

DNS サーバに名前解決を問い合わせた DNS クライアントは、その回答を一定期間、キャッシュする仕様になっている。キャッシュの有効期間は、DNS サーバ側で指定している。

ここで問われているメール転送において、この DNS クライアントに該当するのは、社外メールサーバだ。宛先となる MGW の名前解決を行ったら、キャッシュの有効期間中、宛先を変えないのである。つまり、1 台の MGW にのみ転送し続けるのだ。

具体例を挙げて説明しよう。仮に送信元となる社外メールサーバが 30 台あるとし、それらは個々に独立した存在であるとしよう。以下、それらを丸数字 (①～③⑩) で表記する。

それぞれの社外メールサーバは、初めはキャッシュをもたないものとする。1 通目のメール転送の際、D 社の MX レコードを問い合わせ、そのホスト名 MGW の名前解決が行われる。

この結果、30 台の社外メールサーバは、MGW の IP アドレスを次のようにキャッシュする。ここでは、数字の昇順でメールを転送してくるものとしている。

表：社外メールサーバがキャッシュする、MGW の IP アドレス

社外メールサーバ	キャッシュする IP アドレス
①③⑤⑦⑨……⑲⑲	MGW1
②④⑥⑧⑩……⑳⑳	MGW2

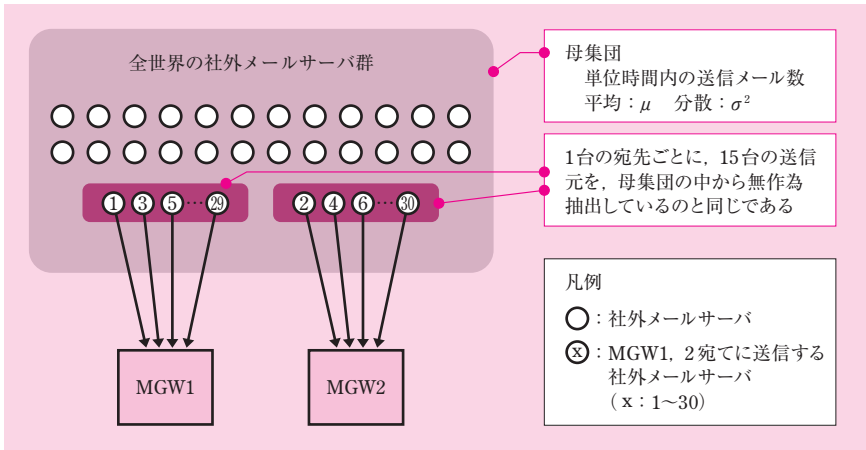
キャッシュの有効期間中、社外メールサーバは、2 通目、3 通目のメールを送信してくる。このとき選択される宛先は、キャッシュされた MGW の IP アドレスだ。

つまり、ある 15 台の社外サーバ (①, ③, ……⑲) が、MGW1 に対してメールを送信してくる。もちろん、別の 15 台の社外サーバ (②, ④, ……⑳) も、MGW2 に対して同様である。

ここで、全世界の社外メールサーバについて、「単位時間内に送信するメールの数は、何らかの分布に従っている」と仮定する。この単位時間の長さをキャッシュ有効期間に合わせたときの、送信メール数の平均値を  $\mu$ 、分散を  $\sigma^2$  としよう。

このとき、ある 15 台の社外サーバ (①, ③, ⑤……⑲) は、この分布に従う母集団 (全世界の社外メールサーバ群) の中から、15 台を無作為抽出したものと同等である。もちろん、別の 15 台の社外サーバ (②, ④, ⑥……⑳) も同様である。

つまり、「1 台の宛先に対して、15 台の送信元を無作為抽出する」という行為を、2 回行っているのと同じである。1 回目は MGW1、2 回目は MGW2 に対するものだ。



図：無作為抽出した社外メールサーバ 15 台が、MGW1, 2 にメールを送信する様子

1 回目の無作為抽出で得た 15 台 (①, ③, ⑤……②⑨) について、社外メールサーバ 1 台当たりの送信メール数を計算してみる。つまり、単位時間内の送信メール数の合計 (15 台全部) を求め、これを台数 (15) で割った数を計算する。要するに、平均値を求めるわけだ。この値を  $\bar{X}_1$  としよう。

同様に、2 回目の無作為抽出で得た 15 台 (②, ④, ⑥……③⑩) について、社外メールサーバ 1 台当たりの送信メール数を計算する。この値を  $\bar{X}_2$  としよう。

この  $\bar{X}_1$ ,  $\bar{X}_2$  は、標本平均と呼ばれる統計量である。標本平均が従う分布は、中心極限定理に基づき、次のとおりとなる。ここで、 $n$  は標本の数を表しており、本例では 15 である。

#### 〔中心極限定理〕

標本平均  $\bar{X}$  は、標本数  $n$  を大きくすると、平均が  $\mu$ 、分散が  $\sigma^2/n$  の正規分布に近づく。

統計学にあまり詳しくない読者がおられるだろうから、簡単に説明しよう。

$\bar{X}_1$  は、MGW1 宛てに送信される、キャッシュ有効期間中の社外メールサーバ 1 台当たりのメール数 (平均値) である。同様に、 $\bar{X}_2$  は、MGW2 宛てに送信される、そのメール数 (平均値) だ。

この  $\bar{X}_1$ ,  $\bar{X}_2$  は、母集団の平均値  $\mu$  と比べたとき、大きいかもしれないし小さいかもしれない。要するに、「差」があるはずだ。

中心極限定理は、その「差」の大きさがどの程度になるかを物語っている。同定理によれば、標本数  $n$  が少なければ少ないほど、その「差」(分散:  $\sigma^2 / n$ ) がどんどん大きくなっていくのである(標本数が少なくなるにつれて正規分布の形から崩れていくが、その辺は厳密に追及せず、ずれが大きくなるという点に注目しておこう)。

別の角度から説明を加えてみよう。標本が少なければ、個々の標本(ある 1 台の社外メールサーバが送信したメール数)の影響を強く受けてしまうため、標本平均の値が、本当の平均値  $\mu$  からずれた値になる可能性が高い。

逆に言うと、標本が多ければ、個々の標本の影響が相殺されていくため、標本平均の値が、本当の平均値  $\mu$  に近い値になる可能性が高いのである。

最後に、 $\bar{X}_1$ ,  $\bar{X}_2$  を比べてみたらどうなるかを説明しよう。これまでの解説から推察できると思うが、標本が少なければ少ないほど、両者の差が大きくなる可能性が高まるのである(正規分布の 1 次結合)。この状況を指して、本文は「偏りが生じやすくなる」と述べているわけだ。

経路 A の始点である MGW1, 2 にメール転送数の偏りが生じるならば、経路 A の負荷分散の効果が損なわれることになる。

### ●解の導出

ここまで理解できれば、解を導くことができる。

問われていることの一つ目は、「送信元(社外メールサーバ)によって選択される宛先(MGW1 又は MGW2)に偏りが生じやすくなる条件」であった。

その条件とは、標本が少ない場合、すなわち、送信元となる社外メールサーバが少数の場合である。

問われていることの二つ目は、その偏りが長時間継続しやすい理由であった。

その理由とは、DNS のキャッシュが有効である間、送信元となる社外メールサーバは宛先を変えないからである。

よって、正解は解答例に示したとおりとなる。

### ●参考：試験センターの用意したヒント

「●DNS ラウンドロビンを用い、どの経路を負荷分散するか」で述べたとおり、本問の解を導くに当たって、経路 A の負荷分散(MGW1 ~ 2 → MSV1)をするという想定を置くことにした。もっとも、本問の解のとおり、この想定で検討したものの、負荷に偏りが生じてしまうわけだが。

この想定を導くヒントは、本文のどこかに存在しているのだろうか。

著者は、下線①に続く文章が、そのヒントであろうと考えている。

ひとまず、下線①に着目しておこう。本問の解を踏まえ、この記述が意味する内容を汲み取ってみる。すると、「送信元が少数であるときは、DNS ラウンドロビンを適用して経路 A を負荷分散しても、負荷の偏りが生じやすい」と述べていることが分かる。

それでは、下線①に続く、ヒントとなる文章に着目しよう。「また」という接続詞で結ばれて、「社外から届くメールを負荷分散しなくても、MSV の性能に問題がないので、MGW の転送先は MSV1 に固定している」と記述されている。

この記述が意味する内容を汲み取ってみると、「MSV の性能に問題がないので、経路 B の負荷分散 (MGW2 → MSV1 ~ 3) は必要ない」と述べていることが分かる。おそらく、これを踏まえ、「DNS ラウンドロビンを用いて負荷分散することを想定するのであれば、経路 A の方である」というロジックを組み立てたのだろう。確かに、一つの解釈としてはあり得るだろう。

しかし、このロジックには綻びがあると著者は考えている。経路 B の負荷分散を二つの観点から否定的に語ることを意図し、「また」という接続詞でつないで併記していると解釈すれば、DNS ラウンドロビンを用いた経路 B の負荷分散を想定しても、下線①の文章は意味が通るからだ。

さらに言えば、設問 1 の空欄 b で解説したとおり、PC から MSV1 ~ 3 への転送経路は DNS ラウンドロビンで振り分けていると考えられるので、経路 B の負荷分散を想定しても違和感はないからだ。

要するに、下線①に続く文章は、ヒントとして不十分なのである。経路 A、B のどちらを負荷分散するのか、論理的には断定できないからだ。

参考までに、経路 B に基づいて解を導くと、解答例の「条件」は「送信メール数が少数の場合」等としたほうが分かりやすいだろう。経路 B に作用する DNS ラウンドロビンに着目したときの「送信元」は、MGW2 の 1 台だからだ。MGW2 が保持する名前解決のキャッシュは、宛先となる MSV1 ~ 3 のうち 1 台のものとなる。ある MSV をキャッシュしている間、MGW2 はその MSV にのみメールを転送する。キャッシュ期間を単位時間とする送信メール数にばらつきが生じるため、それが少数であれば偏りが大きくなる。

## ■設問 2

設問 2 の解説に入る前に、新メールサーバの負荷分散の実現方法について解説する。

その仕様について、〔新メールサーバの負荷分散の仕様〕の第 2 段落、(2) の中に、次のように記述されている。

(2) 新 MSV1, 2 とも正常時には、PC からのアクセスが分散し、一方の故障時には他方にだけアクセスが行われるように、VRRP と DNS ラウンドロビンを併用する。

- ・  と  に、VRRP を 2 グループ設定する。それぞれのグループを VRRPg1, VRRPg2 と呼ぶ。
- ・ 新 MSV1 の実 IP アドレスは IP1, 新 MSV2 の実 IP アドレスは IP2, VRRPg1 の仮想 IP アドレスは VIP1, VRRPg2 の仮想 IP アドレスは VIP2 である。
- ・ VRRPg1 は  の優先度を高く設定し、VRRPg2 は  の優先度を高く設定する。
- ・ 新 MSV1 のホスト名は msv1, 新 MSV2 のホスト名は msv2, 新 MSV1, 2 共通のホスト名は msvc である。
- ・ PC のメールソフトのメール送受信サーバには、msvc を設定する。

まず、(2) の冒頭で、二つの要件が記述されている点に着目しよう。

一つ目は、PC から新 MSV へのアクセス分散である。その点について、「新 MSV1, 2 とも正常時には、PC からのアクセスが分散し」と記述されている。

二つ目は、新 MSV の冗長化である。その点について、「(新 MSV1, 2 とも) 一方の故障時には他方にだけアクセスが行われる」と記述されている。つまり、Active-Active 構成である。

この二つの要件を実現するために、「VRRP と DNS ラウンドロビンを併用する」と記述されているわけだ。

それでは、その具体的な実現方法を順番に解説しよう。まず、実現方法が理解しやすい、Active-Active 構成の冗長化を取り上げる。次いで、PC から新 MSV へのアクセス分散を取り上げることにする。

#### ・ Active-Active 構成の冗長化

2 台のサーバで 1 個の VRRP グループを構成することにより、2 台のサーバで Active-Standby 構成の冗長化を実現できる。VRRP グループのマスタ側が Active となり、バックアップ側が Standby となる。

とはいえ、ここで求められているのは、2 台のサーバ（新 MSV1, 2）で Active-Active 構成の冗長化を実現することである。

そのためには、2 台のサーバで 2 個の VRRP グループを構成すればよい。1 番目の簡条書きに合わせて、それぞれのグループを VRRPg1, VRRPg2 と呼ぼう。

VRRPg1 のマスタ側となるサーバと、VRRPg2 のマスタ側となるサーバを、互いに



異なるものに指定すれば、2 台のサーバで Active-Active の構成になる。

具体的には、次のように設定すればよい。

1. VRRPg1 は新 MSV1 をマスタ側とする。
2. VRRPg2 は新 MSV2 をマスタ側とする。

この結果、正常時は、VRRPg1 の仮想 IP アドレス VIP1 に接続したとき、新 MSV1 にアクセスする。VRRPg2 の仮想 IP アドレス VIP2 に接続したとき、新 MSV2 にアクセスする。

新 MSV1 の故障時は、VRRPg1 の働きによって、マスタ側が新 MSV2 に切り替わる。これにより、VIP1 に接続したとき、新 MSV2 にアクセスする。VRRPg2 の仮想 IP アドレス VIP2 に接続したときは、正常時と変わりなく新 MSV2 にアクセスする。もちろん、新 MSV2 の故障時は、ここで述べた新 MSV1、2 を入れ替えて考えればよい。

このようにして、(2) の冒頭にあるとおり、「一方の故障時には他方にだけアクセスが行われる」という要件を実現できる。

なお、前述の説明において、VRRP グループのマスタ側の設定に関し、新 MSV1、2 の立場を入れ替えても、要件自体は実現できることに留意しておこう。

実際の設定については、第 2 段落の (3) の記述を照らし合わせる必要がある。そこには、MGW から新 MSV へのメール転送について、「正常時には新 MSV1 に転送されるように、転送先を VIP1 に固定する」とある。つまり、正常時に VIP1 に接続すると、新 MSV1 にアクセスするわけだ。したがって、前に書いたとおりの設定となる。

#### ・ PC から新 MSV へのアクセス分散

5 番目の箇条書きにあるとおり、PC から新 MSV にメールを送受信するときに指定するホスト名は、「msvc」である。

このホスト名の名前解決において DNS ラウンドロビンを用いることにより、アクセス分散を実現することができる。すなわち、このホスト名に 2 個の A レコードを登録すればよい。

それでは、ホスト名 msvc に対応付ける IP アドレスとして、何を指定すればよいだろうか。

ここで、先ほど考察した「Active-Active 構成の冗長化」を考え合わせる必要がある。この要件も実現できるように設定することが求められているからだ。そのためには、次のように仮想 IP アドレスを指定すればよい。



1. ホスト名 msvc の 1 個目の A レコードには、VIP1 を指定する。
2. ホスト名 msvc の 2 個目の A レコードには、VIP2 を指定する。

このようにして、(2) の冒頭にあるとおり、「新 MSV1、2 とも正常時には、PC からのアクセスが分散 (する)」という要件を実現できる。さらに言えば、仮想 IP を用いることで、冗長化の要件も実現できる。

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

## (1)

### 解答例

d : 新 MSV1

e : 新 MSV2

問題文は、「本文中の 、 に入れる適切な機器名を、図 2 中の機器名を用いて答えよ」と記述されている。

空欄 d、e は、「新メールサーバの負荷分散の仕様」の第 2 段落、(2) の箇条書きの 1 番目と 3 番目にある。

1 番目には「とに、VRRP を 2 グループ設定する。それぞれのグループを VRRPg1、VRRPg2 と呼ぶ」とあり、3 番目には「VRRPg1 はの優先度を高く設定し、VRRPg2 はの優先度を高く設定する」とある。

設問 2 の冒頭の解説で述べたとおり、新 MSV の 2 台のサーバを Active-Active 構成にして冗長化するため、新 MSV1、新 MSV2 に VRRP を 2 グループ設定する必要がある。正常時、VRRPg1 のマスタ側は新 MSV1 となり、VRRPg2 のマスタ側は新 MSV2 となる。

VRRP の設定でマスタ側を指定する方法は、グループ内で優先度を最も高く設定することである。それゆえ、VRRPg1 のマスタ側を新 MSV1 に指定するには、新 MSV1 の優先度を高く設定すればよい。同様に、VRRPg2 のマスタ側を新 MSV2 に指定するには、新 MSV2 の優先度を高く設定すればよい。

よって、空欄 d に該当する字句は「新 MSV1」となり、空欄 e に該当する字句は「新 MSV2」となる。

## (2)

## 解答例

ホスト名	IP アドレス
msvc	VIP1
msvc	VIP2

問題文は、「本文で定義されている仕様において必要な、社内ゾーン情報に定義する 2 件の A レコードについて、そのホスト名と IP アドレスの組合せを答えよ」と記述されている。

本文で定義されている仕様を満たすには、VRRP と DNS ラウンドロビンを併用する必要がある。DNS サーバに登録する A レコードは、既に設問 2 の冒頭の解説で述べている。再掲すると、次のように設定すればよい。

1. ホスト名 msvc の 1 個目の A レコードには、VIP1 を指定する。
2. ホスト名 msvc の 2 個目の A レコードには、VIP2 を指定する。

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

機器名：FW

設定変更内容：新 M S V と M G W との間、S M T P 通信を、  
双方向とも許可する。(30 字)

問題文は、「現行 NW から移行中 NW への変更において、DNS と MGW 以外で、設定変更が必要な現行 NW の機器名を、図 3 中の機器名を用いて答えよ。また、その設定変更内容を……述べよ」と記述されている。

ここでは二つのことが問われている。

一つ目は、DNS と MGW 以外で、設定変更が必要な現行 NW の機器名である。

二つ目は、その設定変更内容である。「現行 NW から移行中 NW への変更において」

とあるので、あくまで移行中 NW の構築のために必要な変更に限る。つまり、移行工程のうち、「開始工程」で行う変更だけが、ここで問われている。

現行 NW の構成は図 1 に、移行中 NW の構成は図 3 に、それぞれ示されている。両者を見比べると、移行中 NW の構成の中で、現行 NW には存在していない機器が追加されている。それは、新 MSV1、2 の 2 台のサーバだ。

移行期間中、これら 2 台のサーバとの間で通信が行われる。その点について、〔MSV の移行〕の第 3 段落、1 番目の箇条書きの中で、「旧 MSV、新 MSV とともに、社内・社外宛てのメール送信、及び社内・社外からのメール受信を可能にする」と記述されている。

したがって、「新 MSV と MGW 間の通信」、及び、「新 MSV と PC 間の通信」が新たに追加されることが分かる。

さらに、旧 MSV の通信も移行期間中は行われているので、その変更は生じないことも分かる。つまり、既存設定の削除を意図した変更は行われなわけだ。したがって、本問の解を導く上で、こちらは考慮から外してよい。

それでは、新 MSV1、2 の 2 台のサーバが関わる 2 種類の通信に着目して、どの機器に対し、どのような変更が必要となるかを考察してみよう。

### ●新 MSV と MGW 間の通信

まず、新 MSV と MGW 間の通信について考察しよう。

変更が必要な機器を列举すると、DNS、MGW、FW となる。その変更内容は次のとおりとなる。

#### ・ DNS

設問 2 (2) で解説したとおり、DNS ラウンドロビンを設定する。

#### ・ MGW

表 2 「MSV 移行工程の概要」の中の「開始工程」にあるとおり、「MGW1、2 の、社内宛てメールの転送先 IP アドレスを、VIP1 に変更する」。

#### ・ FW

新 MSV と MGW の通信経路上に FW がある。したがって、両者の SMTP 通信を双方向とも許可するために、フィルタリングルールを設定する。

なお、新設される新 MSV には、VRRP の設定、共有ストレージの MBOX の設定な

どが必要となる。しかし、ここで問われているのは、現行 NW から存在する機器についてである。したがって、本問の解を導く上で、新 MSV は考慮から外してよい。

### ●新 MSV と PC 間の通信

次いで、新 MSV と PC 間の通信について考察しよう。

変更が必要な機器を列举すると、PC、LDAP となる。

表 2「MSV 移行工程の概要」の中の「移行工程」の中で、「社員ごとに、メール送受信サーバを新 MSV に変更する」と記述されている。

そこを読み進めると、そのための変更は、PC に対するものと、LDAP に対するものの二つあることが分かる。

この記述が「移行工程」の中にあることから分かるとおり、これらの機器に対する変更は、移行期間中に行われるものである。

ここで問われているのは、移行中 NW の構築のために必要なものであり、移行開始時点までに済ませておくべき変更である。したがって、本問の解を導く上で、PC と LDAP は考慮から外してよい

### ●解の導出

新 MSV1, 2 の 2 台のサーバに関わる 2 種類の通信に着目して考察したところ、DNS と MGW 以外で、設定変更が必要な現行 NW の機器は、「FW」であることが分かる。

その設定変更内容は、「**新 MSV と MGW との間の SMTP 通信を双方向とも許可する**」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

送信元：メール送受信サーバの変更を実施済みの社員 又は 社外  
宛先：未変更社員

問題文は、「本文中の下線②が必要な理由は、移行期間中に、どのような送信元と宛先のメールが送受信されるからか。その組合せを一つ答えよ」と記述されている。

下線②は、「MSV の移行」の第 3 段落、2 番目の箇条書きにある。そこには、「②新 MSV も、旧 MSV と同様に、LDAP の情報を用いてメールルーティングを行う」と記

述されている。

LDAPに登録している情報、及び、メールルーティングについて、〔現行NWの仕様〕の第1段落、(2)の中で、次のように記述されている。

社員のメールボックス（以下、MBOXという）は、MSV1～3に分散収容しており、メールアドレスとそのMBOXを収容するMSVとの対応を、LDAPに登録している。MSV1～3は、LDAPを参照して、受信したメールの宛先メールアドレスに対応するMBOXが収容されているMSVを決定し、他のMSVへの転送、又は自分のMBOXへの格納を行う。この動作をメールルーティングと呼ぶ。

LDAPに登録されている情報は、「メールアドレスに対応するMBOXが収容されているMSV」である。

表2「MSV移行工程の概要」によれば、移行期間中、現行NWの設定のまま旧MSVを使い続けている社員がいることが分かる。このような社員を「未変更社員」と呼ぶ。

ここに記述されたメールルーティングの動作は、現行NWのMSVに当てはまる。新MSVがこれを行うときは、「LDAPを参照して、受信したメールの宛先メールアドレスに対応するMBOXが収容されている旧MSVを決定（する）」ところまでは同じで、その後は「その旧MSVに転送する」と考えればよい。

旧MSVが収容するMBOXを使い続けているのは、未変更社員に他ならない。

以上より、新MSVがメールルーティングを行うときの条件が推論できる。それは、「新MSVが未変更社員宛てのメールを受信し、これを旧MSVに転送する」というものである。

移行期間中、そのようなメールが転送されるケースとして、次の二つが考えられる。

#### 1. 社外から、未変更社員宛てに、メールを送信するケース

表2の「開始工程」の中で、「MGW1, 2の、社内宛てメールの転送先IPアドレスを、VIP1に変更する」と記述されている。したがって、MGWが受信したメールは、VIP1宛てに転送されることが分かる。仮想IPアドレスVIP1が割り当てられているのは、正常時は新MSV1であり、その故障時には新MSV2である。要するに、新MSVだ。

それでは、MGWから新MSVに転送される社内宛てメールは、どこが送信元なのだろうか。それを知るには、MGWが受け取る、社内宛てのメールを確認すればよい。

まず、現行 NW の転送経路について確認しておこう。〔現行 NW の仕様〕の（４）の中で、「社外から社内へのメールは MGW2 が中継先として選択される」とあるので、社外から社内宛でのメールは MGW2 に転送される。

次いで、この転送経路が移行期間中及び更新後に変更されるかどうかについて、確認しておこう。〔新メールサーバの負荷分散の仕様〕の（４）の中で、「メールの転送方向に応じた MGW の選択方法は、〔現行 NW の仕様〕の（４）から変更しない」とあるので、前述の転送経路から変更しないことが分かる。

つまり、MGW が受け取る社内宛でのメールは、その送信元が「社外」となる。そのメールが、MGW から新 MSV に転送されるわけだ。

したがって、社外から、未変更社員宛てにメールを転送するケースで、新 MSV がメールルーティングを行うことが分かる。

## 2. メール送受信サーバの変更を実施済みの社員から、未変更社員宛てに、メールを送信するケース

表２の「移行工程」の中で、「社員ごとに、メール送受信サーバを新 MSV に変更する」と記述されている。これに続いて、「各社員は、任意の日時に、移行工程の作業を実施する」と記述されており、「メール送受信サーバの変更を実施済みの社員と、未実施の社員（未変更社員）が移行期間中に混在する」ことが示されている。

それでは、変更済み社員から、未変更社員にメールを送ったとき、メールの転送経路はどのようになるだろうか。

まず、変更済み社員の PC から、新 MSV に向けてメールが転送される。次いで、新 MSV から、旧 MSV に向けてメールが転送される。

この旧 MSV への転送に際し、未変更社員のメールアドレスの MBOX が旧 MSV (MSV1～3) のどこにあるかを、LDAP から取得する必要がある。

したがって、変更を実施済みの社員から、未変更社員宛てにメールを転送するケースで、新 MSV がメールルーティングを行うことが分かる。

### ●解の導出

新 MSV が、LDAP の情報を用いてメールルーティングを行うのは、次の二つのケースにおいてである。

1. 社外から、未変更社員宛てに、メールを送信するケース
2. メール送受信サーバの変更を実施済みの社員から、未変更社員宛てに、メールを送信するケース

本問は、この中の一つについて、送信元と宛先の組合せを答えることを求めている。  
よって、正解は次のいずれかとなる。

- 一つ目の解

送信元：社外

宛先：未変更社員

- 二つ目の解

送信元：メール送受信サーバの変更を実施済みの社員

宛先：未変更社員

### (3)

#### 解答例

(A) 新 MSV → 旧 MSV

(B) 旧 MSV

問題文は、「表 2 中の移行工程におけるメールの転送経路の例を、次の (ア)、(イ) に示す。“旧 MSV”、“新 MSV”、“→”を用いて、経路を完成させよ」と記述されている。

(ア)、(イ) の経路の一部が空欄になっており、それを解答することが求められている。

(ア) 送信元が社外、宛先が未変更社員

送信元のメールサーバ → MGW → (A)

(イ) 送信元が未変更社員、宛先が社外

送信元 PC → (B) → MGW → 宛先のメールサーバ

それでは、(ア)、(イ) の順に解いてゆこう。

#### ● (ア) 送信元が社外、宛先が未変更社員

この転送経路は、既に設問 3 (2) の中、「1. 社外から、未変更社員宛てに、メールを送信するケース」で解説している。

詳しくはそちらを参照していただき、ここでは結論を述べることにしよう。  
転送経路は次のとおりとなる。

送信元のメールサーバ→MGW→新 MSV→旧 MSV

よって、空欄 (A) に入る字句は、「**新 MSV→旧 MSV**」となる。

#### ● (イ) 送信元が未変更社員、宛先が社外

送信元が未変更社員なので、まずは現行 NW の転送経路を確認しよう。

この転送経路は、既に設問 1 (1) 空欄 b の中、「●現行 NW のメール転送経路」で解説している。

詳しくはそちらを参照していただき、ここでは結論を述べることにしよう。

転送経路は次のとおりとなる。なお、問題文で指定された表記ルールに従い、現行 NW の MSV1～3 を「旧 MSV」と記している。

送信元 PC→旧 MSV→MGW→宛先のメールサーバ

次いで、ここで問われている、移行工程中の転送経路を確認しよう。

表 2「MSV 移行工程の概要」の「移行工程」を見ると、移行工程の間、未変更社員については、現行 NW の設定を残したままにしていることが分かる。

移行期間中、旧 MSV を経由した通信が継続的に行われていることは、〔MSV の移行〕の第 3 段落、1 番目の箇条書きの中で、「旧 MSV、新 MSV とも、社内・社外宛でのメール送信、及び社内・社外からのメール受信を可能にする」と記述されていることから分かる。

したがって、未変更社員に関しては、移行工程中の転送経路は、前述の現行 NW のものと同じであると結論できる。

よって、空欄 (B) に入る字句は、「**旧 MSV**」となる。

## (4)

### 解答例

申	請	者	の	メ	ー	ル	ア	ド	レ	ス	に	対	応	す	る	メ	ー	ル	サ	ー	バ	が	,	新
M	S	V	に	変	更	さ	れ	る	。															

(35字)



問題文は、「表 2 中の下線③では、LDAP のどのような情報がどのように変更されるか」を問うている。

表 2「MSV 移行工程の概要」の「移行工程」の中で、「次の二つの実施によって、社員ごとに、メール送受信サーバを新 MSV に変更する」と記述されている。

「次の二つの実施」とは、すぐ下に記述された二つの箇条書き「(1)、(2)」を指している。

そこを見ると、この「実施」には、PC に対するものと、LDAP に対するものの二つあることが分かる。

PC については、「(1) PC と新 MSV の間でメール送受信を行えるように、PC のメールソフトのメール送受信サーバ設定に、新 MSV を追加する」と記述されている。

LDAP については、「(2) 各社員の申請に基づいて、③ LDAP の情報を変更する」と記述されている。ここに下線③が引かれている。

したがって、ここで問われているのは、PC のメール送受信サーバを新 MSV に変更することに伴い、各社員の申告に基づいて、「LDAP のどのような情報がどのように変更されるか」である。

設問 3 (2) で解説したとおり、LDAP はメールルーティングの際に参照される。移行中 NW において、これを参照するメールサーバは 2 種類ある。

一つ目は、未変更社員のメール送受信サーバである旧 MSV である。つまり、現行 NW から継続して参照している。

二つ目は、設問 3 (2) で解説したとおり、新 MSV である。

メール送受信サーバを変更済みの社員は、MBOX が新 MSV に変更される。そのため、この社員の宛先メールアドレスに基づいて MBOX を検索するとき、LDAP が回答するメールサーバは「新 MSV」でなければならない。

したがって、LDAP がこの回答を行うように、変更済み社員のメールアドレスに対応するメールサーバを、新 MSV に変更する必要がある。この変更は、各社員の申告に基づいて行われるものである。

ここで問われているのは「どのような情報がどのように変更されるか」であるから、それに合わせて答えると、正解は「**申請者のメールアドレスに対応するメールサーバが、新 MSV に変更される**」となる。