# 平成 28 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

Web コンピューティングに関する様々な技術が，開発され実用化されている。利用者が直接使う機器の多くには Web ブラウザが標準搭載されているので，ホームページアクセス以外の多様な用途にも使えるよう，機能強化や標準化が進められている。

本問では，Web コンピューティングにおけるリアルタイム通信を題材に，ネットワーク技術の応用力を問う。

WebRTC（Web Real-Time Communication）の特徴の一つは，Web ブラウザを使って，シグナリングとリアルタイム通信を実現できることである。これを通信プロトコルとして見た場合，応用される通信の特性が同じ SIP（Session Initiation Protocol）と共通点が多い。比較的新しい技術である WebRTC を，従来技術の知識を基に理解すること，そして，それを実システムの拡張計画へ応用することを中心に出題している。

### 採点講評

問 1 では，ネットワークシステムの拡張を題材に，NAT，マルチホーミング，WebRTC（Web Real-Time Communication），SIP などの技術を扱った。前半の技術検討では，比較的限定された範囲での基本的事項に関して出題したが，後半は全体を理解し考察しなければならない問題も含めた。これらの問題群を，初見，かつ，短時間で解答するのは大変だったかもしれないが，全体として，よく理解されていた。

設問 2 では，マルチホーミングの一手法について問うた。(2)は基本的な問題だが，IP 層と TCP 層の動作を勘違いしたり，技術的に不正確だったりする解答が散見された。正確で簡潔な記述を心掛けてほしい。

設問 3 は，WebRTC に関する設問で，Web ブラウザを使ったリアルタイム通信について問うている。(1)，(2)は，知識がなくても本文の記述から解答できるが，(3)，(4)はマルチホーミング環境での WebRTC 利用という応用問題であり，正答率はやや低かった。正答に至らなかった受験者は，解答例を参考に復習してほしい。また，WebRTC のような比較的新しい Web コンピューティング技術についても理解を深めてほしい。

設問 4 は，WebRTC と SIP を組み合わせた設問である。(1)を除き正答率は高かった。(1)は Websocket の知識を求めるものではなく，図 6 や HTTP の一般知識からの推論を期待した設問であるが，SIP そのものに引きずられた誤答が多かった。WebRTC と SIP はシグナリングとリアルタイム通信のための通信プロトコルという点で類似性がある。これらに馴染みのない受験者には，これを機会に復習することを薦めたい。

設問 5 では，これまでの検討内容を移行計画という軸から再確認している。設計と運用の両面から考える必要があるが，一つ一つはそれほど難しくはない。その中で，設計に関する(2)，(7)及び運用に関する(5)，(6)の正答率が低く，時間切れと思われる誤答が多かった。限られた時間で，全問に気配りすることは簡単ではないが，本問程度の量と深さには十分対応できるよう，日頃の学習や実業務での実践を積んでほしい。

©2017 ICT Workshop

| 設問 | | 解答例・解答の要点 | | 備考 |
|---|---|---|---|---|
| 設問 1 | (1) | ア | ip1/29 | |
| | | イ | 10.0.9.0/24 | |
| | | ウ | 送信元ポート番号 | |
| | (2) | 131,072 | | |
| | (3) | ① | ・許可する通信を追加する。 | |
| | | ② | ・宛先 NAT に関する定義を追加する。 | |
| 設問 2 | (1) | 異なる ISP から払い出されている。 | | |
| | (2) | 応答が行きの宛先 IP アドレスとは異なる送信元 IP アドレスから戻る。 | | |
| 設問 3 | (1) | Binding レスポンス中のデータに含まれる IP アドレスと，自分の IP アドレスを比べる。 | | |
| | (2) | ① | ・〈p〉 | |
| | | ② | ・〈g2〉 | |
| | (3) | A | vlan1 | 順不同 |
| | | B | vlan2 | |
| | (4) | エ | ブラウザ 2 の AP | |
| | | オ | STUN サーバ | |
| 設問 4 | (1) | カ | HTTP | |
| | | キ | WebSocket | |
| | (2) | ISP1 と ISP2 から払い出された IP アドレスを一つずつ割り当てる。 | | |
| | (3) | C | vlan1 | 順不同 |
| | | D | vlan2 | |
| | (4) | ク | IP-PBX | |
| | | ケ | DNS | |
| | | コ | LB | |
| 設問 5 | (1) | サ | 切り戻し | |
| | (2) | FQDN 数 | 1 | |
| | | グローバル IP アドレス数 | 4 | |
| | (3) | IP-PBX，STUN サーバ 1，STUN サーバ 2 | | |
| | (4) | FW | | |
| | (5) | ① | ・社外から Web サーバへのアクセス | |
| | | ② | ・社内から Web サーバへのアクセス | |
| | | ③ | ・社内からインターネットへのアクセス | |
| | (6) | ISP2 を経由した外向き DNS 機能を確認する。 | | |
| | (7) | ①’，③，④ | | |

©2017 ICT Workshop

本問は，Web コンピューティングにおけるリアルタイム通信を実現する技術である，WebRTC（Web Real-Time Communication）を題材に取り上げている。同技術については，本文中で詳しく説明されている。従来技術の知識に基づいてその説明を理解すること，それを実システムへ応用することが求められている。

本問は，ブラウザ上でリアルタイム通信する機能を追加するための設計，マルチホーミング導入によるネットワーク構成を変更するための設計，及び，その移行について出題している。

**●本問の全体像**

事例に登場する工務店の A 社は，施主との情報連携を強化するために，情報システムの機能拡張を構想している。

本問を理解するために，現行の機能，及び，機能拡張の構想について，それぞれ整理しておこう。

現行の機能は，次に示す三つである。

**1. 施工情報管理**

データセンタの Web サーバが管理する施工情報に，インターネットからアクセスする。このとき用いられるプロトコルは HTTPS である。

**2. コールセンタ**

公衆電話網から掛かってきた電話を，データセンタの IP-PBX を使って，コールセンタのオペレータが受け付け，必要に応じて社内の IP 電話機に転送する。

**3. インターネットアクセス**

社内のイントラネットからインターネットにアクセスする。

機能拡張の構想内容は，次に示す三つである。

**［1］マルチホーミング**

機能拡張に伴って社外との通信が重要となるため，データセンタとインターネットとの接続を二重化する。

マルチホーミングとは，二つの ISP を同時に利用するネットワークの構成を指す。マルチホーミング用の負荷分散装置（以下，LB という）の機能について，本文の〔マルチホーミング〕の中で詳しく説明されている。

**［2］ブラウザを使ったビデオ電話**

ブラウザ上で動作するアプリケーション（以下，AP という）を用い，施主と

©2017 ICT Workshop

A 社の社員がビデオ電話で交信できるようにする。

このビデオ電話は，AP 間の通信によって実現する。なお，「電話」と銘打っているが，本物の電話機を使ったやり取りではないことに留意しておこう。

この AP 間通信に WebRTC が使われている。その仕組みについて，本文の〔ブラウザを使ったビデオ電話の通信〕の中で詳しく説明されている。

**［3］ブラウザを使った音声電話**

ビデオ電話と同じ AP を用い，施主や外出先の社員が，A 社内の社員と音声電話で交信できるようにする。

これは，A 社データセンタ内の既設 IP-PBX を介し，AP と A 社内の IP 電話機との VoIP 通信によって実現する。

以上を踏まえて本問の構成を概観すると，次のように整理できる。

**表：本問の構成**

| 見出し | 主な内容 | 主に対応する出題箇所 | |
|---|---|---|---|
| | | 設問 | 小問 |
| なし（序文） | 情報システムの現行機能，機能拡張の構想内容 | — | — |
| 現行ネットワーク構成 | 現行ネットワークの IP アドレス空間，NAT，DNS ラウンドロビン | 1 | (1) ～ (3) |
| マルチホーミング | ［1］マルチホーミング | 2 | (1) ～ (2) |
| ブラウザを使ったビデオ電話の通信 | ［2］ブラウザを使ったビデオ電話 | 3 | (1) ～ (4) |
| ブラウザを使った音声電話の通信 | ［3］ブラウザを使った音声電話 | 4 | (1) ～ (4) |
| 移行計画 | ［1］～［3］のためのネットワーク移行計画案の作成 | 5 | (1) ～ (7) |

本問は，見出しと設問との対応が分かりやすいと言えよう。ただし，最後の見出し〔移行計画〕については，これ以前の見出しの内容を含めて総合的に判断することが求められている。

©2017 ICT Workshop

## ■設問 1
### (1)

**解答例**

ア：ip1/29
イ：10.0.9.0/24
ウ：送信元ポート番号

［ア］，［イ］

空欄ア，イを含む文章は，〔現行ネットワーク構成〕の第 2 段落，1 番目の箇条書きの中にある。そこには，「図 2 中のブラウザ 1 が Web サーバ 1 と Web サーバ 2 へアクセスする際に，FW の NAT 機能が宛先 IP アドレスを変換する。変換前と変換後の宛先 IP アドレスは，それぞれ表 1 中の IP アドレス空間［ア］と［イ］に属し，変換前と変換後の IP アドレスの組合せは 1:1 に固定されている（以下，宛先 NAT という）」と記述されている。

図 2 は，「A 社の現行ネットワーク構成」を示している。表 1 は，「図 2 中のスイッチに定義された現行 IP アドレス空間」を示している。

まず，ブラウザ 1 と Web サーバが，図 2 の中でどこに位置しているかを確認しよう。

ブラウザ 1 はインターネットにあり，Web サーバはスイッチ L2SW9 に収容されている。Web サーバの置かれたネットワークセグメントを，表 1 中の「用途」欄に基づき，以降の解説で「DMZ」と呼ぶことにする。

ブラウザ 1 はインターネットからアクセスするので，ブラウザ 1 が送信するパケットの宛先 IP アドレスは，ISP が A 社に払い出したグローバル IP アドレスである。このグローバル IP アドレスをもつネットワークセグメントを，表 1 中の「用途」欄に基づき，以降の解説で「ISP1 接続用セグメント」と呼ぶことにする。

次に，ISP1 接続用セグメントと DMZ の IP アドレス空間が，表 1 の中でどのように定義されているかを確認しよう。

表 1 より，ISP1 接続用セグメントは「ip1/29」であり，DMZ の IP アドレス空間は「10.0.9.0/24」であることが分かる。

次に，これまで確認した内容に基づき，Web サーバに割り当てる IP アドレスについて考察しよう。

Web サーバ 1，2 は DMZ に収容されているので，実 IP アドレスは「10.0.9.0/24」に

©2017 ICT Workshop

属している。

Web サーバ 1，2 はインターネットからアクセスされるので，公開用の IP アドレスは「ip1/29」に属している。つまり，インターネットからは，Web サーバが ISP1 接続用セグメントに存在しているように見えているわけだ。

以上を踏まえ，FW が実施している「宛先 NAT」について考察しよう。

FW は，ISP1 接続用セグメントと DMZ の境界に位置している。この FW において，ブラウザが Web サーバに向けて送信したパケットの宛先 IP アドレスが，NAT により変換される。

インターネットから Web サーバ宛てのパケットは，宛先 IP アドレスが Web サーバの公開用 IP アドレスである。これが，NAT で変換される前の IP アドレスだ。

NAT で変換された後，DMZ の Web サーバに転送されるパケットは，宛先 IP アドレスが Web サーバの実 IP アドレスである。言うまでもなく，これが，NAT で変換された後の IP アドレスだ。

これまでの解説から明らかなとおり，変換前の公開用 IP アドレスが属する空間は，「ip1/29」である。そして，変換後の実 IP アドレスが属する空間は，「10.0.9.0/24」である。

よって，空欄アに該当する字句は「**ip1/29**」となり，空欄イに該当する字句は「**10.0.9.0/24**」となる。

**ウ**

空欄ウは，〔現行ネットワーク構成〕の第 2 段落，2 番目の箇条書きの中にある。そこには，「図 2 中のブラウザ 2 がインターネットへアクセスする際に，FW の NAT 機能が送信元 IP アドレスと［ウ］の両方をそれぞれ動的に変換する（以下，送信元 NAPT という）。変換後の IP アドレス用に二つのグローバル IP アドレスが割り当てられている」と記述されている。

ブラウザ 2 が，図 2 の中でどこに位置しているかを確認してみると，イントラネットにある。それゆえ，プライベート IP アドレスが割り当てられていることが分かる。

ブラウザはインターネットにアクセスするとき FW を経由する。FW はプライベート IP アドレス空間と，ISP 接続用セグメントのグローバル IP 空間の境界に位置しているので，ここで送信元 IP アドレスが NAPT により変換される。

イントラネットからインターネット宛てに通信する端末は，多数存在する。一方，NAPT 用のグローバル IP アドレスは 2 個しかない。端末に IP アドレスを 1：1 に当てはめる方式を採るなら，高々 2 台しかインターネットにアクセスできなくなる。

同時に多数の通信を扱えるようにするため，NAPT は，送信元 IP アドレスだけでな

©2017 ICT Workshop

く，送信元ポート番号も変換する仕組みになっている。

よって，空欄ウに該当する字句は「**送信元ポート番号**」となる。

## (2)

**解答例**

131,072

問題文は，「本文中の下線（a）について，送信元 NAPT が同時に処理できる TCP コネクション数の上限を答えよ」と記述されている。

下線（a）は，〔現行ネットワーク構成〕の第 2 段落，2 番目の箇条書きの中にある。そこには，「(a) 変換後の IP アドレス用に二つのグローバル IP アドレスが割り当てられている」と記述されている。

「送信元 NAPT」とは，(1) の空欄イの解説で触れたが，イントラネット内の端末がインターネットにアクセスする際，FW が実施する NAPT を指している。

ポート番号は 16 ビットなので，取り得る数は $2^{16}$ = 65,536 通りある。この値は，1 個のグローバル IP アドレスにポート番号を組み合わせたときに NAPT が同時に処理できる，TCP コネクション数の上限値になる。

本事例の送信元 NAPT は，下線（a）にあるとおり，変換用のグローバル IP アドレスが 2 個用意されている。したがって，この上限値は 2 倍になる。すなわち，

65,536 × 2 = 131,072 通り

である。

よって，正解は「**131,072**」となる。

言うまでもなく，ここで得た数値はあくまで理論上のものである。実際には機器の性能が頭打ちとなり，実装仕様上の上限値はこれより少なくなる可能性がある。

©2017 ICT Workshop

## (3)

**解答例**

①許可する通信を追加する。（12字）
②宛先NATに関する定義を追加する。（17字）

問題文は，「本文中の下線（b）について，DNS 機能以外の FW の設定変更内容を二つ挙げ（よ）」と記述されている。

下線（b）は，〔現行ネットワーク構成〕の第 2 段落，5 番目の箇条書きの中にある。そこには，「2 台の Web サーバ（Web サーバ 1，2）は，FW の DNS ラウンドロビン機能を使って負荷分散しており，3 台以上の構成へもスケールアウトができる。（b）スケールアウトの際には，DNS 機能に関する設定変更など，FW に複数の設定変更が必要となる」と記述されている。

本問を解くには，まず，FW の機能を確認する必要がある。下線（b）を見る限り，少なくとも DNS 機能があることは読み取れるが，他にも機能があると推察される。

次に，インターネットから Web サーバにアクセスする際，それらの機能がどのように作用しているかを考察する。

最後に，Web サーバをスケールアウトしたときに，それらの機能にどのような影響が及ぶのかを考察することで，その機能が関わる設定変更が分かるはずだ。それが本問の解となる。

**●現行ネットワークで実行している，FW の機能**

第 2 段落の箇条書きを見ると，FW の機能は全部で三つあることが分かる。

**1. NAT 機能**

NAT 機能は，通信の方向に応じて異なる設定が行われている。

インターネットから入ってくる方は，1 番目の箇条書きにある，宛先 NAT である。

インターネットへ出ていく方は，2 番目の箇条書きにある，送信元 NAPT である。

**2. フィルタリング機能**

3 番目の箇条書きに「FW のフィルタリング定義は，図 1 に示す情報システムの通信だけを許可している」と記述されている。

©2017 ICT Workshop

フィルタリング機能は，まさに本来 FW が果たす機能だと言えよう。ここには「情報システムの通信だけを許可している」。

冒頭で解説したとおり，情報システムの現行機能は三つある。このうち，FW を経由する通信は，「1. 施工情報管理」の HTTPS 通信，「3. インターネットアクセス」の様々な通信である。これらを許可する設定が行われている。

**3. DNS 機能**

4 番目の箇条書きに「FW には，A 社のドメイン権限をもった DNS 機能がある」と記述されている。それゆえ，上位ドメインの DNS サーバのゾーン情報に，A 社ドメインの権威サーバとして，FW を指定していることが分かる。この権威サーバの指定は，NS レコードに登録されている。

5 番目の箇条書きに「2 台の Web サーバ（Web サーバ 1，2）は，FW の DNS ラウンドロビン機能を使って負荷分散して（いる）」と記述されている。それゆえ，インターネットに公開している Web サーバのホスト名に，2 個の IP アドレスを対応付けて登録していることが分かる。1 個目は Web サーバ 1 の公開用 IP アドレス，2 個目は Web サーバ 2 の公開用 IP アドレスである。

**● Web サーバにアクセスする仕組み**

インターネットの端末が Web サーバにアクセスするとき，これら三つの機能がどのような仕組みで作用しているかを考察しよう。

まず，Web サーバのホスト名に対する名前解決の問合せがある。DNS ラウンドロビン機能により，Web サーバ 1 又は 2 のどちらかの公開用 IP アドレスが回答される。

次に，その公開 IP アドレスを宛先に指定した HTTPS のアクセスがある。宛先 NAT 機能により，宛先 IP アドレスが Web サーバ 1 又は 2 の実 IP アドレスに変換される。

その際，フィルタリングルールで許可されているかをチェックする。これは現行の機能「施工情報管理」の通信であるため，許可される。

このような仕組みにより，インターネットからアクセスしたパケットが Web サーバに到達している。

**●スケールアウトに伴う設定変更の内容**

スケールアウトは，振分け先の Web サーバを増設することである。Web サーバにアクセスする仕組みを踏まえ，この増設がどのような影響を及ぼすか，どのような設定変更が求められているかを考察しよう。

以降の解説で，増設した Web サーバを「Web サーバ 3」と呼ぶことにする。

まず，DNS ラウンドロビン機能を考えてみる。増設したサーバも振分け先となる必

©2017 ICT Workshop

要があるので，DNS ラウンドロビンの設定に影響を及ぼすことが分かる。したがって，Web サーバ 3 の公開用 IP アドレスを新たに用意した上で，Web サーバのホスト名に，この公開用 IP アドレスとの対応付けも追加することが求められている。

次に，宛先 NAT 機能を考えてみる。Web サーバ 3 の公開用 IP アドレスを宛先に指定したアクセスがあるので，宛先 NAT の変換に影響を及ぼすことが分かる。したがって，Web サーバ 3 の公開用 IP アドレスを，その実 IP アドレスに変換する定義を追加することが求められている。

最後に，フィルタリング機能を考えてみる。Web サーバ 3 を宛先とする通信が FW を経由することになるので，フィルタリングルールの設定に影響を及ぼすことが分かる。したがって，インターネットから Web サーバ 3 への HTTPS 通信を許可するルールを追加することが求められている。

**●解の導出**

これまでの解説から，DNS ラウンドロビン機能，宛先 NAT 機能，フィルタリング機能のそれぞれについて，設定変更が必要であることが分かった。

ここで問われているのは，「DNS 機能以外の FW の設定変更内容」である。

したがって，解答する内容は，宛先 NAT の定義を追加すること，許可する通信を追加することなる。よって，その旨を字数に収まるように答えればよい。正解は解答例に示したとおりとなる。

## ■設問 2

設問 2 の解説に入る前に，LB を使ったマルチホーミングについて解説する。

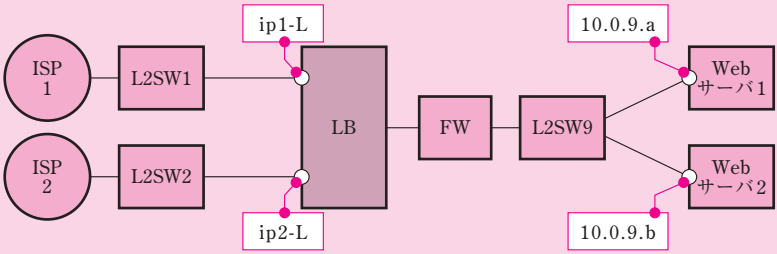
その点について，〔マルチホーミング〕の第 4 段落に，次のように記述されている。

> LB を使ったマルチホーミングの概要を次に示す。
>
> ・インターネット向けの DNS 機能を FW から LB へ移し，ISP2 を経由してもその DNS 機能を提供できるように，ドメイン登録業者に定義の追加を依頼する。その際，ISP1，ISP2 のいずれからでも同じゾーンファイルが参照されるようにする。
>
> ・LB の DNS ラウンドロビン機能を使い，インターネットから A 社内への通信の負荷分散を行う。現行の Web サーバ用のグローバル IP アドレスに，新たなグローバル IP アドレスを加え，DNS クエリに対してそれらが交互に返るようにする。

©2017 ICT Workshop

・A 社内からインターネットへの通信は，ISP1 と ISP2 への接続ポートに対して負荷分散を行う。その際，ISP へ送信する IP パケットの送信元 IP アドレスは，送信先の ISP から貸与されたグローバル IP アドレスに変換されるので，FW の NAT 機能を LB へ移して一元化する。
・LB は，通信の行きと戻りを同じ ISP 経由にする。
・LB から ISP1 のルータ及び ISP2 のルータへそれぞれ定期的に ping 確認を行い，ISP の障害を検知した場合には，正常な ISP だけを利用する。

マルチホーミングを導入した A 社の新ネットワーク構成図は，本文の図 3 に示されている。LB が関わる部分を抜粋し，様々な設定を書き添えたものを，次の図に示す。




LB の DNS ラウンドロビンの定義

```
$ORIGIN   a-sha.co.jp.

www       IN    A     ip1-Wa
          IN    A     ip2-Wa
          IN    A     ip1-Wb
          IN    A     ip2-Wb
```

LB の宛先 NAT の定義

| 接続ポート | 変換前 | 変換後 |
|---|---|---|
| ip1-L | ip1-Wa | 10.0.9.a |
| | ip1-Wb | 10.0.9.b |
| ip2-L | ip2-Wa | 10.0.9.a |
| | ip2-Wb | 10.0.9.b |

| 用語 | 意味 |
|---|---|
| www | Web サーバのホスト名 |
| ip1-XXX | ISP1 から払い出されたグローバル IP アドレス |
| ip2-XXX | ISP2 から払い出されたグローバル IP アドレス |

**図：A 社の新ネットワーク構成（LB が関わる部分を抜粋）**

以下，この箇条書きの内容に沿って，マルチホーミングの実現方法，そのために必要な LB の機能などを確認しよう。

©2017 ICT Workshop

・A 社ドメインの権威サーバの設定

以降の解説で，A 社のドメイン名を「a-sha.co.jp」とする。

1 番目の箇条書きに，「インターネット向けの DNS 機能を FW から LB へ移し，ISP2 を経由してもその DNS 機能を提供できるように，ドメイン登録業者に定義の追加を依頼する」と記述されている。

少々込み入っているので，この記述を三つに分けて解説する。

まず，「インターネット向けの DNS 機能を FW から LB へ移（す）」という記述から始めよう。

ここから，LB が A 社ドメインの権威サーバとなることが分かる。

現行ネットワークにおいて，A 社ドメインの権威サーバの定義は，上位ドメイン「co.jp」の DNS サーバに登録済みである。この DNS サーバの IP アドレスは ISP1 が払い出したものなので，ISP1 経由で DNS 機能を提供している。この IP アドレスを「ip1-L」とする。これは，現行ネットワークでは FW の DNS 機能用に割り当てられているものだ。

本文には，この DNS 機能を「FW から LB へ移（す）」とあるので，今後は LB が権威サーバとなることが分かる。そのためには，ip1-L を FW から LB の ISP1 接続ポートに移せばよい。

こうすれば，DNS クエリが LB の ISP1 接続ポートに到達するので，ISP1 経由で DNS 機能を LB が提供できる。

次に，1 番目の箇条書きの「ISP2 を経由してもその DNS 機能を提供できるように（する）」という記述について解説しよう。

これを実現するには，ISP1 経由での DNS 機能提供に実施している方法を，ISP2 経由に対しても同じように実施すればよいはずだ。

LB の ISP2 接続ポートには，ISP2 から払い出された IP アドレスが割り当てられている。これを「ip2-L」とする。

この IP アドレスを，A 社ドメインの権威サーバの IP アドレスとして公開したらどうなるだろうか。

こうすれば，DNS クエリが LB の ISP2 接続ポートに到達するので，ISP2 経由で LB が DNS 機能を提供できる。

本文には，「ISP2 を経由しても」とあるので，従来の ISP1 経由の DNS 機能に加えて，ISP2 経由の DNS 機能を提供する必要がある。それゆえ，A 社ドメインの権威サーバの IP アドレスとして，ip2-L を追加することが分かる。

最後に，1 番目の箇条書きの「ドメイン登録業者に定義の追加を依頼する」という記述について解説しよう。

©2017 ICT Workshop

前述のとおり，ドメイン登録業者に依頼する内容は，上位ドメイン「co.jp」の DNS サーバのゾーン情報に，A 社ドメインの権威サーバの IP アドレスとして，ISP2 から払い出されたグローバル IP アドレスを追加することである。そのアドレスとは ip2-L である。

この結果，LB 宛ての DNS クエリは，ISP1 経由では ISP1 接続ポートにアクセスし，ISP2 経由では ISP2 接続ポートにアクセスする。インターネットから見ると，それぞれの接続ポートが権威サーバのように映る。ISP1，2 のどちらを経由しても，LB が権威サーバとして応対することになる。

このようにして，二つの ISP を経由して，DNS 機能を提供することができる。

これまで解説した内容に基づき，上位ドメイン「co.jp」の DNS サーバに登録する，A 社ドメインの権威サーバの定義内容を次の図に示す。

DNS のゾーン情報の定義

| | | | |
|---|---|---|---|
| a-sha.co.jp. | IN | NS | ns1.a-sha.co.jp |
| a-sha.co.jp. | IN | NS | ns2.a-sha.co.jp |
| ns1.a-sha.co.jp. | IN | A | ip1-L |
| ns2.a-sha.co.jp. | IN | A | ip2-L |

| 用語 | 意味 |
|---|---|
| a-sha.co.jp. | A 社のドメイン名 |
| ns1 | LB の ISP1 側接続ポートに定義されたホスト名 |
| ns2 | LB の ISP2 側接続ポートに定義されたホスト名 |
| ip1-L | LB の ISP1 側接続ポートの IP アドレス |
| ip2-L | LB の ISP2 側接続ポートの IP アドレス |

**図：上位ドメイン（co.jp）に登録する A 社ドメインの権威サーバの定義**

**・DNS ラウンドロビンの定義**

以降の解説で，A 社の Web サーバのホスト名を「www」とする。

現行ネットワークでは，Web サーバを 2 台用意し，それぞれの公開用 IP アドレスを同一のホスト名に対応付ける DNS ラウンドロビンを実施して，サーバの負荷分散と冗長化を実現している。

©2017 ICT Workshop

このたびマルチホーミングを導入することにより，二つの ISP をまたがる DNS ラウンドロビンを実施する。その点について，2 番目の箇条書きに，「LB の DNS ラウンドロビン機能を使い，インターネットから A 社内への通信の負荷分散を行う。現行の Web サーバ用のグローバル IP アドレスに，新たなグローバル IP アドレスを加え，DNS クエリに対してそれらが交互に返るようにする」と記述されている。

Web サーバの公開用 IP アドレスとして，従来から使用している ISP1 のグローバル IP アドレス 2 個と，新たに ISP2 から払い出されるグローバル IP アドレス 2 個を用意しておく。DNS ラウンドロビン機能を用い，ホスト名 www にこれらを対応付けて登録しておく。

この結果，ホスト名 www の名前解決の問合せに対し，ISP1，2 のそれぞれの IP アドレスを交互に回答するようになり，Web サーバへのアクセスを二つの ISP 経由に分散することができる。

しかも，5 番目の箇条書きにあるとおり，LB は各 ISP に ping 確認を定期的に実施し，「正常な ISP だけを利用する」機能も併せもつ。言い換えると，LB の DNS ラウンドロビンは，異常を検知した ISP の公開 IP アドレスを回答しない仕組みになっている。

この結果，二つの ISP を Active-Active 構成で冗長化することができる。

このように，ISP 経由のアクセスについて，負荷分散と冗長化の両方を実現できることが，まさしくマルチホーミングを導入するメリットと言えよう。

**・宛先 NAT の定義**

現行ネットワークでは，Web サーバに対して，ISP1 の公開用 IP アドレスを 2 個用意している。宛先 NAT の定義によって，公開用 IP アドレス 1 個につき実 IP アドレス 1 個を対応付けて変換を実施していた。

このたびマルチホーミングを導入することにより，新たに追加される ISP2 についても，Web サーバの公開用 IP アドレスを 2 個用意する。

そして，ISP1 のときと同様に，その公開用 IP アドレス 1 個につき実 IP アドレス 1 個を対応付けて変換を実施する。その定義を宛先 NAT に追加する。

**・インターネットアクセスの負荷分散と送信元 NAPT の定義**

3 番目の箇条書きに「A 社内からインターネットへの通信は，ISP1 と ISP2 への接続ポートに対して負荷分散を行う」と記述されている。したがって，インターネットへのアクセスを二つの ISP 経由に分散することができる。

本文には特に明記されていないが，一つの TCP コネクション通信を負荷分散する

©2017 ICT Workshop

とき，当該コネクションの開始から完了まで同じ ISP が選択され，変換後の送信元 IP アドレスと送信元ポート番号の組合せが維持されなければならない。

現行ネットワークでは，インターネットにアクセスする際に 2 個のグローバル IP アドレスを使って送信元 NAPT を実施していた。

このたびは，経由する ISP を LB が選択した時点で，ISP 接続ポートに割り当てられた 1 個のグローバル IP アドレスを使って，送信元 NAPT を実施する。

もっとも，二つの ISP 接続ポートがあるわけだから，同時に NAPT が処理できる通信の上限値は，従来と同等であると言える。

**・ISP 接続ポートの IP アドレスの設定**

「・A 社ドメインの権威サーバの設定」の解説を振り返ると，ISP1 接続ポートには ip1-L を，ISP2 接続ポートには ip2-L を割り当てる。それら二つの IP アドレスを，A 社ドメインの権威サーバの IP アドレスとして公開する。

LB 宛ての DNS クエリは，ISP1 経由では ISP1 接続ポートにアクセスし，ISP2 経由では ISP2 接続ポートにアクセスする。この結果，インターネットから見ると，それぞれの接続ポートが権威サーバのように映る。

経由する ISP ごとに接続ポートが異なっているものの，LB が回答するゾーン情報は，LB 本体に登録された一つのゾーンファイルから得たものである。つまり，1 番目の箇条書きにある，「ISP1，ISP2 のいずれからでも同じゾーンファイルが参照されるようにする」という要件が実現されることが分かる。

「・DNS ラウンドロビンの定義」「・宛先 NAT の定義」の解説を振り返ると，Web サーバの公開用 IP アドレスは，ISP ごとに 2 個ずつ用意する。

この公開用 IP アドレスを宛先とする通信は，ISP1 経由では LB の ISP1 接続ポートにアクセスし，ISP2 経由では LB の ISP2 接続ポートにアクセスする。

したがって，ISP 接続ポートには，その ISP から払い出された 2 個の公開用 IP アドレスも受信できるように設定する（詳細を割愛するが，公開用 IP アドレスの Proxy ARP 設定が必要となる）。

「・インターネットアクセスの負荷分散と送信元 NAPT の定義」を振り返ると，送信元 NAPT の変換では，ISP 接続ポートに割り当てられた IP アドレス（ip1-L，ip2-L）をそのまま使用する。つまり，送信元 NAPT のために別の IP アドレスを用意するわけではない。

本事例では，このように LB に IP アドレスを設定する必要がある。一つの ISP から払い出されたグローバル IP アドレス空間はサブネットマスク長が 29 なので，ホスト用に 6 個しか割り当てられない点に留意する必要があるからだ。

©2017 ICT Workshop

その 6 個は，LB の ISP 接続ポート，Web サーバの公開用（2 個），この後の設問で登場する STUN サーバ，IP-PBX，及び，図 3 に明記されていないがインターネット接続回線終端装置（ルータ）に割り当てる。

ここまで理解できれば，設問 2 を解く準備は整った。さらに，マルチホーミングの実現方法を理解しておくことは，移行計画を問う設問 5 の準備にもなっている。それでは，いよいよ小問の解説に移ろう。

## (1)

**解答例**

異 な る I S P か ら 払 い 出 さ れ て い る 。（17字）

問題文は，「本文中の下線（c）について，現行のグローバル IP アドレスと追加するグローバル IP アドレスとの違いを……述べよ」と記述されている。

下線（c）は，〔マルチホーミング〕の第 4 段落，2 番目の箇条書きにある。そこには，「LB の DNS ラウンドロビン機能を使い，インターネットから A 社内への通信の負荷分散を行う。(c) 現行の Web サーバ用のグローバル IP アドレスに，新たなグローバル IP アドレスを加え，DNS クエリに対してそれらが交互に返るようにする」と記述されている。

設問 2 の冒頭の解説「・DNS ラウンドロビンの定義」で述べたとおり，マルチホーミングを導入することにより，二つの ISP をまたがる DNS ラウンドロビンを実施する。2 番目の箇条書きにある，「新たなグローバル IP アドレス」とは，新たに利用する ISP2 から払い出されたグローバル IP アドレスを指している。これを，Web サーバの公開用 IP アドレスとして追加する。

したがって，現行のグローバル IP アドレスと追加するグローバル IP アドレスとの違いは，異なる ISP から払い出されているという点である。

よって，正解は解答例に示したとおりとなる。

©2017 ICT Workshop

## (2)

**解答例**

応答が行きの宛先IPアドレスとは異なる送信元IPアドレスから戻る。（33字）

問題文は，「本文中の下線（d）において，通信の行きと戻りが同じ ISP ではない場合の問題を，社外から Web サーバへのアクセスを例に，IP アドレスという用語を用いて……述べよ」と記述されている。

下線（d）は，〔マルチホーミング〕の第 4 段落，4 番目の箇条書きにある。そこには，「(d) LB は，通信の行きと戻りを同じ ISP 経由にする」と記述されている。

本問は，下線（d）の仕様を除外して考え，「行きと戻りの ISP 接続ポートが異なる」という条件の下で，解を導くことを求めている。

解説に先立ち，本問について著者の見解を述べることにする。滅多にないことだが，「本問は解答不能である」と著者は考えている。

試験センターの解答例は「応答が行きの宛先 IP アドレスとは異なる送信元 IP アドレスから戻る」となっているが，この結論を導く確たる根拠を，本文中の記述から見出せないからだ。

本問は，本文中で自らが定義した下線（d）の仕様をわざわざ撤回した上で，当該仕様が実装されていないときに生じ得る問題点を考えさせようとしている。

これを解くには，下線（d）の仕様を除外した，残りの仕様に基づいて推論していく必要がある。ネットワークスペシャリスト試験でよく出題される，「従来技術を理解していれば解答できる」ことを狙ったものだ。

とはいえ，本問に限っては本文中の記述からヒントを見出すことが困難である。架空の製品とはいえ，相当複雑な内部構造をもっているはずである。「行きと戻りの接続ポートが異なる」という外側から見た仕様を除外することが，当該仕様に関わる内側の機能にどの程度まで悪影響が及ぶと考えるべきなのか，本文中のわずか十数行の説明だけでは，因果関係を判断しづらいのだ。

試験センターの解答例を導くには，「応答パケットの送信元 IP アドレスを生成する機能にまで悪影響を及ぼしてしまう」という前提を設けてなくてはならない。このような欠陥が内部にあるとした上で，

©2017 ICT Workshop

本来の IP アドレス（行きのパケットで指定した宛先 IP アドレス）ではなく，応答パケットが出ていく接続ポートに基づく IP アドレスを，送信元 IP アドレスとして設定してしまう

と推論していくことが求められる。

ただ，この欠陥によって，行きの宛先 IP アドレスと戻りの送信元 IP アドレスが異なるパケットが生じ得る。そうなると，TCP コネクションの通信自体が成り立たなくなる。当初の「行きと戻りの接続ポートが異なる」という問題を超え，そもそも「通信できない」という大問題に発展してしまう。

それゆえ，この欠陥を前提に置いてみたものの，「不能という致命的な欠陥まで想定するのは，考えすぎではないか」と違和感を覚えた受験者がいたかもしれない。

そこで，「応答パケットを生成する機能は，本来の仕様どおりに動作する」という前提を崩さずに，下線（d）の仕様を除外できる別の欠陥が想定できないかを考えてみる。すると，例えば「配線ミスにより，戻りパケットの接続ポートを固定的に選ぶ」「ファームウェアのバグにより，戻りパケットの接続ポートをランダムに選ぶ」などが思いつくだろう。要は，「行きのパケットが ISP1 から入り，戻りのパケットが ISP2 から出ていく」といった振る舞いが一度でも発生すればよいのだから。

こういった別の欠陥を想定して本問に取り組むと，どうなるか。残念ながら，試験センターの“正解”を導けないのである。

本問は，「下線（d）の仕様を除外する」という条件で推論させることを狙っているのだが，その条件を満たし得る欠陥として，複数の候補を想定できる。試験センターが想定したものとは異なる欠陥を前提に置くなら，“不正解”となってしまう。

少なくとも著者には，唯一の解を導くだけの確たる根拠を，本文中から見出せなかった。

## ■設問 3

設問 3 の解説に入る前に，WebRTC（Web Real-Time Communication）について解説する。

本事例に登場する AP は，WebRTC を使ったビデオ電話を行っている。AP の通信については本文中に詳しく説明されているので，従来技術の知識に基づいて推論すれば正解を導くことができるように配慮されている。

本書では，本問を解くために必要な程度まで，WebRTC について簡単に解説しよう。

設問 3 の冒頭の解説では，WebRTC の全体像をざっくりイメージしてもらうことを狙って，AP 通信手順の概略を説明する。

©2017 ICT Workshop

より詳しい説明は，設問 3 の小問の解説の中で，必要に応じて補っていくことにする。

● WebRTC

WebRTC は，ブラウザをエンドポイントとした P2P（Peer-to-Peer）通信を実現する技術である。

本書執筆時点（2017 年 1 月）のブラウザ対応状況を見ると，Chrome，Firefox が対応済み，Safari，Internet Explorer がプラグイン搭載により対応可能であり，普及が進んでいると言えよう（http://caniuse.com/#search=WebRTC）。

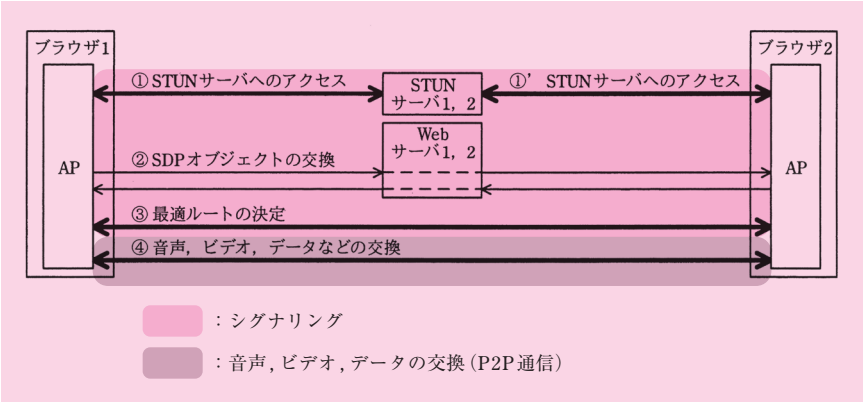
WebRTC で規格化されている通信は，大きく 2 種類ある。

一つ目は，P2P 通信の準備を目的とした，エンドポイント間で情報を交換する通信である。これをシグナリングという。通常，シグナリングは，特別なサーバを介して通信する。

二つ目は，音声，ビデオなどのメディア，メッセージなどのデータを交換する P2P 通信である。シグナリングによって，特別なサーバを介さずとも，ブラウザ間で直接通信することができる。

本文の図 5「AP 間通信の概要」は，WebRTC の通信手順を示している。

この通信のエンドポイントは，ブラウザである。本事例では，ブラウザに AP（アプリケーション）がダウンロードされている。




**図：WebRTC の通信手順の概要（図 5 に加筆）**

シグナリングは，図中の①～③である。P2P 通信は，図中の④である。

ブラウザはプライベートネットワークに存在していることも多いため，NAT 越えに

©2017 ICT Workshop

対応したシグナリングが求められている。図中の①が，NAT 越えを考慮した手順となっている。ここでは「STUN サーバ」が用いられているが，WebRTC では STUN 以外にも複数の方法（TURN，ICE）を用いることが可能だ。STUN について，詳しくは設問 3（1）で解説する。

図中の②では，ブラウザの IP アドレス，P2P 通信でやり取りするメディア種別などの情報を交換している。このときに交換する IP アドレスについて，詳しくは設問 3（2）で解説する。

図中の③では，最適ルートの決定が行われている。ここは設問で取り上げられていないので，詳細は割愛する。

図中の④では，音声，ビデオ，データなどの交換が行われている。本事例では，AP 間でビデオ電話を行う。ここも設問で取り上げられていないので，詳細は割愛する。

以上，WebRTC の全体像を概観した。それでは，いよいよ小問の解説に移ろう。

## （1）

**解答例**

Binding レスポンス中のデータに含まれる IP アドレスと，自分の IP アドレスを比べる。（44 字）

問題文は，「本文中の下線（e）において，STUN クライアントはどのようにして NAT 機能の有無を判定するかを……述べよ」と記述されている。

STUN プロトコルの概要が本文に述べられているので，本文の記述を引用しつつ，まずはその点を解説する。引用箇所の中に下線（e）も含まれているので，何が問われているのかを併せて確認しよう。次いで，解を導くことにする。

### ● STUN プロトコル

STUN（Session Traversal Utilities for NATs）とは，通信端末がインターネットにアクセスする際，インターネット側から自らの送信元 IP アドレスと送信元ポート番号がどのように見えるかを知る手段を提供するプロトコルである。RFC5389 で標準化されている。

端末がプライベート IP アドレス空間のネットワーク（以下，プライベートネットワークという）にいるとき，端末とインターネットの間に NAT 機器が介在している。

©2017 ICT Workshop

端末は，STUN を用いることで，同機器によって変換された IP アドレスとポート番号を知ることができる。

STUN を用いるには，グローバル IP アドレスをもつ STUN サーバを事前に設置しておく。

端末は，NAT 変換された IP アドレスとポート番号を知りたいとき，この STUN サーバに対し，自端末がどのように見えるかを通知してもらう仕組みになっている。

その具体的な手順について，〔ブラウザを使ったビデオ電話の通信〕の第 4 段落の箇条書きで，次のように説明されている。

> STUN プロトコルの概要は次のとおりである。
> ・STUN クライアントは，STUN サーバへ Binding リクエストを送る。
> ・STUN サーバは，受け取った IP パケットのヘッダから送信元の IP アドレスとポート番号を取り出し，Binding レスポンス中のデータに格納して返す。
> ・(e) STUN クライアントは，Binding レスポンス中のデータから，自分と STUN サーバ間の NAT 機能の有無を知り，NAT 機能が介在する場合には，そのデータから NAT 機能が変換した自分の IP アドレスを得る。

この説明にある「STUN クライアント」とは，NAT 変換された IP アドレスとポート番号を知りたい端末を指す。

1 番目の手順は，STUN クライアントは，STUN サーバへ Binding リクエストを送信する。この説明にはないが，通常は，STUN サーバへのアクセスには UDP を用いる。ポート番号は，RFC5389 によれば 3478 番だが，これ以外の番号を使ってもよい（Google が提供する STUN サーバは 19302 番）。

2 番目の手順は，STUN サーバが，STUN クライアントへ Binding レスポンスを返信する。このレスポンス中にデータに，STUN サーバが受け取った Binding リクエストパケットのヘッダから取り出した，送信元の IP アドレスとポート番号を格納する。

Binding レスポンスパケットに格納された，この IP アドレスとポート番号は，STUN クライアントがインターネット側からどのように見えるかを示している。

3 番目の手順は，「(e) STUN クライアントは，Binding レスポンス中のデータから，自分と STUN サーバ間の NAT 機能の有無を知（る）」と記述されている。ここが下線（e）となる。

もし STUN クライアントがプライベートネットワークにあり，STUN サーバの間に NAT 装置が介在しているならば，この IP アドレスは NAPT 処理によってグローバル IP アドレスに変換されたものになる。STUN クライアントは，受信した Binding レス

©2017 ICT Workshop

ポンス中のデータに含まれる IP アドレスと，自分の IP アドレスを比較することにより，両者が異なっているとき，NAT 装置によって IP アドレスが変換されたことを知ることができる。

**●解の導出**

ここで問われていることは，「下線（e）について，STUN クライアントはどのようにして NAT 機能の有無を判定するか」であった。

前述のとおり，STUN クライアントは Binding レスポンスを受信すると，そのデータに含まれる IP アドレスと自分の IP アドレスとを比較し，両者が異なっているか否かで，NAT 機能の有無を判定する。異なっていれば NAT 機能があることになる。

よって，正解は「**Binding レスポンス中のデータに含まれる IP アドレスと，自分の IP アドレスを比べる**」となる。

## (2)

**解答例**

① 〈p〉
② 〈g2〉

問題文は，「本文中の下線（f）について，図 4 の通信のために，ブラウザ 2 が SDP オブジェクトに格納する二つの IP アドレス候補を，図 4 中の字句を用いて答えよ」と記述されている。

下線（f）は，〔ブラウザを使ったビデオ電話の通信〕の第 7 段落で，「(f) 図 4 の AP 間通信は，このようにして確立した最適ルートを使っている」と記述されている。

下線（f）を含む，第 5 ～ 8 段落は，図 5「AP 間通信の概要」を説明している。

第 6 段落に「AP をダウンロードしたブラウザは，図 5 中の①～③で NAT 機能を経由した最適ルートを確立する（以下，ホールパンチという）」とあるので，下線（f）中の「最適ルート」とは，図 5 中の①～③のやり取りで確立されたものを指す。

図 5 中の「④音声，ビデオ，データなどの交換」は，「③最適ルートの決定」の後に続くわけだから，確立した最適ルートを使っていることが明らかである。したがって，第 7 段落（下線（f））の記述より，図 4 中の AP 通信は，図 5 中の「④音声，ビデオ，データなどの交換」に該当することが分かる。

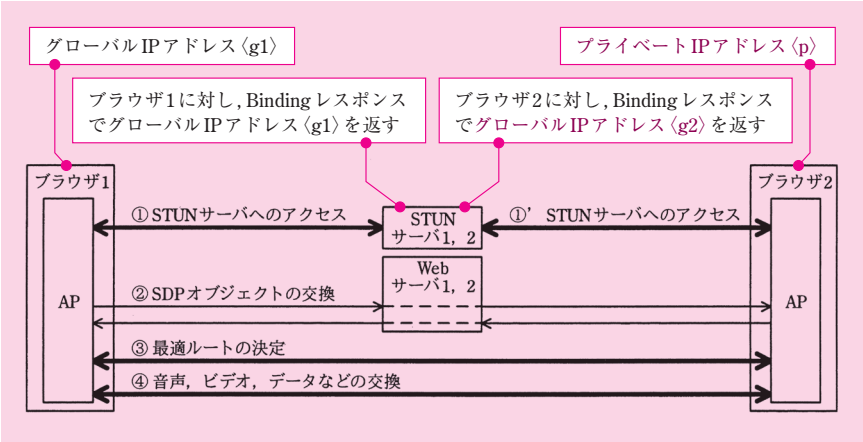
ここで問われているのは，「図 4 の通信のために，ブラウザ 2 が SDP オブジェクト

©2017 ICT Workshop

に格納する二つの IP アドレス候補」である。「図 4 の通信」を「図 5 の④の通信」と読み替えて，図 5 の中で考えてみると，本問の見通しが良くなるだろう。

### ● AP 間通信の手順

本問を解くには，図 5 の通信手順を理解しておく必要がある。そこで，その手順を説明した，第 6 段落の記述を確認しよう。




**図：AP 間通信の概要（図 5 に加筆）**

具体的な通信手順の解説に入る前に，図 5 に登場する，STUN サーバ 1，2 について触れておこう。

設問 3（1）で解説したとおり，STUN を用いるときは，グローバル IP アドレスをもつ STUN サーバを事前に設置しておく。

「STUN サーバ 1，2」は，図 3「新ネットワーク構成（抜粋）」に示されている。本事例では，STUN サーバをデータセンタに設置し，グローバル IP アドレスを割り当てる。マルチホーミングを導入するので，STUN サーバ 1 には ISP1 から払い出されたグローバル IP アドレスを，STUN サーバ 2 には ISP2 から払い出されたグローバル IP アドレスを，それぞれ割り当てる（詳しくは，設問 3（3）の解説で述べる）。

それでは，第 6 段落に記述された通信手順①～③を，順を追って確認しよう。

> ①，①’ AP は STUN サーバ 1，2 にアクセスし，NAT 機能が介在する場合の変換後のブラウザの IP アドレスを取得する。

©2017 ICT Workshop

ブラウザ 1，2 の IP アドレスは，図 4 に示されている。ブラウザ 1 はグローバル IP アドレス〈g1〉を，ブラウザ 2 はプライベート IP アドレス〈p〉をもつ。

ブラウザ 2 はプライベートネットワークに存在しており，NAT 装置を経由してインターネットにアクセスする。図 4 は，このプライベート IP アドレスが，NAT 機能によってグローバル IP アドレス〈g2〉に変換されることを示している。

したがって，手順①で，ブラウザ 1 の AP が STUN サーバから受け取る Binding レスポンスは，ブラウザの IP アドレスと同じ〈g1〉である。一方，手順①’で，ブラウザ 2 の AP が STUN サーバから受け取る Binding レスポンスは，NAT 機能により変換された〈g2〉となる。この結果，ブラウザ 2 の AP は，自分がプライベートネットワークに存在していることが分かる。

②AP は，SDP（Session Description Protocol）オブジェクトを使って，①，①’で取得した IP アドレスとブラウザ自身の IP アドレスを，通信相手の AP へ通知する。その際，ブラウザ 1，2 と Web サーバ 1，2 間に HTTPS が使われる。
③AP は，通知された IP アドレスを宛先 IP アドレスにして通信相手との通信を試み，相互に通信が成功した場合に，その宛先 IP アドレスの組合せを最適ルートとする。

ブラウザ 1 は，先の手順①で IP アドレス〈g1〉を取得している。手順②において，これとブラウザ自身の IP アドレス〈g1〉を，SDP オブジェクトを使ってブラウザ 2 の AP へ通知する。

同様に，ブラウザ 2 は，先の手順①’で IP アドレス〈g2〉を取得している。手順②において，これとブラウザ自身の IP アドレス〈p〉を，SDP オブジェクトを使ってブラウザ 1 の AP へ通知する(*)。

（*）ブラウザ 1 と 2 がアクセスする Web サーバは，それぞれが DNS ラウンドロビンによって決定される。
したがって，アクセス先となる Web サーバが，ブラウザによって異なる可能性がある。それにもかかわらず，手順②では，Web サーバを介し，ブラウザ 1 と 2 の間で情報を交換している。したがって，本文に説明されていない何らかの方法で，Web サーバ 1 と 2 の間で情報を共有しているはずだ。一般的に言うと，データベースを用いる方法，セッションクラスタリング（ネットワークを介したセッション情報の共有）を用いる方法などが考えられる。

手順③において，通知された IP アドレスを宛先 IP アドレスにして通信相手との通信を試みる。図の例では，相手から通知されたグローバル IP アドレス〈g1〉と〈g2〉

©2017 ICT Workshop

を宛先にする通信が成功する。したがって，これが最適ルートとなる。

仮に，通信相手が同じプライベートネットワークに存在している場合は，どうなるのだろうか。このとき，相手から通知された，ブラウザ自身の IP アドレスを宛先にする通信も成功するはずだ。複数成功した場合，本文には明記されていない何らかの基準にしたがって，「最適」なルートが選ばれる。

**●解の導出**

ここで問われているのは，手順②において，ブラウザ 2 が SDP オブジェクトに格納する二つの IP アドレス候補である。

ブラウザ 2 は，先の手順①’で IP アドレス〈g2〉を取得している。これとブラウザ自身の IP アドレス〈p〉を，SDP オブジェクトを使ってブラウザ 1 の AP へ通知する。

よって，正解は「**〈g2〉，〈p〉**」となる。

## (3)

**解答例**

A：vlan1
B：vlan2
（順不同）

問題文は，「本文中の下線（g）の接続先を，表 2 中の VLAN 名でそれぞれ答えよ」と記述されている。

下線（g）は，〔ブラウザを使ったビデオ電話の通信〕の第 9 段落にある。そこには，「（g）片方の ISP が障害の場合にも利用できるように，STUN サーバのインタフェース（図 3 中の A，B）を，図 3 中の適切なスイッチに接続することにした」と記述されている。

本事例の新ネットワークでは，マルチホーミングを導入し，ISP 経由の通信を冗長化する。したがって，「片方の ISP が障害の場合にも利用できるように（する）」とは，このマルチホーミングを使って実現することが分かる。

**● STUN サーバのマルチホーミング対応**

マルチホーミングを用いることで，STUN サーバへのアクセスについて，負荷分散と冗長化を実現できる。そのためには，次に示す設定が必要となる。

©2017 ICT Workshop

1. IP アドレスの割当て

2 台の STUN サーバ 1，2 を設置し，それに割り当てるグローバル IP アドレスを，それぞれ異なる ISP から払い出されたものにする。

以降の解説で，ISP1 のアドレスを「ip1-S」，ISP2 のアドレスを「ip2-S」と呼ぶことにする。

この解説では，STUN サーバ 1 に ip1-S を，STUN サーバ 2 に ip2-S を，それぞれ割り当てるものとする。もちろん，この IP アドレスは入替可能だ。

2. DNS ラウンドロビンの定義

LB の DNS ゾーン情報に，STUN サーバのホスト名とその IP アドレスの対応を登録する。DNS ラウンドロビン機能を用い，STUN サーバのホスト名に，STUN サーバ 1，2 の 2 個の IP アドレスを対応付ける。

この結果，STUN サーバへのアクセスを二つの ISP 経由に分散することができる。

設問 2 の冒頭の解説「・DNS ラウンドロビンの定義」で述べたとおり，LB の DNS ラウンドロビンは「正常な ISP だけを利用する」機能を併せもつ。それゆえ，異常を検知した ISP の IP アドレスを回答しない仕組みになっている。

この結果，下線（g）にあるとおり，「片方の ISP が障害の場合にも利用」できる。すなわち，Active-Active 構成の冗長化を実現できる。

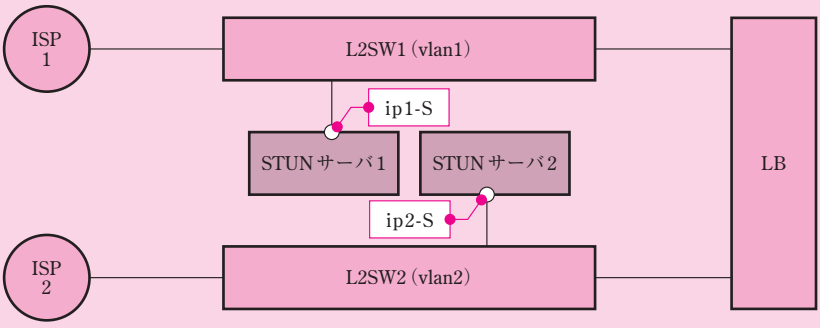
●解の導出

さて，本問で問われているのは，STUN サーバ 1，2 の接続先となる VLAN 名である。

この解説では，STUN サーバ 1 に ip1-S を割り当てるものとしている。それゆえ，図 3「A 社の新ネットワーク構成（抜粋）」中の接続先は，ISP1 のグローバル IP アドレス空間をもつネットワークセグメントである。したがって，接続する機器名は「L2SW1」である。そのネットワークセグメントの VLAN 名は，表 2「図 3 中のスイッチに定義された新 IP アドレス空間」を見ると，「vlan1」である。

同様に，STUN サーバ 2 に ip2-S を割り当てるものとしているので，図 3 中の接続する機器名は「L2SW2」であり，VLAN 名は「vlan2」である。

©2017 ICT Workshop




LB の DNS 機能の定義

| | | | |
|---|---|---|---|
| $ORIGIN | a-sha.co.jp. | | |
| stun | IN | A | ip1-S |
| | IN | A | ip2-S |

| 用語 | 意味 |
|---|---|
| stun | STUN サーバのホスト名 |
| ip1-S | ISP1 から払い出された<br>グローバル IP アドレス |
| ip2-S | ISP2 から払い出された<br>グローバル IP アドレス |

**図：A 社の新ネットワーク構成（STUN が関わる部分を抜粋）**

よって，正解は，「vlan1」「vlan2」となる。

STUN サーバ 1，2 に割り当てるグローバル IP アドレスは入替可能なので，解は順不同である。

## (4)

**解答例**

エ：ブラウザ 2 の AP
オ：STUN サーバ

［エ］，［オ］

空欄エ，オを含む文章は，〔ブラウザを使ったビデオ電話の通信〕の第 10 段落にある。そこには，「A 社のマルチホーミング運用によって，図 5 中の通信が ISP1 と ISP2 に負荷分散されるかどうかを検討した。そして，図 5 から，データ量が多い④に用いられる ISP は，［エ］が［オ］をアクセスするときの LB の振分け結果によって決まることを確認し，負荷分散が行われると判断した」と記述されている。

©2017 ICT Workshop

本問を解くには，AP 通信の手順について，IP アドレスとポート番号の組に着目して，より深く理解する必要がある。まずはその点について解説し，次いで解を導こう。

**● AP 間通信の手順（IP アドレスとポート番号の組に着目）**

AP 間通信の手順の概要は，設問 3（2）で既に解説した。そのときは，ポート番号にはあえて言及しなかった。設問 3（2）の解を導くことには関係がなかったので，説明を必要以上に複雑にしたくなかったからだ。

ここでは，先ほどの説明（本文の第 6 段落の記述に基づく説明）を土台にして，ポート番号がどのように設定されているかに着目しよう。

まず，幾つかの前提条件を置くことにする。

IP アドレスについては，次の条件を置く。

- ブラウザ 1，ブラウザ 2 の IP アドレスは，図 4，図 5 と同じにする。

ポート番号について，次の条件を置く。

- STUN サーバ宛てにアクセスするときの宛先ポート番号を，RFC5389 に基づく「3478 番」に指定する。
- AP 間通信の手順①～④の間，AP がパケットを送信するときの送信元ポート番号は変わらない。ブラウザ 1 の AP のポート番号を「$\alpha$」，ブラウザ 2 の AP のポート番号を「$\beta$」とする。

ポート番号に関する 2 番目の条件は，本文の第 9 段落の「AP 間通信において AP が使用するポート番号はあらかじめ決められている」という記述に基づいている。$\alpha$ と $\beta$ は等しいというより強い条件を置いてもよかったが，別々でも動作することを示すため，この解説ではあえて異なる値にしてある。

ブラウザが STUN サーバにアクセスするとき，そのアクセスに先立って，LB の DNS 機能で名前解決する。この結果，ブラウザ 1 は STUN サーバ 1 の IP アドレスを，ブラウザ 2 は STUN サーバ 2 の IP アドレスを，名前解決の回答として受け取るものとする。アクセス先の STUN サーバ 1 と 2 は入替可能なので，重要視しなくてよい。

ブラウザ 2 が STUN サーバにアクセスするとき，LB の負荷分散機能により，ISP1 側又は ISP2 側のどちらかの接続ポートを経由する。ここでは，次の条件を置く。

- ブラウザ 2 は，ISP2 接続ポートを経由して STUN サーバにアクセスする。

©2017 ICT Workshop

ブラウザ 2 はプライベートネットワークに存在しているので，ブラウザ 2 の AP から STUN サーバへパケットを送信する際，送信元 NAPT による変換が行われる。それゆえ，NAPT 変換後の IP アドレス g2 を，この解説では ISP2 から払い出されたグローバル IP アドレスとしているわけだ。

送信元 NAPT について，次の条件を置く。

- ブラウザ 2 からインターネットへ送信する際，送信元の IP アドレス，ポート番号の組は，「p，$\beta$」から「g2，$\gamma$」に変換される。
- インターネットからブラウザ 2 が受信する際，前記とは逆に変換される。
- AP 間通信の手順①～④の間，前記の変換ルールは保たれる。

送信元 NAPT に関する 3 番目の条件は，本文の第 8 段落の「ホールパンチには，ブラウザの IP アドレスと NAT 機能の変換ルールが，それぞれ一定時間変わらないという前提条件が必要である」という記述に基づいている。

この記述に，先ほど引用した第 9 段落のポート番号に関する記述を結び付けるなら，この部分は「ブラウザの IP アドレス，AP のポート番号，NAT 機能の変換ルールが一定時間変わらない」と読み替えることができる。

さて，これらの前提条件に基づき，IP アドレスとポート番号の組に着目して，AP 間の通信手順を改めて考察しよう。

手順①，①’では，両ブラウザの AP はそれぞれ，STUN を用い，NAT 機能が介在する場合の変換後のブラウザの IP アドレスとポート番号を取得する。手順①’では，ブラウザ 2 から STUN サーバへのアクセスが，LB によって ISP2 接続ポートに振り分けられる。このとき動的に生成された，送信元 NAPT の変換ルールが一定時間保たれる。

手順②では，各 AP と Web サーバ間の HTTPS 通信が行われる。

本文の第 6 段落にある手順②の記述では，「IP アドレス」を通知し合う旨，説明されている。本文には記述されていないが，ポート番号も一緒に通知していると推論できる。このように考えられる理由は，続く手順③，④において AP 同士が直接通信するためにポート番号が必要不可欠だからだ。

手順③，④では，両ブラウザの AP 間の通信が行われる。このとき，手順①’で動的に生成された送信元 NAPT の変換ルールが継続して適用されることで，通信が成り立っている。

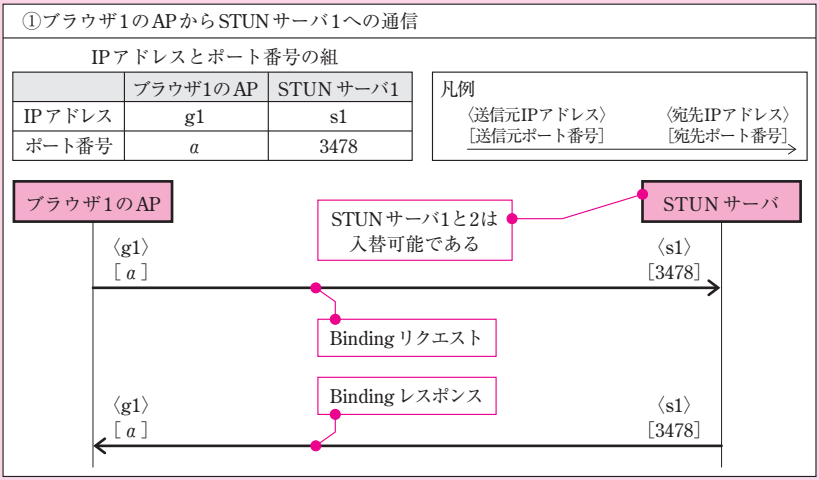
©2017 ICT Workshop

ブラウザ 1 の AP からブラウザ 2 の AP への通信では，宛先の IP アドレスとポート番号の組は「g2，γ」である。LB の ISP2 接続ポートにおいて，この通信に NAPT が適用され，宛先が「p，β」に変換される。その後，プライベートネットワークのブラウザ 2 に向かう。

ブラウザ 2 の AP からブラウザ 1 の AP への通信では，送信元の IP アドレスとポート番号の組は「p，β」である。LB の ISP2 接続ポートにおいて，この通信に NAPT が適用され，送信元が「g2，γ」に変換される。その後，インターネットのブラウザ 1 に向かう。

この AP 間通信の通信シーケンスを次の図に示す。

なお，手順②は，HTTPS 通信で Web サーバにアクセスしているだけに過ぎず，通信シーケンスとしては特筆に値する内容がないため，省略している。




©2017 ICT Workshop

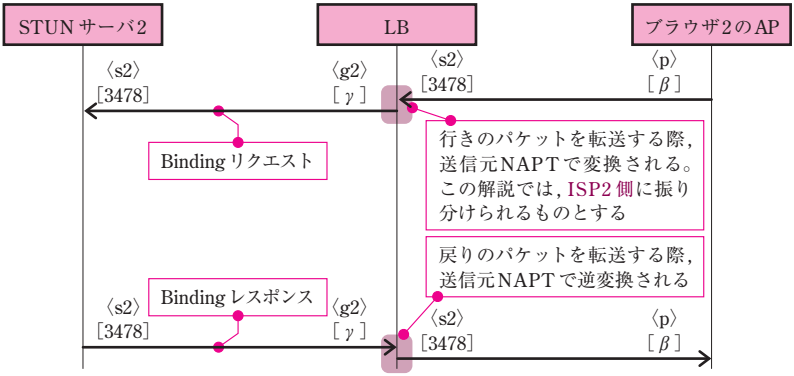
①’ ブラウザ2のAPからSTUNサーバ2への通信

IPアドレスとポート番号の組

| | STUN サーバ2 | ブラウザ2のAP |
|---|---|---|
| IPアドレス | s2 | p |
| ポート番号 | 3478 | β |

LBが実施する送信元NAPT

| | 変換後（グローバル側） | 変換前 |
|---|---|---|
| IPアドレス | g2 | p |
| ポート番号 | γ | β |



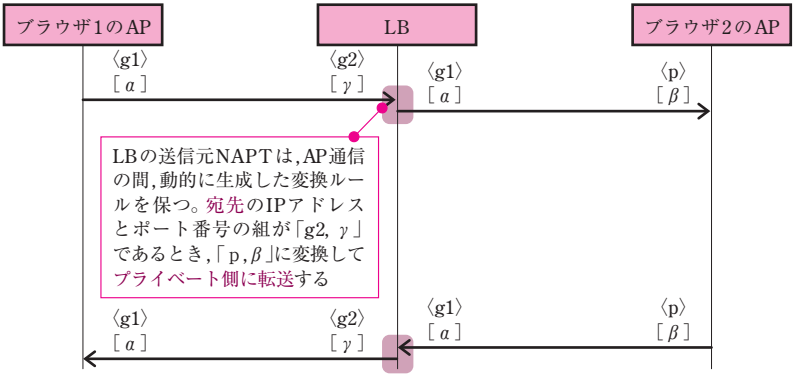

③，④ブラウザ1のAPからブラウザ2へのAPの通信

IPアドレスとポート番号の組

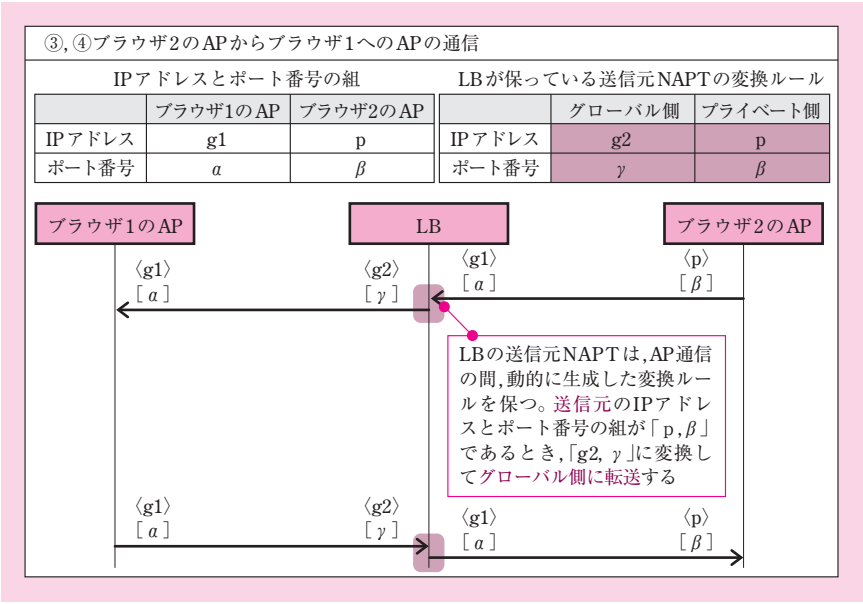
| | ブラウザ1のAP | ブラウザ2のAP |
|---|---|---|
| IPアドレス | g1 | p |
| ポート番号 | α | β |

LBが保っている送信元NAPTの変換ルール

| | グローバル側 | プライベート側 |
|---|---|---|
| IPアドレス | g2 | p |
| ポート番号 | γ | β |




©2017 ICT Workshop




**図：AP 間通信の例（図 5 にポート番号を表記した場合）**

**●解の導出**

さて，ここで問われているのは，「データ量が多い④に用いられる ISP は，［エ］が［オ］をアクセスするときの LB の振分け結果によって決まる」という文の空欄を埋めることだ。

前述のとおり，それは，手順①’において，ブラウザ 2 の AP が STUN サーバにアクセスするときである。

このとき，LB が振り分ける ISP 接続ポートで送信元 NAPT が実施される。このときの送信元 NAPT で変換された IP アドレスとポート番号を通信相手に通知することで，手順③，④に至るからだ。

前述の解説では，ブラウザ 2 が STUN サーバ 2 にアクセスする例を使ったが，アクセス先を STUN サーバ 1 に入れ替えてもよい。つまり，特定の STUN サーバに依存するものではない。空欄オの解答に際して，留意しておきたい点だ。

よって，空欄エに該当する字句は「**ブラウザ 2 の AP**」となり，空欄オに該当する字句は「**STUN サーバ**」となる。

©2017 ICT Workshop

## ■設問 4
## (1)

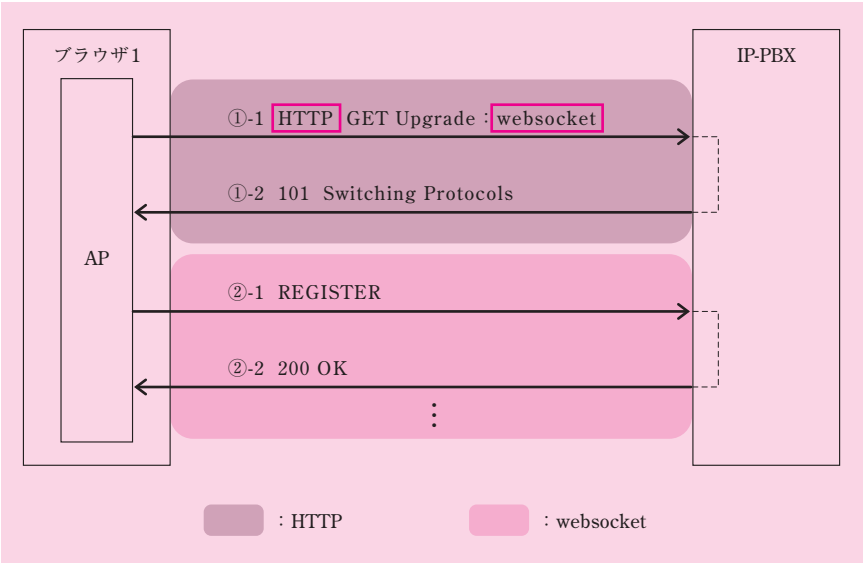
**解答例**

カ：HTTP
キ：WebSocket

カ , キ

空欄カ，キを含む文章は，〔ブラウザを使った音声電話の通信〕の第 3 段落，1 番目の箇条書きにある。

第 3 段落は，図 6「社外の AP から社内の IP 電話機への通信の概要」を説明したものである。1 番目の箇条書きには，「AP は，通信プロトコル［カ］を使って IP-PBX へアクセスし，①-1 と①-2 によって，通信プロトコルを［キ］に切り替え，切り替えた通信プロトコルの上で SIP プロトコルに基づくシグナリングを行う」と記述されている。




図：社外の AP から社内の IP 電話機への通信の概要（図 6 の一部を抜粋）

©2017 ICT Workshop

図 6 の①-1 に「HTTP」とある。したがって，①-1 は HTTP リクエストであり，①-2 は HTTP レスポンスであることが分かる。

よって，空欄カに入る字句は「**HTTP**」となる。

図 6 の①-1 の HTTP リクエストの中に「Upgrade：websocket」とある。これは，AP が IP-PBX に対し，「WebSocket」にプロトコルを切り替えるように要求したことを示している。

これを受けて，①-2 の HTTP レスポンスは，「101」（Switching Protocols）というステータスを返答している。これは，その切替要求を IP-PBX が受理したことを示している。

これ以降のやり取りは，WebSocket 上で行われる。

図 6 の②-1 以降は SIP のメッセージがやり取りされているが，これは WebSocket プロトコル上のデータとして送受信されている。本文はそのことを指して，「切り替えた通信プロトコルの上で SIP プロトコルに基づくシグナリングを行う」と述べている。

よって，空欄キに入る字句は「**WebSocket**」となる。

さて，正答は得られたが，新技術に触れる良い機会なので，WebSocket について簡単に解説しておこう。

### ● WebSocket プロトコル

WebSocket とは，Web コンピューティングにおける双方向のプッシュ配信を実現する技術である。プロトコルの規格は IETF が策定し，RFC6455 で標準化されている。API の規格は W3C が策定しており，これを受けてクライアント側（主要ブラウザの JavaScript），サーバ側（Java EE，PHP，Node.js など）の双方で，WebSocket の実装が普及している。

WebSocket は，プッシュ配信に先立ち，既存の HTTP 通信を用いて，クライアントがサーバに WebSocket 通信の開始を要求する。より正確に言うと，この HTTP 通信を WebSocket 通信に切り替えることを要求する。次いで，サーバがこの要求を受理した旨を応答する。図 6 の①-1 と①-2 がこれに該当する。なお，図 6 は，HTTP のヘッダフィールドをかなり簡略化して記している。

WebSocket 通信に切り替えたら，クライアントとサーバの双方は，いつでもプッシュ配信を行うことができる。図 6 の②-1 以降のやり取りがこれに該当する。

WebSocket 通信は，切り替えた HTTP 通信の TCP コネクションをそのまま用いる。これはすなわち，WebSocket 通信のために，TCP コネクション生成のオーバヘッドを費やさないことを意味している。さらに，クライアントとサーバの両者ともポート番

©2017 ICT Workshop

号を変えないので，経路途上のファイアウォール，NAT 装置から見れば，自分が既に通過させた HTTP 通信のままであるから，こうした経路上の機器によって通信が不意に阻害される恐れがない。

例えば，図 6 の②-1 はクライアント（AP）からサーバ（IP-PBX）へ送信しているが，このときの宛先ポート番号，送信元ポート番号は，それぞれ①-1 の HTTP 通信と同じものになる。

WebSocket プロトコルは，HTTP と比較すると，主に次のような特徴をもつ。

**表：WebSocket と HTTP との比較**

| 項目 | WebSocket の特徴 | HTTP の特徴 |
|---|---|---|
| 通信の方向 | 双方向（プッシュ型）<br>（クライアントとサーバの双方が，任意のタイミングでメッセージを送ることができる） | 単方向（プル型）<br>（クライアントがリクエストを送信し，サーバがレスポンスを返信する） |
| オーバヘッド | ヘッダ部分が2～14バイトである | 多数のヘッダフィールドをもち，ヘッダ部分だけで数十バイトに膨れ上がることもある |
| | 既存の HTTP 通信を切り替えているため，TCP コネクションを新たに生成する必要がない | （最終的にはアプリケーションの作り方に依存する話だが，）ブラウザで普通に閲覧すると，複数のコネクションを同時に生成し得ると考えてよい |
| メッセージ | テキスト形式とバイナリ形式に対応している | 同左 |
| 暗号化 | TLS 暗号化に対応している | 同左 |

HTTP 通信は，クライアントがサーバに要求しない限り，サーバのコンテンツを取得できない。このように，クライアントのリクエストが起点となって，サーバのコンテンツを取得する方式をプル型という。サーバ側のコンテンツを閲覧することや，クライアントからサーバへの単方向にデータ送信することを主目的とするアプリケーションは，プル型で十分である。

その一方で，世の中には，クライアントとサーバの双方がコンテンツをいつでも配信できるようにすることで，利用価値の高まるアプリケーションがある。このように，自分のコンテンツを相手にリアルタイムに配信する方式をプッシュ型という。

プッシュ型の配信を利用するアプリケーションの一例として，多人数によるチャッ

©2017 ICT Workshop

トが挙げられる。これは，全体を管理するサーバに向けてクライアントがメッセージをプッシュし，次いでサーバから全クライアントにそのメッセージをプッシュすることで成り立つアプリケーションだ。

従来の Web コンピューティングの技術では，クライアント側からはフォームを用いてメッセージを送信することはできるが，サーバ側からはリアルタイムにメッセージを配信できなかった。

サーバ側コンテンツのプッシュ配信を擬似的に実現するため，これまでは Ajax を用い，クライアント側のスクリプトが自動的かつ定期的にポーリングするなどしていた。この方式は，所詮はポーリング間隔でのリフレッシュに過ぎずリアルタイムの配信ではないこと，サーバのコンテンツが変化していなくても無駄にポーリングしてしまうこと，ポーリングするたびに HTTP 通信のオーバヘッドが掛かることなどの問題を抱えている。

そこで，Web アプリケーションでプッシュ配信ができない問題を根本的に解決する新技術として，WebSocket が規格化された。前述のとおり，クライアントとサーバの双方向でプッシュ配信ができることや，オーバヘッドが小さいといった特徴をもち，注目を集めている。

参考までに，プッシュ配信ができない問題を克服する別のアプローチがあることも最後に触れておこう。その一つが SSE（Server-Sent Events）である。これは，従来の HTTP 通信の技術（プル型）を用いながら，無闇にポーリングすることなく，見かけ上はプッシュ型と同等の通信が可能になっている。

SSE について簡単に説明すると，サーバから応答してもすぐに切断せず，応答サイズを明示せずに，応答中の状態を維持しておくことにより，サーバ側コンテンツの変化にリアルタイムに追随して何度でも応答する方式を採っている。言うなれば，この応答が，プッシュ配信の役割を担っているわけだ。

## (2)

**解答例**

ＩＳＰ１とＩＳＰ２から払い出されたＩＰアドレスを一つずつ割り当てる。（34字）

問題文は，「本文中の下線（h）について，マルチホーミングのために，グローバル IP アドレスをどのように割り当てるかを……述べよ」と記述されている。

©2017 ICT Workshop

下線（h）は，〔ブラウザを使った音声電話の通信〕の第 3 段落，2 番目の箇条書きにある。そこには，「IP-PBX は，2 組の B2BUA（Back-to-Back User Agent）として動作する。（h）インターネット側の二つの UA（User Agent）には，それぞれグローバル IP アドレスを割り当てる」と記述されている。

本文を解くには，B2BUA の働きについて理解する必要がある。これを知ることで，本来，B2BUA のインターネット側の UA は一つあればよいことが分かる。それを踏まえ，なぜ本事例では二つの UA があるかを考察することにより，解を導くことができる。

### ● B2BUA

B2BUA とは，二つの SIP ネットワークを橋渡しするゲートウェイである。一つの SIP ネットワークは，発呼側 UA と着呼側 UA をエンドポイントとしている。分かりやすく言うと，発呼側 UA は電話を掛ける側で，着呼側 UA は電話が掛かってくる側である。

B2BUA について，詳しくは本書の第 2 章「2.3.2　VoIP ネットワーク」を参照していただきたい。なお，平成 26 年度午後Ⅱ問 2 で出題されており，その本文中に詳しく説明されているので，本書の解説と併せて参考にしてみるのもよいだろう。

ここでは，本問を解くのに必要な程度まで，B2BUA について簡単に説明する。

まず押さえておきたいのは，B2BUA が必要となるのは，通話したい相手に直接発呼できない場合である，という点だ。

あくまで利用者の立場から見ると，発呼側 UA から着呼側 UA に電話を掛けている。しかし，直接やり取りできる相手ではないため，実際には発呼側 UA は B2BUA に発呼している。それを受けて，今度は B2BUA から着呼側 UA に発呼している。つまり，B2BUA を中継して，電話を掛けているわけだ。

まさに本事例のブラウザを使った音声電話が，B2BUA を必要とする場合に該当する。

その点について，音声電話の UA に関する記述を確認しよう。序文の第 4 段落，3 番目の箇条書きには，次のように記述されている。

> ・ブラウザを使った音声電話：施主や外出先の A 社の社員がブラウザを使って，社内の A 社の社員と音声電話ができるようにする。……IP-PBX を介した，社外のブラウザ上で動作する AP と社内の IP 電話機との通信によって実現する。

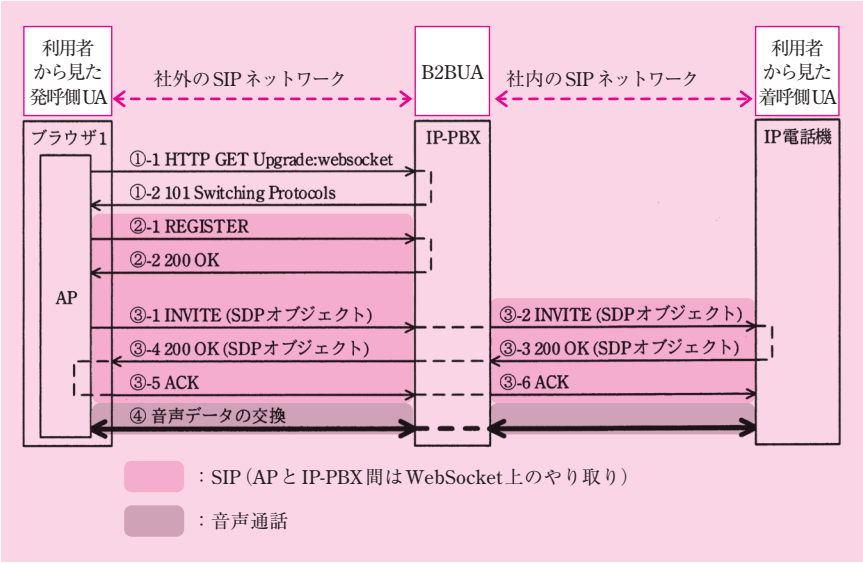
この記述から，利用者から見た発呼側 UA は「社外のブラウザ上で動作する AP」，

©2017 ICT Workshop

利用者から見た着呼側 UA は「社内の IP 電話機」であることが分かる。

社内の IP 電話機はプライベート IP アドレスが割り当てられているため，インターネットから IP 電話機に直接発呼することができない。それゆえ，IP-PBX が B2BUA となり，これら二つの UA 間の通話を中継する必要があるわけだ。

本文の図 6「社外の AP から社内の IP 電話機への通信の概要」を見ると，IP-PBX が，二つの SIP ネットワークを中継するゲートウェイであることが分かる。本文は B2BUA という用語の説明こそないものの，この図を見れば概要をつかめるように配慮されている。




**図：社外の AP から社内の IP 電話機への通信の概要（図 6 に加筆）**

社外の SIP ネットワークは，AP と IP-PBX 間である。通信プロトコル上は，発呼側 UA が AP であり，着呼側 UA が IP-PBX のインターネット側 UA である。言うまでもないが，IP-PBX のインターネット側インタフェースには，グローバル IP アドレスを割り当てる必要がある。

社内の SIP ネットワークは，IP-PBX と IP 電話機間である。通信プロトコル上は，発呼側 UA が IP-PBX のプライベートネットワーク側 UA であり，着呼側 UA が IP 電話機である。IP-PBX のプライベートネットワーク側インタフェースには，プライベート IP アドレスを割り当てる。

IP-PBX は，SIP メッセージを中継する際，メッセージ内に格納されている UA の IP

©2017 ICT Workshop

アドレスを書き換える必要がある。AP に対しては自分が着呼側 UA として振る舞い，IP 電話機に対しては自分が発呼側 UA として振る舞うからだ。その際，社外の SIP ネットワークはグローバル IP アドレス空間にあり，社内の SIP ネットワークはプライベート IP アドレス空間にあるので，〔ブラウザを使った音声電話の通信〕の第 3 段落の 3 番目の箇条書きにあるとおり，「グローバル IP アドレスとプライベート IP アドレスを変換」している。

ここまでの解説を整理すると，IP-PBX は二つの UA をもつことが分かる。一つは社外の SIP ネットワークにおける着呼側 UA であり，これがインターネット側の UA となる。もう一つは社内の SIP ネットワークにおける発呼側 UA であり，これがプライベートネットワーク側の UA となる。

これまでの解説から，B2BUA として振る舞うとき，本来であれば，インターネット側の UA は一つあればよいはずだと理解できる。

それではなぜ，下線（h）には「インターネット側の二つの UA」と記述されているのだろうか。そして，ここで問われている，新ネットワークにおける接続はどうすればよいのだろうか。次にその点を解説しよう。

### ● IP-PBX のマルチホーミング対応

本事例ではマルチホーミングを導入することで，インターネットからの数々のアクセスを二つの ISP 経由に分散している。

この点を踏まえると，5 番目の箇条書きの「図 6 中の AP と IP-PBX 間の通信は ISP1 と ISP2 に負荷分散される」という記述の意味するところが理解できる。AP はインターネットのブラウザにあるので，要するに，インターネットから IP-PBX へのアクセスも，マルチホーミングで負荷分散するわけだ。

したがって，下線（h）に「インターネット側の二つの UA」と記述されている理由は，マルチホーミングを用いて，それぞれの UA に異なる ISP 経由でアクセスさせるためである。実のところ，そもそも問題文に「下線（h）について，マルチホーミングのために，グローバル IP アドレスをどのように割り当てるか」と記述されていることからも，その点は明らかだ。

その具体的な設定は，設問 3（3）で解説した STUN サーバと同様にすればよい。

図 3「A 社の新ネットワーク構成（抜粋）」を見ると，STUN サーバの場合はサーバが 2 台あるが，IP-PBX はサーバが 1 台でインタフェースが二つある点が異なっている。そこだけ適宜読み替えれば，IP アドレスの割当てと DNS ラウンドロビンの定義を，次のように設定することが分かる。

©2017 ICT Workshop

**1. IP アドレスの割当て**

IP-PBX のインターネット側インタフェース C，D に対し，ここに割り当てるグローバル IP アドレスを，それぞれ異なる ISP から払い出されたものにする。

以降の解説で，ISP1 のアドレスを「ip1-P」，ISP2 のアドレスを「ip2-P」と呼ぶことにする。

この解説では，インタフェース C に ip1-P を，インタフェース D に ip2-P を，それぞれ割り当てるものとする。もちろん，この IP アドレスは入替可能だ。

**2. DNS ラウンドロビンの定義**

LB の DNS ゾーン情報に，IP-PBX のホスト名とその IP アドレスの対応を登録する。DNS ラウンドロビン機能を用い，IP-PBX のホスト名に，インタフェース C，D の 2 個の IP アドレスを対応付ける。

この結果，IP-PBX へのアクセスを二つの ISP 経由に分散することができる。

LB の DNS ラウンドロビンは「正常な ISP だけを利用する」機能を併せもつので，異常を検知した ISP の IP アドレスを回答しない仕組みになっている。つまり，Active-Active 構成の冗長化も実現できる。

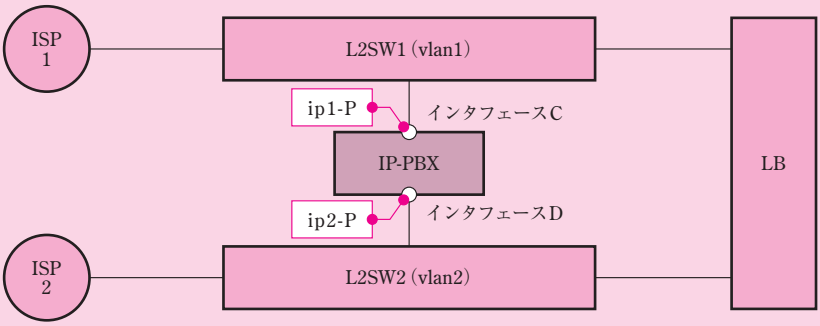
まとめとして，これまでの解説に基づき，IP-PBX のインタフェース C，D を図 3 中の適切な機器に接続してみよう。

この解説では，インタフェース C に ip1-P を割り当てるものとしている。それゆえ，図 3 中の接続先は，ISP1 のグローバル IP アドレス空間をもつネットワークセグメントである。つまり，接続する機器名は「L2SW1」である。

同様に，インタフェース D に ip2-P を割り当てるものとしているので，図 3 中の接続する機器名は「L2SW2」である。

なお，インタフェース C，D に割り当てるグローバル IP アドレスは，本来は入替可能なものである。

©2017 ICT Workshop




LBのDNS機能の定義

```
$ORIGIN   a-sha.co.jp.
ippbx     IN   A   ip1-P
          IN   A   ip2-P
```

| 用語 | 意味 |
|---|---|
| ippbx | IP-PBXのホスト名 |
| ip1-P | ISP1から払い出されたグローバルIPアドレス |
| ip2-P | ISP2から払い出されたグローバルIPアドレス |

**図：A 社の新ネットワーク構成（IP-PBX が関わる部分を抜粋）**

**●解の導出**

本問は，IP-PBX が有する「インターネット側の二つの UA」のグローバル IP アドレスについて，マルチホーミングを実施するために必要な設定を問うている。

これまで解説したとおり，下線（h）に「インターネット側の二つの UA」と記述されている理由は，マルチホーミングを用いて，それぞれの UA に異なる ISP 経由でアクセスさせるためであった。

したがって，二つの UA に対し，それぞれ異なる ISP のグローバル IP アドレスを，一つずつ割り当てればよい。

よって，正解は「**ISP1 と ISP2 から払い出された IP アドレスを一つずつ割り当てる**」となる。

©2017 ICT Workshop

## (3)

**解答例**

C：vlan1
D：vlan2
（順不同）

問題文は，「本文中の下線（i）の接続先を，表 2 中の VLAN 名でそれぞれ答えよ」と記述されている。

下線（i）は，〔ブラウザを使った音声電話の通信〕の第 3 段落，4 番目の箇条書きにある。そこには，「(i) IP-PBX の LAN インタフェース（図 3 中の C，D）を追加し，図 3 中の適切なスイッチと接続する」と記述されている。

小問（2）の「● IP-PBX のマルチホーミング対応」で解説したとおり，IP-PBX のインタフェース C，D には，それぞれ異なる ISP のグローバル IP アドレスを，一つずつ割り当てる。

インタフェース C，D に割り当てるグローバル IP アドレスは入替可能であるが，ここでは前の解説の設定を引き継いで考察しよう。

その場合，インタフェース C には ISP1 のグローバル IP アドレスを割り当てるので，その接続先は L2SW1 となる。インタフェース D には ISP2 のグローバル IP アドレスを割り当てるので，その接続先は L2SW2 となる。

接続先のスイッチが所属するネットワークセグメントの VLAN 名は，表 2「図 3 中のスイッチに定義された新 IP アドレス空間」を見ると，L2SW1 が「vlan1」であり，L2SW2 が「vlan2」である。

よって，正解は，インタフェース C が「vlan1」，インタフェース D が「vlan2」となる。

もちろん，インタフェース C，D に割り当てるグローバル IP アドレスは入替可能なので，解は順不同である。

©2017 ICT Workshop

## (4)

**解答例**

ク：IP-PBX
ケ：DNS
コ：LB

［ク］，［ケ］，［コ］

空欄ク～コを含む文章は，〔ブラウザを使った音声電話の通信〕の第 3 段落，5 番目の箇条書きにある。そこには，「図 6 中の通信の前に，［ク］の FQDN に関する［ケ］クエリが，AP から［コ］へ発行されることによって，図 6 中の AP と IP-PBX 間の通信は ISP1 と ISP2 に負荷分散される」と記述されている。

小問（2）の「● IP-PBX のマルチホーミング対応」で解説したとおり，インターネットから IP-PBX へのアクセスは，マルチホーミングで負荷分散する。

その負荷分散の実現に重要な役割を果たしているのが，LB の DNS ラウンドロビンの定義だ。IP-PBX のホスト名に対し，IP-PBX のインターネット側インタフェースの二つのグローバル IP アドレスを対応付けておくのである。

図 6 中の通信の前に，IP-PBX の FQDN に関する DNS クエリが発行されると，二つのインタフェースのグローバル IP アドレスを交互に回答するようになる。その DNS クエリは，AP から LB へと発行される。

よって，空欄クに該当する字句は「**IP-PBX**」となり，空欄ケに該当する字句は「**DNS**」となり，空欄コに該当する字句は「**LB**」となる。

なお，公表された解答例にはないが，空欄ケは，「**名前解決**」も正解として扱われるはずだ。

## ■設問 5

## (1)

**解答例**

サ：切り戻し

©2017 ICT Workshop

サ

空欄サを含む文章は，〔移行計画〕の第 2 段落の中にある。そこには，「サービス停止時間とは，切替作業，切替作業後の動作確認及び問題発生時の［サ］に要する時間の合計である」と記述されている。

このたび構築する新ネットワークは，マルチホーミングを導入するなど，変更内容が多岐にわたる。それゆえ，移行中は，情報システムのサービスを停止する必要がある。

切替の動作確認をした後，問題が発覚した場合は，現行の状態に戻してサービスを再開する必要がある。この現行の状態に戻すことを「切り戻し」という。サービス停止時間を見積もる際は，切り戻しに要する時間も勘定に入れておく必要がある。

切り戻しが発生するのは，切替の動作確認をした後であるから，切り戻しを考慮に入れたサービス停止時間は，「切替作業時間」「動作確認時間」「切り戻し時間」の三つからなる。

よって，空欄サに入る字句は「**切り戻し**」となる。

## (2)

**解答例**

**FQDN 数：1**
**グローバル IP アドレス数：4**

問題文は，「本文中の下線（j）の四つの A レコードに記述されている，FQDN とグローバル IP アドレスの数をそれぞれ答えよ」と記述されている。

下線（j）は，〔移行計画〕の第 4 段落，（切替 1 について）の 1 番目の箇条書きにある。第 4 段落によれば，移行の切替は 2 段階で行う。

第 1 段階目の切替 1 について，1 番目の箇条書きには「LB の設定は，切替 1 で全ての定義を盛り込み，その後の変更を不要にする。例えば，DNS 機能については，新たなネットワーク構成に必要な次の A レコードを全て設定する」と記述されている。

切替 1 で設定する必要がある A レコードとして，次の 2 種類が挙げられている。

一つ目は，「（j）Web サーバ 1 と Web サーバ 2 に関する四つの A レコード」である。ここに下線（j）が引かれている。

二つ目は，下線（k）が引かれているので，これを問うている次の小問（3）の解説で取り上げることにしよう。

©2017 ICT Workshop

新ネットワークではマルチホーミングを導入するため，その実現に当たって，LB の DNS 機能に様々な設定を行う。

その一つ，「Web サーバ 1 と Web サーバ 2 に関する四つのレコード」の設定内容については，設問 2 の冒頭の解説，「・DNS ラウンドロビンの定義」の中で既に説明済みである。そこでは，Web サーバのホスト名を www と仮置きした上で，次のように述べている。

「Web サーバの公開用 IP アドレスとして，従来から使用している ISP1 のグローバル IP アドレス 2 個と，新たに ISP2 から払い出されるグローバル IP アドレス 2 個を用意しておく。DNS ラウンドロビン機能を用い，ホスト名 www にこれらを対応付けて登録しておく」。

同じ解説の図「A 社の新ネットワーク構成（LB が関わる部分を抜粋）」には，この解説に沿った DNS ラウンドロビンの定義例も示している。

以上より，解を導くことができる。

正解は，FQDN の数が「1」となり，グローバル IP アドレスの数が「4」となる。

## (3)

**解答例**

IP-PBX，STUN サーバ 1，STUN サーバ 2

問題文は，「本文中の下線（k）の FQDN に対応する機器名を，全て答えよ」と記述されている。

下線（k）は，〔移行計画〕の第 4 段落，（切替 1 について）の 1 番目の箇条書きにある。小問（2）で解説したとおり，LB の DNS 機能については，新ネットワークに必要な設定を全て実施する。その A レコードとして次の 2 種類が挙げられている。

一つ目は，「Web サーバ 1 と Web サーバ 2 に関する四つの A レコード」である。これを問うているのが小問（2）であった。

二つ目は，「（k）AP が解決しなければならない FQDN に関する A レコード」である。ここに下線（k）が引かれている。

この二つ目については，「AP 内の定義には，IP アドレスではなく，FQDN を用いることにする」という文が続いている。したがって，AP がアクセスする機器について，A レコードの定義が必要となることが分かる。

新ネットワークにおいて，AP がアクセスする機器は，次の 3 種類である。

©2017 ICT Workshop

- STUN サーバ
- IP-PBX
- 通話相手の AP

このうち，通話相手の AP の利用者端末は，そもそも DNS サーバの A レコードに登録する対象ではない。AP 同士がシグナリング通信中に IP アドレスを交換する仕組みになっている。それゆえ，これは空欄（k）の対象から外す。

したがって，残った STUN サーバ，IP-PBX が，空欄（k）の対象であると推論できる。すなわち，AP 内の定義に FQDN を使用し，AP の処理中に名前解決する機器であるわけだ。

実を言うと，設問 3，4 の解説の中で，STUN サーバ，IP-PBX について，DNS サーバの A レコードに登録する旨の説明を既に行っている。以下，その点を振り返ってみよう。

STUN サーバ，IP-PBX は共に，マルチホーミングによる負荷分散と冗長化を行う。その実現に当たって，LB の DNS 機能に様々な設定を行う。

まず，STUN サーバの設定内容を解説しよう。これに関しては，設問 3（3）の解説，「● STUN サーバのマルチホーミング対応」の「2. DNS ラウンドロビンの定義」の中で既に説明済みである。詳しくはその解説を参照していただくこととし，結論だけ示そう。そこでは，次のように述べている。

「LB の DNS ゾーン情報に，STUN サーバのホスト名とその IP アドレスの対応を登録する。DNS ラウンドロビン機能を用い，STUN サーバのホスト名に，STUN サーバ 1，2 の 2 個の IP アドレスを対応付ける」。

したがって，この記述から，A レコードの設定が必要なサーバとして，「STUN サーバ 1」「STUN サーバ 2」があることが分かる。

次に，IP-PBX の設定内容を解説しよう。これに関しても，設問 4（2）の解説，「● IP-PBX のマルチホーミング対応」の「2. DNS ラウンドロビンの定義」の中で既に説明済みである。詳しくはその解説を参照していただくこととし，結論だけ示そう。そこでは，次のように述べている。

「LB の DNS ゾーン情報に，IP-PBX のホスト名とその IP アドレスを登録する。DNS ラウンドロビン機能を用い，IP-PBX のホスト名に対し，インタフェース C，D の 2 個の IP アドレスを対応付ける」。

したがって，この記述から，A レコードの設定が必要なサーバとして，「IP-PBX」があることが分かる。

以上をまとめると，正解は，「**STUN サーバ 1，STUN サーバ 2，IP-PBX**」となる。

©2017 ICT Workshop

## (4)

**解答例**

FW

問題文は，「本文中の下線（1）について，2 通りの定義ファイルが必要な機器名を答えよ」と記述されている。

下線（1）は，〔移行計画〕の第 4 段落，（切替 1 について）の 3 番目の箇条書きにある。そこには「次の点を考慮し，切替 1 のサービス時間は 2 時間とする」と記述されている。そして，この考慮すべき点の一つが，次のように示されている。下線（1）はここに引かれている。

> ・次の点を考慮し，切替 1 のサービス停止時間は 2 時間とする。
> －（1）機器の変更は，あらかじめ 2 通りの定義ファイルをもたせておき，定義ファイルを指定した再起動によって行う。

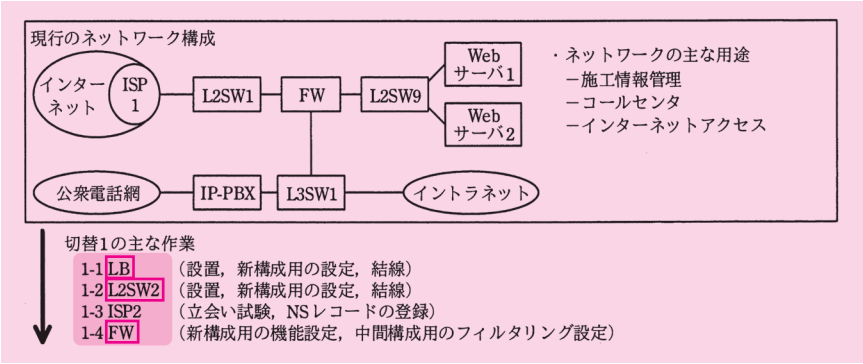
サービス停止時間については，第 2 段落の中で「今回の機能拡張に関して，サービス停止時間を見積もりながら，利用者への影響が極力小さくなるような移行を考えた」と記述されている。このように極力小さくすることを目的として，定義ファイルを指定して再起動するという方法を採用するに至ったわけだ。

したがって，ここで問われているのは，サービス停止時間を極力短くするために，「2 通りの定義ファイルが必要な機器名」である。

本問を解くに当たって，まずは切替 1 において「変更」が必要となる機器を特定する。実はそれが求める解となるのだが，その答えを裏付けるために，サービス停止時間を極力短くするという観点から，当該機器に定義ファイルを 2 通り用意する理由を考察しよう。

まず，切替 1 で設定する機器については，図 7「ネットワークの移行計画案」の中に示されている。その「切替 1 の主な作業」の中を見ると，設定する機器は，「LB」「L2SW2」「FW」の三つであることが分かる。

©2017 ICT Workshop




**図：切替 1 の主な作業（図 7 の一部を抜粋）**

このうち，新設する機器は「LB」「L2SW2」であり，既存の設定から変更する機器は「FW」である。したがって，変更する機器は「FW」となる。これが求める解となる。

次に，その答えを裏付けるためため，サービス停止時間を極力短くするという観点から考察しよう。サービス停止時間の内訳は，設問 5（1）で解説したとおり，「切替作業時間」「動作確認時間」「切り戻し時間」の三つからなる。

まず，切替作業時間を短くする観点から考えてみよう。そのためには，新ネットワーク用の定義ファイルをあらかじめ用意しておき，切り替える際にこれを指定して再起動すればよい。これが，下線（1）の述べる定義ファイルの一つ目である。

もちろん，この方法は，新設する機器の設定においても有効である。移行前に機器単体で起動し，定義ファイルをあらかじめ用意しておくわけだ。

次に，動作確認時間を短くする観点から考えてみよう。これについては，定義ファイルは特に関係がない。

最後に，切り戻し時間を短くする観点から考えてみよう。そのためには，現行ネットワーク用の定義ファイルをあらかじめ保存しておき，切り戻す際にこれを指定して再起動すればよい。これが，下線（1）の述べる定義ファイルの二つ目である。

この方法は，新設する機器には不要である。

したがって，定義ファイルが 2 通り必要となるのは，FW であることが分かる。

よって，正解は「**FW**」となる。

©2017 ICT Workshop

## (5)

**解答例**

①社外からWebサーバへのアクセス（16字）
②社内からWebサーバへのアクセス（16字）
③社内からインターネットへのアクセス（17字）

問題文は，「本文中の下線（m）の 3 種類の通信を……答えよ」と記述されている。

下線（m）は，〔移行計画〕の第 4 段落，（切替 1 について）の 3 番目の箇条書きにある。そこには「約 1 時間，一部の利用者に情報システムを利用してもらい，（m）3 種類の通信を発生させて，動作の正常性を確認する」と記述されている。

本問は，移行に伴うサービス停止のうち，動作確認に関わるものである。

動作確認の目的は，切替後にサービスを提供できるかをテストすることである。

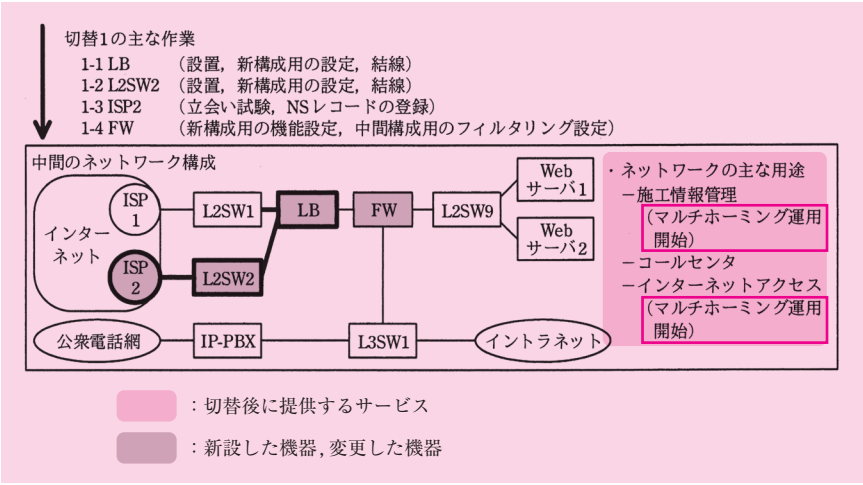
動作確認は，必要なものに留めるべきである。なぜなら，サービス停止時間をできるだけ短くしたいからだ。それゆえ，動作確認は，切替作業で新設した機器と変更した機器を対象とする。

切替 1 の作業に成功したとき，「中間のネットワーク構成」に至る。このときに提供するサービスについて，図 7「ネットワークの移行計画案」の「中間のネットワーク構成」「ネットワークの主な用途」から確認できる。そこには，従来の 3 種類の機能である，「施工情報管理」「コールセンタ」「インターネットアクセス」が挙げられている。ただし，施工情報管理とインターネットアクセスは，マルチホーミング運用を前提としている。

切替 1 の主な作業も，図 7 から確認できる。そこには，「LB」「L2SW2」「ISP2」「FW」に関わる作業が挙げられている。このうち，新設したものは，LB，L2SW2，ISP2 である。変更した機器は，FW である。

したがって，一部の利用者の協力を得て動作確認する，下線（m）の述べる「通信」とは，中間のネットワーク構成において従来機能を実行する際に発生する通信のうち，新設した機器，変更した機器を経由する通信である。下線（m）は，それが 3 種類あると述べている。

©2017 ICT Workshop




**図：中間のネットワーク構成（図 7 の一部を抜粋）**

施工情報管理について，序文の第 1 段落の 1 番目の箇条書きに，「外出先又は社内にいる A 社の社員や施主が，……Web サーバが管理する施工情報に HTTPS プロトコルでアクセスする」と記述されている。したがって，この機能を実行する際に発生するトラフィックは，次の［A］［B］である。動作確認の対象となる機器を網掛けで示す。

［A］社外から Web サーバへのアクセス
ISP1 → L2SW1 → LB → FW → L2SW9 → Web サーバ 1 又は 2
ISP2 → L2SW2 → LB → FW → L2SW9 → Web サーバ 1 又は 2
［B］社内から Web サーバへのアクセス
イントラネット→ L3SW1 → FW → L2SW9 → Web サーバ 1 又は 2

［A］は，新設した機器，変更した機器のどちらも経由する。［B］は，変更した機器である FW を経由する。したがって，動作確認する通信に該当する。

コールセンタについて，序文の第 1 段落の 2 番目の箇条書きに，「施主からの問合せ電話を，データセンタの IP-PBX を使って……受け付け（る）。必要に応じて営業部や技術部に転送する」と記述されている。したがって，この機能を実行する際に発生するトラフィックは，次の［C］，［D］である。

［C］公衆電話網から IP-PBX へのアクセス
［D］IP-PBX からイントラネットの IP 電話機へのアクセス

©2017 ICT Workshop

［C］，［D］はいずれも，新設した機器，変更した機器を経由しない。したがって，動作確認する通信には該当しない。

インターネットアクセスについて，序文の第 1 段落の 3 番目の箇条書きに，「社内からブラウザを使ってインターネットにアクセスする」と記述されている。したがって，この機能を実行する際に発生するトラフィックは，次の［E］である。動作確認の対象となる機器を網掛けで示す。

［E］社内からインターネットへのアクセス
イントラネット→ L3SW1 → FW → LB → L2SW1 → ISP1
イントラネット→ L3SW1 → FW → LB → L2SW2 → ISP2

［E］は，新設した機器，変更した機器のどちらも経由する。したがって，動作確認する通信に該当する。

以上より，3 種類の通信とは，［A］，［B］，［E］となる。

よって，正解は解答例に示したとおりとなる。

## (6)

**解答例**

| I | S | P | 2 | を | 経 | 由 | し | た | 外 | 向 | き | D | N | S | 機 | 能 | を | 確 | 認 | す | る | 。 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

（23 字）

問題文は，「本文中の下線（n）の確認内容を……述べよ」と記述されている。

下線（n）は，〔移行計画〕の第 4 段落，（切替 1 について）の 3 番目の箇条書きにある。そこには「(n) ドメイン登録業者に依頼する定義変更に関しては，情報システム部が正常性を確認する」と記述されている。

この作業を示す記述が本文中に二つある。

一つ目は，図 7「ネットワークの移行計画案」の「切替 1 の作業」の「1-3 ISP2」の中にある。そこには「NS レコードの登録」とある。これは，ドメイン権威サーバの登録を意味している。

二つ目は，〔マルチホーミング〕の第 4 段落にある。この第 4 段落は，LB を使ったマルチホーミングの概要を説明している。その 1 番目の箇条書きの中で，「インターネット向けの DNS 機能を FW から LB へ移し，ISP2 を経由してもその DNS 機能を提供できるように，ドメイン登録業者に定義の追加を依頼する」と記述されている。

©2017 ICT Workshop

この記述に関しては，設問 2 の冒頭の解説，「・A 社ドメインの権威サーバの設定」の中で既に説明済みである。詳しくはその解説を参照していただくこととし，結論だけ示そう。そこでは，A 社のドメイン名を「a-sha.co.jp」と仮置きした上で，次のように述べている。

「ドメイン登録業者に依頼する内容は，上位ドメイン『co.jp』の DNS サーバのゾーン情報に，A 社ドメインの権威サーバの IP アドレスとして，ISP2 から払い出されたグローバル IP アドレスを追加することである」。

同じ解説の図「上位ドメイン（co.jp）に登録する A 社ドメインの権威サーバの定義」には，この解説に沿った登録内容例も示している。

それでは，「ドメイン登録事業者に依頼する定義変更」が分かったところで，本問の解を導こう。

ここで問われているのは，「確認作業」ではなく「確認内容」である。つまり，「どのような作業を行うのか」ではなく，「何を確認するのか」を答える必要があるわけだ。

その確認内容とは，インターネット向けの DNS 機能が，ISP2 経由で提供できているかどうかである。

よって，その旨を字数に収まるように解答すればよい。正解は，解答例に示したとおりとなる。

## (7)

**解答例**

①’，③，④

問題文は，「本文中の下線（o）のフィルタリング変更について，切替 2 で許可する通信を全て挙げ，図 5 中の記号（①，①’，②～④）を用いて答えよ」と記述されている。

下線（o）は，〔移行計画〕の第 4 段落，（切替 2 について）の 1 番目の箇条書きにある。そこには「(o) FW のフィルタリング変更は，新たなネットワーク構成の通信に関して変更する」と記述されている。

切替 2 の変更点は大きく二つある。

一つ目はネットワークの用途である。その点は，図 7「ネットワークの移行計画案」の「新たなネットワーク構成」，その右側の「ネットワークの主な用途」から確認でき

©2017 ICT Workshop

る。そこには，新たに追加される用途として，「ブラウザを使ったビデオ電話」「ブラウザを使った音声電話」の 2 種類が挙げられている。

二つ目はネットワークの構成である。この構成変更は新たに追加される用途に対応しており，中間のネットワーク構成から新ネットワーク構成に変更される。

切替 2 の主な作業も，図 7 から確認できる。そこには，「STUN サーバ」「IP-PBX」「FW」に関わる作業が挙げられている。このうち，新設した機器は，STUN サーバである。変更した機器は，IP-PBX，FW である。

本問は，この FW について，新たなネットワーク構成で許可する通信を，図 5 の中から答えるよう求めている。

図 5「AP 間の通信」は，ブラウザを使ったビデオ電話の通信である。

それでは，ここに挙げられた 5 種類の通信（①，①’，②～④）について，一つずつ考察しよう。このうち，そもそも FW を通過しないものと，フィルタリングルールの中で既に許可されているものを除外すれば，解が得られる。

図 5 の通信手順については，設問 3（4）の解説「● AP 間通信の手順（IP アドレスとポート番号の組に着目）」の中で既に説明済みである。IP アドレスとポート番号の組に関する詳しい説明はそちらを参照していただくこととし，ここではそれを踏まえて解を導くことにする。

**●通信①，①’について**

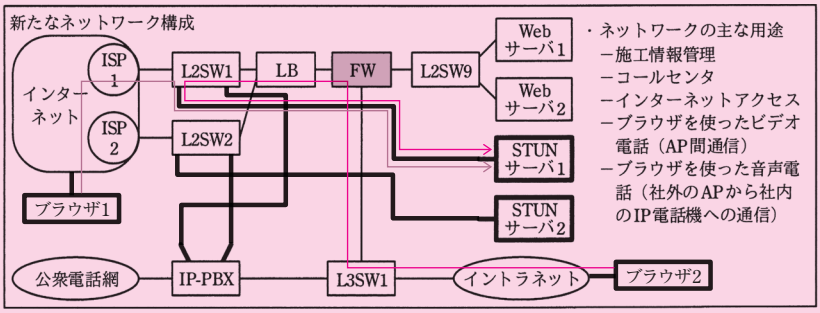
通信①は，送信元がインターネットのブラウザ 1 の AP，宛先が STUN サーバ 1 又は 2 である。通信プロトコルは，STUN プロトコルである。

この通信は FW を経由しないため，フィルタリングの対象から除外する。

通信①’は，送信元がイントラネットのブラウザ 2 の AP，宛先が STUN サーバ 1 又は 2 である。通信プロトコルは，STUN プロトコルである。

この通信は FW を経由し，かつ，新たに追加されるビデオ電話のためのものである。したがって，フィルタリングの対象である。

©2017 ICT Workshop



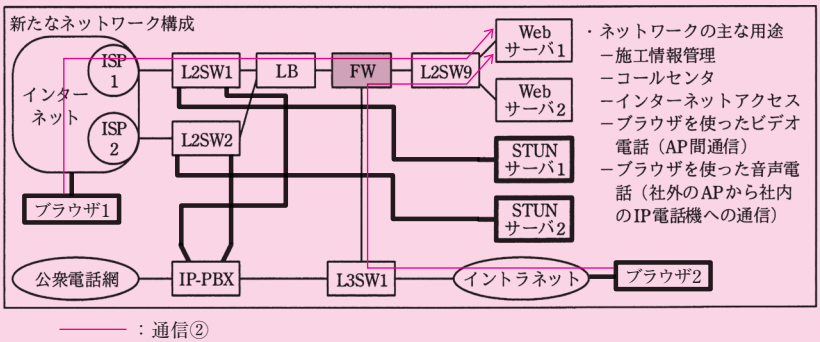

注）STUN サーバへのアクセスは，STUN サーバ 1 が選択されたものとしている。

**図：新たなネットワーク構成における，図 5 中の通信①，①'**

**●通信②について**

通信②は，送信元がインターネットのブラウザ 1 の AP，又は，イントラネットのブラウザ 2 の AP である。宛先が Web サーバ 1 又は 2 である。通信プロトコルは，HTTPS である。

社外及び社内から Web サーバ宛ての HTTPS 通信は，従来の機能「施工情報管理」で既に許可されているため，フィルタリングの対象から除外する。




注）Web サーバへのアクセスは，Web サーバ 1 が選択されたものとしている。

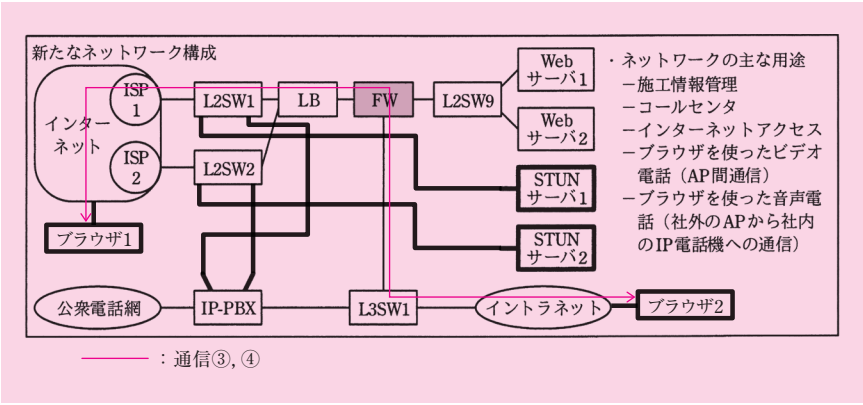
**図：新たなネットワーク構成における，図 5 中の通信②**

**●通信③，④について**

通信③，④は，エンドポイントがインターネットのブラウザ 1 の AP，イントラネッ

トのブラウザ 2 の AP である。通信プロトコルは AP 固有のもので，「AP が使用するポート番号はあらかじめ決められている」（〔ブラウザを使ったビデオ電話の通信〕第 9 段落）。

この通信は FW を経由し，かつ，新たに追加されるビデオ電話のためのものである。したがって，フィルタリングの対象である。




**図：新たなネットワーク構成における，図 5 中の通信③，④**

**●解の導出**

以上より，許可すべき通信は，①’，③，④となる。よって，これが正解となる。

©2017 ICT Workshop

# 問 2

## 出題趣旨

拠点間をインターネット VPN 又は広域イーサネットサービス網（以下，広域イーサ網という）で接続している企業は多い。企業活動が IT によって成り立っている現在，システムの可用性向上は，どの企業においても重要な課題の一つである。

このような状況を基に，本問では，広域イーサ網とインターネット VPN によって，WAN 回線を冗長化する事例を取り上げた。冗長化に当たって，広域イーサ網とインターネット VPN の間でトラフィックを分散させて，WAN 回線を有効に活用することを要件とした。この要件を満たす方策として，2 種類の WAN 回線の間で OSPF を稼働させる方法を解説した。

本問では，多くの企業のネットワークに利用されている IPsec，トンネリング及び OSPF を題材に，ネットワークの設計，構築，運用に携わる受験者が修得した技術と経験が，実務で活用できる水準かどうかを問う。

## 採点講評

問 2 では，WAN 回線の冗長化をテーマに，拠点間を広域イーサ網とインターネット VPN によって冗長化する事例を取り上げた。その中で，IPsec だけでなく，L2TP，GRE 及び GRE over IPsec などのトンネリング技術についても問うた。

設問 1 では，アとイが，踏み込んだ内容を問う設問だったことからか，正答率は低かった。

設問 2 では，IPsec 関連技術を問うた。(1)の正答率は高かったが，(2)の正答率が低かった。IKE フェーズ 1 とフェーズ 2 では，それぞれ認証方式の交渉が行われるが，フェーズ 2 で交渉される認証方式は，IPsec 通信で送受信されるデータの完全性を認証するためのものであることを，表の内容と本文の記述から導き出してほしかった。

設問 3 では，L2TP と GRE について問うたが，(3)の正答率が低かった。図で示した通信手順とパケット形式を基にじっくり考えれば，正答を導き出せたはずである。

設問 4 では，GRE パケットを IPsec でカプセル化する方法について問うた。ネットワークスペシャリスト試験の午後では初めての出題分野であったが，正答率は高かった。

設問 5 は，ネットワーク技術者の主要な業務に直結した設問であったことからか，(3)，(4)及び(6)の“え”を除き正答率は高かった。(3)は，VRRP の動作を基に考えれば，正答が導けたはずである。(4)は，VRRP のマスタルータの状態と経路テーブルの変化後の内容を基に，サーバ宛てのパケットが転送される経路について考える設問だったが，機器間の接続が切断されることによる経路テーブルの変化内容が理解できていない解答が散見された。動的経路制御はネットワークの基盤となる技術なので，是非とも基本技術は習得してほしい。(6)の“う”の解答からは，インターネット VPN の設定についての本文の記述を見落とした受験者が多かったことがうかがえた。

©2017 ICT Workshop

| 設問 | | 解答例・解答の要点 | | | | 備考 |
|---|---|---|---|---|---|---|
| 設問 1 | | ア | 32 | | | |
| | | イ | セレクタ | | | |
| | | ウ | アグレッシブ | | | |
| | | エ | 経路 | | | |
| | | オ | 断片化 | | | |
| 設問 2 | (1) | リキー（ReKey） | | | | |
| | (2) | IPsec 通信で送受信されるメッセージが，通信中に改ざんされていないこと | | | | |
| | (3) | OSPF のリンクステート情報交換は，IP マルチキャスト通信で行われるから | | | | |
| 設問 3 | (1) | あ | 1,436 | | | |
| | | い | 1,414 | | | |
| | (2) | IP ヘッダ 1 | 送信元 IP アドレス | $\alpha$ .0.0.1 | | |
| | | | 宛先 IP アドレス | $\beta$ .0.0.1 | | |
| | | IP ヘッダ 2 | 送信元 IP アドレス | 192.168.0.100 | | |
| | | | 宛先 IP アドレス | 192.168.10.1 | | |
| | (3) | ①の通信で PC が取得する IP アドレスが格納されるヘッダ | IP ヘッダ 1 | | | |
| | | ②の通信で PC が取得する IP アドレスが格納されるヘッダ | IP ヘッダ 2 | | | |
| | (4) | カプセル化によるオーバヘッドが L2TP より小さいので，一つのパケットで転送できるデータ量が多い。 | | | | |
| 設問 4 | (1) | GRE でトンネリングが行われるから | | | | |
| | (2) | ESP 認証データ長は，使用する認証アルゴリズムによって変化するから | | | | |
| | (3) | GRE ヘッダ，IP ヘッダ 2，TCP/UDP ヘッダ，データ，ESP トレーラ | | | | |
| 設問 5 | (1) | 172.16.128.0/20，172.16.17.0/24 | | | | |
| | (2) | L2SWa と L2SWb を異なるサブネットにする。 | | | | |
| | (3) | 本社 | 2 | | | |
| | | 営業所 | 1 | | | |
| | | データセンタ | 2 | | | |
| | (4) | どのサーバアクセスも，VRRP のマスタルータが稼働する機器に接続された WAN 回線を経由して行われる。 | | | | |
| | (5) | インターネット VPN 経由のコスト値が最小 230 であるのに対して，専用線経由のコスト値は 200 で最も小さい。 | | | | |
| | (6) | う | 広域イーサ網→本社→専用線 | | | |
| | | え | インターネット VPN →データセンタ→専用線 | | | |

©2017 ICT Workshop

本問は，IPsec，GRE，L2TP，OSPF，VRRP を題材に，それら要素技術の知識，及び，それらの要素技術を用いた WAN 回線の冗長化設計について出題している。

**●本問の全体像**

事例に登場する Y 社は，東京本社の他に名古屋，大阪，福岡に営業所がある。
現行ネットワークの主な特徴は，次のとおりである。

- 本社と営業所間は広域イーサ網で接続されている。
- 本社で各種サーバを運用し，営業所は広域イーサ網経由でサーバにアクセスしている。
- 本社及び営業所からのインターネットアクセスは，本社のプロキシサーバ経由で行っている。

Y 社では，WAN 回線の可用性向上を目的に，ネットワーク再構築を検討している。
序文の第 2 段落，及び，〔WAN の設計〕の第 1 から第 4 段落に，再構築の要件が記述されている。

**要件 1. WAN 回線の冗長化**

インターネット VPN を新たに導入する。インターネット VPN と既設のイーサネット網との間で，WAN 回線を冗長化する。

その際，アクセス先のサーバによって使用する WAN 回線を分ける。

**要件 2. 本社サーバをデータセンタに移設**

本社の DM サーバ以外のサーバを，Z 社のデータンセンタに移設する。
本社とデータセンタ間を専用線で接続する。
インターネットアクセスは，データセンタを経由する。

これら要件のうち，ほとんどの設問が一つ目の要件に関する出題である。
一つ目の要件を実現するために，新ネットワークの構築に用いる主な要素技術は，次のとおりである。

［1］IPsec

IPsec を用い，インターネット VPN を構築して，そこを通過するパケットを暗号化する。

©2017 ICT Workshop

［2］トンネリング技術（GRE，L2TP）

IP マルチキャストパケットをインターネット VPN で通過させるには，パケットをトンネリングプロトコルでいったんカプセル化して IP ユニキャストパケットに仕立て，これを IPsec でカプセル化する必要がある。

本事例では，そのトンネリングプロトコルの候補として，GRE，L2TP の二つの要素技術を調査する。その結果，GRE に優位性があると判断し，インターネット VPN 上で GRE over IPsec を用いる。

なお，本事例において，インターネット VPN 経由でやり取りされる IP マルチキャストパケットは，後述する OSPF のリンクステート情報交換パケットだ。

［3］OSPF

OSPF を用い，一つ目の要件である，WAN 回線の冗長化，及び，アクセス先に応じた WAN 回線の使い分けを実現する。

［4］VRRP

前述のとおり，本社，営業所，データセンタ間は，2 系統の WAN 回線で結ばれる。各拠点の回線終端に設置する装置として，インターネット VPN 接続には IPsec ルータを，広域イーサ網接続には既設の L3SW を，それぞれ用いる。

VRRP を用い，IPsec ルータと L3SW を各拠点で冗長化する。

以上を踏まえて本問の構成を概観すると，次のように整理できる。

**表：本問の構成**

| 見出し | 主な内容 | 主に対応する出題箇所 | |
|---|---|---|---|
| | | 設問 | 小問 |
| なし（序文） | 現在のネットワーク構成，新ネットワークの要件 | — | — |
| インターネット VPN の構築技術の検討 | ［1］IPsec | 1 | 空欄ア～ウ |
| | | 2 | (1) ～ (3) |
| トンネリング技術の調査 | ［2］トンネリング技術 | 1 | 空欄エ～オ |
| | | 3 | (1) ～ (4) |
| GRE over IPsec の稼働方法の検討 | ［1］IPsec | 4 | (1) ～ (3) |
| WAN の設計 | 要件 2 のサブネット設計 | 5 | (1) |
| | ［3］OSPF<br>［4］VRRP | 5 | (3) ～ (6) |

©2017 ICT Workshop

本問を首尾よく解くには，トンネリング技術の仕組みを理解しておく必要がある。そこで，設問の解説に入る前に，トンネリング技術の概要を解説しよう。

**●トンネリングとは**

トンネリングとはどのような技術であろうか。その点について，本文の〔インターネット VPN の構築技術の検討〕の第 1 段落，「(2) IPsec の通信」の 6 番目の箇条書きに，次のように説明されている。

> ・トンネリングは，インターネットのような共用ネットワーク上の 2 点間で，仮想の専用線を構築することである。トンネリングは，あるプロトコルのトラフィックを別のプロトコルでカプセル化することで実現する。

ここに「仮想の専用線を構築すること」とある。トンネリング技術を理解する上で，このイメージをもつことが重要である。

**●図 4 の例**

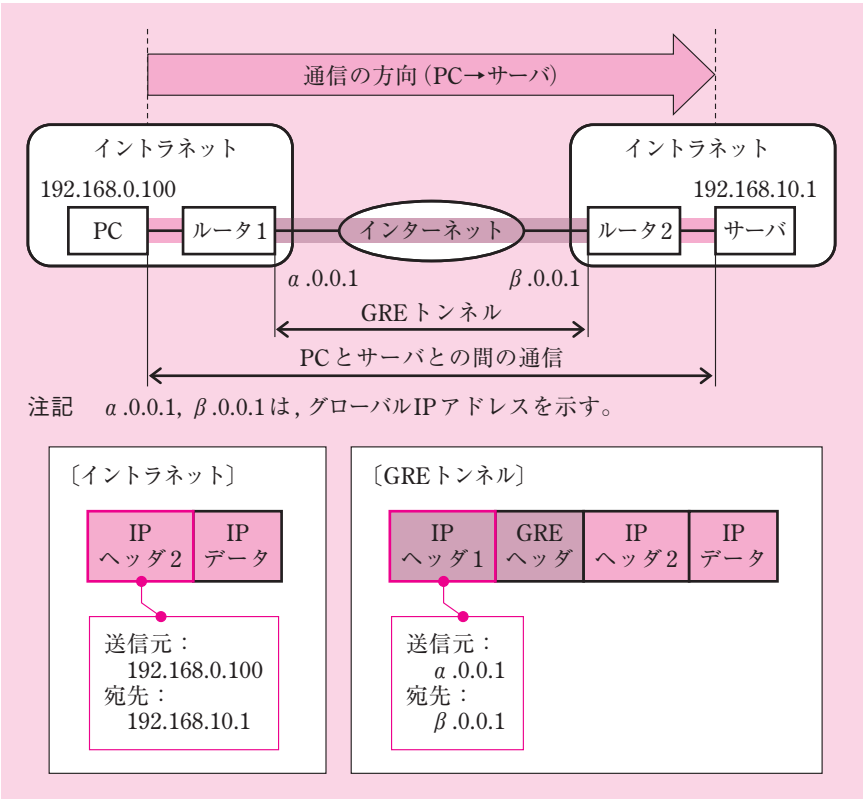
本文中の図を使って，この仮想的な専用線がどのように構築されるのか，そして，パケットがどのように送信されるのかを解説しよう。

〔トンネリング技術の調査〕の第 5 段落の図 4「GRE 利用時の通信例」には，インターネットを介して接続された二つのイントラネットが登場する。一方のイントラネットには PC があり，他方のイントラネットにはサーバがある。

この PC とサーバ間の通信において，インターネット区間をトンネリングしている。

このときトンネリングに用いられているカプセル化用プロトコルは，GRE である。もっとも，GRE であろうと他のカプセル化用プロトコルであろうと，「トンネリングとは仮想的な専用線を構築することである」という本質的な仕組みには変わりがない。

©2017 ICT Workshop




**図：GRE 利用時の通信例（図 4 に加筆）**

**・インターネット区間に構築された，仮想的な専用線**

この図で，GRE トンネル区間は，インターネット区間である。この区間を通過するとき，パケットがカプセル化される。その点について，〔トンネリング技術の調査〕の第 4 段落には，「カプセル化とカプセル化の解除は，GRE トンネリングを行う両端の機器で行われる」と記述されている。この図でそれを行っているのは，ルータ 1 とルータ 2 である。したがって，GRE でカプセル化したパケット（以下，GRE パケットという）は，送信元と宛先が，ルータ 1 とルータ 2 になることが分かる。

**・PC からサーバにパケットを送信するケース**

図のネットワーク構成について理解できたところで，次に，PC からサーバに IP パケットを送信するケースを例に，パケットがどのようにカプセル化されるのかを解説しよう。

©2017 ICT Workshop

前述のとおり，トンネルは，仮想的な専用線の役割を果たす。実際には二つのイントラネットがインターネットで接続されているにもかかわらず，仮想的には専用線で直接接続されているかのように見えているわけだ。

それゆえ，イントラネットの区間（PC とルータ 1 間，ルータ 2 とサーバ間）では，PC からサーバに送信される IP パケットは，送信元が PC（192.168.0.100），宛先がサーバ（192.168.10.1）である。要するに，何の変哲もない，イントラネットを流れる通常のパケットだ。この IP ヘッダを，「IP ヘッダ 2」と表記しよう（本文の図 3 に合わせている）。

ルータ 1 が PC からこの通常パケットを受け取ると，ルータ 1 内の GRE トンネルインタフェースに転送する。実際の振舞いは，ルータ 1 が GRE パケットを生成し，これをインターネット側に転送している。

この GRE パケットは，送信元がルータ 1（$\alpha$ .0.0.1），宛先がルータ 2（$\beta$ .0.0.1）である。この IP ヘッダを，「IP ヘッダ 1」と表記しよう（本文の図 3 に合わせている）。図の注記から分かるとおり，この IP ヘッダの宛先と送信元は，グローバル IP アドレスである。

これまでの解説から，トンネリングが仮想的な専用線であるといわれる理由が明らかになる。

インターネットはグローバル IP アドレス空間なので，プライベート IP アドレスの経路情報をもたない。それゆえ本来であれば，IP ヘッダ 2 をもつパケットは，インターネット区間を通過できない。

しかし，二つのイントラネットがあたかも専用線で結ばれているかのように，IP ヘッダ 2 をもつパケットが，PC からサーバ宛てに送信されている。これを可能にしているのがトンネリング技術なのである。

インターネット区間が GRE トンネル区間となっているため，実際にここを通過しているのは，GRE パケットである。これは IP ヘッダ 1 をもっており，その宛先と送信元はグローバル IP アドレスである。この経路情報はインターネットに存在しているため，この区間を通過できるのだ。

**●本事例で用いる GRE over IPsec**

実際に本事例で用いるカプセル化のプロトコルは，GRE over IPsec である。

少々複雑だが，これは，GRE パケットを IPsec でさらにカプセル化したものである。

その点について，〔GRE over IPsec の稼働方法の検討〕の第 4 段落には，次のように記述されている。

©2017 ICT Workshop

> PC とサーバからインターネット VPN 向けに送信されるパケット，及び OSPF によってインターネット VPN に広告されるリンクステート情報には，GRE によるカプセル化と IPsec による暗号化を設定する。

「GRE によるカプセル化と IPsec による暗号化を設定する」とあるとおり，トンネリングに GRE を用い，暗号化に IPsec を用いている。

つまり，本事例では，GRE でカプセル化することによって，インターネット区間を仮想的な専用線とみなして通信することを可能にしている。そして，GRE パケットを IPsec でカプセル化することによって，インターネット区間を通過する GRE パケットを暗号化し，セキュリティを確保しているのである。

本事例では，カプセル化の対象となるパケットは，大きく 2 種類ある。一つ目は「PC とサーバからインターネット VPN 向けに送信されるパケット」であり，これは IP ユニキャストパケットである。二つ目は，「OSPF によってインターネット VPN に広告されるリンクステート情報」であり，これは IP マルチキャストパケットである。

詳しくは設問 2 のところで解説するが，IP マルチキャストパケットをインターネット VPN 経由でやり取りするために，トンネリング技術の GRE が用いられている。

最後に，本事例で構築するトンネルについて，確認しよう。

〔WAN の設計〕の第 2 段落には，次のように記述されている。

> インターネット VPN は，データセンタと本社間，及びデータセンタと営業所間で設定する。

この記述から，特定の拠点間にのみ，トンネルを構築することが分かる。

この一文は，設問 5 で問われる WAN 設計において，経路情報を正しく読み解くために必要となるため，ぜひとも見落とさないように留意しておきたい。

「トンネリングとは仮想的な専用線である」ということを理解していれば，本問に限らずトンネリング技術が出題されたときに，「どの拠点間にトンネルを構築しているか」を確認するよう意識が働くはずだ。

それでは，設問の解説に移ろう。

©2017 ICT Workshop

## ■設問 1

**解答例**

ア：32
イ：セレクタ
ウ：アグレッシブ
エ：経路
オ：断片化

空欄ア～ウは IPsec の基礎知識を問うている。

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

**ア**

空欄アを含む文章は，〔インターネット VPN の構築技術の検討〕の第 1 段落，「(1) IPsec ルータ」の 2 番目の箇条書きの中にある。そこには，「SA の内容が確定すると，SA に関連付けされた SPI（Security Parameters Index）が，［ア］ビットの整数値で割り当てられる。SPI は，IPsec 通信の各パケット中に挿入され，そのパケットに適用された SA の識別キーとなる」と記述されている。

SA について，すぐ前の 1 番目の箇条書きの中で，「IPsec で使用される認証方式，暗号化方式，暗号鍵などは，IPsec ルータ同士による IKE（Internet Key Exchange）のネゴシエーションによって，IPsec ルータ間で合意される。この合意は，SA（Security Association）と呼ばれる」と記述されている。

この SA を識別する SPI のサイズが，ここで問われている。その答えは，「32」ビットである。

よって，正解は「**32**」となる。

**イ**

空欄イを含む文章は，〔インターネット VPN の構築技術の検討〕の第 1 段落，「(1) IPsec ルータ」の 4 番目の箇条書きの中にある。そこには，「SP を選択するキーを［イ］と呼び，IP アドレス，プロトコル，ポート番号などが利用される」と記述されている。

SP（セキュリティポリシ）について，すぐ前の 3 番目の箇条書きの中で，「IPsec ルータは，通信相手の IPsec ルータにパケットを送信するとき，IPsec 通信を行うか否

©2017 ICT Workshop

か，IPsec 通信を行うときはどの SA を使うかなど，当該パケットに施す処理を示したセキュリティポリシ（以下，SP という）を選択する」と記述されている。

セキュリティポリシを選択する条件は，IP アドレス，プロトコル（TCP，UDP の種別），ポート番号などが利用される。この条件のことを「セレクタ」という。

よって，正解は「**セレクタ**」となる。

**ウ**

空欄ウは，〔インターネット VPN の構築技術の検討〕の第 1 段落，「(2) IPsec の通信」の 2 番目の箇条書きの中にある。そこには，「IKE フェーズ 1 では，IKE フェーズ 2 で使用する ISAKMP（Internet Security Association and Key Management Protocol）SA 又は IKE SA（以下，両方を ISAKMP SA という）に必要なパラメータの交換，鍵交換及び認証が行われる。IKE フェーズ 1 には，メインモードと［ウ］モードがある。メインモードでは 3 往復の通信が行われるが，［ウ］モードは 1 往復半の通信で完了する」と記述されている。

IKE フェーズ 1 には 2 種類のモードがある。

一つ目は，メインモードである。

メインモードは，通信相手の IP アドレスが固定である場合に使用される。パラメータ交換，鍵交換及び認証のために，3 往復の通信が行われる。

二つ目は，アグレッシブモードである。

アグレッシブモードは，通信相手の IP アドレスが動的である場合に使用される。メインモードに比べて処理が簡略化されており，パラメータ交換，鍵交換及び認証のために，1 往復半の通信が行われる。

よって，空欄ウに該当する字句は「**アグレッシブ**」となる。

参考までに，本問が出題している IKE のバージョンは，バージョン 1 である。今日ではバージョン 2 が標準化されており，アグレッシブモードの廃止，IKE 通信の簡素化などが図られている。

以降は，ここで出題されたバージョン 1 に合わせて解説する。

**エ**

空欄エは，〔トンネリング技術の調査〕の第 5 段落にある。そこには，「IP パケットを GRE でカプセル化すると，カプセル化された元のパケットの宛先への［エ］情報をインターネットがもたなくても，元のパケットによるエンドツーエンドの通信が可能になる」と記述されている。

本問の冒頭で解説したように，トンネルは仮想的な専用線の役割を果たしている。

©2017 ICT Workshop

そこで述べたとおり，インターネットをトンネル区間に設定すると，実際にはインターネットで接続している区間が，仮想的に見ると専用線で接続している区間となる。それゆえ，カプセル化した元のパケットの宛先 IP アドレスがプライベート IP アドレスであっても，通信することができる。

したがって，空欄エが示しているのは経路情報だと考えれば，文全体の意味が通る。

要するに，ここで言わんとしているのは，次のような内容である。

プライベート IP アドレスを宛先とする経路情報を，インターネットはもっていない。にもかかわらず，GRE でカプセル化することによって，プライベート IP アドレスを用いたエンドツーエンドの通信が可能になる。

よって，空欄エに該当する字句は「**経路**」となる。

**オ**

空欄オは，〔トンネリング技術の調査〕の第 6 段落にある。そこには，「図 3 に示したカプセル化によって，図 4 中の，GRE トンネルインタフェースの MTU は，イーサネットインタフェースの MTU よりも 24 バイト小さくなる。このとき，図 4 中の PC 及びサーバのイーサネットインタフェースの MTU サイズを適切な値に変更することによって，パケットの［　オ　］を防げる」と記述されている。

ここに「PC 及びサーバのイーサネットインタフェースの MTU サイズを適切な値に変更する」とあるので，適切な値に変更しなかった場合，空欄オが示す事態を防げない可能性があることが分かる。

まず，図 4 中の機器のインタフェースについて，それぞれの MTU を確認しよう。次いで，「PC 及びサーバのイーサネットインタフェースの MTU サイズ」を既定のまま変更しないときにどのような事態が生じるかを考察しよう。それが本問の解答となる。

**●各インタフェースの MTU**

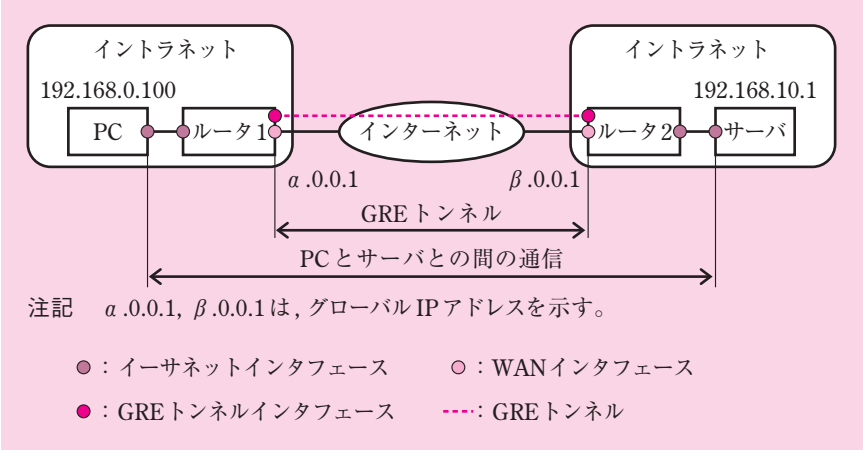
図 4 を見ると，大きく 3 種類のインタフェースがある。

一つ目は，イーサネットインタフェースである。これをもつのは，PC，サーバ，及び，ルータのイントラネット側のインタフェースである。

二つ目は，WAN インタフェースである。これをもつのは，ルータのインターネット側のインタフェースである。

三つ目は，GRE トンネルインタフェースである。このインタフェースをもつのはルータである。このインタフェースにパケットを転送すると，仮想的には，パケットがトンネル（仮想的な専用線）へ送り出されている。実際には，GRE でカプセル化されたものがインターネットへ送り出されている。

©2017 ICT Workshop




**図：各インタフェースの MTU（図 4 に加筆）**

インタフェースが 3 種類あることが分かったので，これらインタフェースの MTU を求めてみよう。

本文の図 3 にあるとおり，通常のパケットを GRE でカプセル化すると，GRE パケット用 IP ヘッダと GRE ヘッダが付与される。このサイズは 24 バイトである。したがって，GRE トンネルインタフェースの MTU は，WAN インタフェースの MTU より 24 バイト小さくなる。

空欄オを含む文章に「図 4 中の，GRE トンネルインタフェースの MTU は，イーサネットインタフェースの MTU よりも 24 バイト小さくなる」とある。この記述から，図 4 においては，WAN インタフェースとイーサネットインタフェースの MTU は，既定値が同じ大きさになっていると推論できる。

**● PC とサーバのイーサネットインタフェースの MTU を変更しなかった場合に生じる事態**

PC がサーバにパケットを送信すると（あるいは，サーバが PC にパケットを送信すると），当該パケットはルータのイーサネットインタフェースに到達する。

次に，ルータがこれを GRE トンネルインタフェースに転送する。実際には，カプセル化して 24 バイト分のヘッダを付与している。

PC から送信した IP パケットのサイズが，イーサネットインタフェースの既定値いっぱいだったとき，どうなるだろうか。

GRE トンネルインタフェースの MTU はそれより 24 バイト小さいので，IP パケッ

©2017 ICT Workshop

トが断片可される。

**●解の導出**

本問の解は，「PC 及びサーバのイーサネットインタフェースの MTU サイズ」を既定のまま変更しないときに生じる事態であった。

前述のとおり，そのときには IP パケットが断片化される。

よって，正解は「**断片化**」となる。

## ■設問 2

### (1)

**解答例**

リキー（ReKey）

問題文は，「表 2 中のライフタイムの終了時点に，IPsec ルータで行われる処理を答えよ」と記述されている。

表 2「IKE フェーズ 2 で決定されるパラメータ」は，〔インターネット VPN の構築技術の検討〕，「(2) IPsec の通信」の 3 番目の箇条書きにある。表題のとおり，表 2 は，IKE フェーズ 2 で決定されるパラメータに関する説明を掲載している。「ライフタイム」の説明には，「IPsec SA の生存期間」と記述されている。

「IPsec SA」とは，IPsec 通信で用いられる SA を指す。SA とは，「(1) IPsec ルータ」の 1 番目の箇条書きにあるとおり，「IPsec で使用される認証方式，暗号化方式，暗号鍵など……の合意」である(*)。「(2) IPsec の通信」の 3 番目の箇条書きにあるとおり，IPsec SA は，IPsec 通信に先立つ「IKE フェーズ 2」で合意した内容に基づいて，生成される。

（*）SA について，本文では「IPsec で使用される認証方式，暗号化方式，暗号鍵など……の合意」と述べ，受験者に分かりやすい平易な言葉で説明している。より厳密に言うと，IPsec の規格を定めた RFC（本書執筆時点の最新版は RFC4301）によれば，「SA は単方向のコネクションであり，SA によって伝送されるトラフィックに対し，セキュリティサービスを供給するものである」(An SA is a simplex "connection" that affords security services to the traffic carried by it.)。

一般的に言って，暗号化通信で同じ鍵を長期間にわたって使用し続けると，解読されるリスクが高まる。そこで，IPsec 通信では，暗号化通信の安全性を確保するため，

©2017 ICT Workshop

SA の生存期間を定め，生存期間が満了するたびに暗号鍵を作り替えている。

このように，生存期間ごとに SA を作り替えることを「リキー」（ReKey）と呼ぶ。

IPsec SA のリキーは，IPsec 通信が途切れないように，生存期間が満了する前に実施しておく。

したがって，IPsec SA のライフタイムの終了時点に，IPsec ルータで行われる処理は，リキーである。

よって，これが正解となる。

## (2)

**解答例**

IPsec通信で送受信されるメッセージが，通信中に改ざんされていないこと（36字）

問題文は，「表 2 中の認証方式によって認証できる対象と，その認証内容を……述べよ」と記述されている。

表 2「IKE フェーズ 2 で決定されるパラメータ」は，〔インターネット VPN の構築技術の検討〕にある。図のすぐ上，「(2) IPsec の通信」の 3 番目の箇条書きに，「IKE フェーズ 2 では，IPsec SA に必要なパラメータが決定される」と記述されているので，ここで問われている表中の「認証」とは，IPsec SA の認証を指していることが分かる。

ここまで整理できたところで，この続きは IPsec 通信に関する基礎知識に基づいて，解を導く。

一般的に言って，「認証」には，大きく二つの種類があることを押さえておこう。

一つ目は，エンティティ認証（相手認証）である。これは，相手がなりすましをしていないことを確かめるために行われる。その代表例は，パスワード認証である。

二つ目は，メッセージ認証である。これは，相手から受信したメッセージが改ざんされていないことを確かめるために行われる。その代表例は，電子署名，パケットに付与された改ざん検出用のコード，などである。

それでは，表 2 中の IPsec SA の「認証」は，どちらを指しているのだろうか。

その答えを導くには，IPsec 通信の基礎知識が欠かせない。

実は，IPsec 通信（IPsec SA）は，通信で送受信されるメッセージ認証を行っているが，エンティティ認証は行っていない。それゆえ，表 2 中の「認証」は，メッセージ認証を指している。

©2017 ICT Workshop

IPsec でカプセル化する際，AH 又は ESP を用いる。そのどちらも，（パケット内の認証範囲に若干相違はあるものの，）パケットごとに，改ざん検出用のコードを付与する。そのコード値はハッシュ技術を用いて生成される。

この点を踏まえて表 2 を読み返すと，IKE フェーズ 2 で，このハッシュ方式に関わるパラメータを決定していることが確認できる。

したがって，「認証できる対象」は，「送受信されるメッセージ」となる。「認証内容」は，「メッセージが改ざんされていないこと」となる。

よって，その旨を字数に収まるように解答すればよい。正解は解答例に示したとおりとなる。

参考までに，IPsec 通信のエンティティ認証は，IKE フェーズ 1 で実行される。これは，IPsec 通信を行う通信機器同士の認証である。この点について，表 1「IKE フェーズ 1 で決定されるパラメータ」の「認証方式」の中で，「IPsec 通信相手の認証方式」と記述されている。この認証方式としてよく用いられているのは，事前共有鍵方式である。

さらに，オプションの扱いであるが，ユーザ認証を行うことも可能だ。それには XAUTH と呼ばれる仕組みを用いることが規定されており，フェーズ 1 とフェーズ 2 の間に実行される。

## (3)

**解答例**

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O | S | P | F | の | リ | ン | ク | ス | テ | ー | ト | 情 | 報 | 交 | 換 | は | , | I | P | マ | ル | チ | キ | ャ |
| ス | ト | 通 | 信 | で | 行 | わ | れ | る | か | ら | | | | | | | | | | | | | | |

（36字）

問題文は，「本文中の下線（a）について，カプセル化できない理由を，“OSPF”及び“リンクステート情報”という字句を用いて……述べよ」と記述されている。

下線（a）は，〔インターネット VPN の構築技術の検討〕の第 2 段落にある。そこには，「調査の結果，（a）Y 社で検討中の IPsec ルータは，OSPF の通常の設定では，リンクステート情報の交換パケットをカプセル化できないので，……IPsec によってインターネット VPN を構築したとき，OSPF を稼働することができない」と記述されている。

この文章には，本問を解く上で着目すべき点を二つ見出せる。

一つ目は，「調査の結果」とあるので，調査によって，IPsec のカプセル化に関して

©2017 ICT Workshop

どのような制限が明らかになったのか，という点である。

二つ目は，OSPF のリンクステート情報の交換パケット（以下，OSPF パケットという）が，この制限に抵触するどのような特徴を有しているか，という点である。

もちろん，下線（a）には「カプセル化できない」とあるので，抵触するという点は既に明らかだ。ここで問われているのは，「カプセル化できない理由」なので，OSPF パケットがこれに抵触する内容を，具体的に解答することが求められている。

まず，一つ目の，IPsec のカプセル化に関する制限について考察しよう。

この「調査結果」は，第 1 段落の「(1) IPsec ルータ」，「(2) IPsec の通信」にわたって記述されている。この中から，IPsec のカプセル化に関する制限を見つけることができる。「(2) IPsec の通信」の 7 番目の箇条書きに，「IPsec では，ユニキャストの IP パケットをカプセル化して転送する」とあるのだ。

この記述を踏まえ，さらには他の見出しを含めた本文全体の流れを考察する。その結果，「IPsec は IP マルチキャストパケットのカプセル化を行えない」という制限をもつと推論できる。なお，他の見出しを含めた本文全体の考察については，少々長くなるので，解を導いた直後に扱うことにする。

次に，二つ目の，OSPF パケットについて考察しよう。本問を解く上で注目すべき特徴は，このパケットが IP マルチキャストパケットであるという点だ。

したがって，OSPF パケットを IPsec でカプセル化できない理由は，これが IP マルチキャストパケットだからである。この内容を，設問の指示に従い，「OSPF」及び「リンクステート情報」という字句を用いて解答すればよい。

よって，正解は解答例に示したとおりとなる。

**●本文全体を考察することによって，「IPsec が IP マルチキャストパケットのカプセル化を行えない」と推論できる理由**

下線（a）に続く文章を見ると，「OSPF を稼働させたい」ので，「他のトンネリング技術を調査（する）」という流れになっている。つまり，この段階では，OSPF パケットを IPsec でカプセル化できないことが明らかになったわけだ。

そして，次の見出し〔トンネリング技術の調査〕につながっている。

その見出しの文章を読み進めると，トンネリング技術の一つである GRE の調査内容が記されている。

注目に値するのは，その第 4 段落の「GRE では，IP ブロードキャストも IP マルチキャストもカプセル化して転送できる」という記述である。つまり，GRE を用いれば，「WAN 回線の冗長化」という要件を満たせることが明らかになったわけである。

さらに読み進めると，最終的には，GRE over IPsec を用いることが決定されている。

©2017 ICT Workshop

その点は，〔GRE over IPsec の稼働方法の検討〕の第 4 段落に「OSPF……には，GRE によるカプセル化と IPsec による暗号化を設定する」と記述されていることから分かる。

このように本文が続いていることから，「IPsec は IP マルチキャストパケットのカプセル化を行えない」と推論できるのである。

冒頭で解説したとおり，本事例の要件の一つは，「WAN 回線の冗長化」である。

その要件に含まれる内容を細かく見てみると，IPsec を用いてインターネット VPN を構築すること，マルチキャスト通信の OSPF を用いて冗長化を実現すること，これらを一緒に実現することが求められている。

そのために調査を行い，GRE over IPsec の採用によって要件を満たすことが可能となった次第である。

**●参考：IPsec が IP マルチキャストパケットのカプセル化を行えない理由**

実を言うと，IPsec の仕様上，IP マルチキャストパケットのカプセル化を行うことができない。最後にその点を簡単に解説しよう。

幾つかの理由からそのように言えるが，代表的なものを二つ挙げておく。

一つ目は，IKE の制約である。

IKE では鍵交換を行うが，この暗号鍵は「共通鍵」である。これは，1 対 1 の通信を暗号化するときに用いられるものである。

IKE では，この 1 対 1 の通信を前提に，様々なパラメータ（共通鍵の基となる乱数など）を交換する手順が規定されている。それゆえ，IPsec ではマルチキャスト通信をカプセル化できない。

二つ目は，IPsec 通信のリプレイ攻撃防御の制約である。

リプレイ攻撃とは，暗号化されたパケットを第三者が傍受し，なりすましなどの不正行為を目論んで，当該パケットを第三者が再び送信する攻撃である。それを防御するため，ESP ヘッダはシーケンス番号をもち，パケットを送信するたびにカウンタが増える仕組みになっている。このシーケンス番号を受信時にチェックすればリプレイ攻撃を見破ることができる。

この仕組みは，1 対 1 の通信ではうまくいく。しかし，1 対多の通信ではシーケンス番号の同期を取ることが困難となるため，リプレイ攻撃防御が機能しなくなる。それゆえ，IPsec ではマルチキャスト通信をカプセル化できない。

©2017 ICT Workshop

## ■設問 3
## (1)

**解答例**

あ：1,436
い：1,414

問題文は,「図 3 中の［あ］及び図 5 中の［い］に入れる最大バイト数を，それぞれ答えよ。ここで，ジャンボフレームは使用されないものとする」と記述されている。

本問は「ジャンボフレームを使用しない」とあるので，イーサネット上で IP パケットを送受信したとき，その MTU は，1,500 バイトである。PC，サーバがイーサネットに接続されていることを前提に考えると，IP ヘッダを含めた IP パケット全体のサイズは，最大 1,500 バイトとなる。

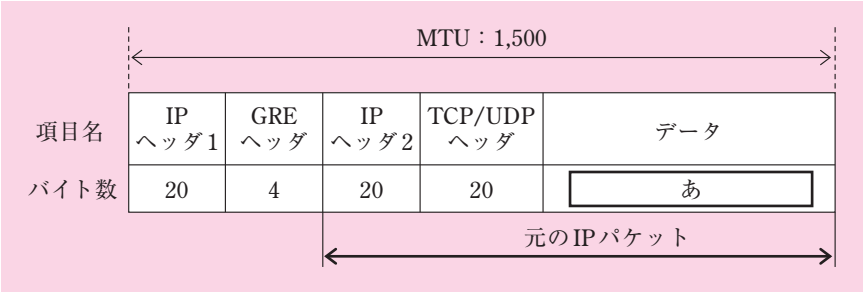
トンネリングプロトコルを用いるとき，カプセル化によってヘッダが付加される。

カプセル化した状態の IP パケットを 1,500 バイトに収めるには，元の IP パケット（カプセル化の対象となるパケット）の最大サイズは，カプセル化に伴うヘッダ部分のサイズを差し引いた値となる。

**あ**

元の IP パケットのヘッダは，IP ヘッダ 2 ～ TCP/UDP の 40 バイトである。

GRE カプセル化によって付加されたヘッダは，IP ヘッダ 1 ～ GRE ヘッダの 24 バイトである。




**図：IP パケットが GRE でカプセル化されたときのパケット形式（図 3 に加筆）**

©2017 ICT Workshop

元のイーサネットの MTU である 1,500 バイトから，両者を差し引く。

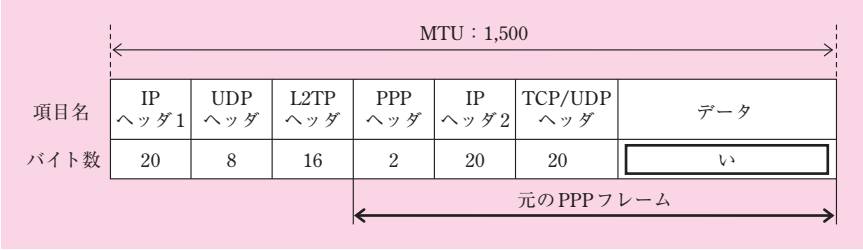
1,500 －（24 ＋ 40）＝ 1,436 バイト

よって，空欄あに該当する字句は，「**1,436**」となる。

**い**

元の PPP フレームのヘッダは，PPP ヘッダ～ TCP/UDP ヘッダの 42 バイトである。

L2TP カプセル化によって付加されたヘッダは，IP ヘッダ 1 ～ L2TP ヘッダの 44 バイトである。




**図：L2TP でカプセル化されたときのパケット形式（図 5 に加筆）**

元のイーサネットの MTU である 1,500 バイトから，両者を差し引く。

1,500 －（44 ＋ 42）＝ 1,414 バイト

よって，空欄いに該当する字句は，「**1,414**」となる。

## (2)

**解答例**

| | |
|---|---|
| IP ヘッダ 1 | 送信元 IP アドレス：α .0.0.1 |
| | 宛先 IP アドレス：β .0.0.1 |
| IP ヘッダ 2 | 送信元 IP アドレス：192.168.0.100 |
| | 宛先 IP アドレス：192.168.10.1 |

©2017 ICT Workshop

問題文は，「図 4 中の PC からサーバへの通信における，図 3 中の IP ヘッダ 1 と IP ヘッダ 2 の送信元 IP アドレス及び宛先 IP アドレスを，図 4 中の字句を用いて，それぞれ答えよ」と記述されている。

〔トンネリング技術の調査〕の中に，図 3「IP パケットが GRE でカプセル化されたときのパケット形式」，図 4「GRE 利用時の通信例」がある。

本文を解くには，GRE の仕組みについて理解する必要がある。まずはその点について解説し，次いで解を導こう。

### ● GRE

GRE（Generic Routing Encapsulation）について，本文の記述を適宜引用しながら解説しよう。

GRE は，「ネットワーク層のプロトコルのパケットをカプセル化して転送する機能」をもつ（第 4 段落）。本事例では，IP パケットのカプセル化に用いられる。

図 4 のネットワーク構成では，二つのイントラネットがインターネットを介して接続されている。インターネット区間が，GRE トンネルでカプセル化される区間となっている。

図 4 において，GRE トンネルは，仮想的な専用線の役割を果たす。それゆえ，イントラネット内の端末（PC，サーバ）から見ると，二つのイントラネットがあたかも専用線で直接接続されているかのように見える。

そのため，PC からサーバにパケットを送信するとき，PC は，サーバ宛てに通常のパケットを送信する。サーバは，これをただ受信しているだけだ。PC とサーバが直接送受信しているパケットが，図 3 の「元の IP パケット」である。この「元の IP パケット」の IP ヘッダ 2 は，送信元 IP アドレスが PC，宛先 IP アドレスがサーバとなる。

さて，「図 4 において，GRE トンネルは，仮想的な専用線の役割を果たす」と述べたが，実際には，二つのイントラネットはインターネットを介して接続されている。このインターネット区間は，GRE でカプセル化された IP パケット（GRE パケット）が通過する。

この点について，第 4 段落には「カプセル化とカプセル化の解除は，GRE トンネリングを行う両端の機器で行われる」と記述されている。

図 4 を見ると，インターネット区間，すなわち GRE トンネル区間は，その両端の機器がルータ 1 とルータ 2 である。それゆえ，PC からサーバに送信するとき，ルータ 1 でカプセル化され，ルータ 2 でカプセル化が解除されることが分かる。

GRE トンネルの両端の機器間で GRE パケットが送受信されることから，GRE パケットの送信元と宛先は，両端の機器であることが分かる。

©2017 ICT Workshop

したがって，PC からサーバに送信するとき，GRE パケットの IP ヘッダ 1 は，送信元 IP アドレスがルータ 1，宛先 IP アドレスがルータ 2 となる。より正確に言うと，それぞれのルータのインターネット側 IP アドレス（グローバル IP アドレス）である。

**●解の導出**

本問は，PC からサーバに送信するという条件で，IP ヘッダ 1 と IP ヘッダ 2 の送信元 IP アドレス，宛先 IP アドレスを問うている。

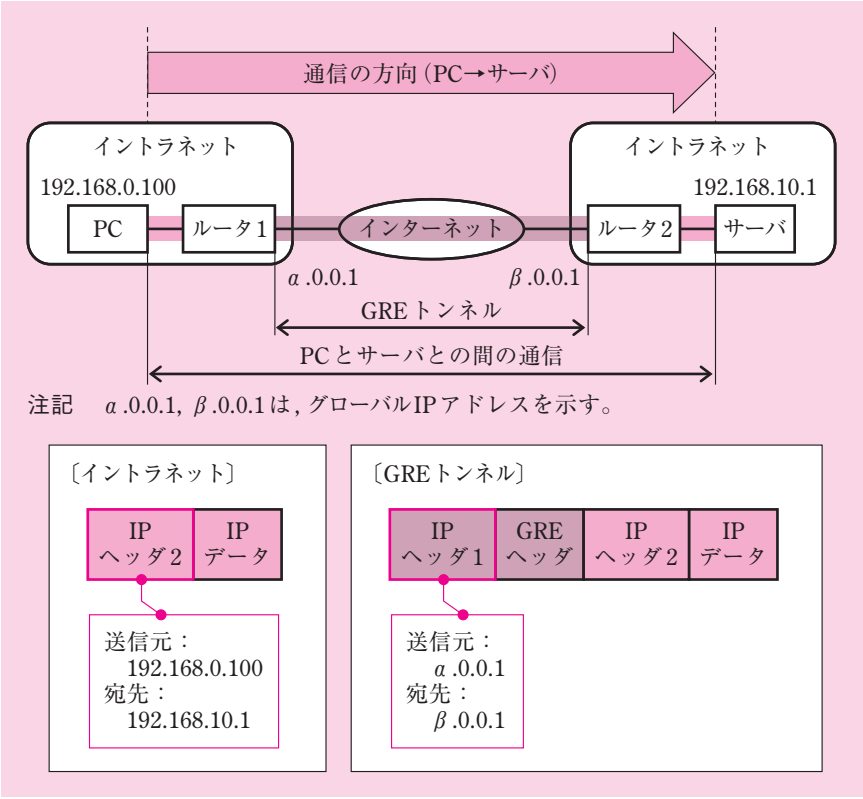
「元の IP パケット」の IP ヘッダ 2 は，送信元 IP アドレスが PC であり，宛先 IP アドレスがサーバである。それぞれの IP アドレスは，PC が「192.168.0.100」であり，サーバが「192.168.1.10」である。

GRE パケットの IP ヘッダ 1 は，送信元 IP アドレスがルータ 1 のグローバル IP アドレスであり，宛先 IP アドレスがルータ 2 のそれである。それぞれの IP アドレスは，ルータ 1 が「$\alpha$ .0.0.1」であり，ルータ 2 が「$\beta$ .0.0.1」である。

これまで解説した内容を整理するため，図 4 に各区間のパケット形式を書き添えたものを次の図に示す。

よって，正解は解答例に示したとおりとなる。

©2017 ICT Workshop




**図：GRE 利用時の通信例（図 4 に加筆）（再掲）**

## (3)

**解答例**

**①の通信で PC が取得する IP アドレスが格納されるヘッダ：IP ヘッダ 1**
**②の通信で PC が取得する IP アドレスが格納されるヘッダ：IP ヘッダ 2**

問題文は，「図 6 中の①及び②の通信で PC が取得する IP アドレスが格納されるヘッダを，図 5 中の項目名でそれぞれ答えよ」と記述されている。

〔トンネリング技術の調査〕の中に，図 5「L2TP でカプセル化されたときのパケット形式」，図 6「L2TP 利用時の通信例」がある。

©2017 ICT Workshop

図 6 について，第 9 段落には，「LAC 機能を実装した PC は，LNS 機能をもつ VPN 装置にインターネット経由で接続して，イントラネット内のサーバにリモートアクセスできる」と記述されている。さらに，図 6 の注記に「本例では，PC が PPPoE によって，IP アドレスを動的に取得する構成例を示す」と記述されている。

したがって，図 6 は，インターネット上にある PC が，PPPoE によりインターネットアクセス回線網から IP アドレスを動的に取得した上で，イントラネット内のサーバにリモートアクセスしたときの構成を示している。この構成において，PC（LAC）と VPN 装置（LNS）間のインターネット区間が，L2TP トンネル区間となっている。

本文を解くには，PPPoE，L2TP の仕組みについて理解する必要がある。まずはその点について解説し，次いで解を導こう。

### ● PPPoE

PPPoE（PPP over Ethernet）とは，PPP フレームをイーサネットフレームでカプセル化して転送するのに用いられる，データリンク層のプロトコルである。

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。

PPP の用途は多岐にわたる。例えば，ブロードバンドルータを介さず，ISP と PC 間で直接通信するときに用いられている。要は，リモートアクセスでインターネットに接続するときだ。両者間のデータリンク層のプロトコルが，PPP である。

他には，ISP がブロードバンドルータと直接通信するときも同様である。このときも，両者間のデータリンク層のプロトコルは，PPP だ。

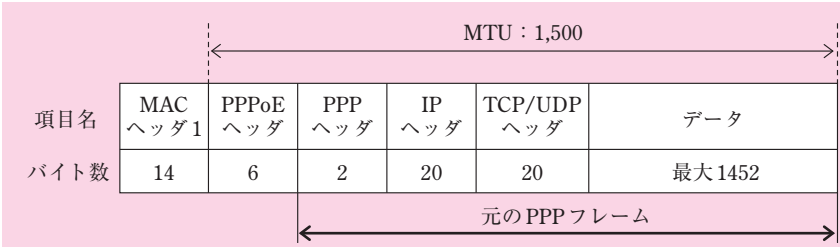
話を PC に戻そう。インターネット上の PC が ISP に直接接続してくる環境は，実に様々である。無線であったり，有線であったり，ダイアルアップ回線であったりするだろう。とはいえ，データリンク層に PPP を使うことで，物理層がどのような媒体であろうとも，ISP と PC 間が専用線で結ばれて通信しているのと同じになるのだ。

ISP は，PPP がもつユーザ認証機能を用い，接続してきた PC の利用者を認証する。認証に成功した後，PPP がもつ IP アドレスの割当て機能を用い，グローバル IP アドレスを動的に割り当てている。

もしも ISP と PC との間がイーサネットで接続されている場合には，この PPP フレームはイーサネットフレームにカプセル化されて，PC と ISP 間で送受信される。このカプセル化を規定した通信規格が，PPPoE である。

PPPoE の仕組みにより，実際にはイーサネットで接続されているのに，仮想的には専用線で接続されているようになって，PPP 通信が行われるのだ。

©2017 ICT Workshop




注） イーサネットフレームにカプセル化されていることを強調するため，本文の図 3（GRE パケット），図 5（L2TP パケット）にはなかった，MAC ヘッダを明示している。
言い換えると，図 3 も図 5 も，イーサネット区間を通過するときは，MAC ヘッダが先頭に存在している。

**図：PPPoE でカプセル化されたときのパケット形式**

この点を踏まえ，図 6 を見てみよう。

インターネット上の PC とアクセス回線網内の PPPoE サーバが，PPPoE で通信している。この目的は，図 6 の注記にあるとおり，PC が「IP アドレスを動的に取得する」ためである。

したがって，このアクセス回線網は ISP のものであり，PC に対し，グローバル IP アドレスを割り当てている様子を表していることが分かる。

### ● L2TP

L2TP（Layer 2 Tunneling Protocol）について，本文の記述を適宜引用しながら解説しよう。

L2TP は，「PPP フレームをカプセル化して転送する機能」をもつ（第 8 段落）。

先ほど，PPP について，「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」と説明した。L2TP は UDP の上位層として規格化されており，L2TP でトンネリングしたパケットは，IP パケットとなる。

L2TP の仕組みにより，実際には IP ネットワークで接続されているのに，仮想的には専用線で接続されているようになって，PPP 通信が行われるのだ。

図 6 のネットワーク構成では，VPN 装置を経由して，PC がイントラネットのサーバにリモートアクセスしている。PC と VPN 装置がインターネットを介して接続されている。このインターネット区間が，L2TP トンネルでカプセル化される区間となっている。

図 6 において，L2TP トンネルは，仮想的な専用線の役割を果たす。それゆえ，PC と VPN サーバ間があたかも専用線で直接接続されているかのように見える。

©2017 ICT Workshop

さらに，PPP がもつ IP アドレスの割当て機能を用い，VPN 装置は PC に対し，イントラネットのプライベート IP アドレスを動的に割り当てている。この結果，PC はサーバと同じイントラネットに存在しているかのように見える。

PC からサーバにパケットを送信するとき，PC は，このプライベート IP アドレスを用いる。つまり，このパケットの IP ヘッダは，送信元 IP アドレスが PC のプライベート IP アドレス（VPN 装置から動的に取得したもの）であり，宛先 IP アドレスがサーバである。

両者は仮想的な専用線（L2TP トンネル）で結ばれているので，データリンク層には PPP が用いられる。つまり，この IP パケットを PPP フレームでカプセル化してから送信している。この PPP フレームが，図 5 の「元の PPP フレーム」である。

以上より，PC からサーバに送信するとき，L2TP パケットの IP ヘッダ 2 は，送信元 IP アドレスが PC のプライベート IP アドレス（VPN 装置から動的に取得したもの），宛先 IP アドレスがサーバとなる。

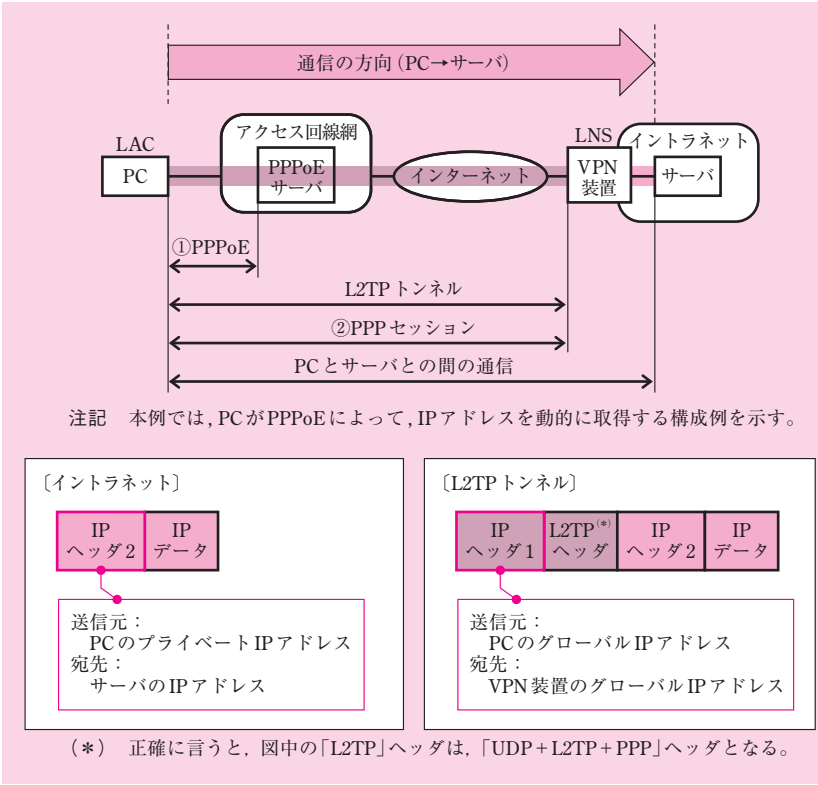
さて，「図 6 において，L2TP トンネルは，仮想的な専用線の役割を果たす」と述べたが，実際には，PC と VPN 装置はインターネットを介して接続されている。このインターネット区間は，L2TP でカプセル化された IP パケット（以下，L2TP パケットという）が通過する。

この点について，第 8 段落には「カプセル化とカプセル化の解除は，L2TP トンネリングを行う LAC（L2TP Access Concentrator）又は LNS（L2TP Network Server）の機能をもつ両端の機器で行われる。LAC は，トンネリングを要求する機器で，LNS は受け入れる機器である」と記述されている。

図 6 を見ると，インターネット区間，すなわち L2TP トンネル区間は，その両端の機器が PC と VPN 装置である。自らの意思でリモートアクセスをしてくる側は PC であるから，これが LAC である。それを受け入れる VPN 装置が，LNS である。それゆえ，PC からサーバに送信するとき，PC でカプセル化され，VPN 装置でカプセル化が解除されることが分かる。

以上より，PC からサーバに送信するとき，L2TP パケットの IP ヘッダ 1 は，送信元 IP アドレスが PC のグローバル IP アドレス（ISP から動的に取得したもの），宛先 IP アドレスが VPN 装置となる。

©2017 ICT Workshop




**図：L2TP 利用時の通信例（図 6 に加筆）**

参考までに，L2TP については，平成 26 年度午後 I 問 2 で出題されており，本書の解説で L2TP を詳しく取り上げているので，参考にしていただきたい。

**●解の導出**

本問は，図 6 中の①及び②の通信で PC が取得する IP アドレスが格納されるヘッダを問うている。

図 6 中の①は，PPPoE セッションである。「● PPPoE」で解説したとおり，このとき，PC は ISP からグローバル IP アドレスを割り当てられている。

「● L2TP」で解説したとおり，PC からサーバにパケットを送信するとき，L2TP パケットの IP ヘッダ 1 は，送信元 IP アドレスが PC のグローバル IP アドレス（ISP から動的に取得したもの）になる。

したがって，①で取得したグローバル IP アドレスは，「IP ヘッダ 1」に格納される。

©2017 ICT Workshop

図 6 中の②は，PPP セッションである。「● L2TP」で解説したとおり，このとき，PC は VPN 装置からイントラネットのプライベート IP アドレスを割り当てられている。PC からサーバにパケットを送信するとき，L2TP パケットの IP ヘッダ 2 は，送信元 IP アドレスが PC のプライベート IP アドレス（VPN 装置から動的に取得したもの）になる。

したがって，②で取得したプライベート IP アドレスは，「IP ヘッダ 2」に格納される。

よって，正解は解答例に示したとおりとなる。

## (4)

**解答例**

カプセル化によるオーバヘッドがＬ２ＴＰより小さいので，一つのパケットで転送できるデータ量が多い。（48字）

問題文は，「本文中の下線（b）について，GRE を利用する利点を，L2TP を利用する場合と比較して……述べよ」と記述されている。

下線（b）は，〔トンネリング技術の調査〕の第 11 段落にある。そこには，「（b）GRE を利用することに（した）」と記述されている。

前の段落からの文脈を考慮に入れると，下線（b）がよりいっそう理解しやすくなる。

第 10 段落の中で，「GRE 及び L2TP の機能と動作については理解できたが，どちらのプロトコルを利用すべきか判断できなかった」とある。その後，「トンネリングプロトコルを使用する目的と，使用したときの影響の度合いを考慮して判断する」こととし，下線（b）にあるとおり「GRE を利用する」ことを決定した次第である。

したがって，解を導くには，目的と影響度合いの二つの観点から考察すればよい。そこで明らかになった GRE の利点が，求める解となる。

まず，トンネリングプロトコルを利用する目的を考えてみよう。その目的は，インターネット VPN を構築したとき，OSPF を稼働させることである。

その点は，前の見出し〔インターネット VPN の構築技術の検討〕からここに至るまでの話の流れから分かる。かいつまんで言うと，インターネット VPN の構築技術を検討したところ，IPsec 通信の仕様上，マルチキャスト通信を行う OSPF をカプセル化できないことが明らかになった。そこで，「OSPF を稼働させ（る）」ことを目的とし

©2017 ICT Workshop

て,「他のトンネリング技術を調査」したのである（〔インターネット VPN の構築技術の検討〕の第 3 段落）。

それでは，この目的を果たすという観点から，GRE は L2TP と比較して利点をもつだろうか。

その点について，〔トンネリング技術の調査〕の第 2 段落には，「OSPF のリンクステート情報の交換パケットを，GRE 又は L2TP でカプセル化すれば，そのパケットは IPsec でカプセル化できるので，インターネット VPN で OSPF を稼働できることが分かった」と記述されている。したがって，どちらも目的は果たせることが分かる。つまり，GRE に優位性はない。

次に，トンネリングプロトコルを利用したときの影響度合いを考えてみよう。

トンネリングすると，元の IP パケットをカプセル化するため，ヘッダが付加される。

カプセル化に伴うオーバヘッドが大きいほど，1 個の IP パケットで転送できるデータ量が少なくなるという悪影響が生じる。

それでは，このオーバヘッドの影響度合いという観点から，GRE は L2TP と比較して利点をもつだろうか。

設問 3（1）で解説したとおり，GRE のカプセル化に伴って付加されるサイズは，24 バイトである。一方，L2TP のカプセル化に伴って付加されるサイズは，44 バイトである。したがって，GRE は，L2TP に比べてオーバヘッドが小さい。それゆえ，転送データ量が多いという利点をもつ。

よって，正解は，「**カプセル化によるオーバヘッドが小さいので，一つのパケットで転送できるデータ量が多い**」となる。

## ■設問 4

設問 4 の解説に入る前に，IPsec の通信モード，ESP について解説する。これから述べることは，IPsec の基礎知識に位置付けられる。

IPsec について，詳しくは本書の第 8 章「8.4.5　IPsec」を参照していただきたい。そこから一部を引用して解説しよう。

### ●通信モード

IPsec は，通信経路上でカプセル化する範囲を一部の区間とするのか，それとも全区間とするのかに応じて，2 種類ある通信モードのうち一つを選択する。全区間にわたって実施する場合はトランスポートモードを用い，一部の区間だけで実施する場合はトンネルモードを用いる。

©2017 ICT Workshop

ここで言う「全区間」は，IPsec のカプセル化対象となる IP パケットに基づいて定義されるものである。すなわち，全区間とは，その IP パケットの送信元から宛先までの区間を指している。

それゆえ，IPsec のカプセル化対象となる IP パケットが，既に別のトンネリングプロトコルでカプセル化済みであった場合，そのトンネリングプロトコルで付加された IP ヘッダの送信元と宛先を両端とする区間を，全区間ととらえる必要がある。

本事例では GRE over IPsec を用いるので，GRE パケットの送信元と宛先が，IPsec でカプセル化する「全区間」となる。したがって，このときの IPsec カプセル化区間は，GRE トンネル区間と一致する。

● ESP

IPsec 通信（IPsec SA）で，パケットの暗号化とメッセージ認証を実施する場合，IPsec プロトコル（表 2 では「セキュリティプロトコル」と表記）として ESP（Encapsulating Security Payload）を選択する。

本事例ではインターネット VPN を構築するので，インターネット区間を通過する IPsec パケットを暗号化する必要がある。したがって，ESP を選択する。

IPsec SA 生成時に選択された通信モードに基づき，カプセル化対象となるオリジナル IP パケットを，IPsec でカプセル化する。

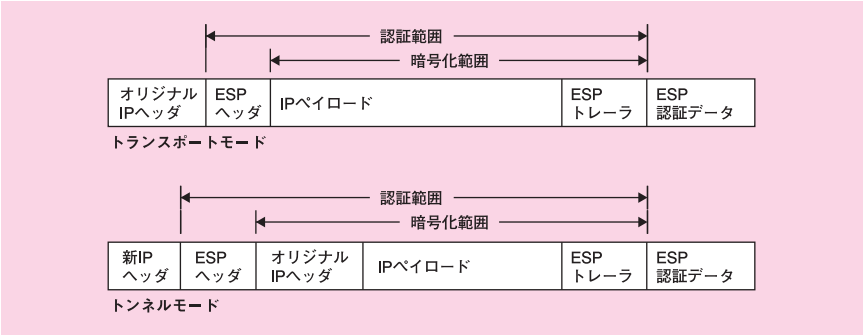
トランスポートモードの場合，全区間をカプセル化するので，オリジナル IP パケットの IP ヘッダをそのまま用いることができる。その IP ヘッダと IP ペイロードの間に ESP ヘッダを挿入する。そして，IP ペイロードを暗号化し，ESP ヘッダと IP ペイロードのメッセージ認証を行う。

トンネルモードの場合，一部の区間をカプセル化するので，カプセル化区間を通過するときだけ使用する新 IP ヘッダを付加する。この新 IP ヘッダの送信元と宛先は，カプセル化区間の両端にあるゲートウェイである。

新 IP ヘッダの後に ESP ヘッダを挿入し，その後にオリジナル IP パケットが続く。そして，オリジナル IP パケット全体を暗号化し，ESP ヘッダとオリジナル IP パケットのメッセージ認証を行う。

ESP の認証範囲及び暗号化範囲を次の図に示す。

©2017 ICT Workshop




**図：ESP の認証／暗号化範囲**

暗号化は，秘密鍵（共通鍵）を用いている。この鍵及び暗号化アルゴリズムは，IPsec SA の生成時（IKE フェーズ 2）で交換されている。

メッセージ認証は，パケットごとに改ざん検出用コードを付加することによって実現している。図中の「ESP 認証データ」がこのコードに該当する。これは，認証範囲のデータから生成されたメッセージダイジェスト値（ハッシュ値）から生成される。このときに用いられるハッシュアルゴリズムも，IPsec SA の生成時（IKE フェーズ 2）で交換されている。

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**

GREでトンネリングが行われるから（17字）

問題文は，「本文中の下線（c）については，トンネルモードで行う必要がない。その理由を，トンネリングに着目して……述べよ」と記述されている。

下線（c）は，〔GRE over IPsec の稼働方法の検討〕の第 1 段落にある。そこには，「(c) 通信モードは，トランスポートモードを選択する」と記述されている。

解を導く上で留意しておきたいのは，本問が，「トンネルモードで行う必要がない理由」を問うている点である。下線（c）に「トランスポートモード」と記されているが，「トランスポートモードを行う必要がある理由」を問うているわけではない。

©2017 ICT Workshop

設問 4 の冒頭で解説したとおり，IPsec 通信は，トランスポートモードとトンネルモードの 2 種類の中から，どちらか一つを選ぶ必要がある。

トンネルモードでは，IPsec カプセル化区間を通過する際，カプセル化用の新 IP ヘッダが必ず付加される仕組みになっている。この新 IP ヘッダの送信元と宛先が，カプセル化区間の両端となる。

この点に着目して，トンネルモードで行う必要があるのはどのような場合かを考察しよう。これを，新 IP ヘッダを付与する必要があるのはどのような場合か，と読み替えると分かりやすくなる。その答えは，IPsec カプセル化区間が，オリジナル IP パケットの送信元と宛先を両端とする区間と，異なっている場合だ。

それでは，オリジナル IP パケットの送信元と宛先を両端とする区間が，IPsec カプセル化区間と同じ場合は，どのように言えるだろうか。

論理的に考えれば，トンネルモード，トランスポートモードのどちらを用いても構わない。ただ，実用性から考えれば，トンネルモードの新 IP ヘッダの送信元と宛先が，オリジナル IP ヘッダのそれと一致するわけだから，新 IP ヘッダをわざわざ付加する必要性がないと言える。つまり，実用上，トンネルモードで行う必要がないわけだ。

これまでの解説で，「トンネルモードで行う必要がない理由」を考察するに当たって着目すべき点は，「オリジナル IP パケットの送信元と宛先を両端とする区間が，IPsec カプセル化区間と同じかどうか」だということが明らかになった。もし同じであることが分かれば，それを根拠に解を導けばよい。

それでは，本事例で用いる GRE over IPsec の場合はどうだろうか。

GRE over IPsec は，IPsec のカプセル化対象パケットは，GRE パケット（GRE でカプセル化済みのパケット）である。それゆえ，ここまでの解説の中で用いてきた「オリジナル IP パケット」という用語は，GRE パケットに当てはまるわけだ。

この点を踏まえて，図 8「GRE over IPsec を稼働させたときの OSPF の通信の概要」を見てみよう。この図から，IPsec カプセル化区間と，GRE トンネル区間が一致していることが分かる。

つまり，オリジナル IP パケット（すなわち，GRE パケット）の送信元と宛先を両端とする区間（すなわち，GRE トンネル区間）が，IPsec カプセル化区間と同じだということになる。したがって，トンネルモードは必要ないと結論することができる。

ここではトンネルモードが必要ない理由が問われているので，IPsec カプセル化区間と同じであるという根拠を具体的に解答すればよい。

よって，正解は「**GRE でトンネリングが行われるから**」となる。

©2017 ICT Workshop

## (2)

**解答例**

ESP 認証データ長は，使用する認証アルゴリズムによって変化するから（33 字）

問題文は，「図 7 中の ESP 認証データ長は，表 2 中のパラメータで選択された方式によって変化する。その理由を……述べよ」と記述されている。

設問 4 の冒頭の解説「● ESP」で説明したとおり，ESP 認証データとは，パケットごとに付加された改ざん検出用コードである。

これは，認証範囲のデータから生成されたメッセージダイジェスト値（ハッシュ値）から生成される。

このときに用いられる認証アルゴリズムは，IPsec SA の生成時（IKE フェーズ 2）で交換されている。表 2「IKE フェーズ 2 で決定されるパラメータ（抜粋）」の中で，それはパラメータ「認証方式」と掲載されている。表中の説明欄では，より具体的に「IPsec 通信で使用する認証アルゴリズム」と記述されている。

認証方式を SA の生成時に決定する仕様になっているので，SA の合意形成の際，セキュリティ強度の高い認証アルゴリズムを選択肢に含めることが可能となっている。

したがって，決定された認証アルゴリズムに基づいてメッセージダイジェスト値が生成されるわけだから，ESP 認証データのサイズが変化し得ることが分かる。

よって，正解は「**ESP 認証データ長は，使用する認証アルゴリズムによって変化するから**」となる。

## (3)

**解答例**

GRE ヘッダ，IP ヘッダ 2，TCP/UDP ヘッダ，データ，ESP トレーラ

問題文は，「図 7 において，暗号化される項目名を全て答えよ」と記述されている。

設問 4 の冒頭の解説「● ESP」で説明したとおり，トランスポートモードで暗号化される範囲は，「（オリジナル IP パケットの）IP ペイロード」「ESP トレーラ」となる。

本事例では GRE over IPsec を用いるので，オリジナル IP パケットは GRE パケット

©2017 ICT Workshop

となる。

GRE パケットのパケット形式は，本文の図 3 に示されている。「（オリジナル IP パケットの）IP ペイロード」を，図 3 の表記に置き換えると，「GRE ヘッダ～データ」となる。

この点を踏まえ，「（オリジナル IP パケットの）IP ペイロード」を図 7 の表記に置き換えると，図 3 と同じく「GRE ヘッダ～データ」となる。

暗号化範囲は，これに ESP トレーラを付加したものであるから，「GRE ヘッダ～ESP トレーラ」となる。

よって，正解は，「**GRE ヘッダ，IP ヘッダ 2，TCP/UDP ヘッダ，データ，ESP トレーラ**」となる。

## ■設問 5

### (1)

**解答例**

172.16.128.0/20，172.16.17.0/24

問題文は，「図 9 の構成において，図 1 の構成からサーバをデータセンタに移設するのに伴い，サブネットを再設計して，データセンタに移動するサブネットを全て答えよ。ここで，移動するサブネットのプレフィックス長は 16，20 又は 24 とする」と記述されている。

本問を解くに当たって，まず，移設するサーバとそのネットワークセグメントに関する情報を整理しよう。次いで，それを踏まえて解を導こう。

**●移設するサーバとそのネットワークセグメント**

図 1「現在の Y 社のネットワーク構成」は序文の第 1 段落にあり，図 9「J 君が設計した WAN 回線の構成」は〔WAN の設計〕の第 1 段落にある。

図 1 の中で，新ネットワークのデータセンタに移設する機器が網掛けで示されている。そのうち，ここで問われているサーバを列挙すると，Web サーバ，中継サーバ，プロキシサーバ，社内メールサーバとなる。

これら 4 台のサーバを，ネットワークセグメントごとに整理しよう。

Web サーバ，中継サーバ，プロキシサーバの 3 台は，本社の DMZ に設置されている。このセグメントにある全ての機器を，新ネットワークのデータセンタの DMZ へ

©2017 ICT Workshop

移設する。

以降の解説で，このセグメントを「DMZ」と呼ぶことにする。

社内メールサーバは，DM サーバと同じセグメントに設置されている。このネットワークセグメントにある機器は，一部の機器を新ネットワークのデータセンタへ移設する。

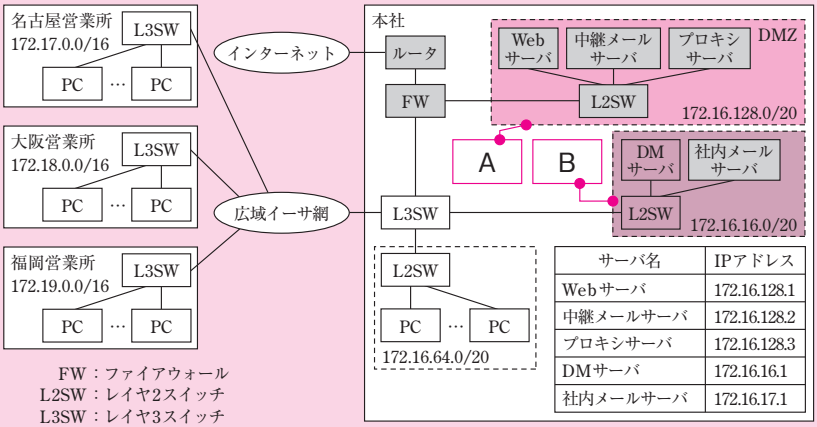
以降の解説で，現行ネットワークの社内メールサーバ，DM サーバが設置されたネットワークセグメントを「現行社内サーバ用セグメント」，新ネットワークのデータセンタにメールサーバが設置されたネットワークセグメントを「新社内メールサーバ用セグメント」，本社に残った DM サーバが設置されたネットワークセグメントを「新 DM サーバ用セグメント」と呼ぶことにする。

項番を付与して整理したものを次の表に示す。

**表：現行ネットワークから新ネットワークへのサーバ移設**

<table>
<tr><th>現行ネットワーク</th><th colspan="2">新ネットワーク</th></tr>
<tr><th>本社</th><th>本社</th><th>データセンタ</th></tr>
<tr><td>［A］DMZ<br>（Web サーバ，中継サーバ，プロキシサーバ）</td><td></td><td>［A］DMZ<br>（Web サーバ，中継サーバ，プロキシサーバ）</td></tr>
<tr><td rowspan="2">［B］現行社内サーバ用セグメント<br>（社内メールサーバ，DM サーバ）</td><td></td><td>［B1］新社内メールサーバ用セグメント<br>（ 社内メールサーバ ）</td></tr>
<tr><td>［B2］新 DM サーバ用セグメント<br>（ DM サーバ ）</td><td></td></tr>
</table>

この項番で示すネットワークセグメントを図 1，図 9 に書き添えたものを次の図に示す。




| サーバ名 | IPアドレス |
|---|---|
| Webサーバ | 172.16.128.1 |
| 中継メールサーバ | 172.16.128.2 |
| プロキシサーバ | 172.16.128.3 |
| DMサーバ | 172.16.16.1 |
| 社内メールサーバ | 172.16.17.1 |

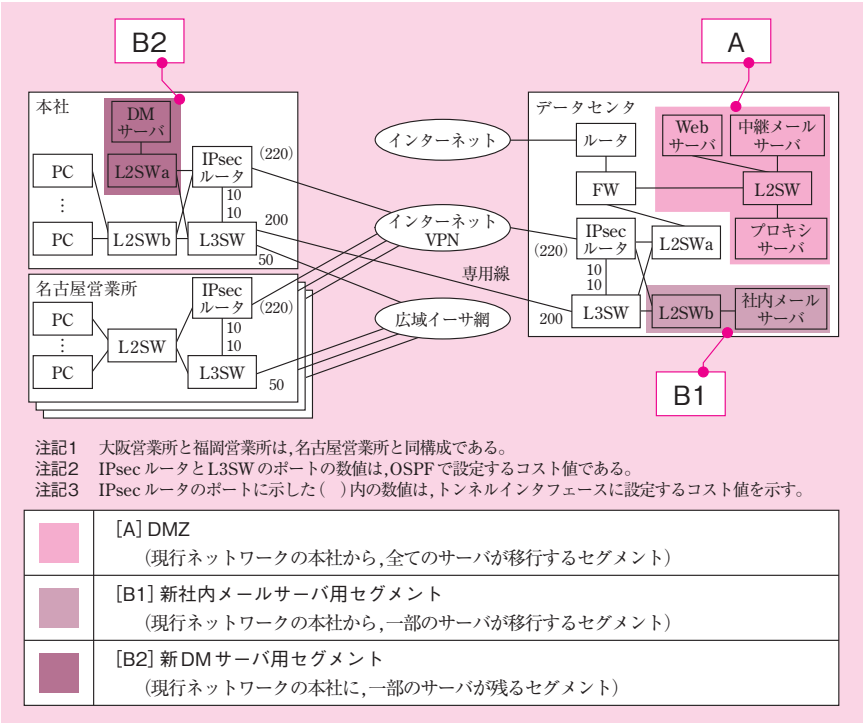
FW：ファイアウォール
L2SW：レイヤ2スイッチ
L3SW：レイヤ3スイッチ
DMサーバ：文書管理サーバ

注記1　網掛け部分は,データセンタに移設する予定の機器を示す。
注記2　FWは,ルータに接続するポートでNATを行っている。
注記3　広域イーサ網へのアクセス回線は,本社が100Mビット/秒,営業所が10Mビット/秒である。
注記4　インターネットへのアクセス回線は,100Mビット/秒である。

| | |
|---|---|
| | [A] DMZ<br>（新ネットワークのデータセンタへ,全てのサーバが移行するセグメント） |
| | [B] 現行社内サーバ用セグメント<br>（新ネットワークのデータセンタへ,一部のサーバが移行するセグメント） |

**図：現行ネットワーク構成（図 1 に加筆）**

©2017 ICT Workshop




注記1　大阪営業所と福岡営業所は，名古屋営業所と同構成である。
注記2　IPsec ルータと L3SW のポートの数値は，OSPF で設定するコスト値である。
注記3　IPsec ルータのポートに示した（　）内の数値は，トンネルインタフェースに設定するコスト値を示す。

| | |
|---|---|
| | ［A］DMZ<br>（現行ネットワークの本社から，全てのサーバが移行するセグメント） |
| | ［B1］新社内メールサーバ用セグメント<br>（現行ネットワークの本社から，一部のサーバが移行するセグメント） |
| | ［B2］新 DM サーバ用セグメント<br>（現行ネットワークの本社に，一部のサーバが残るセグメント） |

**図：新ネットワーク構成（図 9 に加筆）**

**●解の導出**

本問では，データセンタに移設するサブネットを問うている。

サブネットの設計に関し，本文の要件，及び，問題文の条件を確認しよう。

本文の要件は，序文の第 2 段落の 2 番目の箇条書きに，「本社の DM サーバ以外のサーバを，Z 社のデータセンタに移設する。このとき，サーバの IP アドレスの変更が生じないようにすること」と記述されている。

問題文の条件は，「移動するサブネットのプレフィックス長は 16，20 又は 24 とする」と記述されている。

本文の要件から，［A］DMZ，［B1］新社内メールサーバ用セグメントのサーバの IP アドレスは変化しないことが分かる。さらに，本社に残る［B2］新 DM サーバ用セグメントのサーバの IP アドレスも変化しないことが分かる。

これらを考慮に入れるなら，次に示す方針の下，設計する必要がある。

©2017 ICT Workshop

**方針 1.［A］DMZ のサブネットを引き継ぐ**

［A］DMZ は全てのサーバを移設するので，サブネットをそのまま現行ネットワークから新ネットワークに引き継ぐ。

**方針 2.［B］現行社内サーバ用セグメントのサブネットを分割する**

［B］現行社内サーバ用セグメントを，［B1］新社内メールサーバ用セグメントと，［B2］新 DM サーバ用セグメントに分割する。その際，問題文にあるプレフィックスの条件を満たすようにする。

データセンタに移設するネットワークセグメントは，［A］DMZ，［B1］新社内メールサーバ用セグメントである。したがって，前述の方針の下でサブネットを設計すれば，解が求まる。

**［A］DMZ**

図 1 を見ると，現行ネットワークの DMZ は，サブネットが「172.16.128.0/20」である。方針 1 に従い，ここから新ネットワークにおける DMZ のサブネットは，これを引き継げばよい。

**［B1］新社内メールサーバ用セグメント**

図 1 を見ると，［B］現社内サーバセグメントは，サブネットが「172.16.16.0/20」である。その中にあるサーバの IP アドレスは，社内メールサーバが「172.16.17.1」，DM サーバが「172.16.16.1」である。

方針 2 に従い，社内メールサーバ，DM サーバを別々のサブネットに分割する。両サーバの IP アドレスは第 24 ビット目以降が異なっており，一方が「17」，他方が「16」である。

問題文にあるプレフィックスの条件を考慮するなら，第 1 ～第 3 オクテットをネットワークアドレス部とする，プレフィックス長「24」で分割すればよい。

したがって，［B1］新社内メールサーバ用セグメントのサブネットは「172.16.17.0/24」，［B2］新 DM サーバ用セグメントのサブネットは「172.16.16.0/24」となる。

データセンタに移動するサブネットは，前述のとおり，DMZ が「172.16.128.0/20」，新社内メールサーバ用セグメントのサブネットが「172.16.17.0/24」となる。

よって，正解は解答例に示したとおりとなる。

©2017 ICT Workshop

## (2)

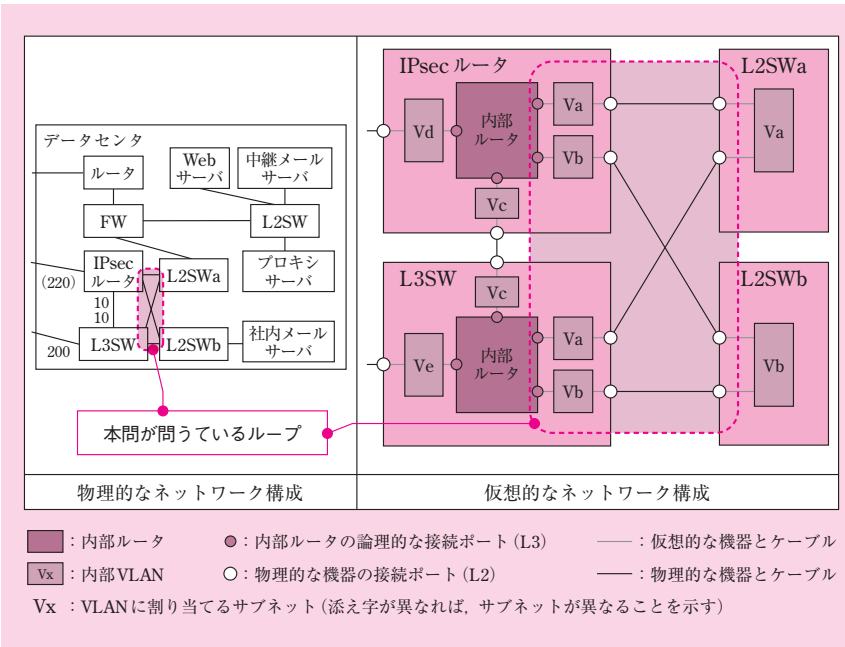
**解答例**

| L | 2 | S | W | a | と | L | 2 | S | W | b | を | 異 | な | る | サ | ブ | ネ | ッ | ト | に | す | る | 。 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

（24字）

問題文は，「図 9 中のデータセンタの IPsec ルータ，L3SW，L2SWa 及び L2SWb の間でレイヤ 2 のループを発生させないためには，どのようにサブネットを設計すればよいか。“L2SWa”及び“L2SWb”という字句を用いて……述べよ」と記述されている。

図 9「J 君が設計した WAN 回線の構成」の中で，本問が問うているループに該当する箇所を，次の図中の点線枠で示す。




**図：データセンタ内の IPsec ルータ，L3SW のサブネット設計**

「レイヤ 2 のループ」とは，一つのサブネット（ブロードキャストドメイン）の中に存在するループを指している。このようなループ状の結線があると，ブロードキャストストームに起因するネットワーク障害を引き起こしてしまう。

©2017 ICT Workshop

レイヤ 2 のループが発生しないようにするには，サブネットをどのように設計すればよいだろうか。

その答えは，ループを複数のサブネットに分割することである。複数のサブネットに結線を分断する箇所は，ルータとなる。要するに，見かけ上はループ状に結線されていたとしても，実際にはルータを越えており，複数のサブネットをまたがっていればよいわけだ。

したがって，ここで問われているループの発生箇所についても，ルータを越えるようにネットワークを構築すればよいことが分かる。

そのためには，ループが経由している IPsec ルータと L3SW において，それぞれの機器の内部にある仮想的なルータ（以下，内部ルータという）を越えるように，結線すればよい。

本問の解を導くには，この内部ルータを含めた機器内部の VLAN 設定，及び，それら機器を含んだネットワークの論理的な構成について，考察する必要がある。それを踏まえて，解を導こう。

### ● IPsec ルータの VLAN 設定

まず，IPsec ルータについて考察する。

IPsec ルータは，4 個の物理的な接続ポートをもち，L2SWa，L2SWb，インターネット VPN，L3SW にそれぞれ接続されている。

IPsec ルータでレイヤ 2 のループを分断するには，ループの出入り口となる接続ポートが，互いに異なるサブネットに所属していればよい。

機器内部では，それぞれの物理的な接続ポートに VLAN を割り当てている。そして，それら VLAN にサブネットを割り当て，内部ルータの配下に収容している。

それゆえ，少なくとも，L2SWa，L2SWb につながる接続ポートの VLAN には，互いに異なるサブネットを割り当てる必要がある。

それでは，他の接続ポートの VLAN はどうだろうか。

インターネット VPN は仮想的な専用線なので，明らかに，その接続ポートの VLAN には別のサブネットを割り当てる必要がある。

L3SW につながる接続ポートの VLAN は，結論から言うと，別のサブネットを割り当てる必要がある。なぜなら，もし L2SWa につながる接続ポートのサブネットと同じであれば，IPsec ルータ，L3SW，L2SWa の三者間で新たなループ状の結線ができてしまう。とはいえ，スパニングツリーを用いることは本文中に示されていないので，そもそもループになっていないことが分かる。ゆえに，別のサブネットだと結論できるわけだ（同じことが，L2SWa を L2SWb に入れ替えても言える）。

©2017 ICT Workshop

したがって，IPsec ルータの接続ポートには，それぞれ異なる VLAN，異なるサブネットが割り当てられていることが分かる。

**● L3SW の VLAN 設定**

IPsec ルータの説明と同じことが，L3SW にも言える。

結論から言うと，L3SW の接続ポートにも，それぞれ異なる VLAN，異なるサブネットが割り当てられている。

ほぼ繰り返しとなるが，念のため，解説しておこう。

L3SW は，4 個の物理的な接続ポートをもち，L2SWa，L2SWb，専用線，IPsec ルータにそれぞれ接続されている。

レイヤ 2 のループを分断するため，少なくとも，L2SWa，L2SWb につながる接続ポートの VLAN には，互いに異なるサブネットを割り当てる必要がある。

インターネット VPN は仮想的な専用線なので，明らかに，その接続ポートの VLAN には別のサブネットを割り当てる必要がある。

IPsec ルータにつながる接続ポートの VLAN も，別のサブネットを割り当てない限り，新たなループ状の結線ができてしまうため，そのようにする必要がある。

**●ネットワークの論理的な構成**

最後に，両機器を含む，ネットワーク全体の論理的な構成について考察する。

これまで考察した内容を VLAN の観点からいったん整理すると，IPsec ルータ，L3SW のそれぞれに対し，VLAN を 4 個ずつ構築することが分かった。

このうち，同一の L2SW を外部接続先とする VLAN に，同一のサブネットを割り当てるように設計する。具体的に言うと，L2SWa を外部接続先とする VLAN が，IPsec ルータにも L3SW にも存在する。そこで，両機器の VLAN には，同一のサブネットを割り当てる。L2SWb を外部接続先とする VLAN も同様である。

さらに，IPsec ルータと L3SW を接続する VLAN に，同一のサブネットを割り当てるように設計する。

以上の解説に基づき，機器内部に構築した VLAN，内部ルータ，及び，それらを外部の機器と接続したネットワークを，前図の右枠の「仮想的なネットワーク構成」に示す。同一のサブネットを割り当てる VLAN には，同一の添え字を付与している。

この図の中で，本問で問われているループの発生箇所は，内部ルータによって分断されている。それゆえ，「レイヤ 2 のループ」は発生していない。

©2017 ICT Workshop

**●解の導出**

本問は「どのようにサブネットを設計すればよいか」を問うている。そして，解答に際し，「“L2SWa”及び“L2SWb”という字句」を用いるよう指示している。

よって，L2SWa と L2SWb がそれぞれ異なるサブネットに所属している旨を解答すればよい。正解は解答例に示したとおりとなる。

## (3)

**解答例**

**本社：2**
**営業所：1**
**データセンタ：2**

問題文は，「図 9 において，本社，営業所及びデータセンタで設定する仮想 IP アドレスの最少の個数を，それぞれ答えよ」と記述されている。

この「仮想 IP アドレス」とは何であろうか。

これは，〔WAN の設計〕の中で初めて登場する，VRRP の仮想 IP アドレスを指している。

本問の冒頭の解説で，新ネットワークを構築するのに用いる要素技術を四つ挙げた（IPsec，GRE，OSPF，VRRP）。その中で，「仮想 IP アドレス」を設定するのは，VRRP しかない。

その第 3 段落には，「本社，営業所及びデータセンタ内の L3SW と IPsec ルータ間では，それぞれ VRRP を稼働させる」と記述されている。

本問は，この VRRP で設定する仮想 IP アドレスの個数を問うている。

仮想 IP アドレスは，VRRP グループにつき 1 個設定するので，「VRRP グループの個数」を問うているものと読み替えることができる。

VRRP グループは，通常，サブネットにつき 1 個構築するので，「VRRP グループを構築するサブネットの個数」を問うているものとさらに読み替えることもできる。

なお，技術的には複数の VRRP グループを設計することは可能であるし，過去問題にそのような出題例はあるものの（平成 28 年度午後 I 問 3 など），本文に明記されていない限り，通常の設計を前提にして解を導くべきである。それに，本問は「最少」の個数を問うているので，サブネットにつき 1 個の VRRP グループと考えて，個数を求める必要がある。

©2017 ICT Workshop

そこで，本問の解を導くに当たり，「仮想 IP アドレスの最少の個数」の問いを「VRRP グループを構築するサブネットの個数」と読み替えて，解を導くことにしよう。

**●各拠点における VRRP グループの設計**

VRRP を構築するサブネットは，大きく二つの特徴を有している。

一つ目は，VRRP はルータを冗長化する技術なので当然であるが，VRRP を構築するサブネットには，ルータが複数存在していなければならない。そのうちの一つがマスタとなり，残りが全てバックアップとなる。

二つ目は，そのサブネットにはルータ以外にホストが存在していなければならない。そのホストのデフォルトゲートウェイとなるルータを冗長化することが，通常，VRRP の目的だからだ。

本事例では，その複数のルータに該当するのが，L3SW と IPsec ルータである。

したがって，L3SW と IPsec ルータを収容しているサブネットに，それぞれ VRRP グループを設計すると考えればよい。

ただし，L3SW と IPsec 間を直接接続するサブネットは，前述の特徴の一つ目を有しているが二つ目を有していないため，本問の考察から外す。

本問を解くには VRRP グループの個数が分かればよいので，ここでは VRRP 設計の詳細には踏み込まず，どのサブネットに VRRP を設計するのかが理解できる程度まで，解説しよう。

それでは，拠点を一つずつ考察する。

**●データセンタ**

L3SW と IPsec ルータの両方を収容し，かつ，ルータ以外の端末を収容しているサブネットを，設問 5（2）の解説に基づいて探してみよう。すると，VRPP グループを構築するサブネットは，次の二つであることが分かる。

- L2SWa があるサブネット
- L2SWb があるサブネット

**●本社**

データセンタと比較したときの構成上の相違点は，本社の L3SW の WAN 側に，広域イーサネット網との接続が存在することである。とはいえ，広域イーサネット網と接続するサブネットは L3SW しか収容していないので，本問の考察から外す。

そこで，L3SW の LAN 側に着目すると，IPsec，L3SW，L2SWa，L2SWb を接続す

©2017 ICT Workshop

る仮想ネットワーク部分は，本社と同じ構成になることが分かる（もちろん，設定するパラメータの値は異なっている）。

したがって，データセンタからの類推により，VRPP グループを構築するサブネットは，次の二つであることが分かる。

- L2SWa があるサブネット
- L2SWb があるサブネット

念のため，L2SWa があるサブネットと，L2SWb があるサブネットが，それぞれ異なったものであることを確認しよう。次に述べる二つの根拠から，そのように言うことができる。

一つ目は，L2SWa に接続された DM サーバと，L2SWb に接続された PC は，現行ネットワークのときから，サブネットがもともと異なっていたからである。

現行ネットワークの構成を示した図 1 を見ると，DM サーバは 172.16.16.1 が割り当てられており，PC を収容するネットワークは 172.16.64.0/20 が割り当てられている。

新ネットワークに移行しても DM サーバと PC は本社に残り，IP アドレスはそのままであるから，引き続きサブネットが異なっていると推論できる。DM サーバを収容するサブネットは，設問 5（1）で解説したように 172.16.16.0/24 になるはずだ。

それゆえ，接続しているホストの IP アドレスに基づき，L2SWa があるサブネットと，L2SWb があるサブネットは異なっていると言える。

二つ目は，設問 5（2）で問われていた，データセンタの IPsec ルータ，L2SWa，L3SW，L2SWb を巡るループ発生の指摘が，本社にも当てはまるからである。当然，レイヤ 2 のループを発生させてはならないので，データセンタのときと同じように，ループ状の結線はルータで分断されているはずだ。

それゆえ，レイヤ 2 のループを発生させないために，L2SWa があるサブネットと，L2SWb があるサブネットは，異なっていると言える。

**●営業所**

本社と比較したときの構成上の相違点は，営業所は，LAN 側のスイッチが一つしかないことである。さらに WAN 側が異なるが，VRRP グループ本問の考察から外す。

そこで，LAN の LAN 側に着目してみよう。

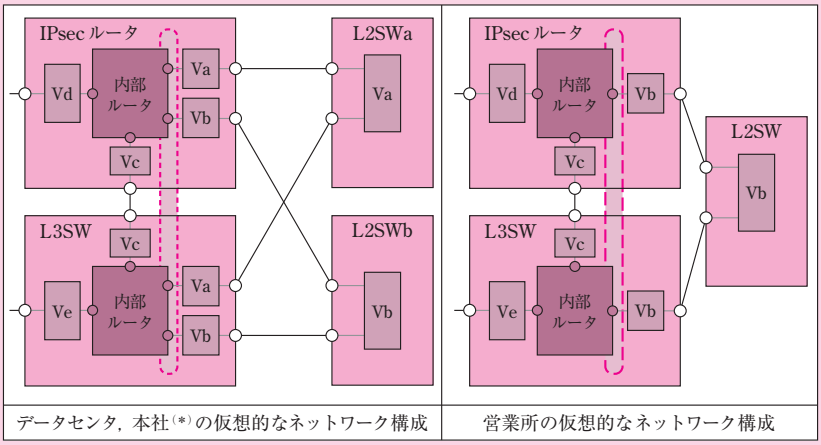
本社の L2SWa を取り除き，本社の L2SWb を営業所の L2SW に置き換えて考えてみる。すると，IPsec，L3SW，L2SW を接続する仮想ネットワーク部分は，営業所と同じ構成になることが分かる（もちろん，設定するパラメータの値は異なっている）。

©2017 ICT Workshop

したがって，本社からの類推により，VRPP グループを構築するサブネットは，次の一つであることが分かる。

- L2SW があるサブネット

これまでの解説に基づいて，それぞれの拠点で設計される VRRP グループを次の図に示す。




**図：VRRP グループの設計**

**●解の導出**

本問を解くに当たり，「仮想 IP アドレスの最少の個数」の問いを「VRRP グループを構築するサブネットの個数」と読み替えて，解を導くことにした。

ここまでの解説を整理しよう。各拠点で VRRP を設計するサブネットは，次のとおりである。

- データセンタ　2 個

©2017 ICT Workshop

- 本社　　2 個
- 営業所　　1 個

よって，この個数をそのまま解答すればよい。正解は解答例に示したとおりとなる。

## (4)

**解答例**

どのサーバアクセスも，VRRPのマスタルータが稼働する機器に接続されたWAN回線を経由して行われる。（50字）

問題文は，次のように記述されている。

> 図 9 中の名古屋営業所の IPsec ルータと L3SW を直接接続する経路が切断されたときの，名古屋営業所の PC から本社及びデータセンタのサーバへのアクセス経路を，“VRRP マスタルータ”という字句を用いて……述べよ。

名古屋営業所から本社又はデータセンタにアクセスする際，名古屋営業所のデフォルトゲートウェイを経由する。IPsec ルータと L3SW 間は VRRP を稼働させているので，VRRP マスタルータがデフォルトゲートウェイとなる。それでは，二つのルータのどちらが VRRP マスタルータなのだろうか。

結論から言うと，どちらを VRRP マスタルータと仮定しても，同じ解答が得られる。もっとも，それは後から気がつく話だ。

最初のうちは，二つのルータをそれぞれ VRRP マスタルータであると仮定し，その仮定ごとに，別々に考えることにする。

［A1］IPsec ルータを VRRP マスタルータであると仮定したときのアクセス経路
［A2］L3SW を VRRP マスタルータであると仮定したときのアクセス経路

アクセス先のサーバとして，データセンタ，本社を指定している。

アクセス先が異なると経路が異なるかもしれないので，アクセス先ごとに，別々に考えることにする。その際，問題文にある「IPsec ルータと L3SW を直接接続する経路が切断された」という条件に基づいて，アクセス経路を求める必要がある。

©2017 ICT Workshop

［B1］名古屋営業所の PC から本社のサーバへのアクセス経路
［B2］名古屋営業所の PC からデータセンタのサーバへのアクセス経路

これまで述べたことを整理すると，VRRP マスタルータであると仮定するルータで二つ，アクセス先で二つを，それぞれ別々に考えるので，全部で四つのケースを考察しようというわけだ。

次いで，本問で問われているアクセス経路について，“VRRP マスタルータ”という字句を用いて，どのような解を導き出せるのかを考察しよう。

### ●［A1］IPsec ルータを VRRP マスタルータであると仮定したときのアクセス経路

どのサーバが宛先であっても，PC からパケットを送信すると，デフォルトゲートウェイである VRRP マスタルータを必ず経由する。

この点を念頭に置きつつ，このたびは IPsec ルータを経由することに留意して，アクセス先ごとに考察しよう。

- **［B1］本社のサーバへのアクセス経路**

  名古屋営業所と本社間の経路は，少々複雑である。

  一見すると，両拠点は，インターネット VPN を介して接続されているように見える。しかし，インターネット VPN は，**トンネリング技術によって，拠点間を仮想的な専用線で接続している**と考えなければならない。

  インターネット VPN を介した拠点間の接続について，〔WAN の設計〕の第 2 段落の中で，「インターネット VPN は，データセンタと本社間，及びデータセンタと営業所間で設定する」と記述されている。それゆえ，名古屋営業所と本社は，インターネット VPN を介し，次のように接続していることが分かる。

  名古屋営業所
  ↓
  インターネット VPN（営業所とデータセンタ間のトンネル）
  ↓
  データセンタ
  ↓
  インターネット VPN（データセンタと本社間のトンネル）
  ↓
  本社

©2017 ICT Workshop

加えて，データセンタと本社間は，〔WAN 設計〕の第 1 段落に示されているように，専用線で接続されている。

以上を踏まえ，問題文にある「IPsec ルータと L3SW を直接接続する経路が切断された」という条件を考慮すると，どのような経路を通るのだろうか？その経路が切断された結果，IPsec ルータがもつ OSPF のルーティングテーブルから，L3SW を経由する経路情報が削除される。さらに，そこに接続された広域イーサ網を経由する経路情報も削除される。

それゆえ，VRRP マスタである IPsec ルータにパケットが転送されたら，そこに接続されている唯一の WAN 回線であるインターネット VPN を経由して，本社のサーバにアクセスすることが分かる。

以上より，次のような経路となる。ここで，VRRP マスタルータを網掛けで強調しておく。

PC →VRRP マスタルータ（名古屋営業所の IPsec ルータ）
→インターネット VPN →データセンタの IPsec ルータ
→データセンタ［ルータ間］→データセンタの L3SW
→専用線→本社の L3SW
→ DM サーバ

- **［B2］データセンタのサーバへのアクセス経路**

本社サーバとデータセンタ間は，インターネット VPN を介して接続している。

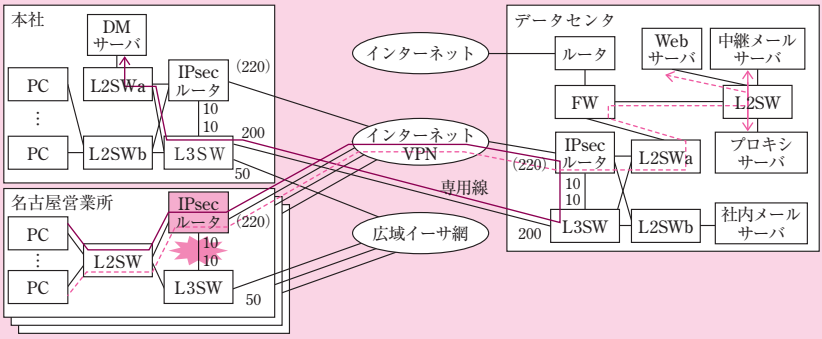
前述のとおり，「IPsec ルータと L3SW を直接接続する経路が切断された」という条件があるので，VRRP マスタである IPsec ルータにパケットが転送されたら，そこに接続されている唯一の WAN 回線であるインターネット VPN を経由して，データセンタのサーバにアクセスする。

以上より，次のような経路となる。ここで，VRRP マスタルータを網掛けで強調しておく。

PC →VRRP マスタルータ（名古屋営業所の IPsec ルータ）
→インターネット VPN →データセンタの IPsec ルータ→ FW
→データセンタサーバ

これまで解説した内容に基づいて，アクセス経路を次の図に示す。

©2017 ICT Workshop




注記1　大阪営業所と福岡営業所は，名古屋営業所と同構成である。
注記2　IPsec ルータと L3SW のポートの数値は，OSPF で設定するコスト値である。
注記3　IPsec ルータのポートに示した（　）内の数値は，トンネルインタフェースに設定するコスト値を示す。

：デフォルトゲートウェイ　　：アクセス先が本社のサーバ
：切断している箇所　　：アクセス先がデータセンタのサーバ

**図：IPsec ルータを VRRP マスタルータであると仮定したときのアクセス経路**

### ●［A2］L3SW を VRRP マスタルータであると仮定したときのアクセス経路

前述のとおり，全ての経路について，PC からパケットを送信すると，デフォルトゲートウェイである VRRP マスタルータを必ず経由する。

このたびは L3SW を経由することに留意して，アクセス先ごとに考察しよう。

- **［B1］本社のサーバへのアクセス経路**

  広域イーサ網は，イーサネットと同じく，マルチアクセスネットワークと考える。それゆえ，全ての拠点同士がつながっているとみなしてよいわけだ。ここがインターネット VPN のトンネルと異なる点である。それゆえ，名古屋営業所と本社は，広域イーサ網を介し，直接接続されている。

  以上を踏まえ，問題文にある「IPsec ルータと L3SW を直接接続する経路が切断された」という条件を考慮すると，どのような経路を通るのだろうか？ その経路が切断された結果，L3SW がもつ OSPF のルーティングテーブルから，IPsec ルータを経由する経路情報が削除される。さらに，インターネット VPN を経由する経路情報も削除される。

  それゆえ，VRRP マスタである L3SW にパケットが転送されたら，そこに接続されている唯一の WAN 回線である広域イーサネット網を経由して，本社の

©2017 ICT Workshop

サーバにアクセスすることが分かる。

以上より，次のような経路となる。ここで，VRRP マスタルータを網掛けで強調しておく。

PC → VRRP マスタルータ（名古屋営業所の L3SW）→広域イーサ網
→本社の L3SW → DM サーバ

- **［B2］データセンタのサーバへのアクセス経路**

データセンタサーバへのアクセスは少々複雑である。

名古屋営業所とデータセンタは，広域イーサ網，本社，及び，専用線を介して，接続されている。

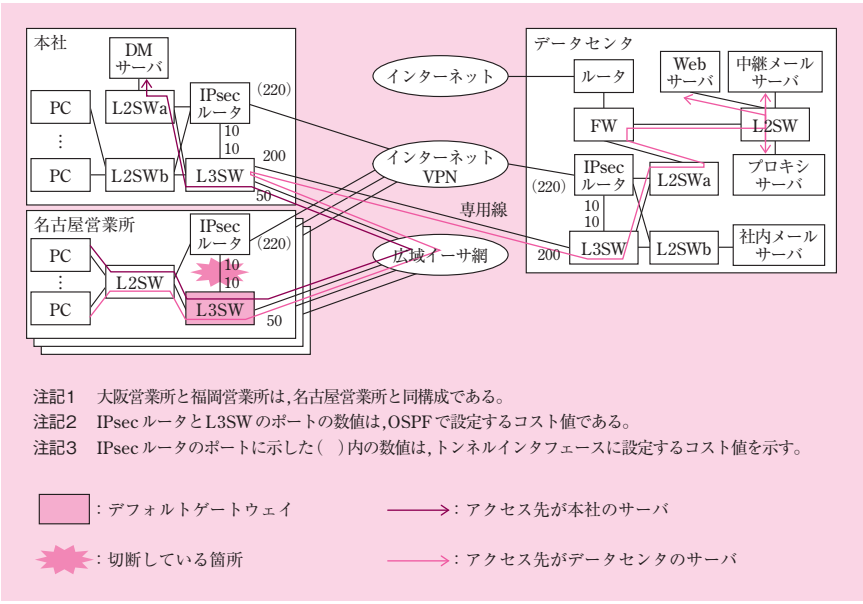
前述のとおり，「IPsec ルータと L3SW を直接接続する経路が切断された」という条件があるので，VRRP マスタである IPsec ルータにパケットが転送されたら，そこに接続されている唯一の WAN 回線である広域イーサネット網を経由して，データセンタのサーバにアクセスする。

したがって，次のような経路となる。ここで，VRRP マスタルータを網掛けで強調しておく。

PC → VRRP マスタルータ（名古屋営業所の L3SW）→広域イーサ網
→本社の L3SW →専用線→データセンタの L3SW → FW
→データセンタのサーバ

これまで解説した内容に基づいて，アクセス経路を次の図に示す。

©2017 ICT Workshop




**図：L3SW を VRRP マスタルータであると仮定したときのアクセス経路**

**●解の導出**

これまで，VRRP マスタルータであると仮定するルータで二つ，アクセス先で二つ，それぞれ別々に考察した。

その考察を通し，どのケースにも共通する，ある重要な事実が明らかになる。それは，次の点である。

- VRRP マスタルータ，及び，VRRP マスタルータに接続された WAN 回線を経由する。

まさしくこれは，問題文の指示にある「VRRP マスタルータ」という字句を使って，言い表されている。したがって，これが本問の解になると言えよう。

よって，その旨を字数に収まるように解答すればよい。正解は解答例に示したとおりとなる。

©2017 ICT Workshop

## (5)

**解答例**

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| イ | ン | タ | ー | ネ | ッ | ト | V | P | N | 経 | 由 | の | コ | ス | ト | 値 | が | 最 | 小 | 2 | 3 | 0 | で | あ | る | の | に | 対 |
| し | て | , | | 専 | 用 | 線 | 経 | 由 | の | コ | ス | ト | 値 | は | 2 | 0 | 0 | で | 最 | も | 小 | さ | い | 。 | | | | | | |

（53字）

問題文は，次のように記述されている。

> 表3中の下線（d）について，インターネットVPN経由の経路とならないことを，コスト値を示して……述べよ。ここで，PCが接続するVRRPのマスタルータは，L3SWで稼働しているものとする。

表3「PCからサーバへのアクセス経路の一覧（抜粋）」は，〔WANの設計〕の第4段落にある。下線（d）を含む行は次のとおりである。

**表：表3からの抜粋（下線（d）を含む行のみ）**

| 障害箇所 | 送信元 | 宛先 | 経路 |
|---|---|---|---|
| なし | 本社のPC | インターネット | (d) PC→専用線→データセンタ→プロキシサーバ→インターネット |

本問は，下線（d）のとおり「専用線」を経由した場合のコスト値と，問題文にある「インターネットVPN」を経由した場合のコスト値を比較し，後者を経由しないことを解答するよう求めている。

本社のPCのVRRPのマスタルータは，L3SWで稼働している。それゆえ，これがデフォルトゲートウェイとなる。

専用線を経由してインターネットへアクセスする経路は，機器も含めて詳しく記すと，次のようになる。

PC→本社のL3SW→専用線→データセンタのL3SW→FW
→プロキシサーバ→インターネット

この経路上に設定されているOSPFのコストは，L3SWから見た専用線のコスト値「200」だけである。したがって，この経路全体のコスト値は「200」となる。

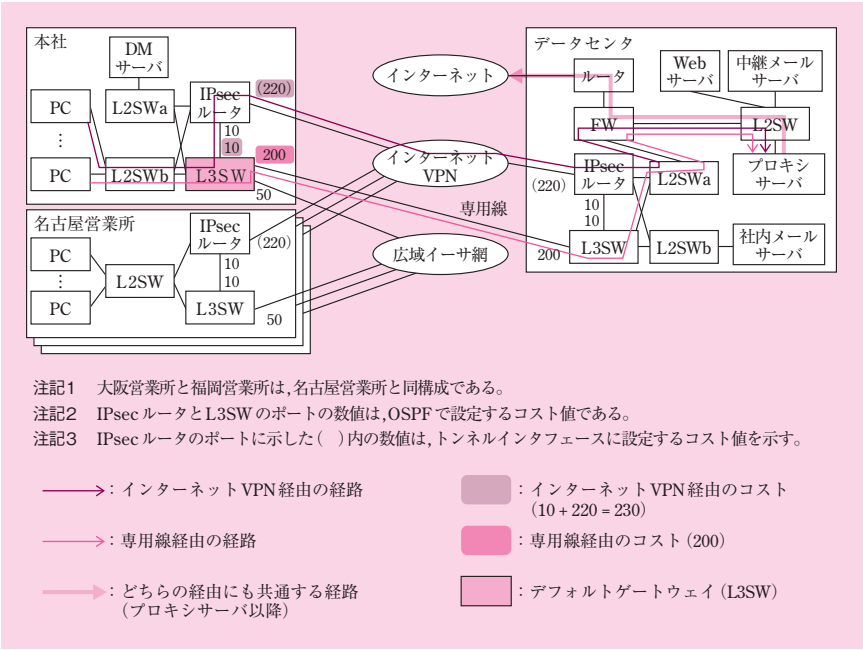
インターネットVPNを経由してインターネットへアクセスする経路は，機器も含め

©2017 ICT Workshop

て詳しく記すと，次のようになる。

PC →本社の L3SW →本社の IPsec ルータ→インターネット VPN
→データセンタの IPsec ルータ→ FW →プロキシサーバ→インターネット

この経路上に設定されている OSPF のコストは，L3SW から見た IPsec ルータに接続しているリンクのコスト値「10」，IPsec ルータから見たインターネット VPN のコスト値「220」の二つである。したがって，この経路全体のコスト値は，これらを合計した「230」となる。




**図：本社の PC からインターネットへのアクセス経路とコスト値**

したがって，専用線経由のコスト値が 200 であり，インターネット VPN 経由のコスト値が 230 であるので，後者のコスト値が大きい。それゆえ，後者を経由しないことが分かる。

詳細は割愛するが，本社の PC からインターネットへのアクセスに関し，候補となりうる経路は前記以外にも考えられる（例：広域イーサ網経由）。とはいえ，最小のコスト値となる経路は，専用線を経由するものとなる。

©2017 ICT Workshop

よって，その旨を字数に収まるように解答すればよい。正解は解答例に示したとおりとなる。

## (6)

**解答例**

**う：広域イーサ網→本社→専用線**
**え：インターネット VPN →データセンタ→専用線**

本問は，表 3 中の空欄に入れる適切な経路を問うている。

解答に際して，表 3 中の表記に従うことを求めている。具体的に言うと，経路として列挙する必要があるのは，送信元，経由する拠点，経由する WAN 回線，経由するサーバ，宛先となる。

本問の解を導くに当たって，インターネット VPN のトンネルが特定の拠点間にのみ設定されている点に留意する必要がある。

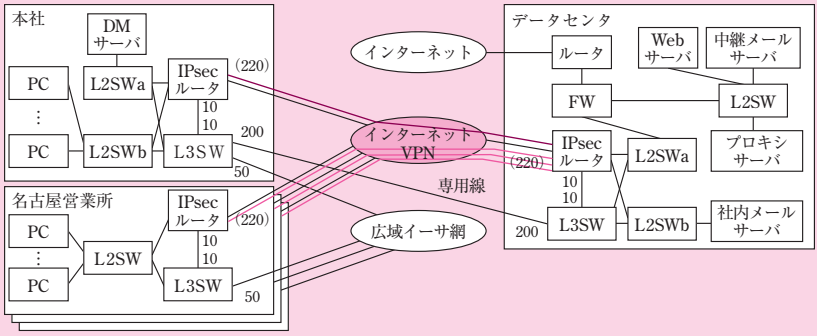
インターネット VPN を介した拠点間の接続について，〔WAN の設計〕の第 2 段落の中で，次のように記述されている。

> インターネット VPN は，データセンタと本社間，及びデータセンタと営業所間で設定する。

この記述から，次の図に示すとおり，トンネルを構築することが分かる。

冒頭の解説で触れたが，この一文を見落とすと，経路情報を正しく読み解くことができなくなる。後述する空欄えの正解を導けなくなってしまうのだ。

©2017 ICT Workshop




注記1　大阪営業所と福岡営業所は，名古屋営業所と同構成である。
注記2　IPsec ルータと L3SW のポートの数値は，OSPF で設定するコスト値である。
注記3　IPsec ルータのポートに示した（　）内の数値は，トンネルインタフェースに設定するコスト値を示す。

――――：データセンタと本社間のトンネル　――――：データセンタと営業所間のトンネル

**図：インターネット VPN のトンネル設定**

［う］

表 3 の中でこの空欄がある行は，次のとおりである。

**表：表 3 からの抜粋（下線（d）を含む行のみ）**

| 障害箇所 | 送信元 | 宛先 | 経路 |
|---|---|---|---|
| 名古屋営業所のインターネット VPN 接続 | 名古屋営業所の PC | データセンタのサーバ | PC →［う］→データセンタ→サーバ |
| | | インターネット | PC →［う］→データセンタ→プロキシサーバ→インターネット |

どちらの行も，空欄の前後を含む経路が「PC →［う］→データセンタ」となっているので，名古屋営業所の PC からデータセンタに至る経路を求めればよい。

インターネット VPN 接続で障害が発生した結果，OSPF のルーティングテーブルから，インターネット VPN（名古屋営業所とデータセンタ間のトンネル）を経由する経路情報が削除される。

その結果，名古屋営業所の PC から本社に至る経路は，次の 2 通りが考えられる。このうち，コストの小さい項番①の経路が選択される。

©2017 ICT Workshop

**表：名古屋営業所の PC から本社に至る経路**

| 項番 | 経路（パスコスト） | 経路全体のコスト |
|---|---|---|
| ① | PC →広域イーサ網（50）→本社→専用線（200）<br>→データセンタ | 250 |
| ② | PC →広域イーサ網（50）→本社［ルータ間］（10）<br>→インターネット VPN（220）→データセンタ | 280 |

この経路のうち，空欄に該当する部分を網掛けで示す。

PC →広域イーサ網→本社→専用線→データセンタ

よって，正解は「**広域イーサ網→本社→ 専用線**」となる。

なお，解答に際しては，IPsec ルータ，L3SW を経路に含めることは求められていないので，省略している。参考までに，それらを含めると次のようになる。

（L3SW が VRRP マスタルータの場合）
PC →名古屋営業所の L3SW →広域イーサ網→本社の L3SW →専用線
→データセンタ

（IPsec ルータが VRRP マスタルータの場合）
PC →名古屋営業所の IPsec ルータ
→名古屋営業所の L3SW（ここから先の経路は，前記と同様）

え

表 3 の中でこの空欄がある行は，次のとおりである。

**表：表 3 からの抜粋（下線（d）を含む行のみ）**

| 障害箇所 | 送信元 | 宛先 | 経路 |
|---|---|---|---|
| 名古屋営業所の広域イーサ網接続 | 名古屋営業所の PC | DM サーバ | PC →［え］→本社→ DM サーバ |

空欄の前後を含む経路が「PC →［え］→本社」となっているので，名古屋営業所の PC から本社に至る経路を求めればよい。

広域イーサ網接続で障害が発生した結果，OSPF のルーティングテーブルから，広域イーサ網を経由する経路情報が削除される。

©2017 ICT Workshop

それゆえ，名古屋営業所の PC から本社に至る経路は，インターネット VPN を経由するしかない。ただし，本問の冒頭で解説したとおり，名古屋営業所に設定されたトンネルは，接続先がデータセンタである。名古屋営業所から本社に直に接続しているトンネルは存在しないことに留意しよう。

その結果，名古屋営業所の PC から本社に至る経路は，次の 2 通りが考えられる。このうち，コストの小さい項番①の経路が選択される。

**表：名古屋営業所の PC から本社に至る経路**

| 項番 | 経路（パスコスト） | 経路全体のコスト |
|---|---|---|
| ① | PC →インターネット VPN（220）→<br>データセンタ［ルータ間］（10）→専用線（200）→本社 | 430 |
| ② | PC →インターネット VPN（220）→<br>データセンタ→インターネット VPN（220）→本社 | 440 |

この経路のうち，空欄に該当する部分を網掛けで示す。

PC →インターネット VPN →データセンタ→専用線→本社

よって，正解は「**インターネット VPN →データセンタ→専用線**」となる。

なお，解答に際しては，IPsec ルータ，L3SW を経路に含めることは求められていないので，省略している。参考までに，それらを含めると次のようになる。

（IPsec ルータが VRRP マスタルータの場合）
PC →名古屋営業所の IPsec ルータ
　→インターネット VPN（名古屋とデータセンタ間のトンネル）
　→データセンタの IPsec ルータ→データセンタの L3SW →専用線→本社

（L3SW が VRRP マスタルータの場合）
PC →名古屋営業所の L3SW
　→名古屋営業所の IPsec ルータ（ここから先の経路は，前記と同様）

©2017 ICT Workshop

Column ▶▶▶

## 試験本番で役立つ心構え

本書の締めくくりとして，試験本番で役立つ心構えを挙げておきます。

- **合格点をねらおう**

  本試験の合格ラインは，100 点満点中，60 点です。
  ここは試験と割り切り，完全主義を捨てましょう。「6 割取れれば合格」という心構えでよいのです。そう思うと，大分気持ちが楽になります。

- **分からない問題でも，あきらめずに部分点をねらおう**

  完全主義を捨てますが，必死になって合格圏内に食い込むように努力しましょう。よく分からない小問の一つ，二つは早々と切り上げ，「部分点ねらいでいく」と割り切るくらいの大胆さが必要です。そういう問題に出くわしたならば，せめてキーワードの一つだけでも書いて，「一矢報いる」くらいの気構えで臨みましょう。

- **手強そうな問題でも，「特殊な知識は問われないはずだ」と信じよう**

  あまり馴染みのない新技術が登場して，何やら手強そうに思えても，焦りは禁物です。一呼吸置いて，次のように自分に言い聞かせましょう。

  「新技術そのものに関する前提知識は極力必要がないように配慮されているはずだ（平成 25 年度午後Ⅱ採点講評）。出題に値するテーマを選んでいるはずなので，その題材としてこの新技術が登場しているだけに過ぎない。素直に考えれば，きっと出題の意図が分かるはずだ。解法の糸口が見つかるはずだ」
  おそらく，焦りを覚えた受験者は自分だけではないはずです。あなたはいち早く落ち着きを取り戻して，問題に取り掛かりましょう。

- **最後の 1 分 1 秒まであきらめない！**

  必死になって解いているうちに，答えがひらめくことがあります。最後の 1 分 1 秒まで，答案に向って部分点を積み上げましょう。決してあきらめないことが，何より大切です。

©2017 ICT Workshop