

平成 30 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

センサ、アクチュエータなどが情報ネットワークに接続され、企業間にまたがった情報システムが構築されている。そのような分野に応用されることを目的とした、様々なネットワークの規格化も進んでいる。

本問では、製造業のスマート化の基盤となるネットワークシステムの設計を題材にした。その中で、以前から広く用いられている、“Web コンピューティング”に関する知識と設計能力を前提にして、比較的新しい“メッセージ通信プロトコル MQTT”と“Web サービスの連携に用いる仕組み”に関して、本文の記述を理解し、それらを情報システムに応用できるネットワーク技術の能力を問う。

## 採点講評

問 1 では、製造業のスマート化の基盤となるネットワークシステムを題材に、ネットワークセキュリティ、メッセージ通信プロトコル MQTT、及び Web サービスの連携に用いる仕組みについて出題した。後半の 2 テーマについては、知識がなくても本文を読むことで解答を導けるようにした。

設問 1 は、ネットワークセキュリティについて問うた。設問の中では設問 1(2)の正答率が低かった。導入構成例（図 1）では、インターネットを介した二つの拠点に、三つのファイアウォールが設置されている。X システムに関する記述を正しく理解し、注意深く解答してほしい。

設問 2 は、MQTT について問うた。通信プロトコルに関する設問 2(3)の正答率は高かったが、QoS レベルに関する設問 2(2)の正答率は低かった。MQTT の QoS レベルの考え方は、メッセージ交換の重要な概念の一つである。通信シーケンス（図 3）をもう一度よく読み、その仕組みを理解してほしい。

設問 3 は、API アクセス認可の仕組みについて問うた。この仕組みは“The OAuth 2.0 Authorization Framework (RFC6749)”に記述があり、広く利用されている。認可のプロセスでは、二つのトークンとともに、URI が固定された WebAP が重要な役割を担う。設問では、それらの知識を前提とせずに通信シーケンスから解答を導くようにした。正答率は比較的高かったが、リダイレクトに関する通信シーケンスを正しく理解していない誤答が散見された（設問 3(1)シ）。リダイレクトは、Web サービスの基本的概念の一つであり、よく理解しておいてほしい。

設問 4 は、ネットワークシステムの拡張性について問うた。顧客ネットワーク側の MQTT クライアントを接続する際の考慮点について出題している。設問をよく読み、メッセージ交換システムが有する拡張性と、NAT を用いて運用主体が異なる二つのネットワークを接続した際の制約について、それぞれ理解した上で解答してほしい。

設問		解答例・解答の要点	備考
設問 1	(1)	ア 暗号化	
		イ 検知	
		ウ 認証	
		エ TCP	
	(2)	X 社が運用・保守を行う機器から X 社 FW の方向に確立される TCP コネクションだけを許可する。	
	(3)	クライアント証明書を配布してクライアント認証を行う。	
設問 2	(1)	TCP の送信処理中に、デバイスの電源断などで TCP コネクションが開放された場合	
		メッセージの重複を防止する。	
	(3)	オ SUBSCRIBE	
		カ config/Di	
		キ デバイス Di	
		ク 交換サーバ	
		ケ 業務サーバ	
		コ 業務サーバ, 交換サーバ	
	(4)		
設問 3	(1)	サ 認可	
		シ WebAP	
		ス リフレッシュトークン	
		セ 認可応答	
		ソ 認可	
	(2)	10	
	(3)	WebAP の URI を固定にし、絶対 URI を事前に通知してもらう。	
設問 4	(1)	送信元 IP アドレスを NAT ルータ -P に、宛先 IP アドレスをエッジサーバ -P に、それぞれ変換する。	
		顧客サーバ -P' から NAT ルータ -P' のポート 8883 番への通信	
		config/Di, status/Di	
	(4)	① ・1:1 静的双方向 NAT の設定を NAT ルータに追加する。 ② ・通信を許可するルールを通信装置内の FW に追加する。	

今日では、センサ、アクチュエータなどが情報ネットワークに接続され、企業間にまたがった情報システムが構築されている。

本問は、機械メーカ X 社が、顧客に販売した機械を遠隔から運用・保守することを目的に、顧客工場に設置された機械と X 社をインターネット経由で接続するシステム（以下、X システムという）を構築する事例を取り上げている。

## ●本問の全体像

### ・X システムの目的と機能

X システムは、顧客工場内の機械を運用・保守することを目的とし、次に示す三つの機能①～③を主に提供している。

#### [機能① 運用保守情報交換機能]

X 社の業務サーバが、顧客工場に設定された機械（デバイス）との間で、運用・保守に関する情報を自動的に交換する機能

#### [機能② 運用保守情報提供機能]

顧客サーバが、インターネット経由で X 社の業務サーバの API にアクセスすることにより、顧客工場の機械（デバイス）の運用・保守に関する情報を顧客に提供する機能

#### [機能③ 内部情報交換機能]

顧客ネットワークと顧客工場内の X システムを接続することにより、顧客サーバが、機械との間で、企業秘密を含む内部情報を自動的に交換する機能

なお、ここに記した機能①～③の名称は、本書が独自に名付けたものである。機能名を用いると説明しやすくなるので、以降の解説で適宜使用している。

機能①、②は、当初から構想されている内容である。

機能③は、将来構想の位置付けである。将来構想ではシステムの構成が変化する。

### ・X システムの構成（当初の構想）

まず、X システムの重要な構成要素である「機械」について解説しよう。

機械の構成について、序文の第 2 段落、及び本文の図 1「X システムの導入構成例（抜粋）」に記されている内容を整理すると、次の表のようにまとめられる。

表：機械の構成

機械	工作装置	デバイス, L2SW
	通信装置	エッジサーバ, FW, L3SW

次いで、X システム全体の構成を解説しよう。

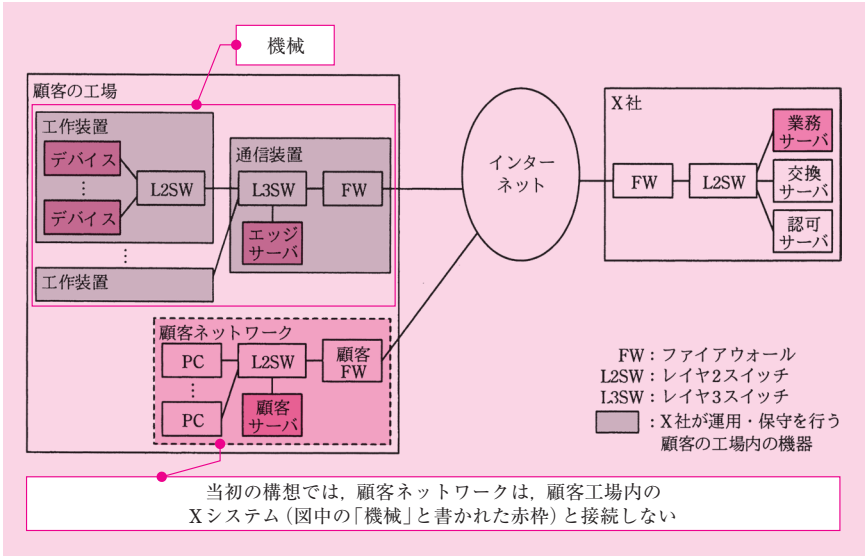
ここでは当初の構想に基づいて説明する。

「X システムの構想」の第 1 段落には、「X システムは、X 社が運用・保守を行う顧客の工場内の機器、X 社内のサーバ、及びそれらを接続するためのネットワーク機器から構成されている」と記述されている。

つまり、X システムは、顧客工場内の機械、及び X 社内のサーバ等から構成される。

当初の構想では、顧客工場の機械は顧客ネットワークとは接続しない。この点は、第 3 段落に「工作装置と通信装置を接続し、顧客の工場内に X システム専用のネットワークを構成する。顧客ネットワークは利用しない」と記述されていることから分かる。

以上の内容を、図 1「X システムの導入構成例（抜粋）」に書き加えて整理しておく。



図：X システムの構成

・機能① 運用保守情報交換機能

X 社の業務サーバは、顧客工場に設定された機械（デバイス）との間で、運用・保守に関する情報を自動的に交換する。

本書は、この機能を「運用保守情報交換機能」と呼ぶことにする。

当機能について、〔X システムの構想〕の第 3 段落を見てみよう。

運用・保守に関する情報（以降の解説で、「運用保守情報」と称する）を交換するには、専用のアプリケーションが必要となる。この点について、次のように記述されている。

X システムの業務アプリケーションプログラムは、エッジサーバと業務サーバ上で動作する。これらのサーバとデバイスは、デバイスの運用・保守に関する情報を、自動的に交換する。

第 3 段落内の 2 番目と 3 番目の箇条書きには、運用保守情報のやり取りについて、次のように記述されている。

- ・ publish/subscribe 型のメッセージ通信プロトコル MQTT（Message Queuing Telemetry Transport）を使って、交換サーバを介して、デバイス、エッジサーバ及び業務サーバの間でメッセージを交換する。
- ・ デバイス、エッジサーバ及び業務サーバに MQTT クライアント機能を、交換サーバに MQTT サーバ機能をそれぞれ実装する。

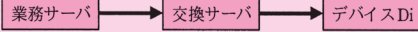
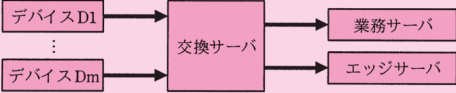
この記述から分かることは、デバイス、エッジサーバ及び業務サーバ間のメッセージ交換に MQTT を使うこと、そのやり取りは交換サーバを介して行うことである。

MQTT を使った通信について、より詳しい説明が〔MQTT を使ったメッセージ交換方式〕に記されている。

図 4「X システムのメッセージ交換」には、交換サーバを介した 2 種類の通信を示している。

一つ目は、業務サーバが特定のデバイスに対して設定情報を送信するものである。これは項番 1 に示されている。

二つ目は、全てのデバイスが、業務サーバに対し、及び、同じ工場のエッジサーバに対し、稼働情報を定期的に変送するものである。これは項番 2 に示されている。

項番	メッセージ交換の概要	QoS レベル	トピック 名	メッセージ
1	<p>業務サーバから、特定のデバイス <math>D_i</math> に対して、設定情報を送信する。</p> 	2	config/ $D_i$	デバイス $D_i$ の設定情報
2	<p>全てのデバイス <math>D_i</math> (<math>i=1, 2, \dots, m</math>) から、業務サーバ及び同じ工場のエッジサーバに対して、稼働情報を定期的に送信する。</p> 	0	status/ $D_i$	デバイス $D_i$ の稼働情報

注記  $D_i$  は、デバイスの識別子を表す。

図：X システムのメッセージ交換（図 4 の抜粋）

メッセージ交換について設問 2 で問われているので、詳しくはそこで解説しよう。

・機能② 運用保守情報提供機能

顧客は、インターネット経由で業務サーバにアクセスし、自社工場のデバイスの運用保守情報を参照することができる。業務サーバへのアクセスは、顧客ネットワークに設置した顧客サーバを経由して行う。

当機能について、[X システムの構想] の第 4 段落を見てみよう。

業務サーバは、顧客向けに API（Application Programming Interface）を提供する。顧客は、インターネット経由で API にアクセスし、デバイスの運用・保守に関する情報を参照する。この API に関する説明を次に示す。

- ・ X 社の業務サーバと認可サーバに HTTP サーバ機能をそれぞれ実装する。
- ・ 顧客は、顧客サーバに、API アクセス用の Web アプリケーション（以下、WebAP という）と HTTP サーバ機能を実装する。
- ・ 顧客は、PC の Web ブラウザを使い、顧客サーバを経由して、API にアクセスする。
- ・ X 社の認可サーバは、顧客サーバから API へのアクセスを許可する。

まず、顧客の観点に立って整理してみよう。

顧客は、PC の Web ブラウザを使い、顧客サーバの WebAP にアクセスする。

顧客サーバには HTTP サーバ機能があり、WebAP はここに登録されている。WebAP は特定の URI と紐付けられており、当該 URI にアクセスすることで、HTTP サーバが WebAP を起動する仕組みになっている。

TCP コネクションは、PC のブラウザと WebAP の間に張られている。クライアントに当たるのが PC のブラウザで、サーバに当たるのが顧客サーバの WebAP である。

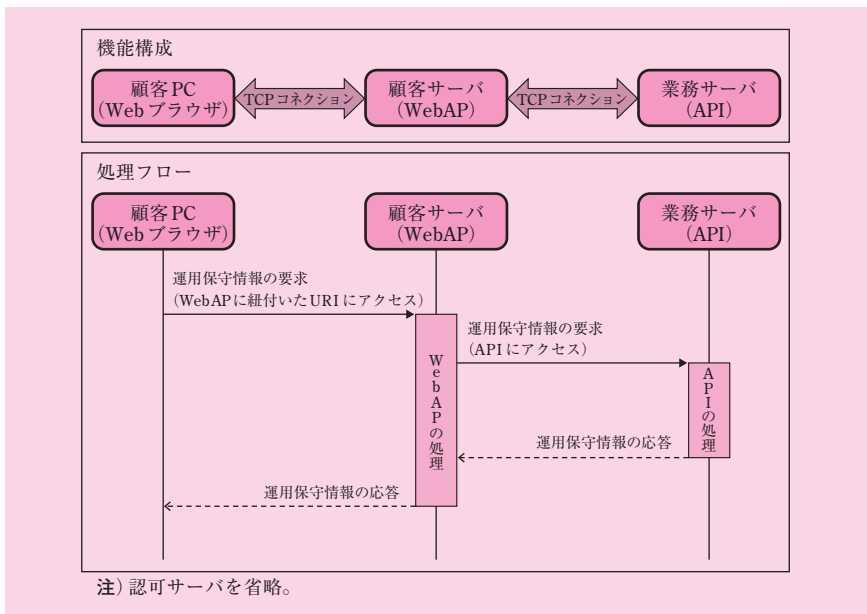
次に、WebAP の観点に立って整理してみよう。

WebAP は、顧客からのリクエストに基づき、業務サーバの API にアクセスする。

この API とは、言うなれば、特定のアプリケーションに紐付いた URI である。API (すなわち URI) にアクセスすると、業務サーバは、このアプリケーションを起動する仕組みになっている。

このとき、TCP コネクションは、WebAP と API の間に張られている。クライアントに当たるのが顧客サーバの WebAP で、サーバに当たるのが業務サーバの API である (厳密に言うと、サーバに当たるのは API に紐付くアプリケーションである)。

ここまで解説した内容を整理するため、当機能の基本的な構成、及び処理のフローを、次の図に示す。ただし、ここでは認可サーバを省略している。



図：運用保守情報提供機能の構成と処理フロー

最後に、認可サーバについて整理してみよう。

〔API にアクセスする顧客サーバの管理〕の第 2 段落には、「X システムでは、認可サーバを使って、顧客サーバからの API アクセスを認可する」と記述されている。

つまり、アクセス可能な API を顧客ごとに割り当てる仕組みを導入するわけだ。

これに続く文には、「契約及びサービス仕様の変更が顧客ごとに発生するので、それを前提とした認可の仕組みが必要になる」と記述されている。

つまり、アクセス可能な API の定義が適宜変更されるので、それに迅速に追従できるような認可の仕組みが必要となっている。

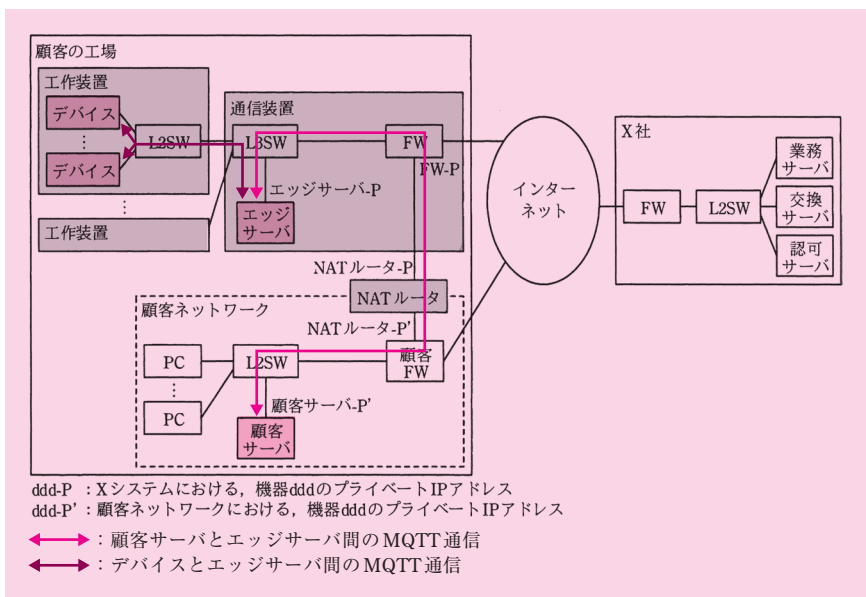
そのため、第 2 段落の最後で、「認可コード、アクセストークン、及びリフレッシュトークンを使った、認可の仕組みを採用することにした」と記述されている。

この点について設問 3 で問われているので、詳しくはそこで解説しよう。

### ・機能③ 内部情報交換機能

将来構想では、内部情報（顧客の企業秘密を含むような設定情報及び稼働情報）を、顧客サーバとデバイスとの間で交換する。

内部情報は、端的に言う、これまでと同様に、設定情報及び稼働情報の 2 種類がある。ただし、顧客の企業秘密を含んでいるので、既存の設定情報及び稼働情報とは



図：将来構想におけるネットワーク構成案



区別しているわけだ。

内部情報のうち、設定情報の方は、配信元が顧客サーバであり、配信先がデバイスとなる。一方、稼働情報は、配信元がデバイスであり、配信先が顧客サーバとなる。

なお、本文の図 7、図 9 は、これら 2 種類の内部情報を一つにまとめて記している。メッセージ交換を示す矢印が双方向になっているのは、そのためである。

この将来構想を実現するため、顧客ネットワークと X システムを接続する。この構成が本文の図 8 に示されている。

内部情報のメッセージ交換について設問 4 で問われているので、詳しくはそこで解説しよう。

### ・本問の構成

以上を踏まえて本問の構成を概観すると、次のように整理できる。

表：本問の構成

見出し	主な内容	主に対応する出題箇所	
		設問	小問
X システムの構想	機械及び X システムの構成 図 1「X システムの導入構成例（抜粋）」	—	—
ネットワーク セキュリティ対策	TLS の利用 侵入及びなりすまし対策	設問 1	(1) ～ (3)
MQTT を使った メッセージ 交換方式	表 1「MQTT コントロールパケットの 種別（抜粋）」 図 2「MQTT を使ったメッセージ交換 方式の通信シーケンス例」 図 3「QoS レベルとメッセージ送信の 通信シーケンス」 図 4「X システムのメッセージ交換」 図 5「W さんが T の概算に用いた通信 シーケンス」	設問 2	(1) ～ (4)
API にアクセスする 顧客サーバの管理	図 6「X システムの API アクセスの通信 シーケンス」	設問 3	(1) ～ (3)
エッジサーバを 活用する将来構想	図 7「将来構想で追加される X システムの メッセージ交換例」 図 8「W さんが考えた将来構想における ネットワーク構成案（抜粋）」 図 9「W さんが考えた将来構想における メッセージの流れ」	設問 4	(1) ～ (4)

それでは、設問の解説に移ろう。

## ■設問 1

本設問は、[ネットワークセキュリティ対策] について問うている。

### (1)

#### 解答例

ア：暗号化  
イ：検知  
ウ：認証  
エ：TCP

本小問は、本文中の空欄ア～エに入れる適切な字句を問うている。

空欄ア～エは、[ネットワークセキュリティ対策] の第 1 段落、1 番目と 2 番目の箇条書きの中にある。

- ・情報の漏えい及び改ざん対策のために TLS を利用する。TLS には、情報を  する機能、情報の改ざんを  する機能、及び通信相手を  する機能がある。
- ・工場内の機器と X 社内の機器との通信は、いずれもクライアントサーバ型の通信であり、機器間の  コネクションの確立要求は、工場から X 社の方向に行われる。

TLS は、TCP/IP 通信のセキュリティを確保するプロトコルである。

トランスポート層プロトコルに TCP を用いるアプリケーション層プロトコルを対象とし、TCP パケットのペイロード部分、すなわち、アプリケーション層のパケット全体を暗号化する。

TLS は、暗号化機能に加え、メッセージ認証及び主体認証の機能ももっている。

- ・主体認証

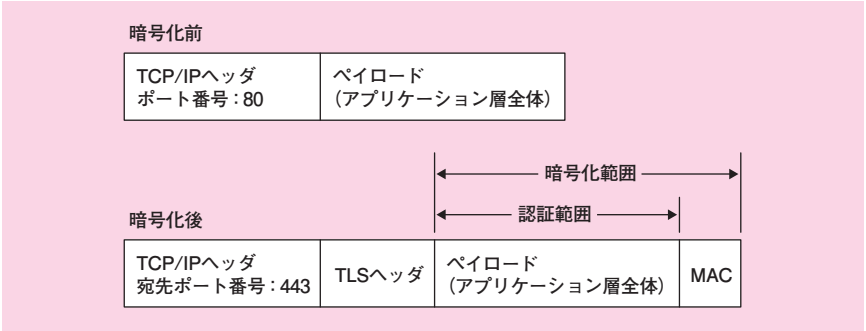
サーバ認証、及び、オプションでクライアント認証を行うことができる。それら主体認証には、通常、電子証明書が用いられる。

- メッセージ認証

TCP パケットのペイロードから MAC (Message Authentication Code) と呼ばれるメッセージダイジェストを生成し、これをパケットに付与する。

- 暗号化

TCP パケットごとに、そのペイロードと MAC の両者を暗号化する。



図：TLS の暗号化とメッセージ認証の範囲

ここで問われている空欄を含む文章を、これら TLS の特徴や機能と照らし合わせることで、解を導くことができる。

ア

空欄アを含む文は、「TLS には、情報を [ア] する機能……がある」と記述されている。

TLS は暗号化機能を有しており、その暗号化の範囲には、アプリケーション層のパケット全体が含まれている。したがって、情報を暗号化することができる。

よって、正解は「暗号化」となる。

イ

空欄イを含む文は、「TLS には、……情報の改ざんを [イ] する機能……がある」と記述されている。

TLS はメッセージ認証機能を有しており、その認証の範囲には、アプリケーション層のパケット全体が含まれている。したがって、情報の改ざんを検知することができる。

よって、正解は「検知」となる。

ウ

空欄ウを含む文は、「TLS には、……通信相手を ウ する機能がある」と記述されている。

TLS は主体認証機能を有している。つまり、通信相手の真正性を認証することができる。

よって、正解は「**認証**」となる。

エ

工場内の機器と X 社内の機器の間でやり取りされる通信に関し、X 社外の通信区間のセキュリティを高めることを目的として、TLS が用いられる。

TLS は、前述の解説のとおり、トランスポート層プロトコルに TCP を用いるアプリケーション層プロトコルを対象としている。

この点を踏まえ、空欄エを含む文を見てみよう。

そこには、「工場内の機器と X 社内の機器との通信は、いずれもクライアントサーバ型の通信であり、機器間の エ コネクションの確立要求は、工場から X 社の方向に行われる」と記述されている。

ここに「コネクション」とあるが、TLS の使用を踏まえた文脈から判断すると、コネクションを用いる通信として考えられるのは、「TCP」であると言える。

さらに、後続の本文を見ると、機器間の通信を説明する際、「TCP コネクション」という字句を随所で用いていることから、この空欄に「TCP」が入ることが察せられる（〔MQTT を使ったメッセージ交換方式〕の第 4、第 6 段落）。

よって、正解は「**TCP**」となる。

TLS について、詳しくは本書の第 8 章「8.4.6 SSL, TLS」を参照していただきたい。

## (2)

### 解答例

X	社	が	運	用	・	保	守	を	行	う	機	器	か	ら	X	社	F	W	の	方	向	に	確	立
さ	れ	る	T	C	P	コ	ネ	ク	シ	ヨ	ン	だ	け	を	許	可	す	る	。					

(45字)

問題文は、「本文中の下線①の対策を……述べよ」と記述されている。

下線①は、〔ネットワークセキュリティ対策〕の第 1 段落、2 番目の箇条書きの中にある。実は、この箇条書きの中には下線②も含まれており、次の小問 (3) で問われて

いる。

この箇条書きは、小問（2）及び（3）に共通する内容が含まれているので、まずはここで説明されているセキュリティ対策について解説する。次いで、それぞれの小問の解を導くことにしよう。

### ●第 1 段落、2 番目の箇条書きで説明されているセキュリティ対策

この箇条書きには、ネットワークのセキュリティを高めるため、「侵入対策」及び「なりすまし対策」を採用すると記述されている。

具体的には、次の 3 つの対策が列挙されている。

- ・工場内の機器と X 社内の機器との通信は、いずれもクライアントサーバ型の通信であり、機器間の TCP コネクションの確立要求は、工場から X 社の方向に行われる。それを踏まえて、次の侵入及びなりすまし対策を採用する。
- X 社に設置された FW を使った対策
- ①通信装置内の FW を使った対策
- ②TLS の機能を使った、デバイス及びエッジサーバに関する対策

冒頭の「・機能① 運用保守情報交換機能」で解説したが、本文の図 4 に示されているとおり、工場内のデバイスとエッジサーバは、それぞれ X 社の交換サーバと通信する。

つまり、ここで言う「工場内の機器と X 社内の機器との通信」は、具体的に言うと、

- ・ デバイスと交換サーバの MQTT 通信
- ・ エッジサーバと交換サーバの MQTT 通信

を指している。

1 番目と 2 番目は FW を使った対策であり、3 番目は TLS の機能を使った対策である。

内容について理解できたところで、それでは、小問の解を導くことにしよう。

### ●解の導出：下線①の対策

下線①は「通信装置内の FW を使った対策」である。

FW は、パケットヘッダ中の IP アドレスやポート番号に基づき、通信をフィルタリングする機能を有している。

したがって、ここで実施する「侵入対策」「なりすまし対策」のうち、下線①に該当するのは「侵入対策」であることが分かる。

下線①の FW は、通信装置内に設置されている。

この通信装置は、図 1 に示されているとおり、顧客の工場内にある。通信は「工場から X 社の方向に行われる」ので、この FW で設定するフィルタリングは、次に示す内容となる。

表：フィルタリングの設定

項目	内容
送信元 IP アドレス	デバイス、エッジサーバ等、図 1 の網掛けに示された、運用・保守を行う顧客の工場内の機器
宛先 IP アドレス	X 社の交換サーバ
宛先ポート番号	MQTT のポート番号

本小問が問うているのは、下線①の対策の具体的な内容である。

要するに、この表に整理したフィルタリングの設定を問うているわけだが、指定字数が 50 字と限られている。それゆえ、解答に際しては、出題者の趣旨に沿ってキーワードを選ぶ必要がある。

そこで、文脈上、ここでは「侵入対策」に言及していることに着目してみるとよい。

TCP コネクションを使った通信において、ハッカーは、送信元 IP アドレスを詐称した通信を行うことができない。なぜなら、これを詐称したならば、往復のやり取りを伴うコネクション確立フェーズの段階で失敗してしまうからだ。

したがって、侵入対策では、送信元 IP アドレスを特定することが肝要となる。

その点を踏まえ、顧客工場に悪意ある者が存在しており、X システムへの不正侵入を試みるとしよう。

このとき、ターゲットとなるのは、X 社の交換サーバ、又は、工場内の機器（エッジサーバ、デバイス）であると考えられる。

まず、交換サーバへの不正侵入を試みるため、例えば、工作装置の代わりに端末を通信装置に取り付けて、これを送信元とし X 社の交換サーバを宛先とする通信を行ったとしよう。

このとき、前記の表のとおり FW のフィルタリングを設定しておけば、この通信の送信元 IP アドレスは許可されていないため、遮断できることが分かる。

次いで、工場内の機器への不正侵入を試みるため、通信装置のインターネット側インタフェースに端末を接続し、これを送信元とし工場内の機器を宛先とする通信を行ったとしよう。

このとき、前記の表のとおりに FW のフィルタリングを設定しておけば、この通信の方向は許可されていないため、遮断できることが分かる。

こうした点を踏まえると、解答に際し、許可する通信の送信元が「運用・保守を行う顧客の工場内の機器」である旨を答案に含めるようにしたい。

それ以外の点については、字数の許す範囲で、宛先が X 社であることなどを述べるとういだろう。

よって、正解は解答例に示したとおりとなる。

### ●参考：下線①の対策の限界

先ほどの解説で、工作装置の代わりに端末を通信装置に取り付けて、これを送信元とし X 社の交換サーバを宛先とする通信を行うケースを例に取り上げた。

このとき、接続する端末の IP アドレスを、正規のデバイスのものに詐称したとしよう。このようになりすまされると、FW では遮断できない。

もう一つ、通信装置のインターネット側インタフェースに端末を接続し、これを送信元とし工場内の機器を宛先とする通信を行うケースを例に取り上げた。

同様にこのときも、接続する端末の IP アドレスを、正規の交換サーバのものに詐称したとしよう。こちらも、このようになりすまされると、FW では遮断できない。

したがって、残念ながら、対策①には限界があるわけだ。

とはいえ、このようななりすましを行うケースは、FW で行える対策の範疇を超えている。それゆえ、本小問の考慮から外してよい。

今ここで問われている対策は、「機器間の TCP コネクションの確立要求は、工場から X 社の方向に行われる」ことを踏まえた、あくまで FW で行えるものに限定したものだからだ。

実は、本事例では、なりすまし対策を講ずるため、TLS の主体認証の機能を用いている。その点が次の小問 (3) で取り上げられているので、詳しくはそこで解説しよう。

## (3)

### 解答例

クライアント証明書を配布してクライアント認証を行う。(26字)

問題文は、「本文中の下線②の対策を……述べよ」と記述されている。

下線②は、〔ネットワークセキュリティ対策〕の第 1 段落、2 番目の箇条書きの中にある。

先ほど、小問 (2) の「●第 1 段落、2 番目の箇条書きで説明されているセキュリティ対策」で解説したとおり、この箇条書きでは、「侵入対策」及び「なりすまし対策」を採用する旨を述べている。

ここまで理解できれば、小問を解く準備は整った。それでは、小問の解を導くことにしよう。

### ●解の導出：下線②の対策

下線②は「TLS の機能を使った、デバイス及びエッジサーバに関する対策」である。

TLS は、先の小問 (1) で解説したとおり、主体認証の機能を有している。

したがって、ここで実施する「侵入対策」「なりすまし対策」のうち、下線②に該当するのは「なりすまし対策」であることが分かる。

TLS の主体認証は、サーバ認証とクライアント認証の 2 種類がある。

デバイス及びエッジサーバは、工場に設置されているので、クライアント側である。この点は、2 番目の箇条書きの中に「機器間の TCP コネクションの確立要求は、工場から X 社の方向に行われる」と記されていることから分かる。

TLS のクライアント認証は、サーバがクライアントの真正性を確認するために実施するものである。正規のクライアント証明書をクライアントがもっていることを検証する仕組みになっている。

したがって、クライアント証明書を発行し、これをデバイス及びエッジサーバにインストールすれば、クライアントのなりすまし対策を講ずることができる。

よって、正解は「クライアント証明書を配布してクライアント認証を行う」となる。

なお、本文には明示されていないが、TLS ではサーバ認証は必ず行うものなので、交換サーバにサーバ証明書がインストールされているものと考えられる。

小問 (2) の「●参考：下線①の対策の限界」でなりすましを懸念したが、TLS の機能を用いることによって、クライアント、サーバの双方において、なりすまし対策を講ずることができるわけだ。

## ■設問 2

本設問は、〔MQTT を使ったメッセージ交換方式〕について問うている。

ここでは、冒頭で解説した「・機能① 運用保守情報交換機能」を取り上げている。

本設問を首尾よく解くには、MQTT の仕組みを理解しておく必要がある。そこで、



これらの点について、概要をまずは解説する。

## ● MQTT の仕組み

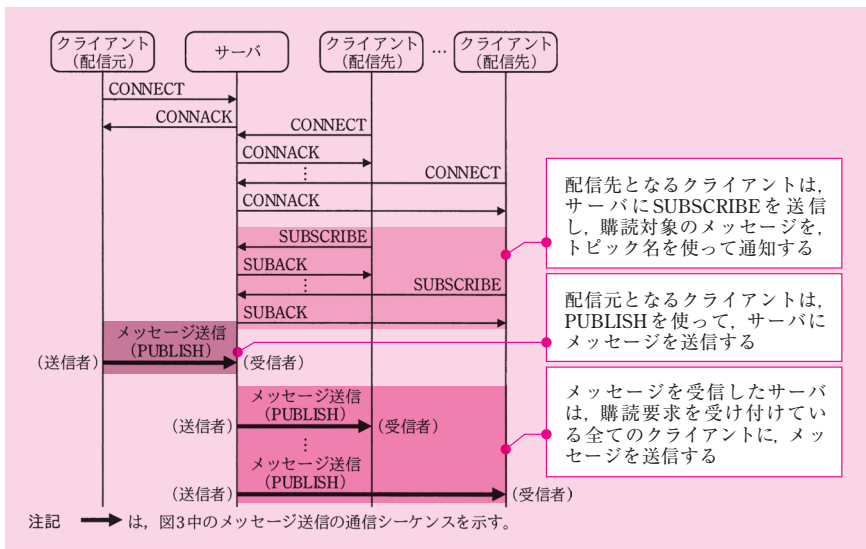
MQTT (Message Queuing Telemetry Transport) は、publish/subscribe 型のメッセージ通信プロトコルである。

MQTT を使用すると、あるクライアント (配信元) から、複数のクライアント (配信先) に、メッセージを送信することができる。

クライアント (配信元) とクライアント (配信先) の通信は、サーバを介して行われている。

本文の図 2 には、その通信シーケンスの例が記されている。さらに、[MQTT を使ったメッセージ交換方式] の第 4 段落は、その通信シーケンスを説明している。

図 2 の通信シーケンスと、これに対応する第 4 段落の記述とを結び合わせると、次の図のようになる。



図：MQTT を使ったメッセージ交換方式の通信シーケンス例

図 2 の注記は、「メッセージ送信 (PUBLISH)」と記されている太い矢印線について、「図 3 中のメッセージ送信の通信シーケンスを示す」と述べている。

図 3 は、PUBLISH を使ったメッセージ送信を示している。

第 5 段落によると、このメッセージ送信は、「QoS レベルを使って送達確認手順を

指定する」と記述されている。

本文は、2 種類の QoS レベルを説明している。

一つ目は QoS レベル 0 であり、MQTT 層における PUBLISH の送達確認を行わない。

二つ目は QoS レベル 2 であり、MQTT 層における PUBLISH の送達確認を行う。

QoS レベル 2 は、TCP コネクションが切断されても、メッセージを再送する仕組みを備えている。

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

## (1)

### 解答例

T	C	P	の	送	信	処	理	中	に	,	デ	バ	イ	ス	の	電	源	断	な	ど	で	T	C	P
コ	ネ	ク	シ	ヨ	ン	が	開	放	さ	れ	た	場	合											

(39字)

問題文は、「図 3 中の QoS レベルが 0 の場合のメッセージ送信について、TCP の再送機能だけではメッセージの消失が防げないのはどのような場合か。……具体的に答えよ」と記述されている。

設問 2 の解説「● MQTT の仕組み」で述べたとおり、QoS レベル 0 のメッセージ送信は「MQTT 層における PUBLISH の送達確認は行わない」ので、PUBLISH は送信者に保存されない（[MQTT を使ったメッセージ交換方式] 第 6 段落）。

送信者が PUBLISH を送信する際、そのメッセージのサイズが大きければ複数のパケットに分割して送信する。その際、PUBLISH を送信している途中で何らかの通信障害が発生し、パケットが消失したとしよう。

もし、その障害が経路上で発生したものであり、機器間の TCP コネクションが張られたままならば、TCP の再送機能により、消失したパケットを再送できる。それゆえ、PUBLISH を送信し終わるまで TCP コネクションが張られていれば、メッセージは受信者に無事に届くことが分かる。

一方、もしその障害が機器上で発生したものであり、機器間の TCP コネクションが切断されたならば、TCP の再送機能が働かない。それゆえ、消失したパケット及びこれ以降のパケットに相当するメッセージが消失し、受信者に届かないことが分かる。

本事例のデバイスは、[MQTT を使ったメッセージ交換方式] の第 9 段落に記され

ているとおり、電源断の可能性が懸念されている（詳しくは、空欄キの解説で取り上げる）。

したがって、デバイスの電源断などで TCP コネクションが解放されるケースを想定できるため、QoS レベルが 0 の場合、TCP の再送機能だけではメッセージの消失を防ぐことができないことが分かる。

本小問は「具体的に答えよ」と指示されているので、事例に特化した内容を解答に含めるとよい。本事例では「電源断」が懸念されているので、これを指摘することで具体性を出すことができる。

よって、正解は解答例に示したとおりとなる。

## (2)

### 解答例

メッセージの重複を防止する。(14字)

問題文は、「本文中の下線③について、PUBRELを受信するまで、メッセージの処理を保留する目的を……述べよ」と記述されている。

下線③は、[MQTTを使ったメッセージ交換方式]の第6段落、2番目の箇条書きの中にある。ここでは、QoS レベルが2の場合の、MQTT 層の送達確認を説明している。

下線③を含む2番目の箇条書きは、次のように記述されている。

- ・ QoS レベルが2の場合、MQTT 層においても PUBLISH の送達確認が行われる。MQTT 層の送達確認の説明を次に示す。
- TCP コネクションが切断された場合のために、PUBLISH 及び PUBREL は送信者によって保存され、送信者から受信者への再送に利用される。
- ③PUBLISH を受信した受信者は、メッセージの処理を始める前に送信者に PUBREC を送信し、その応答である PUBREL を受信してからメッセージの処理を開始する。
- PUBREL を送信した送信者は、その応答である PUBCOMP を受信してから、メッセージ送信を完了する。

本小問では、PUBREL コマンドについて出題されている。PUBREL コマンドは、送信者が受信者に対してメッセージを配信する際、2 往復目のやり取りにおいて送信者

が受信者に向けて送信するコマンドである。

メッセージの配信を 2 往復でやり取りする仕組みは、QoS レベル 2 の特徴である。

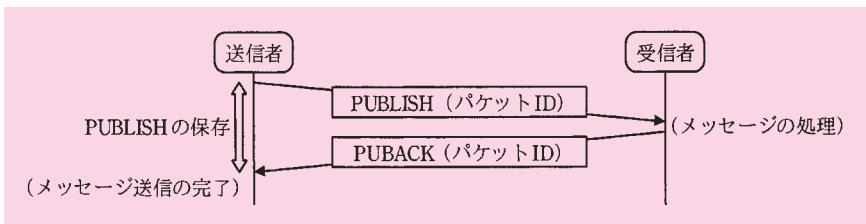
本小問を解く糸口を見つけるため、メッセージの配信を 1 往復でやり取りする QoS レベル 1 と比較してみよう。

QoS レベル 1 とレベル 2 の相違点は、PUBLISH で配信されるメッセージの重複を許容するか（レベル 1）、否か（レベル 2）である。両者を比較することで、メッセージの重複を許容しないために、2 往復のやり取りが必要であることが理解できる。

これを足掛かりにして、本小問の解を導くことができる。

### ● QoS レベル 1 のやり取り

QoS レベル 1 は、1 往復のやり取り（PUBLISH/PUBACK）の間に、メッセージ処理を行う仕組みになっている。



図：QoS レベル 1 のメッセージ送信の通信シーケンス

QoS レベル 1 の送信者は、受信者から PUBACK コマンド（送達確認）を受信しない限り、PUBLISH（すなわちメッセージ）を保存し続ける。そして、同一メッセージの PUBLISH コマンドを再送する。

この送達確認の仕組みを採用しているおかげで、受信者デバイスの電源断などにより TCP コネクションが切断されたときでも、メッセージ消失を防ぐことができる。

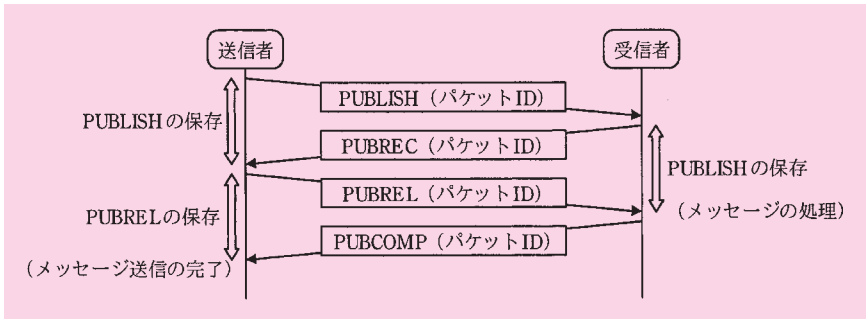
なぜなら、送達確認を受信していないため、TCP コネクションが再開されたとき、送信者はメッセージを保存している。ゆえに、PUBLISH コマンドでこれを再送できるからだ。

QoS レベル 1 の受信者は、PUBLISH コマンドを受信するたびメッセージ処理を行うため、メッセージ処理の重複が発生し得る。

### ● QoS レベル 2 のやり取り

一方、QoS レベル 2 は、図 3「QoS レベルとメッセージ送信の通信シーケンス」に

示されているとおり, 2 往復のやり取りを行う。その 2 往復目 (PUBREL/PUBCOMP) の間に, メッセージ処理を行う仕組みになっている。



図：QoS レベル 2 のメッセージ送信の通信シーケンス (図 3 の一部を抜粋)

QoS レベル 2 の送信者は, PUBREC コマンド (送達確認) を受信しない限り, PUBLISH (すなわちメッセージ) を保存し続ける。そして, 同一メッセージの PUBLISH コマンドを再送する。

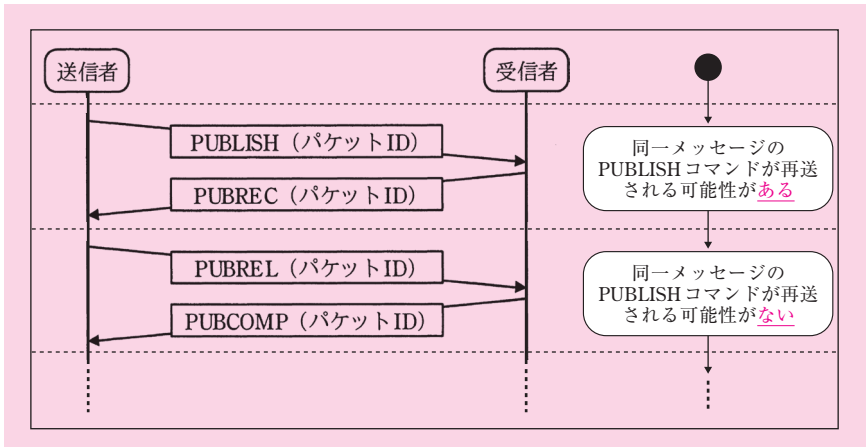
QoS レベル 2 の受信者は, 一度目の PUBLISH コマンドを受信したとき, そのメッセージを保存した上で, PUBREC コマンドを返信する。二度目以降の PUBLISH コマンドを受信したとき, もしも PUBLISH を保存していなかったら, これを保存する。一方, もしも既に保存していたら, 保存時に送ったはずの PUBREC コマンドが届かなかったと判断し, 再び PUBREC コマンドを返信する。

2 往復目に入り, 送信者から PUBREL コマンドを受信すると, 「PUBLISH コマンドで配信されたメッセージに関し, 自分が返信した PUBREC コマンド (送達確認) を送信者が確認できた」ということが分かる。受信者は, 「もう二度と, 当該メッセージの PUBLISH コマンドが再送されることがない」と判断できるわけだ。

ここまでのやり取りを, 状態遷移図を用いて整理してみよう。

QoS レベル 2 の 1 往復目は, 「同一メッセージの PUBLISH コマンドが再送される可能性がある」という状態にある。一方, 2 往復目は, 「同一メッセージの PUBLISH コマンドが再送される可能性がない」という状態にある。

2 往復目の最初に送られる PUBREL コマンドは, この状態遷移を布告する役割を担っていることが分かる。



図：QoS レベル 2 の状態遷移図

さて、QoS レベル 2 の受信者は、2 往復目の PUBREL コマンドを受信すると、メッセージ処理をただ一度だけ行う。

この結果、メッセージ処理の重複が発生しないのである。

なお、QoS レベル 2 の送信者は、PUBCOMP コマンドを受信しない限り、同一メッセージ ID の PUBREL コマンドを再送する。

QoS レベル 2 の受信者は、最初に PUBREL コマンドを受信したときだけメッセージ処理を行うので、二度目以降の PUBREL コマンドを受信したときには、ただ PUBCOMP コマンドを返信するだけである。

### ●解の導出

本小問は、QoS レベル 2 の通信シーケンスに関し、「PUBREL を受信するまで、メッセージの処理を保留する目的」を問うている。

前述のとおり、QoS レベル 2 は、PUBREL を受信するまでメッセージの処理を保留することによって、メッセージ処理の重複が発生しない仕組みになっている。

その処理とは、具体的に何であろうか。図 2 を例に取り上げてみよう。

まず、クライアント（配信元）からサーバに対し、メッセージが配信される。このときサーバが実行するメッセージ処理は、クライアント（配信先）へのメッセージ送信である。

こうして、クライアント（配信先）にメッセージが配信される。このときクライアント（配信先）が実行するメッセージ処理は、この配信を契機に起動される、X シス

テムの処理である。例えば、メッセージを保存したり、メッセージに基づいて設定を変更したりすることが考えられる。

QoS レベルを 2 に設定することによって、こうした業務上の処理に関し、メッセージの重複を防止できるわけだ。

したがって、「PUBREL を受信するまで、メッセージの処理を保留する目的」は、MQTT 通信を利用したシステムにおいて、メッセージの重複を防止するためであると言える。

よって、正解は解答例に示したとおりとなる。

### (3)

#### 解答例

オ：SUBSCRIBE

カ：config/Di

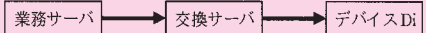
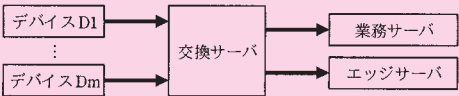
キ：デバイス Di

ク：交換サーバ

ケ：業務サーバ

本小問は、本文中の空欄オ～ケに入れる適切な字句を問うている。

空欄オ～ケは、[MQTT を使ったメッセージ交換方式] の第 9 段落の中にある。この段落は図 4 を説明しているので、図 4 と併せて掲載しよう。

項番	メッセージ交換の概要	QoS レベル	トピック名	メッセージ
1	<p>業務サーバから、特定のデバイス Di に対して、設定情報を送信する。</p> 	2	config/Di	デバイス Di の設定情報
2	<p>全てのデバイス Di (<math>i=1, 2, \dots, m</math>) から、業務サーバ及び同じ工場のエッジサーバに対して、稼働情報を定期的に送信する。</p> 	0	status/Di	デバイス Di の稼働情報

注記 Di は、デバイスの識別子を表す。

図：X システムのメッセージ交換（図 4 の抜粋）

図 4 の説明を次に示す。

- ・ 項番 1 では、デバイス Di は、あらかじめ  オ  を交換サーバに送信し、トピック名が  カ  の PUBLISH が送信されるようにする。
- ・ 項番 1 では、QoS レベルとして 2 が使用されている。交換サーバからデバイス Di への PUBLISH 送信中に  キ  が電源断などで非稼働になった場合、その PUBLISH は、 ク  の中に保存され、稼働再開後に再送される。
- ・ 項番 2 では、QoS レベルとして 0 が使用されている。これは、 ケ  及びエッジサーバは安定した稼働が見込めるからである。

図 4 の項番 1 は、業務サーバから特定のデバイス Di に対して、設定情報を送信するときのメッセージのフローを示している。

図 4 の項番 2 は、全てのデバイス Di ( $i = 1, 2, \dots, m$ ) から、業務サーバ及び同じ工場のエッジサーバに対して、稼働情報を定期的に送信するときのメッセージフローを示している。

〔X システムの構想〕の第 3 段落に記されているとおり、どちらのメッセージフローも、「交換サーバを介して、デバイス、エッジサーバ及び業務サーバの間でメッセージを交換」している。なぜなら、デバイス、エッジサーバ及び業務サーバは「MQTT クライアント」であり、交換サーバは「MQTT サーバ」だからだ。

そこで、クライアント、サーバという役割に着目し、図 4 のメッセージフローに登場する機器を、図 2 の通信シーケンスに登場するクライアントとサーバに当てはめて



みよう。すると、次に示す表のとおりとなる。

表：図 4 のメッセージフローに登場するクライアントとサーバ

図 4		図 2	
項番	クライアント（配信元）	サーバ	クライアント（配信先）
1	業務サーバ	交換サーバ	デバイス Di
2	デバイス D1 ～ Dm	交換サーバ	業務サーバ エッジサーバ

ここまで整理できれば、空欄に入る字句を導くことができる。

オ, カ

空欄オ, カを含む文は、項番 1 に関する MQTT 通信のやり取りについて述べている。

第 4 段落の 3 番目～ 5 番目の箇条書きには、このやり取りに関する説明が記述されている。

この記述を、空欄オ～カを含む文と照らし合わせれば、解を導くことができる。

以下、第 4 段落を引用するが、解を導きやすくするため、クライアント（配信元）を「業務サーバ」に、サーバを「交換サーバ」に、クライアント（配信先）を「デバイス Di」に、それぞれ読み替えておこう（字句を替えた箇所を下線で示す）。

さらに、項番 1 のトピック名である「config/Di」を明記しておこう。

表：第 4 段落と空欄オ～カを含む文章の比較

第 4 段落	<ul style="list-style-type: none"><li>デバイス Di は、<u>交換サーバ</u>に SUBSCRIBE を送信し、購読対象のメッセージを、トピック名「config/Di」を使って通知する。</li><li><u>業務サーバ</u>は、PUBLISH を使って<u>交換サーバ</u>にメッセージを送信する。</li><li>メッセージを受信した<u>交換サーバ</u>は、PUBLISH に含まれるトピック名「config/Di」について購読要求を受け付けている<u>デバイス Di</u>に、そのメッセージを送信する。</li></ul>
空欄オ～カを含む文章	デバイス Di は、あらかじめ <u>オ</u> を交換サーバに送信し、トピック名が <u>カ</u> の PUBLISH が送信されるようにする。

表の 1 番目と 2 番目の箇条書きを見ると、デバイス Di は、PUBLISH の送信に先立ち、SUBSCRIBE を送信する。よって、空欄オは「SUBSCRIBE」となる。

表の 1 番目と 3 番目の箇条書きを見ると、SUBSCRIBE でトピック名を通知することで、当該トピックのメッセージが PUBLISH で配信される。よって、空欄カは「config/

Di」となる。

キ，ク

空欄キ〜クを含む文は、項番 1 に関するやり取りのうち、PUBLISH の送信について述べている。空欄オ〜カの解説から明らかとなり、送信者は交換サーバであり、受信者はデバイス Di だ。

項番 1 は QoS レベル 2 を指定しているため、MQTT 層において、PUBLISH の送達確認が行われる。

第 6 段落の 2 番目の箇条書きには、QoS レベル 2 の PUBLISH のやり取りについて記述されている。

この記述を、空欄キ〜クを含む文と照らし合わせれば、解を導くことができる。

以下、この記述を引用するが、解を導きやすくするため、PUBLISH の送信者を「交換サーバ」に、その受信者を「デバイス Di」に、それぞれ読み替えておこう（字句を替えた箇所を下線で示す）。

表：第 6 段落と空欄キ〜クを含む文章の比較

第 6 段落	TCP コネクションが切断された場合のために、PUBLISH 及び PUBREL は交換サーバによって保存され、 <u>交換サーバ</u> から <u>デバイス Di</u> への再送に利用される。
空欄キ〜クを含む文章	交換サーバからデバイス Di への PUBLISH 送信中に <span style="border: 1px solid black; padding: 2px;">キ</span> が電源断などで非稼働になった場合、その PUBLISH は、 <span style="border: 1px solid black; padding: 2px;">ク</span> の中に保存され、稼働再開後に再送される。

### ●解の導出：空欄ク

まず、空欄クを導こう。

電源断は TCP コネクションの切断を引き起こすので、「電源断などで非稼働になった場合」という記述を、「TCP コネクションが切断された場合」と読み替えることができる。

PUBLISH 送信中に TCP コネクションが切断された場合、PUBLISH は交換サーバによって保存される。

よって、空欄クは「**交換サーバ**」となる。

### ●解の導出：空欄キ

次いで、空欄キを導こう。

素直に考えると、「電源断などで非稼働になる」というリスクを抱えているのは、「デ

バイス」だと言える。工場の判断によって、使用していないデバイスへの電源供給を止めることがあるし、物理的な故障によって非稼働になることがあるからだ。様々な要因でデバイスが稼働しているとは限らないから、項番 2 の稼働情報を取得しているのである。

その点を考慮するなら、空欄キの解は「デバイス Di」となる。

### ●参考：空欄キの別解として「交換サーバ」は考えられるか

「交換サーバ」も電源断になる可能性はあるが、これは空欄キの別解として考えられるだろうか。結論から言うと、そのようには言えない。

空欄キを「交換サーバ」とするなら、空欄クは「交換サーバの不揮発性記憶媒体」といった具合に、交換サーバの電源障害が発生しても再送可能とする対策に言及した内容となるべきだ。

ただ、このようにすると、空欄クが本小問の求める「字句」ではなくなる。問題全体の辻褄が合わなくなってしまう。それゆえ、別解になるとは考えられない。

参考までに、MQTT は、クライアント、サーバのどちらの電源断にも対応できる仕様になっている。ここに書いたように、不揮発性記憶媒体に、PUBLISH、PUBREL を保存すればよいからだ。

ケ

空欄ケを含む文は、「項番 2 では、QoS レベルとして 0 が使用されている。これは、ケ及びエッジサーバは安定した稼働が見込めるからである」と記述されている。

図 4 の項番 2 を見ると、クライアント（配信先）に該当するのは、エッジサーバと業務サーバである。ここで注目できる点は、エッジサーバと業務サーバのどちらも、同じ QoS レベルを使用していることだ。つまり、両者は、このメッセージ交換において同等の扱いを受けており、エッジサーバに当てはまることは業務サーバにも当てはまること分かる（その逆も然り）。

配信先の一つであるエッジサーバについては、「安定した稼働が見込める」と書いてある。空欄ケを含む文は、それが QoS レベル 0 を使用した理由であると述べている。

したがって、もう一つの配信先である業務サーバも、エッジサーバと同程度の「安定した稼働が見込める」ことが分かる。

よって、正解は「業務サーバ」となる。

## (4)

## 解答例

コ：業務サーバ，交換サーバ

コ

本小問は、本文中の空欄コに入れる適切な機器名を全て答えるよう求めている。

空欄コは、[MQTT を使ったメッセージ交換方式] の最後の段落（第 14 段落）の中にある。

文脈を見ると、W さんは、「1 台の業務サーバが 6,000 台のデバイスの設定を変更する場合の送信時間（T）を概算」している（第 10 段落）。

このとき、T の概算に用いた通信シーケンスが図 5 に示されている。

デバイスの設定変更は、図 4 の項番 1「トピック名：config/Di」のメッセージ交換を用いる。その QoS レベルは 2 である。この QoS レベルは、図 5 の注記にも示されている。

図 5 のすぐ下にある第 12 段落は、

図 5 中の  $t_1$  及び  $t_2$  は、それぞれの装置間の RTT（Round Trip Time）の 2 倍に等しい

という仮定を置くと述べている。このように仮定できる理由は、QoS レベル 2 のメッセージ交換は、2 往復のやり取りで行われるからだ。

このすぐ後に、注目に値する記述が登場する。装置間の RTT に関し、さらに次のような仮定を置いているのだ。

LAN の RTT を 20 ミリ秒，WAN の RTT を 200 ミリ秒とする

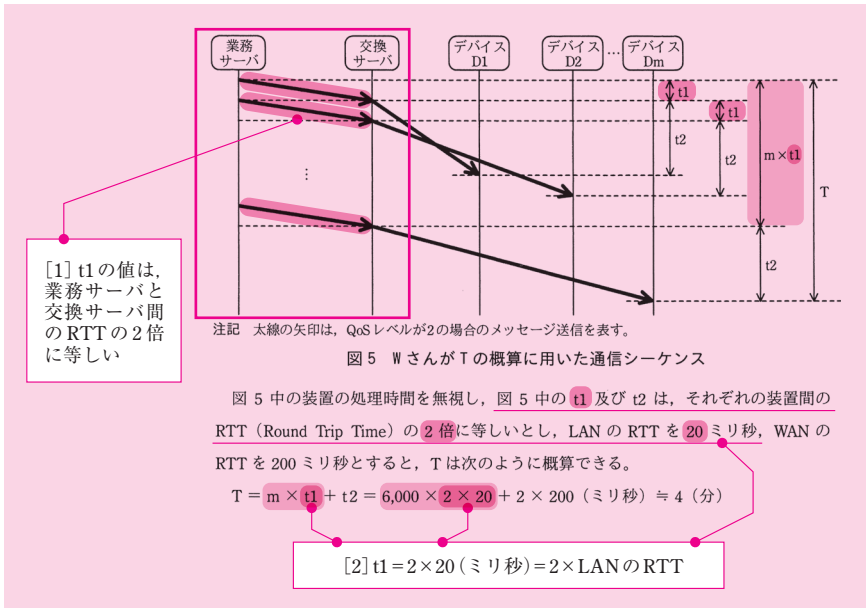
続く第 13 段落には、いよいよ T を求める式が登場する。

$$T = m \times t_1 + t_2 = 6,000 \times 2 \times 20 + 2 \times 200 \text{ (ミリ秒)} \div 4 \text{ (分)}$$

この式と図 5 を照らし合わせることによって、次の二つのことが分かる。

[1]  $t_1$  の値は、業務サーバと交換サーバ間の RTT の 2 倍に等しい。

[2]  $t_1$  の値は、LAN の RTT の 2 倍に等しい。



図： $t_1$  の値、業務サーバと交換サーバ間の RTT の値、LAN の RTT の値

この二つから、「業務サーバと交換サーバ間の RTT は、LAN の RTT に等しい」ことが分かる。そして、このことから、T を求めるに当たって、ある仮定を置いていることに気が付く。それは、

業務サーバと交換サーバは同一の LAN に収容されている

という仮定だ。

実際、図 1 を見てみると、業務サーバと交換サーバは X 社内の LAN に設置されている。この仮定は、図 1 のネットワーク構成を念頭に置いて設けられたものだと言える。

実は、この仮定が、本小問を解くための重要な手掛かりとなる。

空欄コを含む文は、「ただし、図 1 に示すように、コは同一拠点に設置されている必要がある」と記述されている。これは、仮定を付け加えることを

意図した記述である。

「同一拠点」とあることから、同一の LAN に収容されているサーバに関する仮定であることが分かる。

したがって、これまで考察した内容に基づき、空欄コに入る字句は、「業務サーバ、交換サーバ」となることが分かる。

よって、これが正解となる。

### ■設問 3

本設問は、[API にアクセスする顧客サーバの管理] について問うている。

ここでは、冒頭で解説した「・機能② 運用保守情報提供機能」を取り上げている。

#### (1)

##### 解答例

サ：認可

シ：WebAP

ス：リフレッシュトークン

セ：認可応答

ソ：認可

本小問は、本文中の空欄サ～ソに入れる適切な字句を問うている。

空欄サ～ソは、[API にアクセスする顧客サーバの管理] の第 4 段落～第 7 段落にかけて登場する。これらの段落では、本文の図 6 に基づき、X システムの API アクセスの通信シーケンスを説明している。

サ

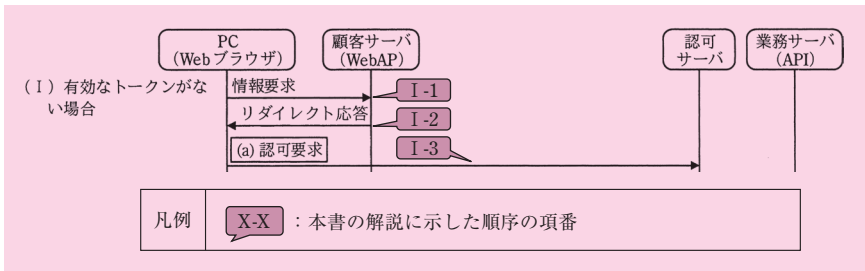
空欄サを含む文は、第 4 段落にある。そこには「図 6 中の (I) に示すように、有効なトークンがない場合、Web ブラウザから WebAP への情報要求は、ササーバにリダイレクトされる」と記述されている。

図 6 中の (I) を見ると、次に示す順序で、Web ブラウザ、顧客サーバ、認可サーバの間でやり取りしている。

[ I-1 ] Web ブラウザは「情報要求」を WebAP に送信する。

[ I-2] WebAP は、リダイレクトを応答する。

[ I-3] Web ブラウザは「認可要求」を認可サーバに送信する。



図：図 6 中の (I) のやり取り (Web ブラウザの情報要求からリダイレクトまで)

この通信シーケンスは、有効なトークンがない場合のやり取りを示している。

[ I-2] で、WebAP はリダイレクトを応答している。なぜなら、このとき WebAP は有効なトークンをもっていないからだ。

[ I-3] で、ブラウザは、リダイレクトで指定された URI にアクセスする。[ I-3] のアクセス先は認可サーバなので、ここにリダイレクトするように指定されたことが分かる。

認可要求を表す HTTP リクエストパケットが、図 6 の下部に抜粋されている。

その図を見ると、リクエスト URI には、パラメタ「redirect\_uri」が付与されている。後ほど空欄シのところで解説するが、これは認可応答の宛先を認可サーバに伝える役割をもっている。

以上を整理すると、有効なトークンがない場合、Web ブラウザから WebAP への情報要求は、認可サーバにリダイレクトされることが分かる。

よって、正解は、「認可」となる。

シ

空欄シを含む文は、第 4 段落にある。そこには「認可応答では、認可要求で通知された URI を用いたリダイレクトによって、シに認可コードが通知される」と記述されている。

認可応答を表す HTTP レスポンスパケットが、図 6 の下部に抜粋されている。

その図を見ると、ステータスが「302」となっているので、リダイレクト応答であることが分かる。

リダイレクト応答では、Location ヘッダフィールドを用い、リダイレクト先を指定

する仕様になっている。そこで、同ヘッダフィールドを見てみよう。

Location: 【WebAP の URI】?code= 【認可コード】

まず、リダイレクト先の URI (「?」より前の部分) に着目しよう。

その値は、【WebAP の URI】である。これは、認可要求のパラメタ「redirect\_uri」に埋め込まれた、【WebAP の URI】と同じものだ。

つまり、次に示す仕組みになっていることが分かる。

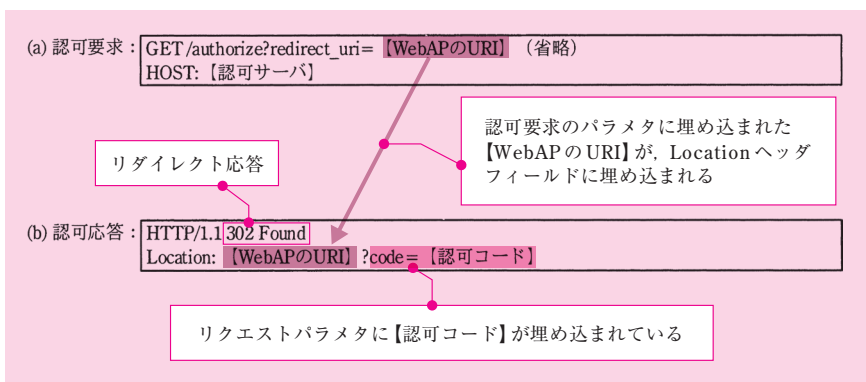
- 認可サーバは、WebAP から認可要求を受信すると、パラメタ「redirect\_uri」の値を読み取る。そこには、認可要求を送信した WebAP 自身の URI が埋め込まれている。
- 認可応答を返信するとき、リダイレクト先として redirect\_uri を指定する。

次いで、URI に付与されたパラメタ「code」に着目しよう。

その値は、【認可コード】である。これは、認可サーバが発行したものだ。

HTTP の仕様上、リダイレクト先の URI にパラメタが付与されていると、それはそのままリダイレクト先に通知される仕組みになっている。

この仕組みを用い、認可サーバは、認可コードをリダイレクト先である WebAP に通知する。

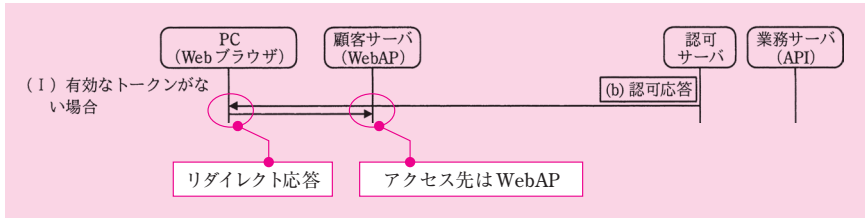


図：図 6 中の認可要求パケットと認可応答パケット

Web ブラウザは、この認可応答を受け取ると、WebAP にリダイレクトする。



図 6 の通信シーケンスを見ると、Web ブラウザが認可応答を受信すると、顧客サーバ (WebAP) にアクセスしている。このアクセスは、リダイレクトによって引き起こされたものである。



図：図 6 中の (I) のやり取り (認可応答から WebAP へのアクセスまで)

以上を整理すると、認可応答の正体は、認可要求で通知された WebAP の URI をリダイレクト先とする、リダイレクト応答である。

ブラウザがこれを受信すると WebAP にリダイレクトするので、リダイレクト URI の code パラメタに設定された認可コードが、WebAP に通知される。

よって、正解は、「WebAP」となる。

ス

空欄スを含む文は、第 5 段落にある。そこには次のように記述されている。

図 6 中の (I)～(Ⅲ) に示すように、業務サーバへの情報要求には、アクセストークンが用いられる。アクセストークンには、アクセス可能な API と有効期間に関する情報が含まれており、業務サーバはそれらの情報からアクセスの可否を決める。アクセストークンの有効期間を過ぎた場合でも、スの有効期間内であれば、利用者の確認を行わずに、新しいアクセストークンが発行される。

ここでは、アクセストークンとリフレッシュトークンという 2 種類のトークンが用いられている。

空欄スの前後の文は、トークンの有効期間について述べている。2 種類のトークンの有効期間について、続く第 6 段落には、「アクセストークンの有効期間を 10 分間、リフレッシュトークンの有効期間を 60 分間」と記述されている。

リフレッシュトークンの有効期間が長いので、アクセストークンが有効期間を過ぎても、リフレッシュトークンは有効期間に収まっている、という場合がある。

図 6 の（Ⅲ）の通信シーケンスは、まさにこの場合のやり取りを示している。

ここを見ると、次に示す順序で、Web ブラウザ、顧客サーバ、認可サーバがやり取りしている。

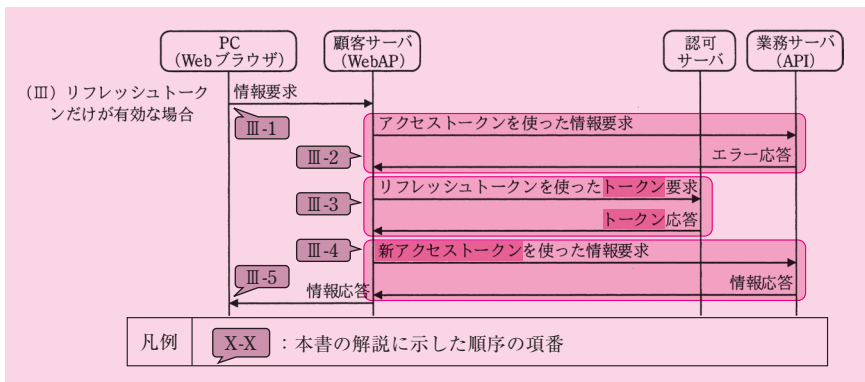
〔Ⅲ-1〕 Web ブラウザは「情報要求」を WebAP に送信する。

〔Ⅲ-2〕 WebAP は、アクセストークンを使った情報要求を業務サーバに送信し、業務サーバはエラー応答を返信する。

〔Ⅲ-3〕 WebAP は、リフレッシュトークンを使ったトークン要求を認可サーバに送信し、認可サーバはトークン応答を返信する。

〔Ⅲ-4〕 WebAP は、新アクセストークンを使った情報要求を業務サーバに送信し、業務サーバは情報応答を返信する。

〔Ⅲ-5〕 WebAP は、情報応答を Web ブラウザに返信する。



図：図 6 中の（Ⅲ）のやり取り

この通信シーケンスは、有効なトークンがない場合のやり取りを示している。

〔Ⅲ-2〕で、WebAP は、アクセストークンを使った情報要求を業務サーバに送信している。このアクセストークンは有効期間を過ぎているため、エラー応答が返信される。

〔Ⅲ-3〕で、WebAP は、リフレッシュトークンを使ったトークン要求を認可サーバに送信している。このとき、認可サーバは「トークン」を応答している。このトークンの正体はこの後すぐ解説しよう。

〔Ⅲ-4〕で、WebAP は、新アクセストークンを使った情報要求を業務サーバに送信している。新アクセストークンは、その名のとおりに新たに発行されたものであるから、

有効期間に収まっている。そのため、情報応答が返信される。

この新アクセストークンは、どの段階で入手したものでしょうか。

〔Ⅲ-2〕の時点では保有しておらず、〔Ⅲ-4〕の時点で保有しているわけだから、その間である〔Ⅲ-3〕のトークン要求で入手したものであると考えられる。つまり、〔Ⅲ-3〕で応答された「トークン」の正体は、新アクセストークンだ。

〔Ⅲ-3〕は、「リフレッシュトークンを使ったトークン要求」であり、要求どおりの応答が返信されている。このことから、リフレッシュトークンは有効期間に収まっていることが分かる。

これら一連のやり取りを利用者の観点から見てみよう。

利用者は Web ブラウザを用いて WebAP にアクセスする。

まず、〔Ⅲ-1〕で「情報要求」を WebAP に送信する。その後、〔Ⅲ-5〕で「情報応答」が返信される。その間、アクセストークンは新しいものに自動的に入れ替わっている。

つまり、アクセストークンの有効期間が過ぎようとも、利用者の手を一切煩わせることがないわけだ。この点が、空欄を含む文の中で「利用者の確認を行わずに」と述べられている。

以上を整理すると、アクセストークンの有効期間が過ぎた場合、リフレッシュトークンの有効期間内であれば、利用者の確認を行わずに、新しいアクセストークンが発行されることが分かる。

よって、正解は、「リフレッシュトークン」となる。

本小問の解は導いたが、良い機会なので、アクセストークン、リフレッシュトークンについて解説しておこう。

### ●参考：アクセストークン

近年、Web 上で API サービス（Web API サービス）を提供するシステムが増えている。

Web API サービスのやり取りは、通常、ステートレス通信である。つまり、各々の API のアクセスは、それぞれ別個のものとして扱われる。

というのは、ちょうどプログラミングの世界で汎用ライブラリが提供する関数（API）のような、副作用のない API と同じような使い方を目指しているからである。ゆえに、「Web API」と呼ばれているのだ。

一般的に言って、Web API サービスを提供するシステムでは、利用者ごとにアクセス可能な API を定めたいことがある。そのためには、正当な利用者からのアクセスであるか否かを識別する必要がある。

この目的のため、多くの Web API サービスでは、トークンを発行する。発行したトークンは、API にアクセスするたびにサーバに送られ、サーバ側で利用者を識別するために用いられる。

本事例では、業務サーバが、WebAPI サービスを提供している。利用者は WebAP を使って業務サーバにアクセスする。業務サーバに直接アクセスするクライアントアプリケーションは利用者の WebAP なので、認可サーバがアクセストークンを発行する先は、WebAP となる。

図 6 中 (I) に示されているように、WebAP は、業務サーバへの情報要求にアクセストークンを提示している。このとき、業務サーバは、情報応答に先立って、WebAP が正当なアクセス権限をもっているのかを検証する必要がある。そのため、(図 6 (I) に明記されていないが) 認可サーバはこのアクセストークンを認可サーバに送信し、有効期間、有効範囲、利用者のユーザ名、クライアントアプリケーションのクライアント ID など、トークンに関わる情報を入手している。これにより、業務サーバは、このアクセストークンが本当に認可サーバから発行されたのか、有効期間内であるのか、情報要求されたリソースへのアクセス権限を有しているのかを検証できる。その後、図 6 (I) にあるとおり、業務サーバは情報応答を WebAP に返信する。

さて、先ほど「アクセストークンは、API にアクセスするたびにサーバに送られる」と述べた。そのため、万が一、アクセストークンが漏えいすると、API にアクセスできてしまう。

この不正利用への対策として、通常、アクセストークンの有効期間をなるべく短く設定するという手法が採用されている。仮に漏えいしても、アクセスが可能なのは有効期間内に収まっているときだけだ。

本事例では、アクセストークンの有効期間を 10 分に設定している。

### ●参考：リフレッシュトークン

本事例では、アクセストークンだけでなく、リフレッシュトークンも用いている。

リフレッシュトークンは、アクセストークンと同様、利用者ごとに発行される。

これは、アクセストークンの有効期間が過ぎたとき、新しいアクセストークンを自動的に発行するために用いられる。これにより、本小問で考察したとおり、利用者の確認を行わずにアクセストークンの再発行が可能となる。

リフレッシュトークンは、新アクセストークンを要求するときだけ、サーバに送られる。したがって、アクセストークンに比べると、漏えいのリスクは少ないと言える。

参考までに、採点講評は、ここで出題された二つのトークンを用いた API アクセス認可の仕組みに言及しており、「この仕組みは“The OAuth 2.0 Authorization Framework

(RFC6749)”に記述があり、広く利用されている」と述べている。興味のある読者は自分の目で仕様を調べてみるとよいだろう。

## セ

空欄セを含む文は、第7段落にある。そこには次のように記述されている。

図6の通信シーケンスでは、図6中の“(a) 認可要求”の `redirect_uri` パラメータが書き換えられ、図6中の セ に含まれる認可コードが意図しない宛先に送信される可能性がある。

空欄シで解説したとおり、認可応答の正体はリダイレクト応答である。

認可応答の `Location` ヘッダフィールドに指定された値は、リダイレクト先 URI と `code` パラメータからなる。

認可サーバは、リダイレクト先 URI として、認可要求の `redirect_uri` パラメータで渡された URI を設定する。これに付与する `code` パラメータとして、自分が発行した認可コードを設定する。

したがって、認可要求の `redirect_uri` パラメータが第三者のサーバの URI に書き換えられると、認可応答がこのサーバに届いてしまう。

よって、正解は、「認可応答」となる。

## ソ

空欄ソを含む文は、第7段落の中、空欄セを含む文の後にある。そこには次のように記述されている。

その対策として“`redirect_uri` パラメータの確認”を行うことにした。これは、図6中の ソ サーバに、HTTP リクエストに含まれる URI とあらかじめ登録されている絶対 URI が一致することを確認させる、という対策である。

文脈上、ここでは、認可要求の `redirect_uri` パラメータの改ざん対策が説明されている。

その対策は、「`redirect_uri` パラメータの確認」である。その具体的な内容は、「HTTP リクエストに含まれる URI とあらかじめ登録されている絶対 URI が一致することを確認させる」というものである。

空欄ソが問うているのは、その確認を行うサーバである。

### ●「HTTP リクエストに含まれる URI」とは何か

本文に「HTTP リクエストに含まれる URI」とあるが、これはいったい何であろうか。

ここで問題視されているのは、認可要求の `redirect_uri` パラメタの改ざんである。

それゆえ、有効な対策は、「`redirect_uri` パラメタの確認」、すなわち、認可要求の `redirect_uri` パラメタが改ざんされていないかを確認することだ。本来は WebAP の URI が設定されているはずなので、それとは異なった値が設定されていなければよい。

したがって、「HTTP リクエストに含まれる URI」とは、「認可要求の `redirect_uri` パラメタに含まれる URI」を指している。

なお、「HTTP リクエスト」と書いてあるが、リダイレクト応答に呼応して送信される認可要求は HTTP リクエストなので、技術的に正しい表現である。

### ●「あらかじめ登録されている絶対 URI」とは何か

本文に「あらかじめ登録されている絶対 URI」とあるが、これはいったい何であろうか。

この文脈から分かることは、認可要求の `redirect_uri` パラメタの正当性を確認するために用いられる、比較対象とする URI ということだ。

`redirect_uri` パラメタの URI と、あらかじめ登録されている絶対 URI が一致することをもって、同パラメタが正当なものであること、すなわち改ざんされていないことを確認することができる。

実を言うと、「あらかじめ登録されている絶対 URI」について、この後の設問 3 (3) で問われている。したがって、詳しくはそこで解説しよう。

本小問を解く際には、「`redirect_uri` パラメタの確認に用いられるものだ」と考えておけばよい。

### ●解の導出：`redirect_uri` パラメタの確認を行うサーバ

Web ブラウザが送信する認可要求は、認可サーバに送信される。

したがって、認可要求の `redirect_uri` パラメタを読み取り、ここに設定された URI の正当性を確認できるのは、認可サーバ以外にない。

その確認に成功したならば、認可サーバは認可コードを発行し、認可応答を返信すればよい。

よって、正解は、「認可」となる。

## (2)

## 解答例

10

問題文は、「本文中の下線④について、提供する API の範囲を変更する場合、変更が有効になるのは、X 社がアクセストークンを変更してから最長で何分後かを答えよ」と記述されている。

下線④は、「API にアクセスする顧客サーバの管理」の第 6 段落の中にある。そこには、「④アクセストークンの有効期間を 10 分間、リフレッシュトークンの有効期間を 60 分間」と記述されている。

アクセストークンには、「アクセス可能な API」に関する情報が格納されている（第 5 段落）。したがって、提供する API の範囲を変更する場合、それに応じてアクセストークンを変更する必要がある。

アクセストークンが有効である場合、図 6 中の（Ⅱ）に基づく通信シーケンスでやり取りされる。このときは、Web ブラウザが情報要求を送信すると、自動的に、業務サーバは情報応答を返信する。つまり、アクセストークンがひとたび発行されたならば、その有効期間中は、当該アクセストークンに格納された情報に基づき、API にアクセスできてしまうわけだ。

その間に提供する API の範囲を変更しても、それが反映されるのは新アクセストークンが発行されるタイミングとなる。

したがって、API の範囲変更が有効になるのは、最長で、アクセストークンの有効期間となる。つまり、10 分だ。

よって、正解は、「10」となる。

## (3)

## 解答例

W	e	b	A	P	の	U	R	I	を	固	定	に	し	,	絶	対	U	R	I	を	事	前	に	通
知	し	て	も	ら	う	。																		

(32 字)

問題文は、「本文中の下線⑤について、顧客への依頼内容を……述べよ」と記述され

ている。

下線⑤は、〔API にアクセスする顧客サーバの管理〕の第 7 段落の中にある。

下線⑤を理解するには、文脈を考慮に入れる必要がある。そこで、空欄セ、ソを埋めた上で、第 7 段落を引用することにしよう。

図 6 の通信シーケンスでは、図 6 中の“(a) 認可要求”の `redirect_uri` パラメタが書き換えられ、図 6 中の認可応答に含まれる認可コードが意図しない宛先に送信される可能性がある。W さんは、その対策として“`redirect_uri` パラメタの確認”を行うことにした。これは、図 6 中の認可サーバに、HTTP リクエストに含まれる URI とあらかじめ登録されている絶対 URI が一致することを確認させる、という対策である。⑤顧客向けの API 利用ガイドラインには、この対策に必要な顧客への依頼内容を明記することにした。

空欄セ、ソで解説したとおり、ここで問題視されているのは、認可要求の `redirect_uri` パラメタの改ざんである。

その対策として、「`redirect_uri` パラメタの確認」を行う旨が述べられている。

`redirect_uri` パラメタの URI が正当なものであれば、WebAP の URI が設定されているはずである。

したがって、これをあらかじめ認可サーバに登録しておき、`redirect_uri` パラメタの URI がこれと一致するかどうかを確認すればよいわけだ。

ただし、WebAP の URI をあらかじめ登録するに当たり、留意すべき点がある。

それは、「WebAP が顧客サーバに実装されている」ことだ（〔X システムの構想〕第 4 段落）。

WebAP の URI は、「顧客サーバのホスト名」と「サーバ内で WebAP に紐付けられた URI のパス」からなる。顧客によってホスト名は異なるので、WebAP の URI の改ざんの確認を行うには、ホスト名を含めた URL、すなわち、絶対 URI を用いる必要がある。

この留意点を踏まえると、`redirect_uri` パラメタの確認を認可サーバで実施するに当たり、顧客に協力を依頼する必要がある。

まず、WebAP の絶対 URI を顧客から通知してもらうよう依頼しなければならない。

さらに、WebAP は顧客サーバに実装されているから、顧客が WebAP の URI パスを勝手に変更しないように依頼しなければならない。さもないと、認可サーバに登録されている絶対 URI との差異が生じ、`redirect_uri` パラメタの確認に失敗してしまうからだ。



本小問は顧客への依頼内容を問うているので、ここに述べた事柄を指定字数に収まるようにまとめればよい。

よって、正解は、「WebAP の URI を固定にし、絶対 URI を事前に通知してもらう」となる。

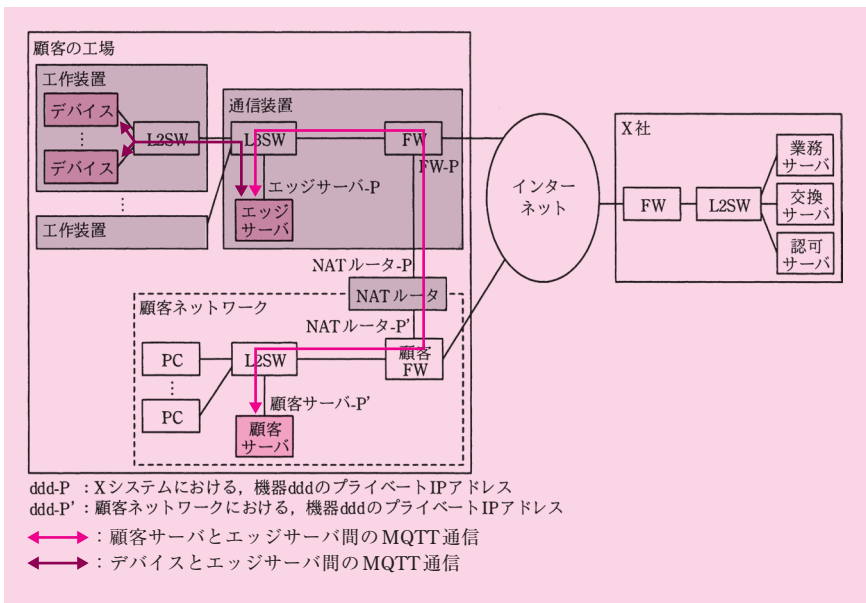
## ■設問 4

本設問は、「エッジサーバを活用する将来構想」について問うている。

ここでは、冒頭で解説した「・機能③ 内部情報交換機能」を取り上げている。

そこで述べたとおり、将来、内部情報（顧客の企業秘密を含むような設定情報及び稼働情報）を、顧客サーバとデバイス間で交換するという構想をもっている。

この将来構想を実現するため、顧客ネットワークと X システムを接続する。この構成が本文の図 8 に示されている。冒頭でも解説したが、ここに再掲しておこう。



図：将来構想におけるネットワーク構成案

(1)

## 解答例

送	信	元	I	P	ア	ド	レ	ス	を	N	A	T	ル	ー	タ	-	P	に	,	宛	先	I	P	ア	
ド	レ	ス	を	エ	ッ	ジ	サ	ー	バ	-	P	に	,	そ	れ	ぞ	れ	変	換	す	る	。			

(48字)

問題文は、「図 8 中の NAT ルータについて、顧客ネットワークから X システムの方向の通信におけるアドレス変換の内容を……具体的に述べよ」と記述されている。

図 8 は、NAT ルータを使って、顧客ネットワークと X システムを接続する構成案を示している。ここで使用する NAT ルータについて、「エッジサーバを活用する将来構想」の第 3 段落には、「NAT ルータは、1:1 静的双方向 NAT として動作させ、図 8 中の NAT ルータ -P と NAT ルータ -P' を利用して、宛先 IP アドレスと送信元 IP アドレスの両方を変換させる」と記述されている。

ここから分かることは、NAT ルータを経由するとき、宛先と送信元がともに変化するということである。

この点を踏まえ、顧客サーバがエッジサーバにパケットを送信するケースを取り上げて、どのように IP アドレスが変換されるのかを具体的に考察してみよう。

顧客サーバがパケットを送信した時点では、送信元 IP アドレスは当然ながら自分自身「顧客サーバ -P」である。このパケットが NAT ルータを通過するとき、宛先／送信元 IP アドレスが変換される。

エッジサーバがパケットを受信した時点では、宛先 IP アドレスは当然ながら自分自身「エッジサーバ -P」であるが、実は NAT ルータによって変換されたものである。

したがって、顧客サーバがパケットを送信した時点の宛先 IP アドレスは、エッジサーバのものとは異なることが分かる。さらに、エッジサーバがパケットを受信した時点の送信元 IP アドレスは、顧客サーバのものとは異なることも分かる。

ここで本文を振り返ってみると、NAT ルータの設定は「1:1 静的双方向」であり、「NAT ルータ -P と NAT ルータ -P' を利用 (する)」とある。

ここから、顧客サーバがパケットを送信した時点の宛先 IP アドレスは、「NAT ルータ P'」であると推論できる。NAT ルータによって、これが「エッジサーバ -P」へと変換されたわけだ。さらに、エッジサーバがパケットを受信した時点の送信元 IP アドレスは、「NAT ルータ P」であると推論できる。NAT ルータによって、これは「顧客サーバ -P'」から変換されたわけだ。

エッジサーバが顧客サーバにパケットを返信するケースについても、これと同様に

考えればよい。

以上より、NAT ルータに設定された変換ルールは、次の表に示す内容であると結論できる。

表：NAT の変換ルール

[顧客ネットワーク→Xシステム]

	送信元	宛先
変換前	顧客サーバ -P'	NAT ルータ -P'
変換後	NAT ルータ -P	エッジサーバ -P

表：NAT の変換ルール

[Xシステム→顧客ネットワーク]

	送信元	宛先
変換前	エッジサーバ -P	NAT ルータ -P
変換後	NAT ルータ -P'	顧客サーバ -P'

このような変換ルールが NAT ルータに設けられているので、顧客サーバとエッジサーバは、お互いの IP アドレスを知らなくても、MQTT 通信を行うことができる。

両サーバは、NAT ルータの IP アドレス（自分と同じネットワークの IP アドレス）を知っておくだけでよいのだ。

具体的に言うと、次のように設定すればよい。

[顧客サーバ]

- MQTT サーバの IP アドレスとして、NAT ルータ -P'（顧客ネットワーク側）を登録しておく。

[エッジサーバ]

- MQTT クライアントの IP アドレスとして、NAT ルータ -P（X システム側）を登録しておく。

ここまで理解できれば、本小問の解を導くことができる。

ここでは、NAT ルータについて、顧客ネットワークから X システムの方向の通信におけるアドレス変換の内容を問うている。

したがって、表「NAT の変換ルール」に示した、「顧客ネットワーク→X システム」方向の内容を解答すればよい。

さて、本小問は「具体的に述べよ」と指示されていた。その理由は指定字数が「60 字」と長いからである。それゆえ、この字数を満たす程度まで具体的に答えるとよい。

そこで、解答に際しては、図中に示されたアドレスを用いることにしよう。こうすることで具体性を出すとともに、字数をかせぐことができる。

よって、正解は、「送信元 IP アドレスを NAT ルータ -P に、宛先 IP アドレスをエッジサーバ -P に、それぞれ変換する」となる。

## (2)

### 解答例

顧	客	サ	-	ー	-	P	,	か	ら	N	A	T	ル	-	タ	-	P	,	の	ポ	ー	ト	8	8
8	3	番	へ	の	通	信		(	32	字	)													

問題文は、「図 8 中の顧客 FW について、X システムとの接続のために、新たに許可が必要になる通信を……答えよ」と記述されている。

将来構想では、顧客サーバとデバイスが、エッジサーバを介してメッセージを交換する。この通信において、顧客 FW を通過するのは、顧客サーバとエッジサーバ間のメッセージ交換である。すなわちこれが、顧客 FW で新たに許可が必要になる通信となる。

本小問は、この通信を許可するための顧客 FW の設定を問うている。

FW のパケットフィルタリングの設定には、トランスポート層プロトコル、宛先ポート番号、宛先 IP アドレス、送信元 IP アドレスなどが必要である。

本小問は、これらを具体的に解き明かすことを求めている。

### ●トランスポート層プロトコル、宛先ポート番号

メッセージ交換には MQTT を使用する。したがって、MQTT が使用するトランスポート層プロトコル、及びポート番号が分かればよい。

この点について、[MQTT を使ったメッセージ交換方式] の第 4 段落、1 番目の箇条書きには、「クライアントは、サーバの TCP ポート 8883 番にアクセスし、TCP コネクションを確立する」と記述されている。

したがって、トランスポート層プロトコルは「TCP」であり、宛先ポート番号は「8883 番」である。

### ●宛先 IP アドレス、送信元 IP アドレス

MQTT は、クライアントからサーバに向けて TCP コネクションを確立する。それ

は、メッセージ交換の配信方向とは関係がない。

つまり、クライアント（配信元）からサーバへの PUBLISH であろうと、サーバからクライアント（配信先）への PUBLISH であろうと、TCP コネクションの方向は常に、クライアントを送信元とし、サーバを宛先とするものなのだ。

将来構想で行われる MQTT 通信のクライアント及びサーバについて、〔エッジサーバを活用する将来構想〕の第 5 段落、1 番目の箇条書きには、「顧客サーバに MQTT クライアント機能を、エッジサーバに MQTT サーバ機能をそれぞれ実装（する）」と記述されている。

したがって、本小問が問うている新たに発生する MQTT 通信は、MQTT クライアントが顧客サーバであり、MQTT サーバがエッジサーバである。

ただし、図 8 のネットワーク構成案では、MQTT 通信は NAT ルータを通過する。その際、MQTT パケットの送信元／宛先 IP アドレスは NAT ルータで変換される。

顧客 FW のフィルタリング設定を導くには、この点を考慮に入れる必要がある。

顧客 FW は、顧客サーバと NAT ルータの間にある。したがって、顧客サーバが MQTT パケットを送信するケースを考察すればよい。

設問 4 (1) で解説したとおり、顧客サーバがこのパケットを送信するとき、宛先 IP アドレスは、「NAT ルータ -P'」となる。送信元 IP アドレスは、言うまでもなく自分自身、すなわち「顧客サーバ -P'」となる。

### ●解の導出

ここまで理解できれば、解を導くことができる。

これまでの解説を振り返ると、顧客 FW で新たに許可が必要になる通信は、顧客サーバとエッジサーバ間の MQTT 通信である。

その宛先ポート番号は「8883 番」、宛先 IP アドレスは「NAT ルータ -P'」、送信元 IP アドレスは「顧客サーバ -P'」である。

したがって、この内容を解答に記せばよい。

よって、正解は解答例に示したとおりとなる。

## (3)

### 解答例

```
config/Di, status/Di
```

問題文は、「本文中の下線⑥について、定義するトピック名を全て答えよ」と記述されている。

下線⑥は、「エッジサーバを活用する将来構想」の第 5 段落、3 番目の箇条書きの中にある。

そこには、「⑥ MQTT ブリッジには、トピック名をあらかじめ定義しておき、そのトピック名のメッセージを交換サーバと送受信させる」と記述されている。

したがって、本小問が問うているのは、「MQTT ブリッジと交換サーバ間で交換されるメッセージのトピック名」である。

第 5 段落は、図 9 を説明したものだ。本小問の解を導くには、図 9 と照らし合わせながら、第 5 段落の内容を理解する必要がある。

### ● MQTT ブリッジ

MQTT ブリッジについて、第 5 段落、2 番目の箇条書きには、次のように記述されている。

・エッジサーバの MQTT サーバ機能は、通常の MQTT サーバ機能に加えて、メッセージをほかの MQTT サーバと送受信する機能（以下、MQTT ブリッジという）をもつ。X システムのデバイスは複数の機器と TCP コネクションを確立できないので、この MQTT ブリッジを利用する。

したがって、下線⑥の「MQTT ブリッジ」は、エッジサーバを指している。

図 9 と照らし合わせると、エッジサーバの「MQTT サーバ機能」が、この MQTT ブリッジである。

### ●図 9 から削除されたメッセージと図 9 に追加されたメッセージ

図 9 を見ると、「将来構想における図 4 中のメッセージの流れ」が、太い矢印で示されている。当初の構想（図 4）と比較すると、次の表のとおり整理できる。

表：当初の構想と将来構想における、メッセージの流れの比較

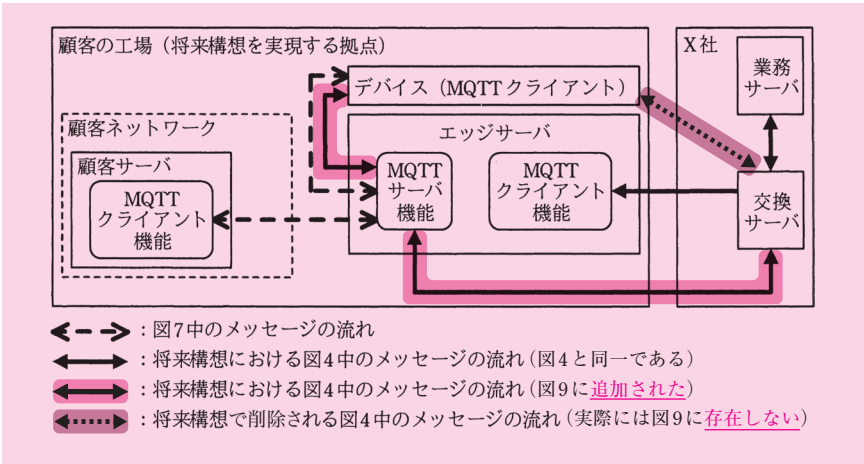
メッセージの流れ		当初の構想(図 4)	将来構想(図 9)
交換サーバ	業務サーバ	あり	あり
交換サーバ	エッジサーバ (MQTT クライアント)	あり	あり
交換サーバ	デバイス	あり	なし

次ページに続く

メッセージの流れ		当初の構想(図 4)	将来構想(図 9)
交換サーバ	エッジサーバ (MQTT ブリッジ)	なし	あり
エッジサーバ (MQTT ブリッジ)	デバイス		

この表から分かるとおり、当初の構想で行われていた「交換サーバとデバイス間」の交換が、図 9 から削除されている。

一方、将来構想では、これに代わって、「交換サーバとエッジサーバ (MQTT ブリッジ) 間」及び「エッジサーバ (MQTT ブリッジ) とデバイス間」が追加されているのだ。



図：図 9 から削除されたメッセージと図 9 に追加されたメッセージ

つまり、交換サーバとデバイス間のメッセージ交換は、エッジサーバ (MQTT ブリッジ) を介して行われるようになったのである。

### ●解の導出

本小問が問うているのは、「MQTT ブリッジと交換サーバ間で交換されるメッセージのトピック名」であった。

図 9 において、交換サーバとデバイス間のメッセージ交換は、エッジサーバ (MQTT ブリッジ) を介して行われている。

したがって、MQTT ブリッジと交換サーバ間で交換されるメッセージの内容は、当初の構想から行われている、交換サーバとデバイス間のメッセージの内容から変化し

ていない。

図 4 には、メッセージのトピック名が記されている。項番 1 は「config/Di」であり、項番 2 は「status/Di」である。

よって、正解はこの二つのトピック名となる。

#### (4)

##### 解答例

- ① 1 : 1 静的双方向 NAT の設定を NAT ルータに追加する。(27字)
- ② 通信を許可するルールを通信装置内の FW に追加する。(25字)

問題文は、「図 7～9 中の顧客サーバを 1 台追加する場合、X システム側で必要となる対応を二つ挙げ（よ）」と記述されている。

つまり、本小問は、図 7～9 中の顧客サーバが 1 台から 2 台に増えた場合を取り上げている。その上で、X システム側での対応について問うている。

X システムで何らかの設定変更を施すわけだが、その際、既存の設定がどのようなものであるかを考慮に入れる必要がある。

本小問では、次に示す二つの設定が重要である。

〔設定 1〕顧客ネットワークと X システムは NAT ルータで接続しており、1:1 静的双方向 NAT を設定している（〔エッジサーバを活用する将来構想〕第 3 段落）。

〔設定 2〕通信装置内の FW は、侵入対策のためパケットフィルタリングを設定している（〔ネットワークセキュリティ対策〕第 1 段落）。

##### ●解の導出：一つ目の対応

まず、〔設定 1〕に着目しよう。

2 台目の顧客サーバが追加されるため、この顧客サーバの IP アドレスに対応した、1:1 静的双方向 NAT の設定を追加する必要がある。

そのために、NAT ルータの二つのインタフェースに、1:1 静的双方向 NAT の IP アドレスをそれぞれ登録しておく。その結果、顧客ネットワーク側、X システム側のそ



それぞれのインタフェースに、IP アドレスが 2 個割り振られる。

かみ砕いて説明すると、1 個目の IP アドレスは既存のものであり、1 台目の顧客サーバの 1:1 静的双方向 NAT で使用されている。2 個目の IP アドレスはこのたび追加されたものであり、2 台目の顧客サーバの 1:1 静的双方向 NAT に使用する。

この 2 個目の IP アドレスを追加するとともに、1:1 静的双方向 NAT の設定を NAT ルータに追加すればよい。

よって、正解は、「1:1 静的双方向 NAT の設定を NAT ルータに追加する」となる。

### ●解の導出：二つ目の対応

次に、[設定 2] に着目しよう。

通信装置内の FW には、パケットフィルタリングが設定されている。

当初の構想に基づく設定内容が、設問 1 (2) で問われていた。それは、「X 社が運用・保守を行う機器から X 社 FW の方向に確立される TCP コネクションを許可する」という内容である。

将来の構想に基づく、パケットフィルタリングのルールを追加する必要がある。

それは、「NAT ルータからエッジサーバの方向に確立される TCP コネクションを許可する」というものである。

1 台目の顧客サーバが通信できるようにするため、このルールが既に設定済みでなければならない。

NAT ルータには 1:1 静的双方向 NAT を設定している。1 台目の顧客サーバからエッジサーバに向けて通信するときに変換される送信元 IP アドレスと、2 台目の顧客サーバのそれとは異なっている。

この点をパケットフィルタリングの観点から考察してみよう。すると、顧客サーバの通信のために設定するルールは、1 台目と 2 台目とで送信元 IP アドレスが異なっていることに気が付くはずだ。

通常、FW のルールは、必要最小限の通信を許可するように設定する。1 台目の顧客サーバ用に設定したルールは、その通信で用いる IP アドレスやポート番号に限定したものであると考えられる。

したがって、2 台目の顧客サーバを追加するとき、2 台目の IP アドレスに応じて、FW のルールを新たに追加する必要があると推察できる。

よって、正解は、「通信を許可するルールを通信装置内の FW に追加する」となる。

## 問 2

## 出題趣旨

クラウドコンピューティングでは、マルチテナントが求められる。マルチテナントは仮想化技術によって実現するが、ネットワークの仮想化は、サーバ仮想化技術の発展に追従できていなかった。しかし、最近、SDN（Software-Defined Networking）の活用によって、ネットワークの仮想化が容易になってきた。

本問では、IaaS のサービス基盤構築を題材として、SDN 技術を用いない従来方式と SDN 方式の、それぞれの方式による構築方法について解説した。その中で、SDN を実現する技術の一つである OpenFlow を取り上げ、OpenFlow による構築例を示した。本問では、受験者が、業務を通して蓄積したネットワーク関連技術を基に、本文中の記述を理解し実務で活用できるかを問う。

## 採点講評

問 2 では、IaaS のサービス基盤構築を題材に、SDN（Software-Defined Networking）技術を用いない従来方式と SDN 方式の、それぞれの方式による構築方法を解説した。SDN 技術としては OpenFlow を取り上げ、マルチテナントのサービス基盤の構築に当たって必要になる技術について出題した。

設問 1 は、ア、ウ、エの正答率は高かったが、イの正答率が低かった。“ステートフル”は、ファイアウォール（以下、FW という）のフィルタリング機能などでも使われている用語なので、是非、知っておいてほしい。

設問 2 では、従来方式による構成について問うた。全体として、正答率は低かった。(3)は、仮想化されたサーバのマイグレーションに対応させるときに不可欠な設定なので、理解しておいてほしい。

設問 4 は、(1)の正答率が低かった。マルチテナント環境では、顧客ごとにネットワークの要件が異なるので、FW の筐体内で、各顧客向けに複数の FW（以下、仮想 FW という）を稼働させる必要がある。仮想 FW は、通常の FW と同様の働きを行うものなので、仮想 FW に対して設定すべきネットワーク情報も、通常の FW とほぼ同じであることを理解しておいてほしい。

設問 5 では、OpenFlow を利用したときの構成とパケットの転送制御について問うた。(1)の正答率が低かった。テストシステムの仮想サーバの配置（図 4）は、生成されるフローテーブル（以下、F テーブルという）の内容を考慮したものだが、この仮想サーバの配置には、物理サーバ 3 に障害が発生すると 3 顧客のシステムが、一時的であるが同時に停止するという問題がある。構成図（図 4）から、この問題点を見つけ出してほしかった。改善策は、顧客ごとの仮想サーバを、それぞれ異なる物理サーバに配置することで、物理サーバの障害の影響を複数の顧客に及ばないようにすることである。

(2)は、正答率が高かった。物理サーバ内の、仮想レイヤ 2 スイッチに接続された仮想サーバ間で行われるパケットの転送制御については、理解が高いことがうかがえた。

(3)、(4)とも、正答率が高かった。本問では、五つの F テーブルによってパケットの転送制御を行う方法を示したが、各 F テーブルの役割や F テーブル間で行われるパケットの転送手順などについても、十分に理解されていることがうかがえた。

設問	解答例・解答の要点		備考
設問 1	ア	スタック	
	イ	ステートフル	
	ウ	負荷分散	
	エ	チーミング	
設問 2	(1)	・顧客ごとに異なるフィルタリングの設定が必要であるから ・顧客ごとにルーティングの設定が必要であるから	
	(2)	① ・FWb による FWa の稼働状態 ② ・FWa による L2SWa への接続ポートのリンク状態 ③ ・FWa による LBa への接続ポートのリンク状態 ・FWa による FWb の稼働状態 ・FWb による L2SWb への接続ポートのリンク状態 ・FWb による LBb への接続ポートのリンク状態	
	(3)	物理サーバへの接続ポートに、全ての顧客の仮想サーバに設定された VLAN ID を設定する。	
設問 3	・OFC の IP アドレス ・自 OFS の IP アドレス		
設問 4	(1)	① ・フィルタリングルール ② ・仮想 FW の VLAN ID ③ ・仮想 FW の IP アドレス ・仮想 FW のサブネットマスク ・仮想 FW の仮想 MAC アドレス ・ルーティング情報	
	(2)	顧客の L2SW 又は L3SW に接続する、L2SWa 及び L2SWb のポート	
設問 5	(1)	発生する可能性がある問題	物理サーバ 3 の障害によって、3 顧客のシステムが同時に停止してしまう。
		仮想サーバの配置	3 顧客向けの仮想サーバを、それぞれ異なった物理サーバに配置する。
	(2)	FWp の内部側ポートと LBp の仮想 IP アドレスをもつポートは、同一セグメントであり、物理サーバ 3 内で処理されるから	
	(3)	オ F テーブル名	F テーブル 1
		項番	2
		カ F テーブル名	F テーブル 0
		項番	6
	キ	F テーブル名	F テーブル 4
		項番	6
	(4)	OFS 名	OFS1, OFS2
		項番	7
		変更後のアクション	p12 から出力

近年では、SDN（Software-Defined Networking）を活用することでネットワークの仮想化が容易となってきた。この技術動向を踏まえ、多くのクラウド事業者は、マルチテナント方式の IaaS サービスを実現するため、SDN 技術を用いている。

本問は、IaaS のサービス基盤を構築する事例を取り上げている。その事例を通し、従来の技術と SDN 技術の比較について、SDN 技術を用いたパケット転送制御方式設計について、問うている。

本問が取り上げている SDN 技術は、標準化が進んでいる OpenFlow である。参考までに、OpenFlow は 3 回目の出題となっている。本問の解説を通じて SDN 技術を理解した後、これら類題にチャレンジしてみることをお勧めしたい。

表：OpenFlow を題材とする問題

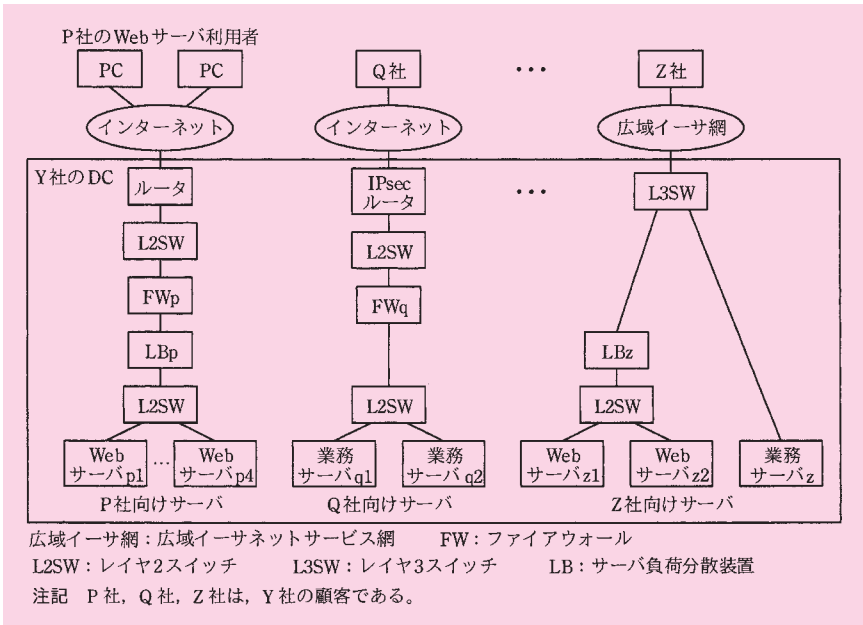
項番	問題	事例
1	平成 30 年午後Ⅱ問 2 (本問)	マルチテナント方式の IaaS サービス基盤の構築
2	平成 29 年午後Ⅱ問 1	ビジネス変化に対応できる柔軟性と拡張性を備えた LAN の構築
3	平成 25 年午後Ⅱ問 2	テナントネットワーク方式の自社基盤の構築

## ●本問の全体像

### ・現状のホスティングサービスの構成

Y 社は、データセンタ（以降の解説で、DC と称する）を運営し、ホスティングサービスを提供している。ホスティングサービスのシステムは、「顧客ごとに独立したネットワークとサーバから構成されている」（序文の第 1 段落）。

本文の図 1 には、顧客の例として P 社、Q 社、Z 社の 3 顧客が記されている。



図：ホスティングサービスのシステム構成（図1の抜粋）

### ・新たに構築するサービス基盤の要件

本事例では、序文の第3段落に示された要件に基づいて、サービス基盤を構築する。

以降の解説で、これらの要件に言及する際、箇条書きの項番を使い、「要件（1）」～「要件（3）」と称することにしよう。

- (1) サーバの仮想化によって、サーバ増設要求に迅速に対応可能とすること
- (2) サービス基盤で稼働する顧客システムは、顧客ごとに論理的に独立させること
- (3) サービス基盤は冗長構成とし、サービス停止を極力抑えられるようにすること

これら三つの要件に基づき、次の二つの方式でネットワークを構築することを検討している。

- 従来方式（従来の技術を用いた方式）
- SDN方式（SDN技術を用いた方式）

従来方式は図 2 に、SDN 方式は図 4 に、それぞれ示されている。

どちらの方式を用いようとも、顧客のネットワークとサーバの構成は、図 1 から変化しない。つまり、物理的な構成は図 2 又は図 4 に変化しているが、論理的な構成は図 1 のままなのだ。

さて、幾つかの要件について補足しておこう。

要件 (1) にある「サーバの仮想化」は、従来方式でも SDN 方式でも同じである。

要件 (2) にある「顧客ごとに論理的に独立させる」とは、端的に言うと、「マルチテナントの実現」である。そのことについて、より詳しい説明が序文の第 2 段落の中で次のように記述されている。

このサービス基盤では、ネットワークと物理サーバを顧客間で共用し、論理的に独立した複数の顧客システムを稼働させる、マルチテナント方式の IaaS (Infrastructure as a Service) を提供する。

要件 (3) にある「冗長構成」は、ネットワークについては、従来方式と SDN 方式で異なっている。サーバについては、どちらも同じである。

ネットワークについては、この後すぐ、「・従来方式によるサービス基盤の構成」「・SDN 方式によるサービス基盤の構成」の中で解説しよう。

サーバについては、ここで簡潔に解説する。

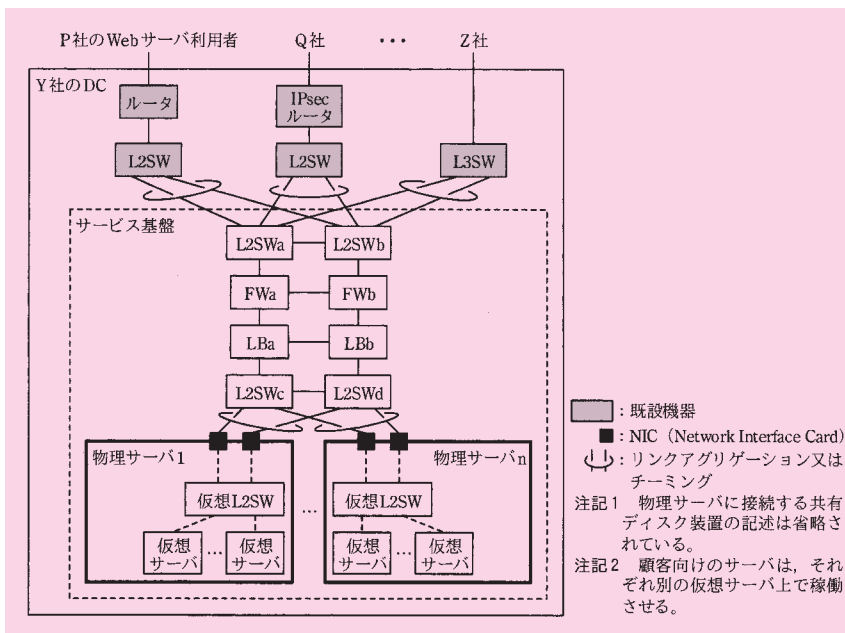
〔従来方式でのサービス基盤の構成案〕の第 7 段落の中で、「仮想サーバの物理サーバ間移動」と記述されている。これは、ある物理サーバで障害が発生したならば、当該物理サーバの仮想サーバが残りの物理サーバのどれかに移動することによって、稼働を継続させることを意味している。

この記述は従来方式を説明する文脈の中で登場するが、SDN 方式にも当てはまると言える。なぜなら、〔SDN 方式でのサービス基盤の構成案〕の第 5 段落の中で、物理サーバについて、「図 2 と同様に」（つまり、従来方式と同様に）と述べられているからだ。

#### ・従来方式によるサービス基盤の構成

顧客間のネットワークを論理的に独立させるため、従来方式では VLAN を用いる（〔従来方式でのサービス基盤の構成案〕の第 2 段落）。

本文の図 2 には、従来方式によるサービス基盤の構成案が示されている。



図：従来方式によるサービス基盤の構成案（図2の抜粋）

まず、要件（3）に着目しよう。

この要件に基づき、図2のサービス基盤は、アクティブ／スタンバイの2系統からなっている。

アクティブの系統は、「FWaとLBaをアクティブに設定する」（第6段落）とあるので、図2の左側（FWa-LBaを通る経路）である。

スタンバイの系統は、図2の右側（FWb-LBbを通る経路）である。

この冗長構成を実現するため、従来方式では、ネットワークの冗長化技術であるリンクアグリゲーション、NIC チーミングなどが使われている。これらについては、設問1で取り上げられている。詳しくはそこで解説しよう。

次いで、要件（2）に着目しよう。

この要件に基づき、図2のサービス基盤は、物理リンク、物理FW、物理LBを、複数の顧客が共用している。

このマルチテナントを実現するため、物理リンク、物理FW、物理LBをどのように設計しているのだろうか。この点について、ここで簡潔に解説しよう。より詳しくは、設問の解説の中で述べることにする。

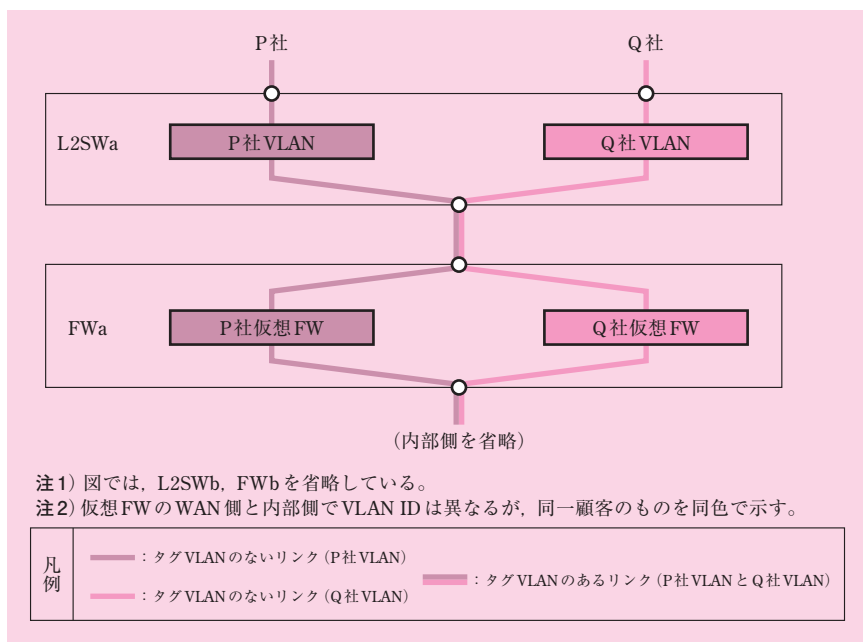
まず、物理リンクについて、「VLANによって顧客間のネットワークを論理的に独立

させる」(第 2 段落)と記述されている。したがって、物理リンクにタグ VLAN を設定することで、マルチテナントを実現する。

次に FW について、「装置の中に複数の仮想 FW を稼働させ(る)」(第 4 段落)と記述されている。したがって、仮想 FW を設けることで、マルチテナントを実現する。

仮想 FW については、設問 2 や設問 4 で取り上げられている。詳しくはそこで解説しよう。

次の図は、物理 FWa の内部に、P 社と Q 社の仮想 FW が存在している構成を示している。サービス基盤内のリンク及び FW のマルチテナントがどのように実現されているかを確認していただきたい。



図：P 社と Q 社のマルチテナントの実現 (L2SWa, FWa)

最後に LB については、「クラスタグループを複数設定」することで「複数の顧客の処理を 1 台で行える」(第 5 段落)と記述されている。したがって、クラスタグループを設定することで、マルチテナントを実現する。

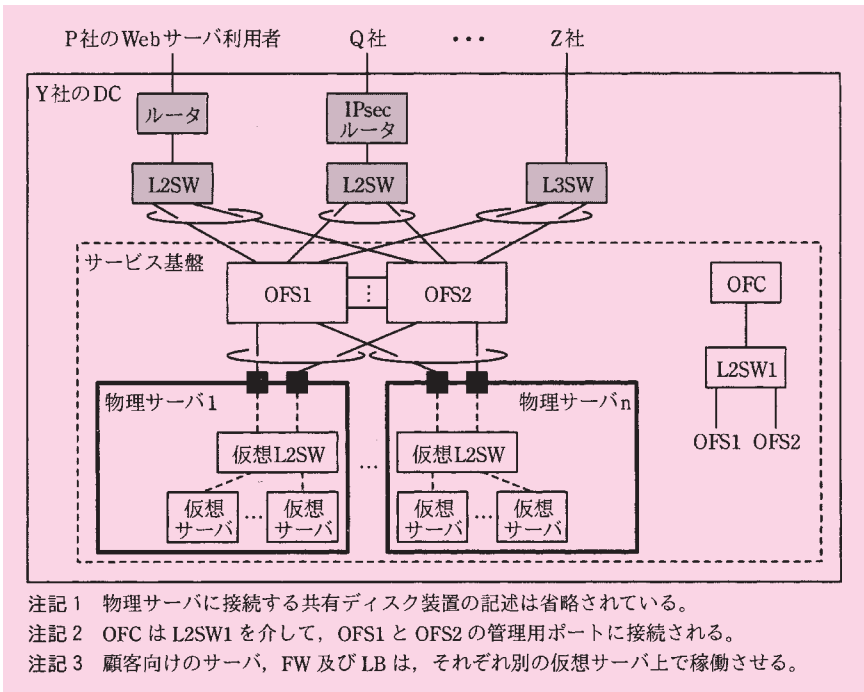
クラスタグループについては、設問 1 で取り上げられている。詳しくはそこで解説しよう。



### ・SDN 方式によるサービス基盤の構成

顧客間のネットワークを論理的に独立させるため、SDN 方式では、従来方式と同じく VLAN を用いる。

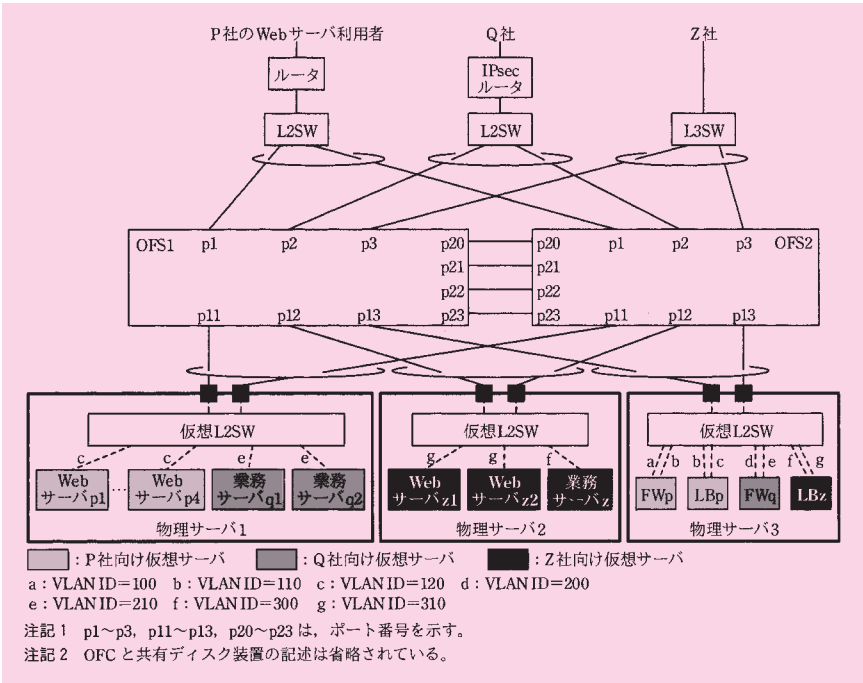
本文の図 3 には、SDN 方式によるサービス基盤の構成案が示されている。



図：OF によるサービス基盤の構成案（図 3 の抜粋）

従来方式と SDN 方式を比較した結果、本事例では SDN 方式が採用されている。

SDN 方式の導入効果を確認するため、SDN 方式に基づくテストシステムを構築することとなった。本文の図 4 には、テストシステムの構成が示されている。



図：テストシステムの構成 (図 4 の抜粋)

SDN 技術については、この後すぐ、「● SDN 技術」で説明する。

SDN 方式、及びそのテストシステムについては、設問 3、設問 5 で取り上げられて  
いる。詳しくはそこで解説しよう。

・本問の構成

以上を踏まえて本問の構成を概観すると、次のように整理できる。

表：本問の構成

見出し	主な内容	主に対応する出題箇所	
		設問	小問
(序文)	サービス基盤構築の 3 要件 図 1「Y 社が運営しているホス ティングサービスのシステム構成 (抜 粋)」	—	—

(表は次ページに続く)

見出し	主な内容	主に対応する出題箇所	
		設問	小問
従来方式でのサービス基盤の構成案	VLAN とサーバ仮想化によるマルチテナントの実現 ネットワークの冗長化対策 図 2「従来方式によるサービス基盤の構成案」	設問 1	空欄 ア～エ
SDN 方式でのサービス基盤の構成案	OpenFlow とサーバ仮想化によるマルチテナントの実現 ネットワークの冗長化対策 図 3「OF によるサービス基盤の構成案」	設問 2	(1) ～ (3)
		設問 3	—
二つの方式の比較	二つの方式を比較し, SDN 方式の採用を決定 表 1「Jさんが作成した二つの方式の比較」	設問 4	(1) ～ (2)
技術習得を目的とした制御方式の設計	MAC アドレスの学習によるパケットの転送制御方式の机上設計 図 4「テストシステムの構成」 表 2「テストシステム中の機器と仮想サーバの MAC アドレス」 表 3「五つの F テーブルの役割」 表 4～表 8 各 F テーブルの設定	設問 5	(1) ～ (4)

## ● SDN 技術

SDN 技術とは, 「ネットワーク機器の機能をソフトウェアで定義できるようにした技術や規格」である。

本問に登場する SDN 技術は, OpenFlow である。

OpenFlow は, 平成 25 年, 平成 29 年に続き, 3 回目の出題である。OpenFlow 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おり, 問題を解くための手掛かりは全て本文に与えられている。

なお, 過去 2 回の出題に比べると, OpenFlow の説明は簡素化されているという印象を受ける。これは, 出題内容に必要な範囲だけを説明しているからだ。本問は従来技術と SDN 技術の双方を取り上げているため, OpenFlow の仕様を深く掘り下げた問題は設けられていない。

多くの受験者は, 試験対策の一環として前年 (平成 29 年) の過去問題を演習したことだろう。そうであれば OpenFlow は既知の技術であったため, 問題に取り組みやすかったに違いない。

## ・ OFC と OFS

本問で取り上げている SDN 技術の方式について、[SDN 方式でのサービス基盤の構成案] の第 2～第 3 段落は次のように述べている。

SDN を実現する技術の中に、OpenFlow（以下、OF という）がある。今回の検討では、標準化が進んでいる OF を利用することにした。

OF は、データ転送を行うスイッチ（以下、OFS という）と、OFS の動作を制御するコントローラ（以下、OFC という）から構成される。OFS によるデータ転送は、OFC によって設定されたフローテーブル（以下、F テーブルという）に基づいて行われる。

ここに「OFS によるデータ転送は、OFC によって設定されたフローテーブル（以下、F テーブルという）に基づいて行われる」とある。

OFS は「スイッチ」と呼ばれているが、具体的にどのようにデータ転送を行うかは OFC が定義することができる。OFS の振る舞いは、従来のスイッチのようにハードウェアで静的に決まっているのではなく、ソフトウェアで動的に決めることができる。

要するに、OFS は、「1 台の L2SW」として機能したり、「1 台の L3SW」として機能したりすることができるというわけだ。まさに変幻自在だが、OFS の実力はそれだけに留まらない。驚くなかれ、OFS は、その内部に「複数台の L2SW や L3SW から構成されたネットワークセグメント」が存在しているかのような振る舞いさえすることができる。しかも、いつでも自由に、その機能を変更することができるのである。

さて、先ほど引用した本文は、「OF は、OFS と OFC から構成される」と述べている。そのネットワーク構成について、続く第 5～第 6 段落は次のように述べている。

OFC は、OFS1 と OFS2 の管理用ポートに接続する。

これらの OFS は、起動すると OFC との間で TCP コネクションを確立する。その後は、OFC との間の通信路となる OF チャネルが開設され、それを経由して OFC から F テーブルの作成や更新が行われる。

本事例では OFS が 2 台登場するので、本文中に OFS1、OFS2 と記述されている。この事例のように、1 台の OFC は、複数台の OFS を集中管理することができる。

OFC と OFS 間は、管理用のネットワークで接続する。OFS が起動すると OFC との間で OF チャネルが開設され、OFC が OFS を管理できるようになる。

### ・F テーブル (フローテーブル)

OFS によるデータ転送は、OFC によって設定された F テーブルに基づいて行われる。

この F テーブルについて、[技術習得を目的とした制御方式の設計] の第 5 ～ 第 6 段落は次のように述べている。

F テーブルは、複数のフローエントリ（以下、F エントリという）からなる。  
F エントリは、OFS に入力されたパケットがどの F エントリに一致するかを判定するためのマッチング条件、条件に一致したパケットに対する操作を定義するアクション、パケットが複数の F エントリに一致した場合の優先度などで構成される。入力されたパケットが、F テーブル内の複数の F エントリのマッチング条件に一致した場合は、優先度が最も高い F エントリのアクションが実行される。また、どのマッチング条件にも一致しないパケットは廃棄される。一つの F エントリには、複数のアクションを定義できる。

OFS の F テーブルは、F エントリが集まったものである。

テーブルの「行」(レコード) に相当するのは、「F エントリ」である。「列」に相当するのは、「マッチング条件」「アクション」である。

スイッチの機能は F テーブルで定義されており、個々の具体的な操作は F エントリで定義されている。この点が少々わかりづらいので、具体例を挙げて説明しよう。

L2SW の「イーサネットパケットを転送する」という機能は、どのように定義されるだろうか。パケットの入力を契機に、「入力パケットの宛先 MAC アドレスの値に基づき、特定のポートからパケットを送信する」とおおよそ定義できる。

もう一つ、L3SW の「IP パケットを転送する」という機能はどうだろうか。パケットの入力を契機に、「入力パケットの宛先 IP アドレスの値に基づき、特定のポートからパケットを送信する」とおおよそ定義できる。

つまり、こうした例から分かるとおり、スイッチは、

- ・入力パケットに基づき、当該パケットに応じた処理を実行する。

という操作によって、その機能を果たしていることが分かる。

ここに書いたことは、F エントリの列名を使って、

- ・「マッチング条件」に合致したとき、「アクション」を実行する。

と言い換えることができる。

ある 1 行の F エントリには、この「マッチング条件」と「アクション」が、具体的な値を指定して記述されている。マッチング条件には、入力されたポート ID、入力パケットの宛先／送信元 MAC アドレスなどの値が具体的に設定される。同様にアクションにも、出力するポート ID などの値が具体的に設定される。

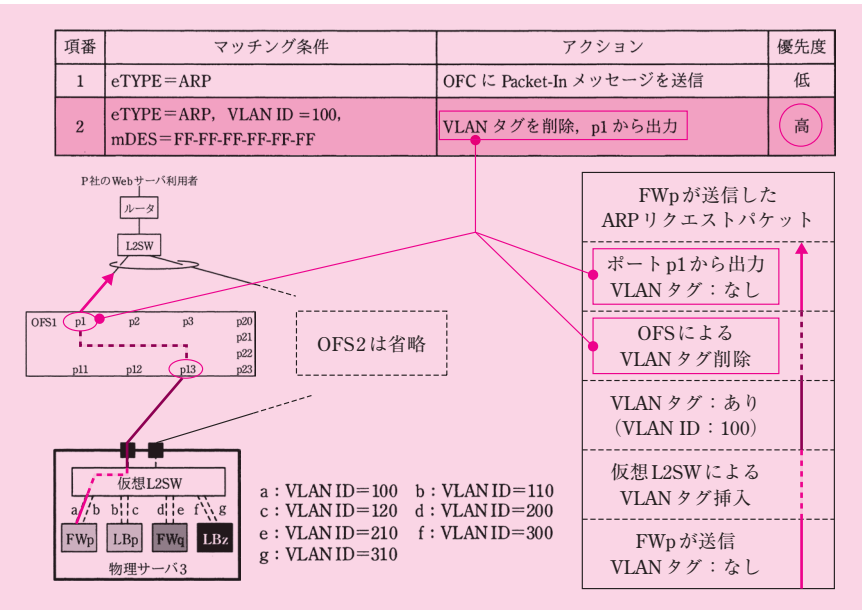
つまり、1 行の F エントリは、入力パケットごとの具体的な一つの操作を登録したものである。この F エントリの集合体が、F テーブルである。

ある入力パケットが、複数の F エントリのマッチング条件に一致した場合は、優先度が最も高い F エントリのアクションが実行される。また、どのマッチング条件にも一致しないパケットは廃棄される。

・F テーブルに基づく転送動作の具体例

F エントリに基づく転送動作について、〔技術習得を目的とした制御方式の設計〕の第 9 段落は、具体例を挙げて次のように説明している。

表 8 中の項番 2 は、イーサタイプが ARP、VLAN ID が 100 及び宛先 MAC アドレスが FF-FF-FF-FF-FF-FF のパケットを、VLAN タグを削除して p1 から出力することを示している。



図中の矢印は、仮想サーバ FWp が送信した ARP リクエストパケットである。

このパケットは、物理サーバ 3 の内部にある仮想 L2SW で VLAN タグが挿入される。この VLAN ID は、FWp が所属する VLAN のものであるから、図 4 によると「100」である。

物理サーバが送信した VLAN タグ付きの ARP リクエストパケットは、OFS のポート p13 に入力される。この結果、F テーブル 4 が評価される。F テーブル 4 は、「物理サーバ 3 から、p13 経由で OFS に入力したパケットの処理」に用いられるものだからだ（表 3 中の項番 5）。

F テーブル 4 の中で、この入力パケットに合致するマッチング条件をもつ F エントリは、項番 1、項番 2 である。

二つの項番の優先度を比べると項番 2 の方が高いので、こちらのアクションが実行される。すなわち、「VLAN タグを削除して p1 から出力」される。

#### ・OFC と OFS 間のメッセージ

本事例では 2 台の OFS が登場し、これら OFS は、1 台の OFC によって集中管理される。

この集中管理は、OFC と OFS 間のメッセージ交換によって行われている。この点について、[技術習得を目的とした制御方式の設計] の第 7 段落は次のように述べている。

OFC と OFS の間では、メッセージの交換が行われる。このメッセージの中には、OFS に対して F エントリを設定する Flow-Mod メッセージ、OFS が受信したパケットを OFC に送信する Packet-In メッセージ、OFC が OFS に対して指定したパケットの転送を指示する Packet-Out メッセージなどがある。

3 種類のメッセージを整理すると、次の表のようにまとめることができる。

表：OFC と OFS 間のメッセージ

メッセージ名	通信の方向	用途
Flow-Mod	OFC → OFS	OFS に対して F エントリを設定する
Packet-In	OFS → OFC	OFS が受信したパケットを OFC に送信する
Packet-Out	OFC → OFS	指定したパケットの転送を指示する

F テーブルに適切な F エントリを登録しておくことで、OFS は、入力パケットに基づくデータ転送を行うことができる。このような振る舞いは、「プロアクティブ型」と呼ばれている。

Flow-Mod メッセージは、このプロアクティブ型の動作を F テーブルに登録・変更するために使われるものである。

これに対し、Packet-In メッセージと Packet-Out メッセージのシーケンスは、「OFS からの通知に基づき、OFC が OFS に指示を出す」という手続きを行っている。このような振る舞いは、「リアクティブ型」と呼ばれている。

#### ・アドレス学習

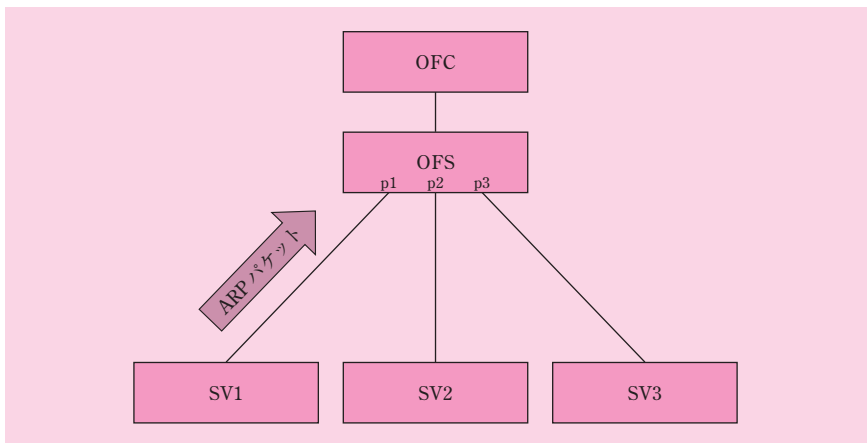
表 5～表 8 の F エントリを見ると、送信元 MAC アドレス、送信先 MAC アドレスの値として、サーバの MAC アドレスが指定されている。当然ながら、これらの MAC アドレスは、OFS の起動時には分からない。

この F エントリはどのように登録されたのだろうか。

その答えは、L2SW の MAC アドレスの学習と同じことを OFC が行い、その学習内容に基づく F エントリを OFS に登録したのだ。

アドレスを学習するには、パケットの入力ポートとパケットの送信元 MAC アドレスを対応付ける必要がある。OFC がこれを学習するため、Packet-In メッセージが使われている。F エントリの登録は、Flow-Mod メッセージが使われている。

例として、ARP リクエストパケットの受信したときの動作シーケンスを考察してみよう。ここでは、話を簡単にするため、本事例のネットワークとは異なり、VLAN を使用しないシンプルな構成を取り上げることにする。



図：「・アドレス学習」の解説で使用するネットワークの構成

次に示す一連の動作を通じ、アドレスの学習、F エントリの登録が行われる。



表：ある ARP リクエストパケットの受信したときの動作シーケンス

項番	動作	詳細
1	ARP リクエストパケットの受信	OFS は、送信元が mSV1（サーバ SV1 の MAC アドレス）からの ARP リクエストパケットをポート p1 で受信する
2	Packet-In メッセージによる通知	OFS は、「項番 1 の ARP リクエストをポート p1 で受信した」旨の通知を OFC に通知する
3	アドレスの学習	OFC は、「mSV1 がポート p1 の先に存在している」ことを学習する
4	Flow-Mod メッセージによる F エントリの登録	OFC は、「mSV1 を宛先とするパケットはポート p1 から出力する」旨の F エントリを OFS に登録する
5	Packet-Out メッセージによる指示	OFC は、ARP リクエストパケットの転送を OFS に指示する。その内容は、「ポート p1 と同一 VLAN に所属する全ポートに ARP リクエストパケットをフラディングする」ことである

注) 項番 5 はここで話題にしているアドレスの学習とは無関係であるが、パケット転送のために必ずこれを行う。

### ・パイプライン処理

OF は、F テーブルを複数設けることができる。1 個の入力パケットに対し、それぞれの F テーブルでエントリを評価し、アクションを実行するのである。これを「パイプライン処理」という。

パイプライン処理により、1 個の入力パケットに対し、一致するマッチング条件をもつ F エントリを複数実行することができる。

本事例では、五つの F テーブルを用いている。この点について、〔技術習得を目的とした制御方式の設計〕の第 4 段落は次のように述べている。

F テーブルは、OFS のデータ転送動作を確認しやすくするために、最初に処理される F テーブル 0 と、パケットの入力ポートに対応して処理される F テーブル 1～4 の五つの構成とした。2 人がまとめた、五つの F テーブルの役割を表 3 に示す。

表：五つの F テーブルの役割（表 3 の抜粋）

項番	F テーブル名	役割
1	F テーブル 0	パケットの入力ポートを基にした、処理の振り分け
2	F テーブル 1	顧客のネットワークから、p1~p3 経由で OFS に入力したパケットの処理
3	F テーブル 2	物理サーバ 1 から、p11 経由で OFS に入力したパケットの処理
4	F テーブル 3	物理サーバ 2 から、p12 経由で OFS に入力したパケットの処理
5	F テーブル 4	物理サーバ 3 から、p13 経由で OFS に入力したパケットの処理

本事例のパイプライン処理について、第 10 段落は具体例を挙げて説明している。

OFS にパケットが入力されると、OFS は表 4 の F テーブル 0 の処理を最初に実行する。例えば、図 4 中の Q 社の IPsec ルータから OFS1 の p2 に ARP リクエストパケットが入力された場合、そのパケットは、表 4 中の項番 2 に一致するので、パケットに VLAN ID が 200 の VLAN タグをセットし、次に表 5 の F テーブル 1 で定義された処理を行う。表 5 の F テーブル 1 では、項番 1 に一致するので、当該パケットは Packet-In メッセージに収納されて、OFC に送信される。

ここに記述されている動作を整理すると、次の表のとおりとなる。

表：第 10 段落の ARP リクエストパケットの受信したときの動作シーケンス

項番	動作	詳細
1	ARP リクエストパケットの受信	OFS1 は、Q 社の IPsec ルータから ARP リクエストパケットをポート p2 で受信する
2	F テーブル 0 の項番 2 のエントリに基づくアクションを実行	各 F エントリを評価した結果、「入力ポート = p2」のマッチング条件をもつ項番 2 の F エントリに合致した VLAN ID が 200 のタグをセットした上で、F テーブル 1 で定義された処理を行う
3	F テーブル 1 の項番 1 のエントリに基づくアクションを実行	各 F エントリを評価した結果、「eType = ARP」のマッチング条件をもつ項番 1 の F エントリに合致した OFC に Packet-In メッセージを送信する
4	Packet-In メッセージによる通知	OFS は、「項番 1 の ARP リクエストをポート p2 で受信した」旨の通知を OFC に通知する

この後の動作について、本文は次のように記述している。

OFC は受信したパケットの内容を基に、Flow-Mod メッセージで F エントリを生成したり、Packet-Out メッセージなどを OFS に送信したりする。

OFS が Packet-In メッセージを通知したことから、OFC は IPsec ルータの MAC アドレスを学習していないものと考えられる。それゆえ、OFC は、「・アドレス学習」の表「ある ARP リクエストパケットの受信したときの動作シーケンス」で解説したように振る舞うはずだ。

すなわち、その項番 3, 4 で述べたとおり、「OFC は受信したパケットの内容を基に、Flow-Mod メッセージで F エントリを生成」する。その後、項番 5 で述べたとおり、ARP リクエストパケットの転送を指示するため、「Packet-Out メッセージを OFS に送信」する。

以上で、SDN 技術の概要を理解できた。本問を解く準備が整ったところで、いよいよ設問の解説に移ろう。

## ■設問 1

### 解答例

ア：スタック  
イ：ステートフル  
ウ：負荷分散  
エ：チーミング

本設問は、本文中の空欄ア～エに入れる適切な字句を問うている。

空欄ア～エは、「従来方式でのサービス基盤の構成案」の第 3～第 7 段落の中にある。

ア

空欄アを含む文は、第 3 段落の中にある。そこには、「L2SWa と L2SWb の間及び L2SWc と L2SWd の間は、ア 接続して、それぞれ、一つの L2SW として動作できるようにする」と記述されている。

2 台の L2SW をスタック接続することにより、1 台の L2SW として動作させる技術を、スタック接続という。

よって、正解は、「スタック」である。

### ●スタック接続された L2SW に対するリンクアグリゲーションの設定

空欄アの解は導いたが、L2SWa と L2SWb、及び L2SWc と L2SWd の設定について解説しよう。

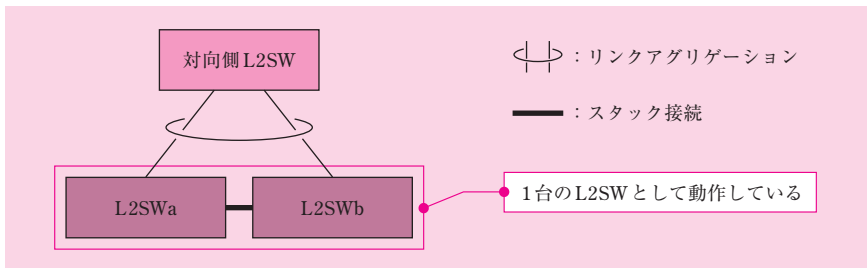
L2SWa と L2SWb には、リンクアグリゲーションが設定されている（図 2、第 3 段落）。同様に、L2SWc と L2SWd にも、リンクアグリゲーションが設定されている（図 2、第 7 段落）。

リンクアグリゲーションは、隣接する 2 台の L2SW の間を複数の物理リンクで接続し、これら物理リンクを 1 本の論理リンクに束ねる技術である。

リンクアグリゲーションにより、論理リンクの信頼性向上と帯域拡大を実現することができる。

図 2 を見ると、L2SWa、L2SWb の対向側に位置する L2SW から 2 本のリンクが出ている。このリンクのうち 1 本は L2SWa に、もう 1 本は L2SWb と接続している。

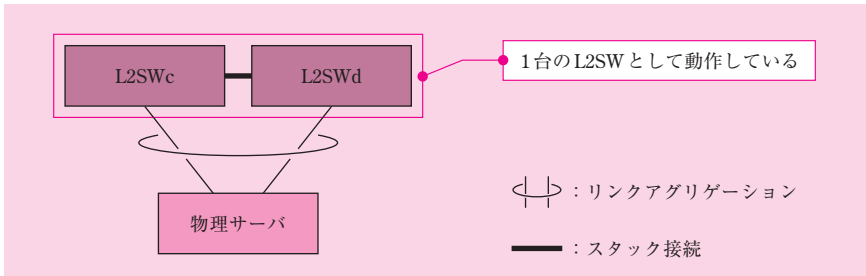
このようなリンクアグリゲーションを構成するには、L2SWa と L2SWb をスタック接続し、一つの L2SW として動作させる必要がある。



図：スタック接続された L2SWa と L2SWb に対するリンクアグリゲーションの設定

同様に、L2SWc、L2SWd の対向側に位置する物理サーバから 2 本のリンクが出ている。このリンクのうち 1 本は L2SWc に、もう 1 本は L2SWd と接続している。

このようなリンクアグリゲーションを構成するには、L2SWc と L2SWd をスタック接続し、一つの L2SW として動作させる必要がある。



図：スタック接続された L2SWc と L2SWd に対するリンクアグリゲーションの設定

イ

空欄イを含む文は、第 4 段落の中にある。そこには、「FW は、装置の中に複数の仮想 FW を稼働させることができ、装置の冗長化ができる製品を選定する。冗長構成では、アクティブの仮想 FW が保持しているセッション情報が、装置間を直結するケーブルを使って、スタンバイの仮想 FW に転送される。セッション情報を継承することで、仮想 FW の イ フェールオーバーを実現している」と記述されている。

図 2 を見ると、FW は、FWa と FWb の 2 台がある。第 6 段落は、「図 2 の構成案では、FWa をアクティブに設定する」旨、述べている。

それぞれの FW の中に、顧客ごとに仮想 FW が稼働している。正常時は、FWa の内部にある仮想 FW は全てアクティブであり、FWb の内部にある仮想 FW は全てスタンバイである。

本事例の FW は、FWa から FWb にフェールオーバーする際、それぞれの仮想 FW でセッション情報を継承する機能を装備している。

セッション情報とは、FW が許可した各々の通信に関する情報（宛先／送信元 IP アドレス、宛先／送信元ポート番号、等）を指している。セッション情報を引き継ぐことによって、FW に障害が発生しても通信を継続することができる。

冒頭の「・新たに構築するサービス基盤の要件」で解説したとおり、本事例では、要件 (2) に基づき、マルチテナントを実現する必要がある。

つまり、顧客ごとに、フィルタリングルール、及び、当該ルールに基づいて許可しているセッションは、当然ながら異なっている。フェールオーバー時のセッション情報の継承は、同一顧客の仮想 FW の間で行われなければならない。

フェールオーバー時にセッション情報を継承する機能のことを、通常、「ステートフルフェールオーバー」という。

よって、正解は、「ステートフル」である。

参考までに、ステートフルフェールオーバーは、平成 26 年午後 I 問 2 に続いて 2 回目

の出題である。本問と同じように仮想 FW が登場し、FW の冗長化について様々な角度から取り上げているので、類題として解いてみることをお勧めしたい。

ウ

空欄ウを含む文は、第 5 段落の中にある。そこには、「LB は、負荷分散対象のサーバ群を一つのグループ（以下、クラスタグループという）としてまとめ、クラスタグループを複数設定できる製品を選定する。クラスタグループごとに仮想 IP アドレスと  
ウ アルゴリズムが設定できるので、複数の顧客の処理を 1 台で行える」と記述されている。

本空欄を解くに当たり、いったん、クラスタグループ機能がない通常の LB について考察してみよう。

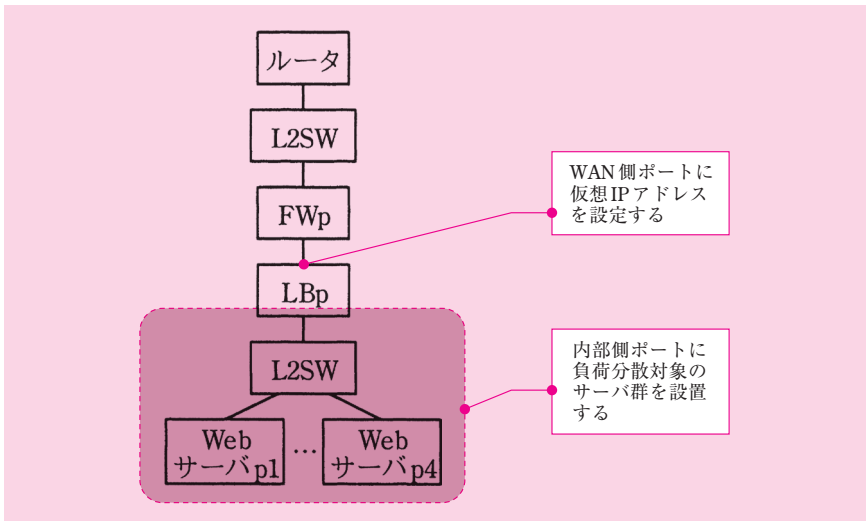
LB は、その配下に負荷分散対象のサーバ群を有している。これらサーバ群は、外部からは 1 台のサーバのように見える。

LB が、これらのサーバ群に負荷を分散する方法は、おおむね次のとおりである。

- LB に、仮想 IP アドレスを設定しておく。この仮想 IP アドレスを外部に公開する。
- 仮想 IP アドレスを宛先とするパケットを受信したら、負荷分散対象のサーバ群の中から 1 台のサーバを選定し、これにパケットを転送する。

このとき、仮想 IP アドレスは WAN 側のポートに設定し、負荷分散対象のサーバは内部側のポートの配下に設置する。

図 1 に登場する LB は通常のもので、P 社を例に取り上げると、次のようになる。



図：通常の LB の仮想 IP アドレスの設定，負荷分散対象のサーバ群の設置（図 1 の P 社の例）

負荷分散対象のサーバ群の中から，転送先とする 1 台のサーバを選定するには，負荷分散アルゴリズムを用いる。その例として，

- ラウンドロビン
- 最小コネクション数
- 最短レスポンス時間

などがある。

こうした負荷分散を行うには，「負荷分散対象のサーバ群」に対し，公開用の「仮想 IP アドレス」と，パケット受信時の「負荷分散アルゴリズム」を設定する必要がある。

通常の LB について理解できたので，それでは，クラスタグループ機能がある LB について考察してみよう。

空欄ウを含む文を見ると，この機能は，「負荷分散対象のサーバ群を一つのクラスタグループとしてまとめ，こうしたクラスタグループを複数設定できる」というものだ。

要するに，通常の LB の「負荷分散対象のサーバ群」が一つのクラスタグループに相当しており，これを複数設定できることを意味している。

空欄ウを含む本文は，この機能により「複数の顧客の処理を 1 台で行える」旨，述べている。冒頭で解説したとおり，要件（2）に基づきマルチテナントを実現する必要がある。それゆえ，この一文は，顧客ごとにクラスタグループを設定し，それぞれの

クラスタグループが互いに独立して負荷分散を行うことを意味している。

そのためには、各々のクラスタグループに対して、公開用の「仮想 IP アドレス」と、パケット受信時の「負荷分散アルゴリズム」を設定する必要がある。

よって、正解は「負荷分散」となる。

負荷分散について、詳しくは本書の第 6 章「6.2.3 サーバの冗長化」を参照していただきたい。

## エ

空欄エを含む文は、第 7 段落の中にある。そこには、「物理サーバには 2 枚の NIC を実装し、エ機能を利用してアクティブ／アクティブの状態にする」と記述されている。

図 2 を見ると、物理サーバの対向側には L2SWc、L2SWd がある。空欄アで解説したとおり、L2SWc と L2SWd 間はスタック接続されているので、これらは 1 台の L2SW として動作する。

対向側 L2SW (L2SWc と L2SWd) にはリンクアグリゲーションが設定されている。これは、複数の物理リンクを 1 本の論理リンクとして束ねる技術である。つまり、物理サーバと対向側 L2SW を接続している物理リンクは、アクティブ／アクティブの状態になっている。

対向側 L2SW にリンクアグリゲーションが設定されている以上、それに合わせて、物理サーバの 2 枚の NIC にもリンクアグリゲーションを設定する必要がある。

それでは、空欄エに入る字句は「リンクアグリゲーション」となるだろうか。

そうではなく、空欄エの正解は「チーミング」となる。

なぜなら、通常、NIC の冗長化技術は「チーミング」と呼ばれているからだ。

なお、「NIC チーミング」と呼ばれることも多いので、こちらを解答してもよい。

空欄に入る字句を選ぶ際、本文や図に登場する技術用語を参考にするとよい。

本文の図 2 に「チーミング」という技術用語が登場する。ここから、出題者は、NIC の冗長化技術を表す一般的な用語を使っていることが分かる。

当然ながら、出題者が用意した模範解答は、この用語を使っているはずである。自分の答案は、この用語に照らして採点されるものと考えなければならない。

したがって、採点者に違和感を与えないよう、答案の作成に際しては、本文や図に登場する技術用語を踏まえ、適切な字句を選ぶように心掛けたい。

## ●参考：NIC の冗長化技術

チーミングは、NIC の冗長化技術である。



これは特に標準化されたものではないため、詳細の仕様は製品依存である。とはいえ、どの製品もおおよそ似通っている。

物理的には 2 枚の NIC がサーバに存在しているが、論理的には（OS から見ると）1 枚の論理的な NIC が存在しているように見える。

2 枚の物理 NIC は、次に示す二つのモードのうちどちらかで動作させる（製品によっては他にもモードがあるが、ここでは割愛する）。

表：NIC の動作モード

モード	内容
アクティブ／ アクティブ	2 枚の NIC のどちらも稼働している。 正常時は、どちらの NIC もパケットを送受信する。 事実上、リンクアグリゲーションを設定するのと同じである。 ある 1 個のパケットが通る NIC は、チーミングの負荷分散アルゴリズムに従って、2 枚のうちどちらかが逐次選択される
アクティブ／ スタンバイ	2 枚の NIC のうち、1 枚がアクティブであり、もう 1 枚がスタンバイである。 正常時は、アクティブ側の NIC のみパケットを送受信する

チーミングについて、詳しくは本書の第 6 章「6.2.4 NIC の冗長化」を参照していただきたい。

## ■設問 2

本設問は、「従来方式でのサービス基盤の構成案」について問うている。

(1)

### 解答例

顧客ごとに異なるフィルタリングの設定が必要であるから (26 字)

又は

顧客ごとにルーティングの設定が必要であるから (22 字)

問題文は、「本文中の下線①の要件が必要になる理由を……述べよ」と記述されている。

下線①は、「従来方式でのサービス基盤の構成案」の第 4 段落の中にある。そこに

は、「FW は、①装置の中に複数の仮想 FW を稼働させることができ（る製品を選定する）」と記述されている。

冒頭の「・新たに構築するサービス基盤の要件」で解説したとおり、本事例では、要件（2）に基づき、マルチテナントを実現する必要がある。

図 1 のネットワーク構成を見ると、現状のホスティングサービスのシステム構成において、FW は顧客ごとに設置されている。それゆえ、顧客ごとに FW のフィルタリングの設定は異なっていることが分かる。

さらに、FW の外部側又は内部側に位置する機器も、顧客ごとに異なっている。それゆえ、FW のルーティング設定も顧客ごとに異なっていることが分かる。

こうした課題を解決するには、図 2 のネットワーク構成において、顧客ごとに異なる FW をもつ必要がある。これを仮想化技術で実現したものが、仮想 FW に他ならない。

したがって、複数の仮想 FW を稼働させるという要件が必要になる理由は、顧客ごとにフィルタリングの設定やルーティングの設定が必要になるからである。

よって、この点を字数に収まるように解答すればよい。

なお、試験センターの解答例を見ると、フィルタリング又はルーティングのどちらか一方を解答すれば正解として扱われていることが分かる。

## (2)

### 解答例

F W b に よ る F W a の 稼 働 状 態 (14 字)

F W a に よ る L 2 S W a へ の 接 続 ポ ー ト の リ ン ク 状 態 (24 字)

F W a に よ る L B a へ の 接 続 ポ ー ト の リ ン ク 状 態 (22 字)

F W a に よ る F W b の 稼 働 状 態 (14 字)

F W b に よ る L 2 S W b へ の 接 続 ポ ー ト の リ ン ク 状 態 (24 字)

F W b に よ る L B b へ の 接 続 ポ ー ト の リ ン ク 状 態 (22 字)

(このうち三つを解答)

問題文は、「本文中の下線②の機能について、アクティブの FW を FWa から FWb に切り替えるのに、FWa 又は FWb が監視する内容を三つ挙げ、図 2 中の機器名を用いて、それぞれ……答えよ」と記述されている。

下線②は、「従来方式でのサービス基盤の構成案」の第 4 段落の中にある。そこには、「FW は、……②装置の冗長化ができる製品を選定する」と記述されている。

冗長化について、さらに第 6 段落の中に、「FW は FWa をアクティブにする」旨が述べられている。さらに「スタンバイの装置がアクティブに切り替わる条件は、両装置とも同様であり、両装置は連動して切り替わる」と記述されている。つまり、FWa と FWb の切り替わる条件が同じであり、監視する内容も同じであることが分かる。

ここまで導いたら、一般的な知識に基づいて解を導くことができる。

まず、FWa の機器自体に障害が発生したときにフェールオーバーするケースを考察してみよう。

この機器障害を検知するために必要となる監視は、次のものとなる。

#### [監視 1] FWb による FWa の稼働状態

FWa と FWb は監視する内容が同じなので、次の監視も行っている。

#### [監視 2] FWa による FWb の稼働状態

次に、FWa の機器自体はダウンしていないが、FWa のリンクに障害が発生したときにフェールオーバーするケースを考察してみよう。

言うまでもないが、FWa のリンクがダウンしたら FWa を経由できなくなる。それゆえ、外部側のリンク（L2SWa に接続するリンク）においても、内部側のリンク（LBa に接続するリンク）においても、とにかくリンク障害が発生したら FWb にフェールオーバーし、トラフィックが FWb を経由するようになしなければならない。

このリンク障害を検知するために必要となる監視は、次のものとなる。

#### [監視 3] FWa による、L2SWa に接続するポートのリンク状態

#### [監視 4] FWa による、LBa に接続するポートのリンク状態

FWa と FWb は監視する内容が同じなので、次の監視も行っている。

#### [監視 5] FWb による、L2SWb に接続するポートのリンク状態

#### [監視 6] FWb による、LBb に接続するポートのリンク状態

したがって、これら監視 1～6 のうち、三つを解答すればよい。

よって、正解は解答例に示したとおりとなる。

### (3)

#### 解答例

物	理	サ	ー	バ	へ	の	接	続	ポ	ー	ト	に	,	全	て	の	顧	客	の	仮	想	サ	ー	バ	
に	設	定	さ	れ	た	V	L	A	N		I	D	を	設	定	す	る	。							

(44字)

問題文は、「本文中の下線③について、VLAN を設定するポート及び設定する VLAN の内容を……具体的に述べよ」と記述されている。

下線③は、「従来方式でのサービス基盤の構成案」の第7段落の中にある。そこには、「L2SWc と L2SWd には、リンクアグリゲーションのほかに、③仮想サーバの物理サーバ間移動に必要となる VLAN を設定する」と記述されている。

図 2 を見ると、L2SWc、L2SWd にはそれぞれ物理サーバ 1 ～物理サーバ n が接続されている。

物理サーバの中には仮想サーバがある。この仮想サーバについて、図 2 の注記 2 には「顧客向けのサーバは、それぞれ別の仮想サーバ上で稼働させる」と記述されている。つまり、図 1 に記された 1 台の顧客サーバ（例えば P 社であれば、Web サーバ p1 ～ Web サーバ p4）が、図 2 に記された 1 台の仮想サーバに対応していることが分かる。

冒頭の「・新たに構築するサービス基盤の要件」で解説したとおり、本事例では、要件 (2) に基づき、マルチテナントを実現する必要がある。

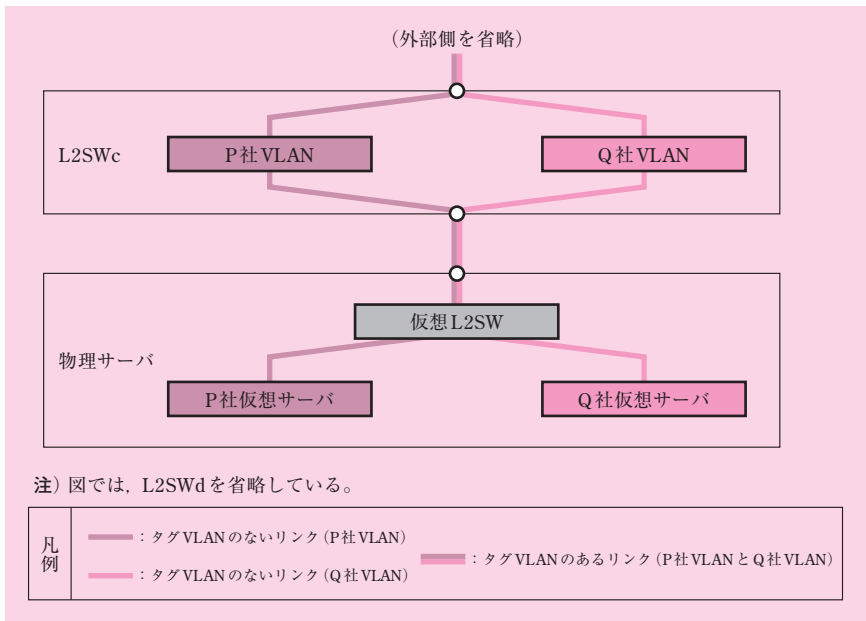
そのため、第 2 段落にあるとおり、「サービス基盤は、VLAN によって顧客間のネットワークを論理的に独立させる」。

この点について、冒頭の解説では、L2SWa と FWa の部分を取り上げた。簡潔に振り返ってみよう。図 2 では L2SWa と FWa 間は 1 本の物理リンクで接続されている。しかし、図「P 社と Q 社のマルチテナントの実現 (L2SWa、FWa)」に示したとおり、このリンクはタグ VLAN が設定されている。1 本の物理リンクの上に、P 社 VLAN の論理リンクと Q 社 VLAN の論理リンクが存在しているのだ。

これと同じようなタグ VLAN の設定が、L2SWc と物理サーバの間の物理リンクにも必要となる。

例えば、物理サーバの中に存在する仮想サーバとして、P 社と Q 社の顧客サーバがあるでしょう。この物理サーバの NIC 及び仮想 L2SW には、P 社 VLAN と Q 社 VLAN を設定する必要がある。したがって、L2SWc と物理サーバ間の 1 本の物理リンクの上

に、P 社 VLAN の論理リンクと Q 社 VLAN の論理リンクが存在しているのだ。



図：P 社と Q 社のマルチテナントの実現 (L2SWc, 物理サーバ)

もしかすると、ある物理サーバには、1 社の顧客の仮想サーバしか存在していないかもしれない。そのときは、L2SWc とこの物理サーバ間の物理リンクにタグ VLAN を設定する必要がないのだろうか。

この点について、下線③は次のように述べている。「③仮想サーバの物理サーバ間移動に必要な VLAN を設定する」。つまり、様々な顧客の仮想サーバが物理サーバ間を移動することが分かる。

冒頭の「・新たに構築するサービス基盤の要件」で解説したとおり、本事例では、要件 (3) に基づき、冗長構成にする必要がある。

この要件を仮想サーバに当てはめると、ある物理サーバに障害が発生したならば、当該物理サーバの仮想サーバは、残りの物理サーバのどれかに移動して稼働を継続させる必要がある。

ここで、物理サーバが残り 1 台になった場合を想定してみよう。

このとき、全ての顧客の仮想サーバが、この物理サーバに移動することになる。その結果、全ての仮想サーバ向けのトラフィックが、L2SWc 又は L2SWd を経由して、

ここに流れてくる。

したがって、L2SWc と物理サーバ間の物理リンクは、全ての顧客の仮想サーバに設定された VLAN を束ねる必要がある。そのため、この物理リンクに接続する物理ポートに、タグ VLAN を設定しなければならない。設定する VLAN ID は、全ての顧客の仮想サーバに設定された VLAN ID だ。

同じことが、L2SWd と物理サーバ間の物理リンクにも当てはまる。

それぞれの物理サーバが「最後の 1 台」になる可能性を秘めているわけだから、これまで解説した設定は、どの物理サーバにも当てはまる。

さて、本小問は、L2SWc、L2SWd について、VLAN を設定するポート及び設定する VLAN の内容 (VLAN ID) を具体的に問うていた。

これまでの解説を踏まえると、タグ VLAN を設定するポートは、「物理サーバへの接続ポート」となる。具体的に設定する VLAN の ID は、「全ての顧客の仮想サーバに設定された VLAN ID」となる。

よって、正解は解答例に示したとおりとなる。

### ■設問 3

#### 解答例

O	F	C	の	I	P	ア	ド	レ	ス
---	---	---	---	---	---	---	---	---	---

 (10 字)

又は

自	O	F	S	の	I	P	ア	ド	レ	ス
---	---	---	---	---	---	---	---	---	---	---

 (11 字)

問題文は、「本文中の下線④の情報を……答えよ」と記述されている。

下線④は、〔SDN 方式でのサービス基盤の構成案〕の第 6 段落の中にある。そこには次のように記述されている。

これらの OFS は、起動すると OFC との間で TCP コネクションを確立する。その後は、OFC との間の通信路となる OF チャネルが開設され、それを經由して OFC から F テーブルの作成や更新が行われる。したがって、OFS の導入時には、④ OFC との TCP コネクションの確立に必要な最小限の情報を設定すればよく、導入作業は容易である。

OFS は、TCP コネクションの確立を要求する側である。すなわち、クライアントである。

一般的に、TCP コネクションを確立するために必要となる、クライアント側の設定として、次のものを挙げることができる。

- 送信元 IP アドレス
- 宛先 IP アドレス
- 宛先ポート番号

クライアントの送信元ポート番号は、ここに列挙していないが、設定不要である。なぜなら、TCP コネクションを確立するとき、クライアント（すなわち送信元）のポート番号は、OS によって任意のものが選ばれるからだ。

それでは、ここに列挙した三つの内容が、下線④の言う「TCP コネクションの確立に必要な最小限の情報」なのだろうか？

もう一度、本文を注意深く読み返してみよう。

そこには、「OFS は、起動すると OFC との間で TCP コネクションを確立する。その後は、OFC との間の通信路となる OF チャネルが開設され（る）」とある。

つまり、OFS が起動すると、自動的に、TCP コネクションの確立と OF チャネルの開設を試みる事が分かる。

このような仕組みになっていることから、設置環境に依存した値は、OFS に設定しておく必要がある。さもないと、この自動実行は必ず失敗に終わるからだ。

それは、次の二つのものである。

- 送信元 IP アドレス（自 OFS の IP アドレス）
- 宛先 IP アドレス（OFC の IP アドレス）

それでは、残った宛先ポート番号はどうだろうか。

OF チャネルに相当するポート番号は、OF の仕様として規定されている。参考までに、その番号は 6653 だ。つまり、これは設置環境に依存した値ではない。

OFS が自動的に OF チャネルの確立を試みる仕様になっているわけだから、宛先ポート番号は、工場出荷時に既定値として与えているものと推察できる。

もちろん、設置環境によっては、宛先ポート番号を標準とは異なる値にするかもしれない。それを踏まえ、工場出荷後に既定値から変更できる仕組みになっているに違いない。

以上より、OFC との TCP コネクションの確立に必要な最小限の情報は、「OFC の IP アドレス」と「自 OFS の IP アドレス」の二つとなる。

ただし、指定字数が 15 字なので、このうち一つを解答すればよい。

## ■設問 4

本設問は、「二つの方式の比較」について問うている。

(1)

### 解答例

フィルタリングルール (10字)

仮想FWのVLANID (12字)

仮想FWのIPアドレス (11字)

仮想FWのサブネットマスク (13字)

仮想FWの仮想MACアドレス (14字)

ルーティング情報 (8字)

(このうち三つを解答)

問題文は、「表 1 中の項番 2 について、従来方式の場合、FW では複数の仮想 FW を設定することになる。仮想FWの設定に伴って、各仮想FWに対して設定が必要なネットワーク情報を三つ挙げ(よ)」と記述されている。

表 1 は、「二つの方式の比較」の第 1 段落の下にある。その表では、従来の方式と SDN 方式を、五つの比較項目に基づいて比較している。

項番 2 の比較項目は、「構築時の設定作業」である。

したがって、本小問は、各仮想FWの構築時の設定で必要となるネットワーク情報を問うている。

冒頭の「・新たに構築するサービス基盤の要件」で解説したとおり、本事例ではマルチテナントを実現する。それゆえ、仮想FWを構築する際、マルチテナントの実現に特化した設定をする必要があると考えられる。

その一方で、マルチテナントをしようがしまいが、通常のFWと同じような設定をする必要もあると考えられる。仮想化されているとはいえ、所詮はFWなのだから。

そこで、解を導くに当たり、マルチテナントに特化したものと、そうではない通常



のものに分けてみよう。

### ●マルチテナントの実現に特化した FW の設定

マルチテナントネットワークを実現するため、本事例では、「VLAN によって顧客間のネットワークを論理的に独立させる」〔従来方式でのサービス基盤の構成案〕第 2 段落)。

VLAN 技術を用いることにより、物理的に見ると 1 台の FW であるが、その内部に複数の仮想 FW を設け、それらを互いに独立させることが可能となる。

冒頭の「・新たに構築するサービス基盤の要件」の図「P 社と Q 社のマルチテナントの実現 (L2SWa, FWa)」は、物理 FWa の内部に、P 社と Q 社の仮想 FW が存在している構成を示している。

物理 FW の物理ポートはタグ VLAN を設定している。ここに入っているフレームには VLAN のタグが挿入されているので、タグ中の VLAN ID を見れば、フレームがどの顧客のネットワークを流れているものなのかを判別できる。

物理 FW は、フレームのタグを取り去ってどちらかの仮想 FW に転送する。それゆえ、その転送先を決定するには、各社の仮想 FW がどの顧客の VLAN に所属するかを設定しておかなければならない。

したがって、各仮想 FW に対して設定が必要なネットワーク情報として、

- 仮想 FW の VLAN ID

を挙げることができる。

### ●通常の FW の設定

通常の FW を構築する際に必要となるネットワーク情報を考察してみよう。それらネットワーク情報を、それぞれの仮想 FW に設定するわけだ。

まず、FW は IP パケットを転送するので、IP アドレスとサブネットマスクの情報が必要である。

次に、FW はイーサネットフレームを送受信するので、MAC アドレスの情報が必要である。なお、この MAC アドレスは通常のものとは異なり、製造時に物理的に割り当てられたものではない。仮想 FW 構築時に割り当てられたものなので、「仮想 MAC アドレス」と称するのが適切だ。

さらに、FW は複数のサブネット間の境界に位置し、ルータの役割を担っているの  
で、ルーティングの情報が必要である。

最後に, FW ならしめる基本的機能であるフィルタリングルールの情報が必要である。  
 ルーティングとフィルタリングルールに関しては, 設問 2 (1) で既に取り上げられていた。これらを顧客ごとに設定する必要があったので, 仮想 FW を稼働させたのである。

以上より, 各仮想 FW に対して設定が必要なネットワーク情報として,

- 仮想 FW の IP アドレス
- 仮想 FW のサブネットマスク
- 仮想 FW の仮想 MAC アドレス
- 仮想 FW のルーティング情報
- 仮想 FW のフィルタリングルール

を挙げることができる。

### ●解の導出

これまでの考察より, 構築時に必要となるネットワーク情報を六つ挙げることができた。

本小問は三つ解答することを求めているので, この中から選べばよい。

よって, 正解は解答例に示したとおりとなる。

## (2)

### 解答例

顧	客	の	L	2	S	W	又	は	L	3	S	W	に	接	続	す	る	,	L	2	S	W	a	及
び	L	2	S	W	b	の	ポ	ー	ト	(35字)														

問題文は, 「表 1 中の項番 3 について, 従来方式の場合, 追加する顧客に対応した VLAN 設定がサービス基盤の全ての機器及びサーバで必要になる。その中でポート VLAN を設定する箇所を, 図 2 中の名称を用いて……答えよ」と記述されている。

前の小問に引き続き, 従来方式と SDN 方式の比較を掲載した表 1 が取り上げられている。

項番 3 の比較項目は, 「顧客追加時の設定作業」である。

本小問は, その作業の中で, ポート VLAN を設定する箇所を問うている。

ポート VLAN を設定できる物理ポートは、一つの VLAN のトラフィック、すなわち、ある 1 社の顧客のトラフィックしか流れない物理ポートに限られる。したがって、そのような物理ポートを導き出すことによって、本小問の解が得られる。

言い換えると、ポート VLAN を設定できない物理ポートは、2 社以上の顧客のトラフィックが流れる可能性のある物理ポートである。したがって、そのような物理ポートを除外することによっても、本小問の解が得られる。

そこで、P 社と Q 社を主に取り上げ、インターネットから両社の顧客サーバ（仮想サーバ）に向かうトラフィックを順にたどりながら、ポート VLAN を設定する物理ポートを考察しよう。

サービス基盤内のネットワークは冗長化されており、一見すると複雑だ。

とはいえ、実を言うと、次の経路だけ着目すれば、解を導くことができるのだ。このようにシンプルに考えることで、解が導きやすくなる。

インターネット → L2SWa → FWa → LBa → L2Wc → 物理サーバ 1

そこで、まずは、この経路だけ着目すればよい理由を解説する。次いで、本小問の解を導こう。

### ●物理サーバ 1 だけ着目する理由

設問 2 (3) で解説したとおり、本事例では、物理サーバの障害発生時に仮想サーバが別の物理サーバに移動する。それゆえ、各社の仮想サーバは、物理サーバ 1 ～物理サーバ n のどこにでも存在するものと考えなければならない。

例えば、P 社、Q 社のそれぞれの仮想サーバが、同じ物理サーバの中に存在する可能性があるわけだ。

先ほどの解説で、「ポート VLAN を設定できない物理ポートは、2 社以上の顧客のトラフィックが流れる可能性のある物理ポートである」と述べた。これに該当するポートを除外するという解法アプローチを、ここで使うことができる。

同じ物理サーバの中に 2 社の仮想サーバが存在する可能性があるわけだから、どの物理サーバの NIC も、及びその対向側の L2SWc、L2SWd の物理ポートも、タグ VLAN を設定する必要がある。つまり、これらを解答の候補から除外できる。

したがって、P 社と Q 社のトラフィックを考察するに当たり、物理サーバ 1 だけを取り上げれば十分である。P 社、Q 社のそれぞれの仮想サーバがこの中に存在するケースを取り上げることで、解の候補が絞り込まれ、考察しやすくなるからだ。

### ●アクティブの経路だけ着目する理由

サービス基盤内のネットワークは冗長化されているが、VLAN の設定に関しては、アクティブ側とスタンバイ側は同一のものとなる。

そのように言える理由は、アクティブ側に存在していた VLAN 設定がスタンバイ側に存在していなかったならば、いざ切り替わったときにその VLAN を流れるトラフィックが途絶えてしまうからだ。そのような欠陥のある冗長化設計は行わないので、アクティブ側とスタンバイ側の VLAN 設定は同じであると言える。

したがって、P 社と Q 社のトラフィックを考察するに当たり、アクティブとなる FWa, LBa を経由する経路だけを取り上げることにする。

以上をまとめると、次に示す経路となる。繰り返しになるが、再掲しよう。

インターネット → L2SWa → FWa → LBa → L2Wc → 物理サーバ 1

この経路だけに着目する理由が分かったところで、それでは、いよいよ本小問の解を導こう。

### ●インターネット → L2SWa

P 社のトラフィックは、次に示す経路を通る。

インターネット → ルーター → L2SW (P 社) → L2SWa

Q 社のトラフィックは、次に示す経路を通る。

インターネット → IPsec ルーター → L2SW (Q 社) → L2SWa

ここに挙げた一連の経路において、P 社と Q 社のトラフィックは、それぞれ別々の物理リンクを流れる。

したがって、この区間の L2SW の物理ポートには、ポート VLAN を設定することが分かる。

本小問は、サービス基盤の機器を対象にしている。そこに着目すると、ポート VLAN を設定するポートは、次のとおりとなる。

- 顧客の L2SW, L3SW に接続している L2SWa のポート

なお、本文の図 2 には単に「L2SW」と記されている。本小問は図 2 の名称を用いて解答することを求めているので、ここでは「顧客の L2SW」と書いた。

さらに、図 2 には Z 社もあり、同社は L3SW を使っているので、それも解答に含める。

#### ● L2SWa → FWa → LBa → L2SWc

FWa の内部には顧客ごとに仮想 FW がある。各社のトラフィックは FWa に入り、内部で分岐して仮想 FW でフィルタリングされる。

したがって、P 社のトラフィックは、次に示す経路を通る。

L2SWa → FWa

同様に Q 社のトラフィックも、次に示す経路を通る。

L2SWa → FWa

LBa はマルチクラスティング機能を有している。各社のトラフィックは LBa に入り、顧客ごとに負荷分散される。負荷分散されたトラフィックは、L2SWc を経由し、サーバに向かう。

したがって、P 社のトラフィックは、次に示す経路を通る。

FWa → LBa → L2SWc

同様に Q 社のトラフィックも、次に示す経路を通る。なお、図 1 を見ると、Q 社は負荷分散装置を利用していないので、LBa を通過するだけだ。

FWa → LBa → L2SWc

ここに挙げた一連の経路において、P 社と Q 社のトラフィックは、同じ物理リンクを流れる。

したがって、ポート VLAN を設定するポートは、この区間には存在しない。

#### ● L2SWc → 物理サーバ 1

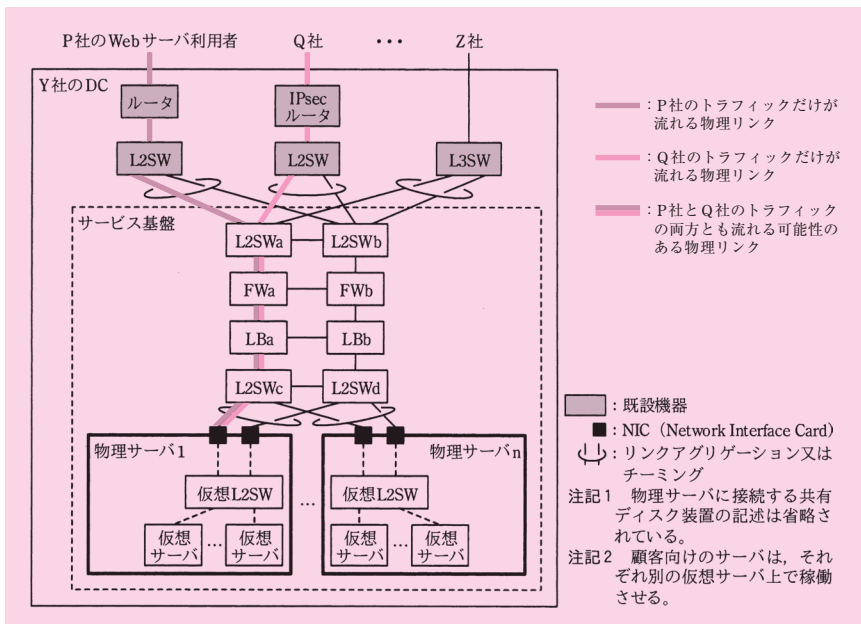
先ほど「●物理サーバ 1 だけ着目する理由」で解説したとおり、L2SWc と物理サーバ

バ間の物理リンクは、全ての顧客のトラフィックが流れる可能性がある。

したがって、ポート VLAN を設定するポートは、この区間には存在しない。

## ●解の導出

インターネットから物理サーバに至る全区間にわたり、P 社と Q 社のトラフィックをを整理すると、次の図のとおりとなる。



図：P 社、Q 社のトラフィック

この区間の中で、ポート VLAN を設定する物理ポートとして、次のものを導き出した。

- 顧客の L2SW, L3SW に接続している L2SWa のポート

ただし、これはアクティブの経路だけを考察したときのものである。シンプルに考えるためにいったん考察の対象から外した、L2SWb も解答に含める必要がある。

- 顧客の L2SW, L3SW に接続している L2SWb のポート

この点を指定字数に収まるように解答すればよい。  
よって、正解は解答例に示したとおりとなる。

## ■設問 5

本設問は、「技術習得を目的とした制御方式の設計」について問うている。

### (1)

#### 解答例

発生する可能性 がある問題	:	物理サーバ3の障害によって、3顧客のシステムが同時に停止してしまう。	(34字)
仮想サーバの 配置	:	3顧客向けの仮想サーバを、それぞれ異なった物理サーバに配置する。	(32字)

問題文は、「本番システムにおいて、図4の形態で3顧客の仮想サーバを配置した場合に発生する可能性がある問題を……述べよ。また、その問題を発生させないための仮想サーバの配置を……述べよ」と記述されている。

図4は、「技術習得を目的とした制御方式の設計」の第2段落の下にある。

仮想サーバは、図4中の物理サーバ1～物理サーバ3に配置されている。

本小問は「発生する可能性がある問題」、及び「その問題を発生させないための仮想サーバの配置」を問うている。

では、いったいどのような観点から問題を指摘すればよいのだろうか。

「機能の観点なのか？それとも非機能の観点なのか？」「仮に非機能だとして、より具体的にはどの観点なのか……信頼性？性能？セキュリティ？」……様々な観点が思い浮かぶかもしれないが、どのようにアプローチするのが有効なのだろうか。

そこで、まずは、有効な解答アプローチについて解説する。次いで、そのアプローチに従って解を導こう。

#### ●有効な解答アプローチ

本書の序章0.4節は、午後Ⅱの解答テクニックを紹介している。

「0.4.6 問題を解く—できる限り、本文事例に特化した解を書く—」の第1段落で、次のように述べている。

午後Ⅱ試験は事例解析ですから、本文事例に特化した解を導くように心掛けてください。

この解答テクニックに基づき、次の順序でアプローチしてみよう。

- ①本文に示された要件，設計等に基づいて考察する。
- ②一般的な知識に基づいて考察する。

項番①のアプローチを具体的に説明しよう。

例えば、「本事例に示された要件を満たしているか？」という妥当性確認 (validation) の観点で考察できる。他には、「本事例に示された設計や構築に技術的な欠陥がないか？」という検証 (verification) の観点から考察できる。

要件を満たしていなかったり、技術的な欠陥があったりしたら、これを「問題」ととらえ、解を導いていく。

一方、本文に明記された要件を十分に満たしており、しかも本文に与えられた情報から具体的な欠陥を見出せないとき、項番②に進む。

項番②は、いわば最後の手段である。本来であれば、要件又は欠陥として指摘されるべき問題が、本文に示唆されていない。これを掘り起こして具体的に解答することを出題者は求めているのだ。

もしも項番②のアプローチで得られる解があるならば、それはあらゆる別解に反駁でき、その正解を見れば技術者が一様に首肯せざるを得ないような、「至極当然の一般的な問題点」であるはずだ。

試験である以上、そのように作問されていなければならない。

### ●解の導出：発生する可能性がある問題点

まず、「発生する可能性がある問題」について解を導こう。

項番①のアプローチから着手する。

本事例の要件は、序文の第3段落の中に次のように記述されている。

- (1) サーバの仮想化によって、サーバ増設要求に迅速に対応可能とすること
- (2) サービス基盤で稼働する顧客システムは、顧客ごとに論理的に独立させること
- (3) サービス基盤は冗長構成とし、サービス停止を極力抑えられるようにすること



図 4 を見れば明らかなが、サーバが仮想化されており、顧客ごとにネットワークは独立しているので、要件 (1), (2) は満たしている。

注目すべきは、要件 (3) 「サービス基盤は冗長構成とし、サービス停止を極力抑えられるようにすること」という点である。

図 4 の物理サーバに障害が発生したとき、仮想サーバは残った物理サーバに移動する。つまり、物理サーバの「冗長構成」は満たしている。

それでは、「サービス停止を極力抑えられるようにすること」という点は満たしているだろうか。

ここで、本文全体の文脈に基づいて整理してみよう。

〔SDN 方式でのサービス基盤の構成案〕に示された構成は、前記の要件を満たすように設計し、かつ、その設計には技術的な欠陥がないはずである。さもないと、〔二つの方式の比較〕のレビューを受けた時点で指摘されるに違いない。

SDN 方式が選ばれた以上、少なくとも、図 3 「OF によるサービス基盤の構成案」に問題はない。

一方、本小問が取り上げている図 4 には、何らかの問題がある（それを答えようとしている）。

つまり、図 3 から図 4 へ変化したときに、要件 (3) の「サービス停止を極力抑えられるようにすること」に関して、問題が発生したと考えられる。

二つの図の相違点として、すぐ目につくのは物理サーバの台数だろう。図 3 は  $n$  台あるが、図 4 は 3 台しかない。

本小問で問われているのは「図 4 の形態で 3 顧客の仮想サーバを配置した場合に発生する可能性がある問題」である。それゆえ、台数の減少だけではなく、そこからさらに踏み込んで、仮想サーバの配置の観点から変化を見出さなければならない。

残念ながら、図 3 には仮想サーバの配置が具体的に書かれていない。さすがに、ただ単に図を見比べただけでは分らない。

とはいえ、台数が少なくなったことを踏まえ、図 4 を改めて見つめ直してみよう。すると、「1 台の物理サーバに、異なる顧客の仮想サーバを配置する」という、余裕がない状況へと変化したことに気が付くはずだ。

それが顕著に現れているのが、物理サーバ 3 である。そこには、P 社、Q 社、Z 社の仮想サーバが配置されている。

もし物理サーバ 3 に障害が発生したらどうなるだろうか。

果たして、要件 (3) の「サービス停止を極力抑えられるようにすること」という要件を満たすことができるだろうか。

一般的に言って、「サービス停止」を抑えることは、二つの観点から実現する必要がある

ある。

一つ目は「時間」であり、サービス停止の時間をできるだけ短くすることである。

二つ目は「範囲」であり、サービス停止の範囲をできるだけ局所化することである。

物理サーバに障害が発生したら、仮想サーバは別の物理サーバに移動する。この仕組みは、図 3 も図 4 も変わりがない。図 3 は要件を満たしているのだから、図 4 も同じだ。それゆえ、時間の観点では要件 (3) を満たしている。

一方、図 4 の物理サーバ 3 に障害が発生したら、その影響が顧客全体（顧客 3 社）に及んでしまう。それゆえ、範囲の観点から考察すると、要件 (3) を満たしていないことが分かる。

したがって、このように仮想サーバを配置する設計には、サービス停止の観点から問題があると言える。

よって、「発生する可能性がある問題点」の正解は、「物理サーバ 3 の障害によって、3 顧客のシステムが同時に停止してしまう」となる。

なお、項番①のアプローチで解が得られたので、項番②を試みる必要はない。

### ●解の導出：仮想サーバの配置

次に、「その問題を発生させない仮想サーバの配置」について解を導こう。

ここで心に留めておきたいことがある。それは、解を導こうとするあまり、「条件を読み落としてたり、自分勝手に条件を加えたりしない」ようにすることだ（序章「0.4.6 問題を解く—できる限り、本文事例に特化した解を書く—」の応用テクニック No. 5）。

ここでは、図 4 に示された物理サーバの台数のままで、仮想サーバの配置を考え直す必要がある。だから、「物理サーバの台数を増やす」など、自分勝手に条件を加えないように留意したい。

本小問で問題視されているのは、障害発生の影響範囲であった。

したがって、各顧客の仮想サーバをそれぞれ異なった物理サーバに配置すれば、1 台の物理サーバに障害が発生しても、その範囲を 1 社にのみ抑えることができる。

幸いにも、物理サーバは顧客の数だけあるので、ぎりぎり対処できる。

よって、「仮想サーバの配置」の正解は、「3 顧客向けの仮想サーバを、それぞれ異なった物理サーバに配置する」となる。

## (2)

## 解答例

F	W	p	の	内	部	側	ポ	ー	ト	と	L	B	p	の	仮	想	I	P	ア	ド	レ	ス	を	も	つ	ポ	ー	ト
は	,	同	一	セ	グ	メ	ン	ト	で	あ	り	,	物	理	サ	ー	バ	3	内	で	処	理	さ	れ	る	か	ら	

(57 字)

問題文は、「表 8 の F テーブル 4 中には、FWp の内部側のポートから LBp の仮想 IP アドレスをもつポートに、パケットを転送させるための F エントリが生成されない。当該 F エントリがなくても FWp と LBp 間の通信が行われる理由を……述べよ」と記述されている。

## ●問題文の整理

本小問が問うていることは、端的に言うと、「F エントリがなくても FWp と LBp 間の通信が行われる理由」である。

「F エントリがない」とは、入力されたパケットにマッチングする条件がないということを示している。

F エントリがないときの処理について、「技術習得を目的とした制御方式の設計」の第 6 段落には、「どのマッチング条件にも一致しないパケットは廃棄される」と記述されている。

それでは、「FWp の内部側のポートから LBp の仮想 IP アドレスをもつポートに、パケットを転送させる」という条件を満たすパケットが OFS に入力されたならば、すなわち、OFS を経由したならば、このパケットはどうなるだろうか。

マッチング条件に合致する「F エントリ」が F テーブル 4 にないわけだから、このパケットは廃棄されてしまう。つまり、FWp と LBp 間の通信が途絶するのだ。

ここまで述べたことを整理すると、次のことが分かる。

- FWp から LBp 宛てのパケットが OFS を経由したならば、FWp と LBp 間の通信はできない。

この対偶を取ると、次のように言える。

- FWp と LBp 間の通信ができるならば、FWp から LBp 宛てのパケットは OFS を

経由しない。

問題文は「FWp と LBp 間の通信が行われる」と述べているので、「FWp から LBp 宛てのパケットは OFS を経由しない」ことが分かる。

さて、本小問は「FWp と LBp 間の通信が行われる理由」を問うていた。

これまでの考察から OFS を経由しないことは分かったが、通信が行われる理由の説明としては不十分だ。

具体的にどの経路を通るのかを示すことにより、その理由をきちんと説明することができる。すなわち、解を導いたことになる。

では、「FWp と LBp 間の通信」は、どの経路を通るのだろうか。

問題文に合わせ、「FWp の内部側のポートから LBp の仮想 IP アドレスをもつポートを宛先とする通信」を取り上げ、具体的に考察しよう。

#### ● FWp の内部側のポートから LBp の仮想 IP アドレスをもつポートを宛先とする通信の経路

図 4 のネットワーク構成は、図 1 のネットワーク構成を SDN 方式で実現したものである。論理的に見て両者は等価である。

図 1 の P 社のネットワーク構成を見ると、三つのサブネットに分かれていることが分かる。

[サブネット 1] ルータ, FWp (WAN 側) に挟まれた区間

[サブネット 2] FWp (内部側), LBp (WAN 側) に挟まれた区間

[サブネット 3] LBp (内部側), Web サーバ p1 ～ p4 に挟まれた区間

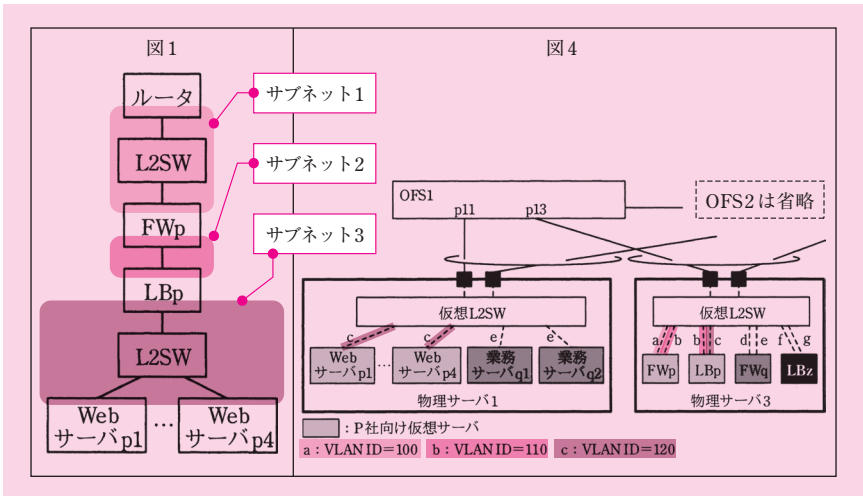
図 4 の P 社の VLAN は、これら三つのサブネットと 1 対 1 に対応している。

VLAN100 (図 4 中の a) は FWp にのみ接続しているから、サブネット 1 に対応していることが分かる。

VLAN110 (図 4 中の b) は FWp, LBp に接続しているから、サブネット 2 に対応していることが分かる。

VLAN120 (図 4 中の c) は LBp, Web サーバ p1 ～ p4 に接続しているから、サブネット 3 に対応していることが分かる。

これまで述べた内容を整理すると、次の図のとおりとなる。



図：図 1 のサブネットと図 4 の VLAN の対応

それでは、「FWp の内部側のポートから LBp の仮想 IP アドレスをもつポートを宛先とする通信」は、どのサブネットの中でやり取りされているのだろうか。

FWp の内部側のポートは、図 1 から明らかなおとおり、サブネット 2 側にある。

LB の仮想 IP アドレスをもつポートは、設問 1 空欄ウの解説で示した図「通常の LB の仮想 IP アドレスの設定、負荷分散対象のサーバ群の設置（図 1 の P 社の例）」から分かったとおり、LB の WAN 側のポートである。これはサブネット 2 側にある。

要するに、この通信は、サブネット 2 の中で閉じているのだ。

図 4 において、サブネット 2 は VLAN110（図 4 中の b）である。それゆえ、物理サーバ 3 の内部にある仮想 SW を経由すれば、FWp と LBp 間の通信が行える。

したがって、FWp の内部側のポートから LBp の仮想 IP アドレスをもつポートを宛先とする通信は、物理サーバ 3 の内部で転送されていることが分かる。

### ● FWp の内部側のポートから LBp の仮想 IP アドレスをもつポートを宛先とする通信の経路

本小問が問うているのは、FWp と LBp 間の通信が行われる理由であった。

その理由は、この通信が同一サブネット内で行われており、物理サーバ 3 の内部で転送されているからである。

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

## (3)

## 解答例

- オ F テーブル名 : F テーブル 1  
項番 : 2
- カ F テーブル名 : F テーブル 0  
項番 : 6
- キ F テーブル名 : F テーブル 4  
項番 : 6

問題文は、次のように記述されている。

P 社の Web サーバ利用者から送信された、Web サーバ宛てのユニキャストパケットが Web サーバ p1 に転送されるとき、パケットの転送は、次の【パケット転送処理手順】となる。

## 【パケット転送処理手順】

ルータ → L2SW → F テーブル 0, 項番 1 →  → FWp → LBp →  
 →  → Web サーバ p1

【パケット転送処理手順】中の  ～  に入れる適切な F テーブル名と項番を答えよ。F テーブル名は、F テーブル 0 ～ 4 から選べ。また、項番は表 4 ～ 8 中の項番で答えよ。ここで、パケット転送制御を行う OFS は特定しないものとする。

インターネットから P 社の Web サーバにアクセスする通信は、設問 1 空欄ウで解説したとおり、パケットの宛先 IP アドレスが、P 社の LB の WAN 側ポートに設定された仮想 IP アドレスとなる。

その後、LB によって Web サーバ p1 に転送されるとき、パケットの宛先 IP アドレスが、転送先となる Web サーバ p1 のものとなる。

したがって、【パケット転送処理手順】の経路は、宛先 IP アドレスの観点から二つに分けることができる。

## [経路 1]

宛先 IP アドレス	LB の WAN 側ポートの仮想 IP アドレス
経路	ルータ→L2SW→F テーブル 0, 項番 1→ <input type="text" value="オ"/> →FWp→LBp

## [経路 2]

宛先 IP アドレス	Web サーバ p1 の IP アドレス
経路	LBp→ <input type="text" value="カ"/> → <input type="text" value="キ"/> →Web サーバ p1

ルータから Web サーバ p1 までの区間は、設問 5 (2) で解説したとおり、サブネット 1 (VLAN100)、サブネット 2 (VLAN110)、サブネット 3 (VLAN120) の三つの VLAN に分割される。具体的に言うと、FWp を境にサブネット 1 とサブネット 2 に分割され、LBp を境にサブネット 2 とサブネット 3 に分割される。

したがって、【パケット転送処理手順】の経路は、宛先 IP アドレス及びサブネットの観点から三つに分けることができる。

## [経路 1-1]

宛先 IP アドレス	LB の WAN 側ポートの仮想 IP アドレス
VLAN	100
経路	ルータ→L2SW→F テーブル 0, 項番 1→ <input type="text" value="オ"/> →FWp→LBp

## [経路 1-2]

宛先 IP アドレス	LB の WAN 側ポートの仮想 IP アドレス
VLAN	110
経路	FWp→LBp

## [経路 2]

宛先 IP アドレス	Web サーバ p1 の IP アドレス
VLAN	120
経路	LBp→ <input type="text" value="カ"/> → <input type="text" value="キ"/> →Web サーバ p1

[経路 1-2] は、設問 5 (2) で解説したとおり、OFS を経由しない。

空欄オは [経路 1-1] に、空欄カ～キは [経路 2] に含まれている。経路ごとに解を導いていこう。

なお、問題文に「パケット転送制御を行う OFS は特定しないものとする」とあるので、OFS1、OFS2 のどちらであるかは問われていない。サービス基盤は冗長化されて

いるので、パケットは OFS1 又は OFS2 のどちらかに入力されるが、どちらであろうと選択される F テーブルの項番は同じである。したがって、解答に差異がないことから、問題文はこのように述べているのである。

そこで、解説でも OFS を特定せず、単に「OFS」と称することにする。

### ●解の導出：空欄オ

ここでは、[経路 1-1] を考察する。

LB の仮想 IP アドレスを宛先とするパケットは、ルータから FW に向けて転送される。その宛先 MAC アドレスは、FW の WAN 側ポートの MAC アドレス「mFWpw」となる。

このパケットが、OFS のポート p1 から入力される。このとき、OFS の F テーブル 0 において、項番 1 のマッチング条件に基づき、アクションが実行される。

表：F テーブル 0 (抜粋)

項番	マッチング条件	アクション
1	入力ポート = p1	F テーブル 1 で定義された処理を行う。

※アクションは、解の導出に必要な内容だけ抜粋している。

次いで、F テーブル 1 において、項番 2 のマッチング条件に基づき、アクションが実行される。

表：F テーブル 1 (抜粋)

項番	マッチング条件	アクション
2	mDes = mFWpw	p13 から出力

よって、空欄オの解は、「F テーブル 1, (項番) 2」となる。

### ●解の導出：空欄カ、キ

ここでは、[経路 2] を考察する。

Web サーバ p1 の IP アドレスを宛先とするパケットは、LB の内部側ポートから Web サーバ p1 に向けて転送される。その宛先 MAC アドレスは、Web サーバ p1 の MAC アドレス「mWSp1」となる。

このパケットが、OFS のポート p13 から入力される。このとき、OFS の F テーブル 0 において、項番 6 のマッチング条件に基づき、アクションが実行される。



表：F テーブル 0（抜粋）

項番	マッチング条件	アクション
6	入力ポート = p13	F テーブル 4 で定義された処理を行う。

よって、空欄カの解は、「F テーブル 0、(項番) 6」となる。

次いで、F テーブル 4 において、項番 6 のマッチング条件に基づき、アクションが実行される。

表：F テーブル 4（抜粋）

項番	マッチング条件	アクション
6	mDES = mWSp1	p11 から出力

よって、空欄オの解は、「F テーブル 4、(項番) 6」となる。

#### (4)

##### 解答例

OFS 名：OFS1, OFS2

項番：7

変更後のアクション：p12 から出力

問題文は、次のように記述されている。

P 社の Web サーバ p4 が物理サーバ 2 に移動し、表 7 の OFS1 の F テーブル 3 中の項番 5 によって、OFC に Packet-In メッセージが送信されると、OFC は表 8 の F テーブル 4 中の二つの項番を変更する。F テーブル 4 が変更される OFS 名を全て答えよ。また、項番 3 のほかに変更される項番及び変更後のアクションを答えよ。

本小問は二つのことを問うている。

一つ目は、F テーブル 4 が変更される OFS 名である。

二つ目は、F テーブル 4 の項番 3 のほかに変更される項番及び変更後のアクションである。

本小問の解を導くには、P 社の Web サーバ p4 が物理サーバ 2 に移動したときの一連の動作について理解する必要がある。そこで、この点についてまずは解説する。

### ● P 社の Web サーバ p4 が物理サーバ 2 に移動したときの動作

冒頭の「● SDN 技術」の「・アドレス学習」で解説したとおり、OFC はパケット入力を契機にアドレス学習を行っている。そして、学習した内容に基づいて、OFS の F エントリを登録している。

したがって、P 社の Web サーバ p4 が物理サーバ 1 から物理サーバ 2 に移動したとき、OFC が行うべきことは、アドレス学習、及び、それに基づく F エントリの登録である。

この移動に呼応して、サブネット内の全ての L2SW がアドレス学習を行うには、次に示すパケットが、移動先である物理サーバの仮想 L2SW から送信されなければならない。

宛先 MAC アドレス	送信元 MAC アドレス
FF-FF-FF-FF-FF-FF	mWSp4

宛先 MAC アドレスが「FF-FF-FF-FF-FF-FF」である理由は、サブネット全域の L2SW に到達させるためである。送信元 MAC アドレスが「mWSp4」である理由は、「入力ポートの先に送信元のホストがある」と学習するからである。

このパケットのイーサネットタイプは、アドレス学習以外に特別な副作用がないものが選ばれる。参考までに、VMware 社の場合、仮想サーバの移動に伴うこのアドレス学習を行わせるパケットは、イーサネットタイプが「RARP」である<sup>(\*)</sup>。

(\*) RARP (Reverse ARP) は、ARP フレームと同じ構造をもつ。RARP は、解決したいアドレスが ARP の逆であり、MAC アドレスに基づいて IP アドレスを取得するために用いられる。とはいえ、ここでは、ブロードキャストドメイン内の各スイッチのアドレス学習テーブルを更新する目的で送信されている。RARP サーバ以外のホストは、RARP パケットを受信すると、ただ単にこれを破棄するだけである。要するに、ホストに対して何ら副作用をもたらさない無害なパケットである。

RARP パケットを用いてアドレス学習テーブルを更新する様子を、

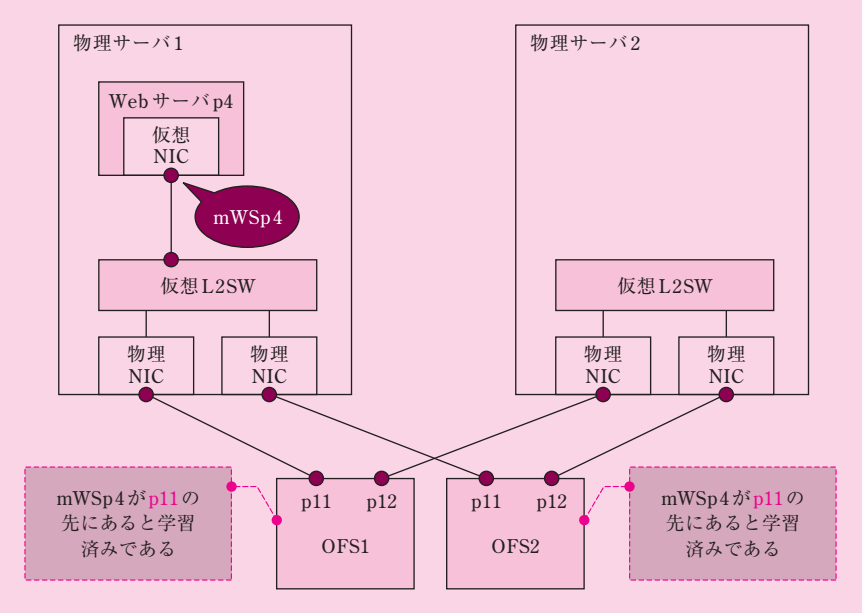
- ① Web サーバ p4 の移動前
- ② Web サーバ p4 の移動後 (RARP 送信前)
- ③ Web サーバ p4 の移動後 (RARP 送信後)

の順に、図を使って解説しよう。

これから述べる OFS の動作は、OFS1 と OFS2 の双方に当てはまるので、単に OFS と称することにする。

① Web サーバ p4 の移動前

移動前には、物理サーバ 1 上で Web サーバ p4 が稼働している。このとき、OFS は、「mWSp4 が p11 の先にある」と学習済みである。



図：Web サーバ p4 の移動前

ここで、OFS が学習済みであると述べたが、実際には OFC が学習している。冒頭の「●SDN 技術」の「・アドレス学習」で解説したとおり、OFS は Packet-In メッセージを OFC に送信することにより、OFC が学習できるようにする。OFC はこの学習内容に基づく F エントリを登録する。この結果、次回以降は、OFS がこの学習内容に基づいてパケットを転送できる。

表 8 の F テーブル 4 において、物理サーバ 1 に Web サーバ 4 が配置されているという学習内容と調和する F エントリは、次のとおりである。

表：F テーブル 4 (抜粋)

項番	マッチング条件	アクション
7	mDES = mWSp4, mSRC = mLbP	p11 から出力

さらに、Web サーバ p4 は VLAN120 に所属することから、次に示す F エントリも、この学習内容と調和したものとなっている。

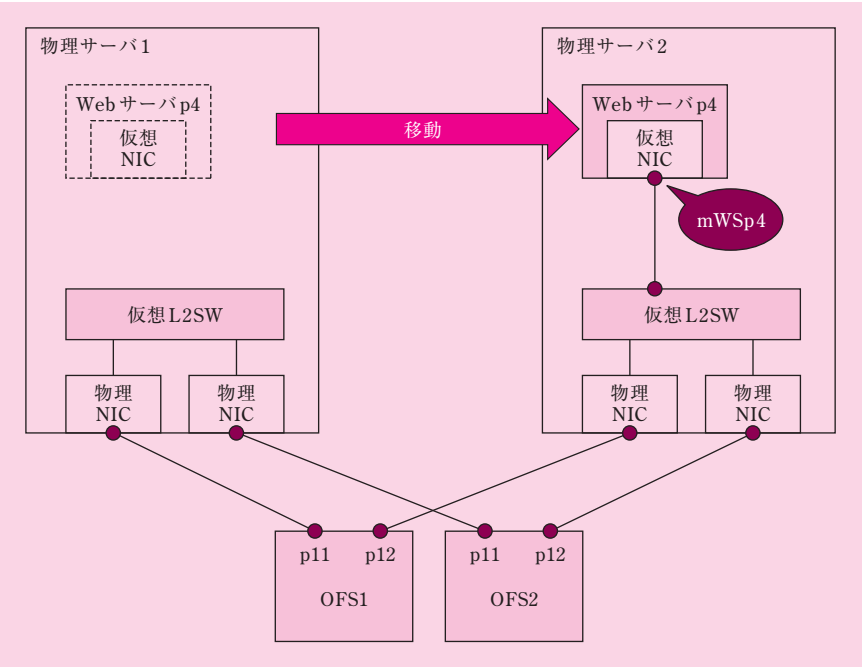
表：F テーブル 4（抜粋）

項番	マッチング条件	アクション
3	eTYPE = ARP, VLAN ID = 120, mDES = FF-FF-FF-FF-FF-FF	p11 から出力

② Web サーバ p4 の移動後（RARP 送信前）

Web サーバ p4 が移動した直後は、依然として、「mWSp4 が p11 の先にある」と学習したままである。

このままでは、Web サーバ p4 を宛先とするパケットを物理サーバ 1 に転送してしまう。さらに、VLAN120 の ARP パケットは物理サーバ 1 にだけ転送されてしまう。



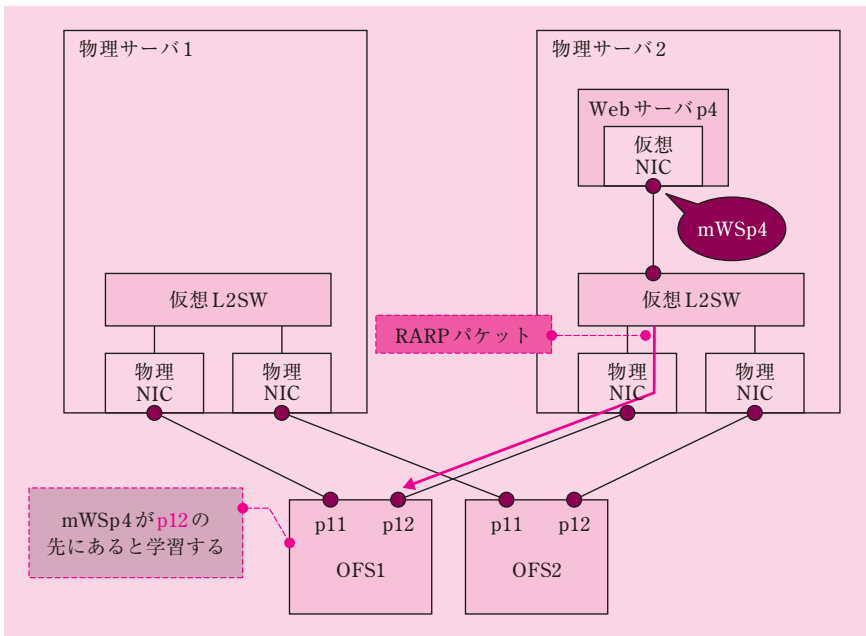
図：Web サーバ p4 の移動後（RARP 送信前）

### ③ Web サーバ p4 の移動後 (RARP 送信後)

送信元 MAC アドレスを mWSp4 とする RARP パケットが、物理サーバ 2 内の仮想 L2SW から送信される。この結果、OFS は、「mWSp4 が p12 の先にある」と新たに学習する。

物理サーバの 2 枚の NIC には、アクティブ/アクティブのチーミングが設定されている（設問 1 空欄エ）。1 個のパケットが通る NIC は、チーミングの負荷分散アルゴリズムに従って、2 枚のうちどちらか一方が逐次選択される。

したがって、この RARP パケットは、OFS1 又は OFS2 のどちらかに入力される。パケット入力を契機とする F エントリのアクションは、入力された OFS が行う。この点について、問題文を読むと、アクションを実行した OFS が「OFS1」であることが分かる。



図：Web サーバ p4 の移動後 (RARP 送信後)

繰り返しになるが、実際に学習しているのは、OFS ではなく OFC の方だ。

OFS（本小問では OFS1）は、物理サーバ 2 から RARP パケットが入力されたことを契機に、Packet-In メッセージを OFC に送信する。

このアクションは、問題文中の「表 7 の F テーブル 3 中の項番 5」の F エントリに

基づいている。そのように言える理由は、表 7 の注記に、「項番 5 は、仮想サーバが物理サーバ 2 に移動してきたことを OFC に知らせるための F エントリである」と述べられているからだ。

表：F テーブル 3（抜粋）

項番	マッチング条件	アクション
5	eTYPE = RARP	OFC に Packet-In メッセージを送信

これにより、OFC は、「物理サーバ 2 に Web サーバ p4 が配置されている」ことを学習する。

次いで、この学習内容と調和させるため、OFC は、「OFS1 及び OFS2」の F エントリを変更する。RARP パケットを受信したのは 1 台の OFS であるが、学習内容に基づく転送は全ての OFS が行わなければならないからだ。

本小問で問われているのは、表 8 の F テーブル 4 なので、この F テーブルに的を絞って解説を続けよう。

まず、F テーブル 4 の項番 7 は、ポート番号を「p11」から「p12」に変更しなければならない。

表：変更後の F テーブル 4（抜粋）

項番	マッチング条件	アクション
7	mDES = mWSp4, mSRC = mLBp	p12 から出力

次に、VLAN120 の ARP パケットを物理サーバ 1 と物理サーバ 2 に転送するため、F テーブル 4 の項番 3 は、ポート番号を「p11」から「p11, p12」に変更しなければならない。

表：変更後の F テーブル 4（抜粋）

項番	マッチング条件	アクション
3	eTYPE = ARP, VLAN ID = 120, mDES = FF-FF-FF-FF-FF-FF	p11, p12 から出力

以上が、P 社の Web サーバ p4 が物理サーバ 2 に移動したときの一連の動作である。

### ●解の導出：F テーブルが変更される OFS 名

これまで解説したとおり、Web サーバ p4 が物理サーバ 2 に移動したとき、OFS の F テーブルが変更される。これは、OFS1 と OFS2 の双方で行われなければならない。

よって、正解は、「OFS1, OFS2」となる。

- 解の導出：F テーブル 4 の項番 3 のほかに変更される項番及び変更後のアクション  
これまで解説したとおり，移動によって，F テーブル 4 の項番 3 と項番 7 の F エン  
トリが変更される。

項番 7 の F エントリのアクションは，「p12 から出力」である。

よって，正解は次のとおりとなる。

項番：7

変更後のアクション：p12 から出力