平成 29 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

ディジタルビジネスや IoT に関連した情報システムが注目されている。クラウドサービスを利用したり SDN（Software-Defined Networking）技術を活用したりする事例も増えている。これらの新しい概念やサービス，技術について，一部の研究開発者だけではなく，一般のネットワーク技術者にも正しい理解と応用力が求められる時代になっている。

本問では，ネットワークの拡張を題材に，自社設備を用いたネットワークと Web システムが，SDN とクラウドサービスの活用によってどのように変わるのかを解説している。従来のネットワーク技術の知識を用いて，SDN とクラウドサービスの基本的概念や技術が理解できること，それらと VLAN や TCP/IP，DNS を組み合わせたネットワークシステム全体が理解でき，さらに，その基本設計ができることについて問うている。

採点講評

問 1 では，SDN（Software-Defined Networking）とクラウドサービスを使ったネットワークの拡張を題材に，SDN，IaaS，CDN（Content Delivery Network）の基本的理解と，VLAN，TCP/IP，DNS などの基本技術の応用について出題した。

設問 1 は，TCP/IP と SDN の基本概念について問うた。正答率は高かった。

設問 2 は，TCP コネクション確立の通信フローを例に SDN の動作について問うた。正答率は高く，SDN に関する理解が高いことがうかがわれた。その中で(2)～(4)では誤った解答が目立った。これらは，“パケット識別条件”と“Action”を定義したり読解したりする問題である。本文中に示された条件をよく読み，SDN の定義によって通信フローがどのように変化するかについて復習しておいてほしい。

設問 3 は，DNS を使ったネットワークの切替えについて問うた。正答率が低い問題が複数あった。(1)では DNS の正しい知識が必要である。(4)，(5)では，それに加え CDN を使ったネットワークの動作について理解することが必要となる。これらは，ネットワークサービス利用の際に有用な技術の一例であり，十分に理解しておいてほしい。

設問 4 は，バックアップ対策を例に，SDN とクラウドサービスを使ったネットワークの運用について問うた。正答率は低かった。(3)では，自社要員だけで構成変更ができるようになることに気付いてほしかった。(4)では，準備作業全体を答えるのではなく一部の切替え作業手順を述べた解答が目立った。(5)では，IaaS 利用とネットワーク運用業務のアウトソーシングを混同する解答が目立った。本文の“内部 NW”と“IaaS 環境”はともに仮想化されたネットワークであり，“OFC の管理ソフトウェア”と“API サービス”を使った運用が行われる。本文のようなプロジェクト発足時には，新ネットワークの運用について明確な指針をもつことが大切である。ネットワークの仮想化やサービスの利用によって，運用業務も変化することを理解しておいてほしい。

設問		解答例・解答の要点		備考
設問 1		あ	i1	
		い	NAT	
		う	i3	
		え	Flow-Mod	
		お	controller	
		か	Packet-Out	
		き	OFS2	
		く	p9	
設問 2	(1)	け	v2	
		こ	なし	
		さ	m2	
		し	m3	
		す	i4	
	(2)	②，⑧，⑨，⑩		
	(3)	ETH_TYPE が ARP のイーサネットタイプに等しい。		
	(4)	外部 NW 内の RT-1 と新 FW の通信		
	(5)	せ	p6	
		そ	なし	
		た	m1	
		ち	m2	
	(6)	Push-VLAN，Set-Field VLAN_VID = v2，Output（p7）		
設問 3	(1)	つ	CNAME	
	(2)	webtest.asha.example.com		
	(3)	weblive.asha.example.com		
	(4)	DNS クライアントと DNS フルリゾルバが，ネットワーク上で離れた位置にある場合		
	(5)	①	・Web-B のサーバ処理能力不足	
		②	・機械と Web-B 間の通信遅延	
設問 4	(1)	転用後の業務サーバの IP アドレスを，LB の振り分け先に追加しておく。		
	(2)	置換え前	weblive IN A i6	
		置換え後	weblive IN A i1	
	(3)	①	・転用する業務サーバに関する物理配線の変更が不要になる。	
		②	・管理ソフトウェアを用いて，社内要員だけで対応できる。	
	(4)	CDN，ISP，IaaS 環境の構築と切替えに関する，API サービスと DNS を使った手順の確立		
	(5)	①	・国外を利用するので国内の広域災害の影響を回避できる。	
		②	・B 社 CDN などを使い通常時と同じ品質を保つことができる。	

本問は，SDN（Software-Defined Networking）とクラウドを活用した，ネットワーク拡張の事例を取り上げている。

本問は，SDN 技術として OpenFlow を活用した社内ネットワークの構築，クラウドサービスの CDN（Content Delivery Network）を活用した Web アクセスの高速化，クラウドサービス拠点の IaaS 環境の DR（Disaster Recovery）について問うている。

●本問の全体像

・ネットワーク拡張の概要

A 社は，国内外に顧客をもつ生産機械メーカである。

顧客の拠点で稼働中の生産機械（以下，機械という）は，国内外に多数ある。

目下，IoT 時代に適応するために，新たな情報システム基盤を整備中である。主に二つの変更を行う予定である。

［変更点 1］SDN 技術を活用した自社工場の LAN の刷新
［変更点 2］クラウドサービスを活用した，新たな情報システム基盤の開発

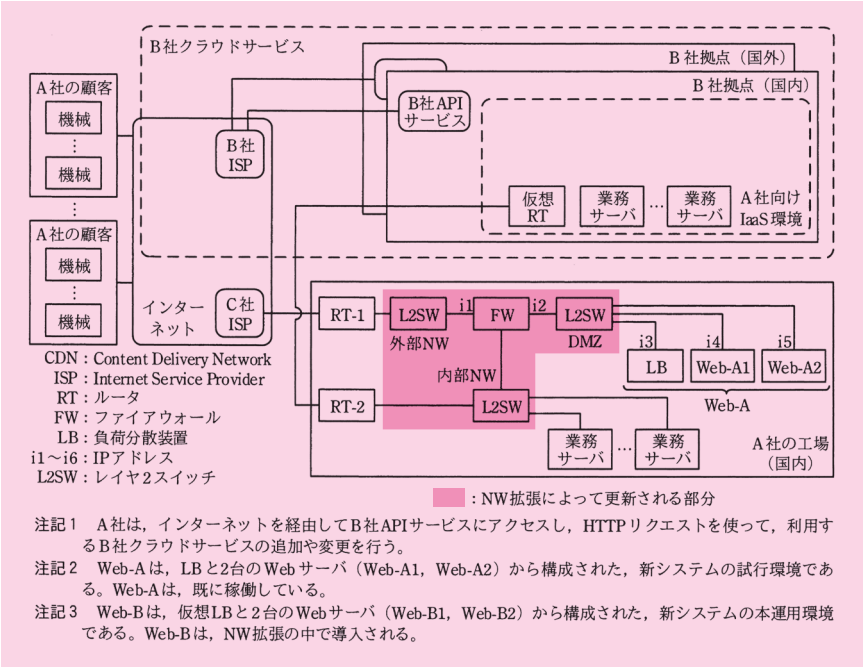
この変更は，ネットワーク（以下，NW）を拡張することによって実現する。

今このタイミングで，本文中で用いられている略称を紹介しておこう。以降の解説は，本文に倣ってこの呼称を使用する。

本文は，新たな工場 LAN を「新工場 LAN」，新たな情報システム基盤を「新システム」と呼んでいる。そして，NW の拡張を「NW 拡張」と呼んでいる。

本文の図 1「NW 拡張の概要（抜粋）」には，現行 NW に対する拡張の概要が示されている。この図 1 から，「NW 拡張によって追加される部分」（図の点線枠内の網掛け部分）を除いたものが，現行 NW の構成である。

それでは，現行 NW の構成を次の図に示す。



注記1　A社は，インターネットを経由してB社APIサービスにアクセスし，HTTPリクエストを使って，利用するB社クラウドサービスの追加や変更を行う。
注記2　Web-Aは，LBと2台のWebサーバ（Web-A1，Web-A2）から構成された，新システムの試行環境である。Web-Aは，既に稼働している。
注記3　Web-Bは，仮想LBと2台のWebサーバ（Web-B1，Web-B2）から構成された，新システムの本運用環境である。Web-Bは，NW拡張の中で導入される。

図：現行 NW の構成（図 1 より作成）

序文の第 2 段落は，現行 NW の構成について説明している。その内容を整理すると次のようになる。

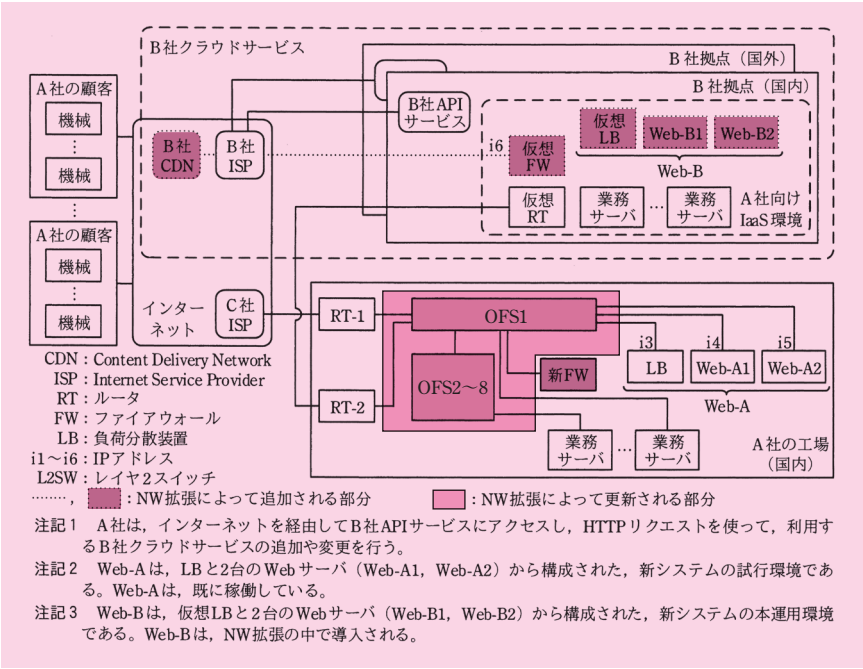
- 国内工場の自社設備と，国内外にサービス用拠点をもつクラウドサービス事業者 B 社の IaaS 環境で構成されている。
- B 社の A 社向け IaaS 環境は国内にあり，工場とは専用線で接続されている。
- インターネットと工場とは，インターネットサービス事業者の C 社の国内拠点を介して接続されている。

この図の A 社工場 LAN に記された，「NW 拡張によって更新される部分」（図の網掛け部分）は，現在稼働している。NW 拡張により，この部分が，図 2「新工場 LAN の物理構成案（抜粋）」に示された「導入機器」で置き換えられる。

具体的に言うと，この部分に，SDN 機器（8 台の OFS，OFC），新 FW が導入される。

それでは，図 1 の更新部分を，SDN 機器と新 FW に置き換えたものを次の図に示す

（OFC は省略）。元の図 1 にある「NW 拡張によって追加される部分」もそのまま残しているので，要するにこの図が，新 NW の構成となる。



図：新 NW の構成（図 1，図 2 より作成）

大きな変更点は，新工場 LAN の SDN 化，新システムの追加の 2 点である。

新システムは，B 社クラウドサービスの枠内にある。新たに追加されるものは次のとおりである。

- B 社拠点（国内）の Web-B と仮想 FW
- B 社 CDN

NW 拡張の概要がつかめたところで，改めて，NW 拡張の目的を確認しておこう。

NW 拡張の目的が，序文の第 4 段落に記述されている。便宜上，［目的 1］［目的 2］と小見出しを掲げて，ここに引用する。

［目的 1］が一つ目の変更点，［目的 2］が二つ目の変更点に対応している。

［目的 1］工場 LAN の SDN（Software-Defined Networking）化
SDN 技術を用いて，現在の工場 LAN を，ビジネス変化に対応できる柔軟性と拡張性を備えた新たな工場 LAN（以下，新工場 LAN という）に刷新する。新工場 LAN では，物理配線の変更なしに，自社要員だけで構成変更ができるようにする。

［目的 2］クラウドサービスの利用拡大
開発中の新システムは，国内外の多数の機械に対する，ファームウェアの一斉更新，稼働状況の定期収集に用いられる。新システムの本運用のために，Web-A よりも大規模な Web-B を構築し，B 社クラウドサービス（図 1 中の B 社 CDN，B 社 ISP）を活用して，Web-A へのアクセス経路よりも高速な Web-B へのアクセス経路を実現する。

［目的 2］の中に，「Web-A」「Web-B」と呼ばれる二つの Web システムが登場する。

両システムについて，図 1 の注記 2，注記 3，序文の第 6 段落，及び，〔クラウドサービス利用拡大の検討〕の中で，順次説明されている。その内容を整理すると次のようになる。

試行環境
Web-A は，LB と 2 台の Web サーバ（Web-A1，Web-A2）から構成された，新システムの試行環境である。Web-A は既に稼働している（図 1 注記 2）。

本運用環境
Web-B は，仮想 LB と 2 台の Web サーバ（Web-B1，Web-B2）から構成された，新システムの本運用環境である。Web-B は，NW 拡張の中で導入される（図 1 注記 3）。
高負荷が予想されるときには，必要な期間だけ B 社 CDN を適用する（〔クラウドサービス利用拡大の検討〕の第 1 段落，4 番目の箇条書き）

機械から新システムへのアクセス
NW 拡張後は，B 社クラウドサービスを使って，機械から Web-B へアクセスが行われるようになる。機械は，Web-A へのアクセスと Web-B へのアクセスを切り換えられるようになっており，試行環境と本運用環境を使い分けながら，新システムの機能拡充を進めていく予定である（序文第 6 段落）。

A 社は NW 拡張を実施するためプロジェクトを発足させようとしている。その発足に先立ち，4 点の準備作業を行う。本問の中核をなしているのはこの 4 点であり，本文中の四つの見出しに対応している。

前述の二つの目的に照らして，この準備作業を整理すると，次のようになる。

表：二つの目的と準備作業

目的	準備作業（本文の見出し）
［目的 1］工場 LAN の SDN 化	新工場 LAN に適用する SDN 技術の調査
	新工場 LAN の運用の調査
［目的 2］クラウドサービスの利用拡大	クラウドサービス利用拡大の検討
（記載なし）	A 社向け IaaS 環境のバックアップの検討

4 番目の準備作業は，二つの目的と直に結び付くものではないが，A 社にとって，検討すべき重要な課題である。

この準備作業がなぜ必要となるのか，具体的にどのような内容であるのかについて，〔A 社向け IaaS 環境のバックアップの検討〕の中で説明されている。最後にこの点に触れて，NW 拡張の解説を終えることにしよう。

このたびの NW 拡張によって，A 社事業の，B 社クラウドサービスに対する依存度は高まっていく。それに加え，この見出しの第 1 段落に「A 社向け IaaS 環境へのサーバ移行を順次進めて（いる）」とあるので，依存度がますます高まっていくことが分かる。

こうした事情から，「A 社向け IaaS 環境が存在する B 社拠点（国内）が長時間使えないリスク」を想定し，バックアップ対策（以下，DR という）を検討する必要が生じたわけだ。

具体的には，次の 2 案について検討することとなった。詳しくは設問 4 で解説する。

DR 案

（1）自社設備利用 DR 案

（2）B 社拠点（国外）利用 DR 案

・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
なし（序文）	• NW 拡張の目的 • 図 1　NW 拡張の概要 • 試行環境（機械から Web-A へのアクセス）の概要	1	空欄 **あ～う**
新工場 LAN に適用する SDN 技術の調査	• SDN 技術の整理 • 図 2　新工場 LAN の物理構成案 • OFS 接続情報収集 • 図 3　OFS 接続情報収集の通信シーケンス例	1	空欄 **え～く**
新工場 LAN の運用の調査	• 新工場 LAN 運用のベンダ提案 • 図 4　新工場 LAN の論理構成（抜粋）と通信シーケンス例 • 図 4 中の通信シーケンスに関する，OFC と OFS の動作	2	(1) ～ (6)
クラウドサービス利用拡大の検討	• 本運用環境（B 社 CDN と B 社 ISP を利用した NW）の概要 • 図 5　B 社 CDN を A 社に適用したときの概念図 • 図 6　D 君が考えたエッジサーバへの切換え方法 • 図 5 と図 6 の概要	3	(1) ～ (5)
A 社向け IaaS 環境のバックアップの検討	• (1) 自社設備利用 DR 案 • (2) B 社拠点（国外）利用 DR 案	4	(1) ～ (5)

● SDN 技術の概要

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 は，OpenFlow 方式を若干簡略化したものである。OpenFlow 方式は，平成 25 年に続き 2 回目の出題である。

平成 25 年のときと同様，OpenFlow とい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。

本問における SDN 技術の出題は，設問 1，2 である。二つの設問にまたがっていることを考慮し，今ここで，概要を解説する。

さて，解説に先立ち，このような新技術を出題する趣旨を知っておくとよいだろう。その趣旨は，「従来の要素技術の知識をしっかり理解しているかどうか」「その知識を

応用して設計する能力があるかどうか」という点を評価するためである。そのように言える根拠について，詳しくは，本書の第 1 章の「1.1　午後試験の出題と試験対策のポイント」において「●試験対策のポイント」の「3. 新技術を用いた設計」で述べている。新技術が出題された過去問題の「出題趣旨」「採点講評」からそのことが分かるので，後ほど自分の目で確認してみることをお勧めしたい。

以下，〔新工場 LAN に適用する SDN 技術の調査〕の第 1 段落にある箇条書きを適宜引用しながら，そこに書かれている内容を解説していく。出題趣旨にたがわず，ITSS レベル 4 の技術力があれば，本問で初めて OpenFlow を知ったとしても十分解けるように配慮されていることを，本書の解説を通して実感していただきたい。

それでは，前置きはこれくらいにして，いよいよ SDN 技術の解説に移ろう。

・OFC と OFS

まず，本問で取り上げている SDN 技術の方式について，1 番目の箇条書きは次のように述べている。

> ・従来のスイッチ機能を，経路制御などの管理機能を実行するフローコントローラ（以下，OFC という）と，データ転送を行うスイッチ（以下，OFS という）に分け，OFS に入るパケットの経路制御を OFC が集中制御する方式を採用する。

ここに「OFS に入るパケットの経路制御を OFC が集中制御する」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。

［目的 1］に「新工場 LAN では，物理配線の変更なしに，自社要員だけで構成変更ができる」とあるが，OFS はまさにその目的を果たすのにうってつけの存在であると言えよう。

・OFC と OFS 間のメッセージ

この OFS は，OFC によって集中管理される。OFC がどのように管理するかについ

て，2 番目の箇条書きは次のように述べている。

> ・OFS と OFC は，管理のための専用 NW（以下，管理 NW という）を介して，通信メッセージを交換する。OFC と OFS 間の通信メッセージを表 1 に示す。

表：OFC と OFS 間の通信メッセージ（表 1 の抜粋）

通信メッセージ名	通信の方向	用途
Packet-In	OFS→OFC	入力パケットと入力ポート ID を，OFC に通知する。
Packet-Out	OFC→OFS	出力パケットと出力ポート ID を送り，OFS に出力させる。
Flow-Mod	OFC→OFS	変更情報を送り，OFS の管理テーブルを変更させる。

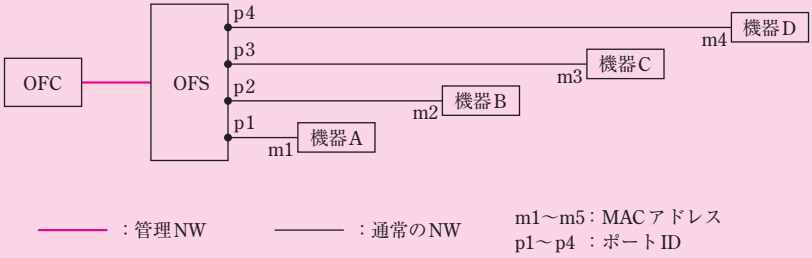
表 1 のメッセージはどのように使用されるのだろうか。

このまま本文を読み進めていき，図 4 と照らし合わせれば，必ずや理解できるに違いない。

とはいえ，今は説明を分かりやすくするため，あえて図 4 より簡単なネットワークを例に挙げることにする。ここで理解したことが後で図 4 の解析に活かせるように，図 4 中のメッセージの項番⑦～⑭あたりを念頭に置いたネットワークにしてみよう。

・通信シーケンスの例（Packet-In メッセージ，Packet-Out メッセージ）

次に示すネットワークにおいて，OFS は 1 台の L2SW として機能するように管理されていたとする。

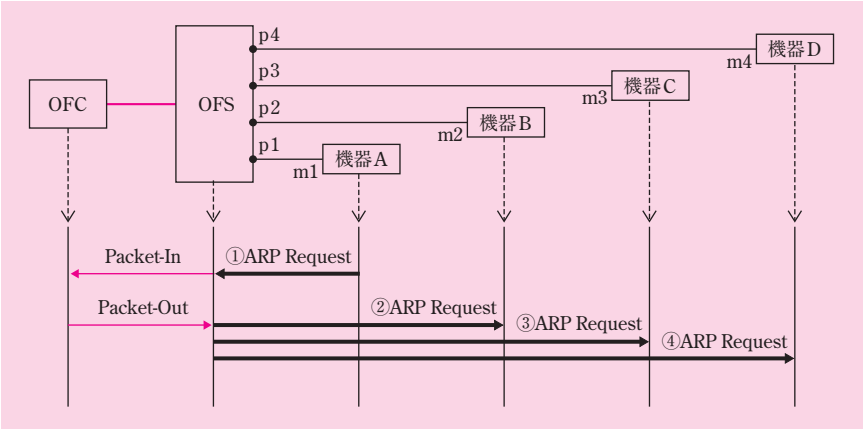


図：L2SW として機能するように管理された OFS と，機器 A ～ D から構成されたネットワーク

機器 A が ARP 要求パケットを OFS に向けて送信したとき，OFS はこれをフラッ

ディングし，同一サブネットワーク内にある機器 B，機器 C，機器 D に向けて，ARP 要求パケットを転送する。

その ARP 要求パケットを OFS が転送するときの通信シーケンスを，次の図に示す。この図を使って，Packet-In メッセージと Packet-Out メッセージをどのように使用するかを解説しよう。



図：ARP 要求パケットを転送する通信シーケンス

OFS は，項番①で ARP 要求パケットを受信する。その後，OFC に Packet-In メッセージを送信している。このメッセージは，表 1 に「入力パケットと入力ポート ID を，OFC に通知する」とあるとおり，OFS から OFC に対する通知である。

このとき OFS は，「このようなパケットを受け取りましたが，どのように処理しましょうか？」と OFC に指示を仰いでいるのである。

次に OFC は，OFS に Packet-Out メッセージを送信している。このメッセージは，表 1 に「出力パケットと出力ポート ID を送り，OFS に出力させる」とあるとおり，OFS に対する指示である。

図の通信シーケンスでは，この指示を受けた OFS が，ARP 要求パケットをフラッディングしている。すなわち，項番②～④に示す ARP 要求パケットを，機器 B ～ D に向けて転送している。

・リアクティブ型とプロアクティブ型

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。

リアクティブ型の通信形態では，OFS が何かパケットを受信するたびに，OFC に通知して指示を待つという手続きを逐一行う。それでは，OFC が大量の通知を受けると，どうなるだろうか。容易に想像できることだが，OFC がボトルネックとなり，OFS は「指示待ち」の状態に置かれる。OFS はパケットを出力しなくなるので，通信が阻害されてしまう。

このような事態を防ぐために，表 1 にはもう一つ，重要なメッセージが定義されている。それが Flow-Mod メッセージである。

表 1 を見ると，Flow-Mod メッセージについて，「変更情報を送り，OFS の管理テーブルを変更させる」と記述されている。

ここで「管理テーブル」という新しい用語が登場する。詳しい説明はすぐ後の「･管理テーブル」のところで述べるが，スイッチの機能は，この管理テーブルで定義されているのである。

OFS の管理テーブルに適切な Action をあらかじめ登録しておけば，OFC に入力パケットを逐一通知して指示を待たなくても，OFS が自ら判断してパケットを処理することができる。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管理テーブルに登録・変更するために使われるものである。

・管理テーブル

続く 3 番目の箇条書きは，OFS の管理テーブルについて説明している。

> ・OFS は，IP アドレス，MAC アドレスなどのパケット識別子（Match Field，以下，MF という）を使ったパケット識別条件と，識別されたパケットの処理（以下，Action という）の組合せ（以下，エントリという）を，OFS 内の管理テーブルで管理する。

OFS の管理テーブルは，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，「エントリ」である。「列」に相当するのは，「パケット識別条件」「Action」である。

スイッチの機能は管理テーブルで定義されており，個々の具体的な動作はエントリで定義されている。この点が少々分かりづらいので，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。

という動作によって，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，エントリの列名を使って，「パケット識別条件に合致したとき，Action を実行する」と言い換えることができる。

ある 1 行のエントリには，この「パケット識別条件」と「Action」が，具体的な値を指定して記述されている。パケット識別条件には，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 Aciton 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 行のエントリは，入力パケットごとの具体的な一つの動作を登録したものである。

このエントリの集合体が，管理テーブルである。エントリを幾つも登録することにより，例えば L2SW の「イーサネットパケットを転送する」といった機能が実現されている。

OFS は，パケットの入力を契機に，管理テーブルの中の特定のエントリを実行する仕組みになっている。この点について，4 番目の箇条書きは，次のように説明している。

> ・OFS は，入力パケットに対して，管理テーブル内のパケット識別条件が一致するエントリを探し，そのエントリの Action を実行する。一致するエントリがない場合は，事前の設定に従い，入力パケットを破棄するか，Packet-In メッセージを使って OFC に入力パケットを転送する。今回の提案では，OFC への通信集中を避けるために，入力パケットを破棄させる設定を全 OFS に対して行う。

ここにあるとおり，様々なパケット識別条件をもつエントリの中から，入力パケットに一致したエントリを探す。

本文には詳しく書いていないが，OpenFlow では，管理テーブル（正式な呼称は「フローテーブル」という）のエントリに優先順位が設定されており，その順位に従って

エントリを次々に評価していく。パケット識別条件が一致したエントリが見つかると，その Action を実行する。

パケット識別条件に一致したエントリが見つかったら，それより下位のエントリは評価されない。したがって，1 個の入力パケットに対し，一致する識別条件をもつエントリが複数存在する場合は，優先順位が最も高いものだけを実行する(*)。

(*) OpenFlow 1.1 以降は，管理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て，それぞれの管理テーブルでエントリを評価し，Action を実行するのである。これを「パイプライン処理」という。この結果，1 個の入力パケットに対し，一致する識別条件をもつエントリを複数実行することができる。
パイプライン処理では，全ての管理テーブルの評価が終わった後，Action がまとめて実行される。それらの Action を実行する順序は，管理テーブルを評価した順序ではなく，Action の内容に基づく優先順位に従う。

一致するエントリがない場合の振る舞いについて，本文に「OFC への通信集中を避けるために，入力パケットを破棄させる設定を全 OFS に対して行う」と記述されている。これは OpenFlow 1.3 以降のデフォルトの振る舞いでもある。

表 2 には，パケット識別条件を構成するパケット識別子（Match Field，以下，MF という）と Action の例が示されている。以降の解説でしばしば確認するので，ここに掲載しておこう。

表：MF と Action の例（表 2 の抜粋）

MF の例

レイヤ	MF 名	説明
L1	IN_PORT	入力ポート ID
L2	ETH_DST	宛先 MAC アドレス
	ETH_SRC	送信元 MAC アドレス
	ETH_TYPE	イーサネットタイプ
	VLAN_VID	VLAN ID
L3	IPV4_SRC	送信元 IP アドレス
	IPV4_DST	宛先 IP アドレス

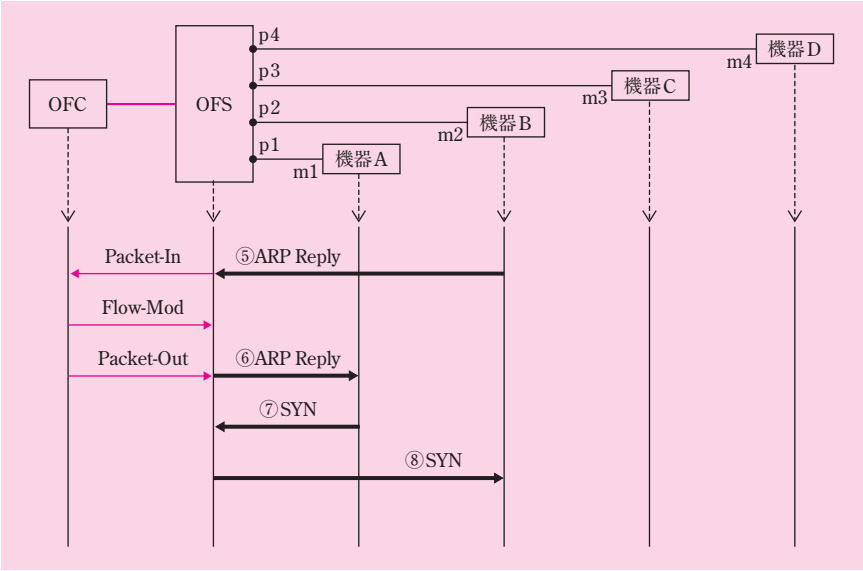
Action の例

Action 名	説明
Output( )	( ) 内に指定された次に示すパラメータに従い，パケットを出力する。 ・ポート ID：指定ポートに出力する。 ・controller：Packet-In メッセージを使い OFC に転送する。
Drop	パケットを破棄する。
Set-Field	パケットのヘッダの一部を書き換える。 ・表記例：Set-Field ETH_DST=m1 （宛先 MAC アドレスを m1 に書き換える場合）
Push-VLAN	パケットに VLAN ヘッダを付加する。
Pop-VLAN	パケットの VLAN ヘッダを削除する。

・通信シーケンスの例（Flow-Mod メッセージ）

管理テーブルについて理解できたところで，通信シーケンスを使って，今度は Flow-Mod メッセージによるエントリの登録，及び，登録後のパケット転送の振る舞いを解説しよう。

次の通信シーケンスは，図「ARP 要求パケットを転送する通信シーケンス」の続きである。こちらの図では，ARP 応答パケット，SYN パケットを転送している。



図：ARP 応答パケットと SYN パケットを転送する通信シーケンス

先ほど機器 A が送信した ARP 要求パケットは，実は機器 B の IP アドレスを目標アドレスとするものであったとしよう。

ARP 要求パケットを受け，機器 B は，機器 A 宛てに ARP 応答パケットを返信する。これが項番⑤のパケットである。このパケットが入力されると，OFC に Packet-In メッセージを送信する。

今度はこの ARP 応答パケットを機器 A に転送するよう，OFC は OFS に Packet-Out メッセージを送信する。この指示を受けて出力されたのが，項番⑥のパケットである。

ここまでの ARP 要求と ARP 応答のやり取りは，リアクティブ型で処理されている。

OFS は，このやり取りを通知されることで，次のことを学習する。

- ポート p1 の先に，MAC アドレス m1 をもつ機器（機器 A）が存在する。
- ポート p2 の先に，MAC アドレス m2 をもつ機器（機器 B）が存在する。

これを踏まえ，機器 A と機器 B 間のやり取りを，これからはプロアクティブ型で処理するように切り替える。すなわち，OFC からの指示を待つことなく，OFS が自ら判断して転送するよう，管理テーブルにエントリを追加するのだ。

それを実現するために，OFC は，Flow-Mod メッセージを用い，次に示す二つのエントリを OFS に送信する。エントリ 1 は機器 A から機器 B 宛ての，エントリ 2 は機器 B から機器 A 宛てのパケット転送に対応した動作である。

表：機器 A と機器 B 間の通信に対応したエントリ

エントリ	パケット識別条件	Action
エントリ 1	IN_PORT = p1 ETH_DST = m2 ETH_SRC = m1	Output（p2）
エントリ 2	IN_PORT = p2 ETH_DST = m1 ETH_SRC = m2	Output（p1）

通信シーケンスを見ると，OFC は，この Flow-Mod メッセージを Packet-Out メッセージより前に送信している。その理由は，ARP 応答パケットが機器 A に返信された後，ただちに機器 A が何かのパケットを機器 B 宛てに送信するかもしれないからだ。そうなる前に確実に管理テーブルを変更しておく必要がある。

管理テーブルにエントリが登録されたら，いよいよ，OFS はプロアクティブ型の転送処理を行う。

早速，項番⑦で，機器 A は，機器 B 宛ての SYN パケットを送信している。

これはエントリ 1 のパケット識別条件に一致する。したがって，エントリ 1 の Action「入力パケットをポート p2 から出力する」という処理を実行する。項番⑧は，この Action を実行した結果，OFS が出力した SYN パケットである。

この「パケット⑦→ OFS →パケット⑧」という通信シーケンスが，まさしく OFS によるユニキャストパケットの転送である。

この後のやり取りは特に記していないが，もしも機器 B が機器 A 宛てのパケットを返信したら，今度はエントリ 2 の Action を実行することになる。

・特別な Action：Output（controller）

本文の 4 番目の箇条書きの中で，A 社の新工場 LAN に導入する OFS について，「一致するエントリがない場合は……入力パケットを破棄させる設定」をしていると記述されている。

これまでに登場した通信シーケンスでは，OFS は入力パケットを破棄していない。ARP 要求パケットや ARP 応答パケットを受け取った後，OFS は，OFC に PacketIn メッセージを送信している。

この点はどう理解したらよいのだろうか。最後にこの点を補足しておこう。

実を言うと，一連の通信シーケンスに先立ち，管理テーブルにあらかじめ特別なエントリを仕込んであったのだ。

その内容は，「ARP パケットを入力されたら，Packet-In メッセージを使い OFC に転送する」というものである。パケット識別条件と Action を書くと，次のようになる。

パケット識別条件：ETH_TYPE が ARP パケット（0x0806）
Action：Output（controller）

このように，「Output（controller）」という特別な Action を登録することで，プロアクティブ型の OFS に対し，特定のパケットに関してはリアクティブ型と同じように振る舞わせることができる。

本文の図 3，図 4 に登場する通信シーケンスにも，これと同様のエントリが管理テーブルに登録されている。OFS が Packet-In メッセージを送っているのは，Output（controller）という Action を含んだエントリが実行されたためである。

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，それでは，いよいよ設問の解説に移ろう。

■設問 1

解答例

あ：i1
い：NAT
う：i3
え：Flow-Mod
お：controller
か：Packet-Out
き：OFS2
く：p9

本設問は，大きく二つの部分に分かれている。

一つ目は，空欄**あ**～空欄**う**である。ここでは，序文の第 5 段落に記述された，機械から Web-A に対する Web のアクセスの概要が問われている。

二つ目は，空欄**え**～空欄**く**である。ここでは，〔新工場 LAN に適用する SDN 技術の調査〕の図 3「OFS 接続情報収集の通信シーケンス例」の内容が問われている。

［あ］，［い］，［う］

序文の第 5 段落は，機械から Web-A に対する Web のアクセスの概要について，四つの箇条書きで説明している。

その 1 番目の箇条書きに，「Web-A を収容している DMZ は，プライベートアドレスが割り当てられている」と記述されている。

国内外の機械が，インターネット経由で Web-A にアクセスできるには，外部に公開する Web-A の IP アドレスがグローバルアドレスになっていなければならない。これをどこかの機器に割り当てておき，この IP アドレス宛てのパケットを受信したとき，Web-A のプライベートアドレスにアドレス変換しなければならない。

この宛先 IP アドレスの変換において，変換前のグローバルアドレスと変換後のプライベートアドレスは 1 対 1 で対応している。したがって，アドレス変換の種類は NAT（静的 NAT）となる。

この点を踏まえて，2 番目の箇条書きを見てみよう。

ここには，「機械から送信された IP パケットは，C 社 ISP を経由し，FW に転送される。その宛先 IP アドレスは，図 1 中の［あ］である」と記述されている。

言うまでもなく，機械から Web-A へアクセスする IP パケットは，インターネットを経由している間，Web-A のグローバルアドレスが宛先である。この IP パケットは，C 社 ISP を経由し，FW の外部 NW 側のインタフェースに転送される。

したがって，Web-A のグローバルアドレスが，FW の外部 NW 側のインタフェースに割り当てられていることが分かる。この IP アドレスは，図 1 中の記号で表すと「i1」である。よって，空欄**あ**の正解は，「**i1**」となる。

次に 3 番目の箇条書きを見てみよう。

ここには，「FW は，受信した IP パケットを LB に転送する。その際，FW の［　い　］機能によって，宛先 IP アドレスは図 1 中の［　う　］に書き換えられる」と記述されている。

空欄**あ**の解を導いたことで，FW の外部 NW 側はグローバルアドレスであることが分かった。前述のとおり，DMZ はプライベートアドレスが割り当てられている。それゆえ，FW の NAT 機能により，グローバルアドレスからプライベートアドレスへの 1 対 1 の変換が行われることが分かる。よって，空欄**い**の正解は，「**NAT**」となる。

このアドレス変換の後，「FW は受信パケットを LB に転送する」と記述されている。

ここから，「Web-A」のプライベートアドレスは LB に割り当てられていることが分かる。

この IP アドレスは，図 1 中の記号で表すと「i3」である。よって，空欄**う**の正解は，「**i3**」となる。

なお，「LB」とは，図 1 に記されているとおり，負荷分散装置を指している（この略称は，試験でよく使用されている）。

LB は，「サーバの稼働状況をチェックしながら，受信した IP パケットを動的に Web-A1 又は Web-A2 に振り分ける」（4 番目の箇条書き）。この記述から，「Web-A」のアクセスはいったん LB が受信することが分かる。

［　か　］，［　き　］，［　く　］

解説の都合上，空欄**え**，空欄**お**より前に，空欄**か**～空欄**く**の解を求めることにする。

空欄**か**～空欄**く**は，〔新工場 LAN に適用する SDN 技術の調査〕の第 4 段落にある。

解を導くに当たり，少し前の第 2 段落から第 4 段落まで，文脈をまずは追ってみよう。

第 2 段落は，SDN 技術を使った新工場 LAN の物理構成案を説明している。この構成案は，図 2 に示している。

この図 2 を見ると，OFS は 8 台あり，OFS1 ～ OFS8 まで横並びにカスケード接続していることが分かる。OFS1 と OFS2 は，OFS1 のポート p8 と OFS2 のポート p9 で

接続している。

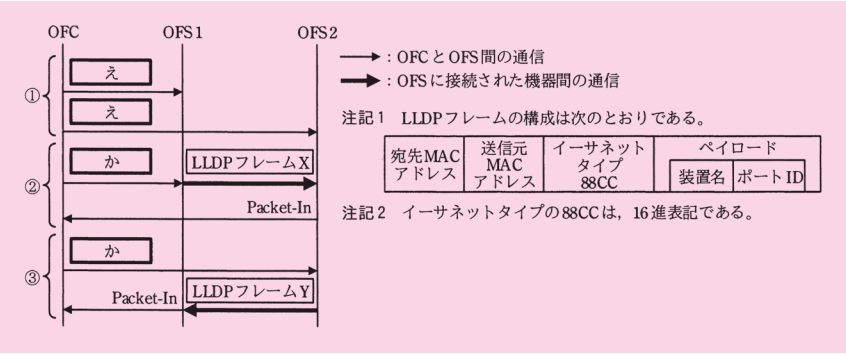
第 3 段落は，OFS 同士の接続情報を OFC が収集する通信シーケンスを説明している。その例として，OFS1 と OFS2 間の通信シーケンスを図 3 に示している。

この図 3 の項番②，③に空欄**か**がある。

第 4 段落は，図 3 の通信シーケンスの内容を，項番①～③にかけて具体的に説明している。このやり取りで LLDP が使われているが，この前提知識がなくても本文から十分理解できる。そこには次のように記述されている。

> OFS 接続情報の収集では，IEEE 802.1AB で規定されている LLDP（Link Layer Discovery Protocol）の仕組みを流用する。図 3 中の OFC は，固有のイーサネットタイプ 88CC をもつ LLDP フレームを使って，次のように，LLDP フレーム X と LLDP フレーム Y の内容から OSF1 の p8 と OFS2 の p9 の接続情報を得ている。

第 4 段落の項番①～③は，図 3 の通信シーケンスの項番に対応している。



図：OFS 接続情報収集の通信シーケンス例（図 3 の抜粋）

第 4 段落の項番②の説明を読むと，LLDP を使った接続情報の収集方法が分かる。図 3 の通信シーケンスの項番②は，OFS1 から OFS2 に LLDP フレーム X を送信している。

そこには，「OFC は，表 1 中の［　か　］メッセージを使って，OFS1 の全ポートについて，OFS1 の装置名とそれぞれのポート ID を格納した LLDP フレームを出力させ（る）」と記述されている。

OFS1 がフレーム X を送信し，OFS2 はこれを受信する。

OFS2 は，OFC に対し，フレーム X を受信したことを通知している。この通知に使

われているのは Packet-In メッセージである。その内容について,「装置名 OFS1 とポート ID p8 が格納された LLDP フレーム X」と記述されている。

続く項番③の説明を見ると,「OFC は，OFS2 に対して②と同様の操作を行（う）」と記述されている。

この一連の流れから，隣接する OFS 同士の接続情報を収集する方法が明らかになる。

1. OFC は，ある OFS に対し，全ポートから LLDP フレームを出力させる。便宜上，これを始点側 OFS と呼ぶことにしよう。このフレームに格納された内容は，始点側 OFS の装置名と，出力ポート ID である。
2. このとき，始点側 OFS のあるポートの先に，別の OFS が接続していたとする。便宜上，これを終点側 OFS と呼ぶことにしよう。この終点側 OFS は，先ほどの「始点側 OFS の装置名と，出力ポート ID」を格納した LLDP フレームを受信し，そのことを OFC に通知する。項番②の例では,「装置名 OFS1 とポート ID p8」となる。

   この結果，OFC は,「始点側 OFS の出力ポートの先に，終点側 OFS が接続している」という情報を得る。

同様のことを，あらゆる OFS に対して実施する。隣接する OFS 同士は，始点側と終点側の立場を入れ替えて実施することになるが，双方向から収集した接続情報を照合して齟齬がないことを確認する。

ここまで理解できると，空欄**か**～空欄**く**の解が求まる。

空欄**か**に該当する字句は，OFS にフレームを出力させるため，OFC が使うメッセージ名である。そのメッセージを表 1 から見つければ解が求まる。表 1 の「Packet-Out」の用途は,「出力パケットと出力ポート ID を送り，OFS に出力させる」とあるので，OFC にフレームを出力させるためのメッセージであることが分かる。

よって，空欄**か**の正解は「**Packet-Out**」となる。

空欄**き**と空欄**く**は，項番③の説明の中にある。そこには,「OFC は，OFS2 に対して②と同様の操作を行い，装置名［　**き**　］とポート ID［　**く**　］が格納された LLDP フレーム Y を OFS1 から受け取る」と記述されている。

項番③は，接続情報収集の始点側が OFS2 となる。これが出力する LLDP フレームに格納されている装置名は，出力ポートにかかわらず，どのフレームも「OFS2」である。

よって，空欄**き**の正解は「**OFS2**」となる。

終点側の OFS1 が受け取る LLDP フレーム Y は，OFS2 のポート p9 から出力されたものである。したがって，LLDP フレーム Y に格納されているポート ID は「p9」である。

よって，空欄**く**の正解は「**p9**」となる。

え，**お**

空欄**え**～空欄**お**は，〔新工場 LAN に適用する SDN 技術の調査〕の第 4 段落，項番①の説明の中にある。

そこには，「OFC は，表 1 中の［**え**］メッセージを使って，ETH_TYPE が 88CC に等しいときの Action として，Output（［**お**］）を，OFS 内の管理テーブルに登録させる」と記述されている。

ここで，項番②，項番③における，終点側 OFS の振る舞いを思い起こしてみよう。

LLDP フレームを受信すると，Packet-In メッセージを使い，この受信を OFC に通知しているのだ。

OFC に対して Packet-In メッセージを通知するには，項番②，③に先立ち，特別なエントリを登録しておく必要がある。

〔新工場 LAN に適用する SDN 技術の調査〕の第 1 段落，4 番目の箇条書きの中で，「OFS は，……一致するエントリがない場合，……入力パケットを破棄させる設定（をする）」と記述されている。つまり，特別なエントリを前もって登録しない限り，項番②，③において，OFS は受信した LLDP フレームを破棄してしまうことが分かる。

そのエントリについて，冒頭の「● SDN 技術の概要」の「・特別な Action：Output（controller）」の中で解説している。そこで述べたとおり，OFS が Packet-In メッセージを送っているのは，Output（controller）という Action を含んだエントリが実行されたためである。

項番①は，この特別なエントリを OFS の管理テーブルに登録する手順を説明したものである。管理テーブルを設定するために，OFC が OFS に送るメッセージは，Flow-Mod メッセージである。

よって，空欄**え**の正解は「**Flow-Mod**」となる。

この特別なエントリは，LLDP フレームを受信したとき，Packet-In メッセージを使って OFC に通知させるために登録する。

したがって，パケット識別条件は，本文に書いてあるとおり，「ETH_TYPE が 88CC に等しい」となる。Action は，「Output（controller）」となる。

空欄**お**は，Output の引数を問うている。よって，正解は「**controller**」となる。

■設問 2
(1)

解答例

け：v2
こ：なし
さ：m2
し：m3
す：i4

け ～ す

本問は，表 3 中の空欄**け**～空欄**す**に入れる適切な字句を問うている。

表 3 は，〔新工場 LAN の運用の調査〕の第 3 段落にある。

この表は，図 4 中のパケット⑥，⑬～⑯のヘッダ情報を掲載したものである。問われている空欄**は**，パケット⑬～⑯のヘッダ情報である。

図 4 は，同見出しの第 2 段落にある。そこには，図 4 について，「機械から送信された SYN パケットが，RT-1 から振り分け先の Web-A1 に転送される場合の，新工場 LAN の論理構成と通信シーケンス例」と記述されている。その SYN パケットは，図 4 中のパケット⑤，⑥，⑬～⑯である。このうち⑬～⑯が今ここで問われているわけだ。

本問の解を導くには，まず，新工場 LAN の NW 構成，及び，RT-1 から振り分け先の Web-A1 に転送される経路を理解する必要がある。その後，これら SYN パケットのヘッダ情報が，機器の間を転送するたびにどのように変遷するかを考察して，解を導こう。

●新工場 LAN の NW 構成

本文の図 1「NW 拡張の概要（抜粋）」の A 社の工場 LAN に，「NW 拡張によって更新される部分」がある。この部分は，現行 NW の構成である。

新工場 LAN の構築に伴って，この部分が置き換えられる。具体的には，図 2 に示す物理構成となる。

図 1 から図 2 への変更点について，〔新工場 LAN の運用の調査〕の第 1 段落に説明されている。

1 番目の箇条書きに，「OFS を使って，図 1 中の工場の外部 NW，DMZ，内部 NW に対応した，仮想的なレイヤ 2 ネットワーク（以下，仮想 NW という）を構成する」と記述されている。図 1 の「NW 拡張によって更新される部分」（網掛け部分）は，こ

こで引用した三つのネットワークセグメントからなる。この部分が，OFS に置き換わると述べていることが分かる。

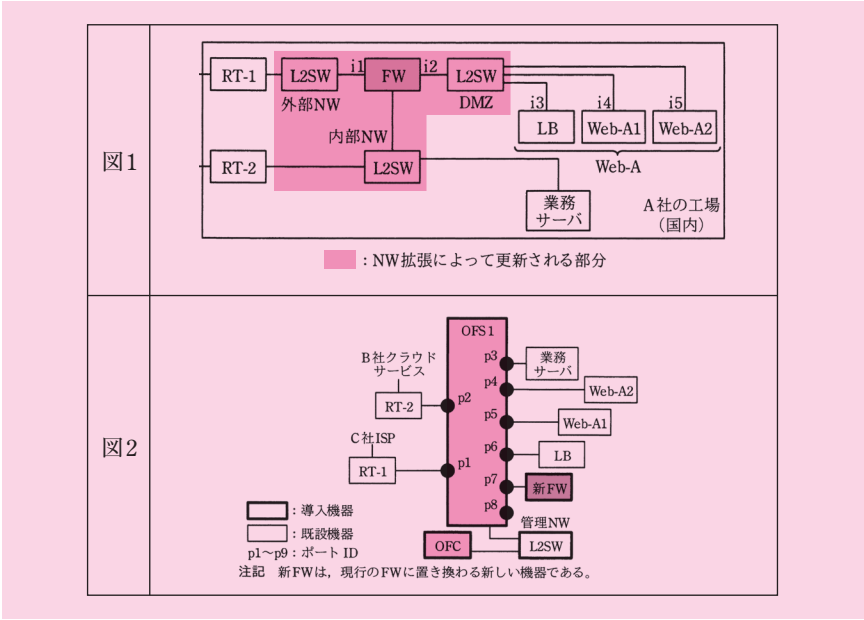
ここで言う「仮想 NW」とは，実は VLAN と同じだ。分かりやすく言い換えると，仮想的な L2SW である。要するに，図 1 の三つのネットワークセグメントにあった L2SW が，OFS 内部の仮想的な L2SW（仮想 NW）に置き換わったと考えればよい。

2 番目の箇条書きに，「仮想 NW 間の通信は，新 FW を経由させる。新 FW と OFS はトランク接続し，仮想 NW に対応した VLAN ID を定義する」と記述されている。

図 2 を見ると，図 1 の FW が新 FW に置き換わっており，OFS のポート p7 に接続されている。

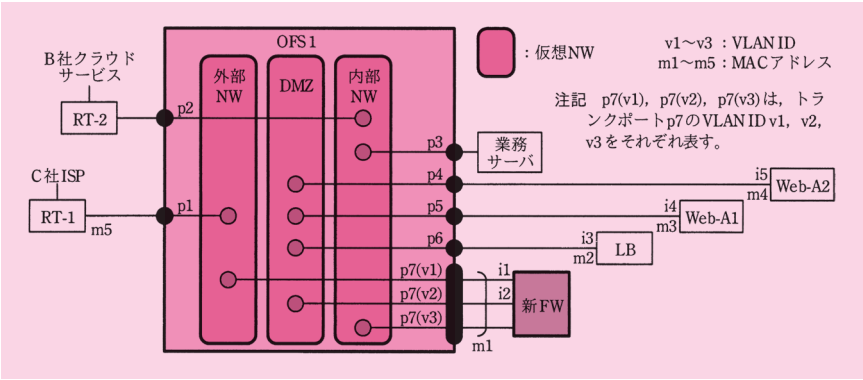
新 FW は，図 1 の FW と同じく，三つのネットワークセグメントに接続している。OFS と新 FW はトランク接続になっており，三つの VLAN（外部 NW，DMZ，内部 NW）を束ねている。したがって，OFS のポート p7 と新 FW 間は，VLAN タグフレームが流れる。図 2 は物理的な構成を示しているため，トランク接続が 1 本の物理リンクで描かれている。

これまでの解説をまとめて，変更点を図に整理してみよう。図 1 と図 2 の中から Web-A が関わる部分を取り上げて，変更箇所を抜粋したものを次の図に示す。



図：現工場 LAN から新工場 LAN への変更点（Web-A が関わる部分）

OFS 内部に構成された三つの仮想 NW は，図 4 の論理構成に示されている。どの仮想 NW がどのポートと接続しているかが分かりやすくまとめられているので，併せて掲載しておこう。この図では，OFS のポート p7 と新 FW 間のトランク接続が，3 本の論理リンクで描かれている。



図：新工場 LAN の論理構成（図 4 の一部抜粋）

● RT-1 から振り分け先の Web-A1 に転送される経路

3 番目の箇条書きに，「現行 FW のフィルタリング機能と NAT 機能を，新 FW に移行する」と記述されている。したがって，新 FW に置き換わっただけで，機械から Web-A へのアクセス経路に変更はないことが分かる。

したがって，機械から Web-A 宛ての通信経路を考察するに当たって，設問 1 空欄**あ**～空欄**う**で解説した内容をそのまま当てはめることができる。図 4 が示しているのは「RT-1 から振り分け先の Web-A1 まで」なので，RT-1 以降の経路に着目する。

新 FW でアドレス変換をしたり，LB で振り分け処理をしたりするので，経路はやや複雑だ。そこで，経路を幾つかの区間に分けて整理してみよう。

IP アドレスと MAC アドレスは，図 4 中の記号を使って表す。

・外部 NW（RT-1 → 新 FW）

Web-A のグローバルアドレスは新 FW の外部 NW 側インタフェースに割り当てられる。

したがって，機械から送信された IP パケットは，宛先 IP アドレスが i1 である。

外部 NW において，これをペイロードに格納するイーサネットフレームは，RT-1 から新 FW の外部 NW 側インタフェース宛てに送信される。宛先 MAC アドレスは

m1，送信元 MAC アドレスは m5 である。

・DMZ（新 FW → LB）

Web-A のプライベートアドレスは LB に割り当てられる。

新 FW は，受信した IP パケットを LB に転送する。その際，NAT 機能により，宛先 IP アドレスが i1 から i3 に変換される。

したがって，新 FW から送信された IP パケットは，宛先 IP アドレスが i3 である。

DMZ において，これをペイロードに格納するイーサネットフレームは，新 FW の DMZ 側インタフェースから LB 宛てに送信される。宛先 MAC アドレスは m2，送信元 MAC アドレスは m1 である。

・DMZ（LB → Web-A1）

LB は，サーバの稼働状況をチェックし，配下の Web サーバに振り分ける。図 4 の例では，受信した IP パケットを Web-A1 に転送する。

したがって，LB から Web-A1 宛てに送信された IP パケットは，宛先 IP アドレスが i4 である。

DMZ において，これをペイロードに格納するイーサネットフレームは，LB から Web-A1 宛てに送信される。宛先 MAC アドレスは m3，送信元 MAC アドレスは m2 である。

●解の導出

本問が問うている表 3 には，四つの項目がある。

項目「宛先 MAC アドレス」「送信元 MAC アドレス」は，イーサネットフレームのヘッダ情報である。「宛先 IP アドレス」は，このペイロードに格納された IP パケットのヘッダ情報である。これらは，前述の「● RT-1 から振り分け先の Web-A1 に転送される経路」の解説で，既に導き出している。

残る項目「VLAN ID」は，VLAN タグ付きのイーサネットフレーム（以下，VLAN タグフレームという）の場合，VLAN タグ中の VLAN ID を記載する。通常のイーサネットフレームの場合，「なし」と記載する。

図 4 の中で，OFS と新 FW 間のトランク接続を通るイーサネットフレームが，VLAN タグフレームである。

その VLAN タグには，仮想 NW の VLAN ID が格納される。それゆえ，表 3 の項目にある VLAN ID の値を知るには，トランク接続を通る VLAN タグフレームがどの仮想 NW 上でやり取りされているのかが分かればよい。

仮想 NW の VLAN ID は，OFS と新 FW 間の論理リンクを見れば分かる。ここにある 3 本の論理リンクは，それぞれ異なる仮想 NW と接続している。トランク接続内で論理リンクを識別するために，仮想 NW の VLAN ID が付与されている。図 4 にはこの論理リンクの VLAN ID が明記されているので，ここを見れば仮想 NW の VLAN ID が分かる。

具体的に言うと，VLAN ID の値は，外部 NW が「v1」，DMZ が「v2」，内部 NW が「v3」である。

それでは，図 4 の通信シーケンスの流れを追いかけていき，その過程で空欄の解を一つずつ求めてゆこう。

・外部 NW（RT-1 → 新 FW）：パケット①～⑥

まず，RT-1 から新 FW 宛ての SYN パケット⑤，⑥を考察する。

これに先立つアドレス解決が，①～④に示された，外部 NW における ARP シーケンスである。このアドレス解決で，RT-1 は，新 FW の外部 NW 側インタフェースの MAC アドレスを取得している。

その後，SYN パケット⑤，⑥が送信されている。

SYN パケット⑤，⑥の宛先 MAC アドレスは m1（新 FW），送信元は m5（RT-1）である。宛先 IP アドレスは i1 である。

SYN パケット⑥は，OFS と新 FW 間のトランク接続を通るため，VLAN タグフレームである。このパケットは新 FW の外部 NW 側インタフェースに向かって出力されるので，VLAN ID は，外部 NW を表す v1 となる。

ここに述べた値は，表 3 に記されているものと一致する。

・DMZ（新 FW → LB）：パケット⑦～⑭

次に，新 FW から LB 宛ての SYN パケット⑬，⑭を考察する。

これに先立つアドレス解決が，⑦～⑫に示された，DMZ における ARP シーケンスである。このアドレス解決で，新 FW は，LB の MAC アドレスを取得している。

その後，SYN パケット⑬，⑭が送信されている。

SYN パケット⑬，⑭の宛先 MAC アドレスは m2（LB），送信元は m1（新 FW）である。宛先 IP アドレスは i3 である。

SYN パケット⑬は，OFS と新 FW 間のトランク接続を通るため，VLAN タグフレームである。このパケットは新 FW の DMZ 側インタフェースから出力されるので，VLAN ID は，DMZ を表す v2 となる。

以上より，解を求めることができる。

空欄けはパケット⑬の VLAN ID なので，正解は「v2」となる。
空欄こはパケット⑭の VLAN ID なので，正解は「なし」となる。
空欄さはパケット⑬，⑭の宛先 MAC アドレスなので，正解は「m2」となる。

・DMZ（LB → Web-A1）：パケット⑮～⑯

最後に，LB から Web-A1 宛ての SYN パケット⑮，⑯を考察する。

これに先立つアドレス解決は，図 4 中では省略されている。このアドレス解決で，LB は，Web-A1 の MAC アドレスを取得している。

その後，SYN パケット⑮，⑯が送信されている。

SYN パケット⑮，⑯の宛先 MAC アドレスは m3（Web-A1），送信元は m2（LB）である。宛先 IP アドレスは i4 である。

SYN パケット⑮，⑯は，OFS と新 FW 間のトランク接続を通らないため，通常のイーサネットフレームである。

以上より，解を求めることができる。

空欄しはパケット⑮，⑯の宛先 MAC アドレスなので，正解は「m3」となる。
空欄すはパケット⑮，⑯の宛先 IP アドレスなので，正解は「i4」となる。

(2)

解答例

②，⑧，⑨，⑩

問題文は，「本文中の下線（ｉ）の Packet-Out メッセージによって送出されたパケットを，図 4 中の①～⑯から選び，①～⑯の記号で全て答えよ」と記述されている。

下線（ｉ）は，〔新工場 LAN の運用の調査〕の第 4 段落，1 番目の箇条書きの中にある。そこには次のように記述されている。

> ・OFC には，次のような仮想 NW の構成に関する構成情報が登録されている。
> － OFS1 の外部 NW の構成要素：p1，p7（v1）
> － OFS1 の DMZ の構成要素：p4，p5，p6，p7（v2）
> （ｉ）ブロードキャスト通信に関する Packet-In メッセージを受信したとき，OFC は，これらの構成情報を基に，OFS に Packet-Out メッセージを使った指示を行う。

下線（ｉ）に「ブロードキャスト通信」とある。図 4 の中にあるブロードキャストパケットは，ARP Request パケットである。この ARP Request パケットに関して，「Packet-In メッセージを受信したとき，OFC は，これらの構成情報を基に，OFS に Packet-Out メッセージを使った指示を行う」と述べている。

図 4 中の ARP Request パケットのうち，Packet-In メッセージの契機になっているものは，次のとおりである。

パケット①，⑦

本問で問うているのは，このパケット①，⑦の受信がきっかけとなり，Packet-Out メッセージによって送出されたパケットである。

L2SW は，ARP Request パケットを受信すると，同一ネットワークセグメントにフラッディングする。したがって，OFS がパケット①，⑦を受信したとき，この通知を受けて OFC が出す指示は，このフラッディング動作である。下線①にある Packet-Out メッセージは，この指示を表している。

Packet-In メッセージで通知する内容は，表 1 にあるとおり「入力パケットと入力ポート ID」である。それゆえ，OFS が ARP Request パケットを受信したとき，OFC は，このパケットが OFS のどのポートから受信したかが分かる。

Packet-Out メッセージで指示する内容は，表 1 にあるとおり「出力パケットと出力ポート ID」である。フラッディングさせる場合でも，出力ポートを具体的に逐一指定する必要がある。要するに，ポートごとにパケット出力の指示を出すのだ。

OFC は仮想 NW の構成情報が分かっており，Packet-In メッセージで入力ポート ID を通知される。したがって，入力ポート ID から仮想 NW を割り出すことができる。

OFS にフラッディングさせるには，仮想 NW に接続されたポートのうち入力ポートを除くもの全てから出力するように指示を出せばよい。

ここまで理解できたところで，このパケット①，⑦の受信をきっかけに出力を指示された ARP Request パケットを，具体的に求めてみよう。これが本問の解となる。

パケット①は，図 4 中の網掛けで示されているとおり，「外部 NW における ARP シーケンス」に含まれている。この入力ポートは p1 である。したがって，これをきっかけに出力を指示される ARP Request パケットは，外部 NW のポート p7（v1）から出力されたものである。すなわち，次のものとなる。

パケット②

パケット⑦は，図 4 中の網掛けに示されているとおり，「DMZ における ARP シーケンス」に含まれている。この入力ポートは p7（v2）である。したがって，これをきっかけに出力を指示される ARP Request パケットは，DMZ のポート p4，p5，p6 から出力されたものである。すなわち，次のものとなる。

パケット⑧，⑨，⑩

よって，正解は「②，⑧，⑨，⑩」となる。

(3)

解答例

E	T	H	_	T	Y	P	E	が	A	R	P	の	イ	ー	サ	ネ	ッ	ト	タ	イ	プ	に	等	し	い	。

（27 字）

問題文は，「本文中の下線（ii）について，エントリに含まれるパケットの識別条件を，表 2 中の MF を用いて，……述べよ」と記述されている。

下線（ii）は，〔新工場 LAN の運用の調査〕の第 4 段落，2 番目の箇条書きの中にある。そこには次のように記述されている。

> ・OFC は，ARP を利用して，ユニキャスト通信に対応したエントリを OFS に登録させる。そのために，図 4 中の通信シーケンスが始まる前に，（ii）OFC は，ARP Request と ARP Reply を OFC に通知するためのエントリを，OFS1 に登録させる。

下線（ii）に「ARP Request と ARP Reply を OFC に通知するためのエントリ」とある。OFS がパケットを受信したとき，これを通知させるには，Output（controller）を Action に設定したエントリを OFS に登録すればよい。

本問は，このエントリの MF を問うている。

このエントリは，ARP Request パケット又は ARP Reply パケットの受信を契機に，管理テーブルの中から選ばれるものである。したがって，パケット識別条件は，この二つのパケットに一致する内容であればよい。

表 2 の中を見ると，ETH_TYPE（イーサネットタイプ）という MF が用意されてい

る。この二つのパケットは，イーサネットタイプがどちらも「ARP」であるから，これを識別条件に指定すればよい。

よって，正解は，「**ETH_TYPE が ARP のイーサネットタイプに等しい**」となる。

(4)

解答例

外部NW内のRT-1と新FWの通信（17字）

問題文は，「本文中の下線（iii）について，表 4 のエントリに対応するユニキャスト通信を，……答えよ」と記述されている。

下線（iii）は，〔新工場 LAN の運用の調査〕の第 4 段落，3 番目の箇条書きにある。そこには次のように記述されている。

> ・（iii）図 4 では，二つのユニキャスト通信について，エントリ登録の通信シーケンスがそれぞれ示されている。Flow-Mod（1）によって登録されるエントリを表 4 に，Flow-Mod（2）によって登録されるエントリを表 5 に，それぞれ示す。

図 4 は，機械から送信された SYN パケットが，RT-1 から振り分け先の Web-A1 に転送される場合の通信シーケンスを示したものである。

ここには，SYN パケットが RT-1，FW，LB，Web-A1 の順に転送されていく通信シーケンス，及び，当該パケットの送信に先立つ ARP シーケンスが記されている。

設問 2（2）で解説したとおり，ARP Request パケットと ARP Reply パケットを OFS が受信すると，Packet-In メッセージを使って，OFC に通知する。

通知する内容は「入力パケットと入力ポート ID」であるから，ARP Request パケットと ARP Reply パケットの両方を通知されることによって，OFC は次の情報が分かる。

- ARP Request パケットを OFS に送信したノードの MAC アドレス，そのノードが接続しているポート
- ARP Reply パケットを OFS に送信したノードの MAC アドレス，そのノードが接続しているポート

したがって，ここに登場した二つのノードでやり取りされるユニキャスト通信を見

越して，エントリを OFS の管理テーブルに事前に登録することが可能となる。2 番目の箇条書きにある，「ARP を利用して，ユニキャスト通信に対応したエントリを OFS に登録させる」とは，この二つのノード間のユニキャスト通信に対応するエントリの登録を指している。

この点を踏まえ，図 4 の外部 NW 内の ARP シーケンス，その後に続く Flow-Mod メッセージの送信，ユニキャスト通信を見てみよう。

ARP Request パケット①を送信したノードは，RT-1 である。これをフラッディングしたものがパケット②である。これを受け，ARP Reply パケット③を送信したノードは，新 FW（外部 NW 側インタフェース）である。

この外部 NW 内の ARP シーケンスから，OFC は，次の二つのノードの情報を得ることができる。

- MAC アドレス m5（RT-1）をもつノードが，OFS1 のポート p1 の先にある。
- MAC アドレス m1（新 FW）をもつノードが，OFS1 のポート p7（v1）の先にある。

ここから得た情報に基づき，RT-1 と新 FW 間のユニキャスト通信に対応するエントリを Flow-Mod（1）メッセージで登録する。それが，表 4「図 4 中の Flow-Mod（1）によって登録されるエントリ」で示されている。

実際に，表 4 のエントリが，RT-1 と新 FW 間のユニキャスト通信に対応していることを確認してみよう。

エントリ 1 のパケット識別条件を見ると，ETH_DST（宛先 MAC アドレス）が m1（新 FW）であり，ETH_SRC（送信元 MAC アドレス）が m5（RT-1）である。IN_PORT（入力ポート）は，送信元の RT-1 が接続しているポートなので p1 である。p1 はトランク接続していないから，VLAN_VID は「なし」となる。

それゆえ，エントリ 1 は RT-1 から新 FW 宛てのユニキャスト通信に対応していることが確認できた。

エントリ 2 は，エントリ 1 と逆方向の通信に対応している。その内容は，ETH_DST と ETH_SRC を入れ替え，IN_PORT が ETH_SRC の接続ポートに変更したものになっている。

このアドレス解決が完了した後，SYN パケット⑤が RT-1 から新 FW 宛てに送信される。これは，表 4 のエントリ 1 によって転送される。

このユニキャスト通信を，本問は問うている。よって，正解は，「**外部 NW 内の RT-1 と新 FW の通信**」となる。

(5)

解答例

せ：p6
そ：なし
た：m1
ち：m2

せ	～	ち

本問は，表 5 中の空欄**せ**～空欄**ち**に入れる適切な字句を問うている。

表 5 は，〔新工場 LAN の運用の調査〕の第 4 段落にある。

この表は，図 4 中の Flow-Mod（2）によって登録されるエントリを掲載したものである。問われている空欄**は**，エントリ 1 のパケット識別条件の MF である。

〔新工場 LAN の運用の調査〕の第 4 段落，3 番目の箇条書きの中で，「図 4 では，二つのユニキャスト通信について，エントリ登録の通信シーケンスがそれぞれ示されている。Flow-Mod（1）によって登録されるエントリを表 4 に，Flow-Mod（2）によって登録されるエントリを表 5 に，それぞれ示す」と記述されている。

ここに，「二つのユニキャスト通信について，エントリ登録の通信シーケンスがそれぞれ示されている」とある。

その一つ目は，設問 2（4）で解説した。一つ目のユニキャスト通信は，「外部 NW 内の RT-1 と新 FW の通信」である。このエントリ登録通信シーケンスは，外部 NW 内の ARP シーケンスの後に続く，Flow-Mod（1）メッセージの送信である。

その二つ目が，本小問で取り上げられている。ユニキャスト通信はこの後すぐ解説しよう。エントリ登録の通信シーケンスは，3 番目の箇条書きに明記されているとおり，Flow-Mod（2）メッセージの送信である。

Flow-Mod（2）メッセージは DMZ 内の ARP シーケンスの後に続いている。

ARP Request パケット⑦を送信したノードは，新 FW（DMZ 側インタフェース）である。これをフラッディングしたものがパケット⑧～⑩である。これを受け，ARP Reply パケット⑪を送信したノードは，LB である。

この DMZ 内の ARP シーケンスを通し，OFC は，次の二つのノードの情報を得ることができる。

- MAC アドレス m1（新 FW）をもつノードが，OFS1 のポート p7（v2）の先に

ある。

- MAC アドレス m2（LB）をもつノードが，OFS1 のポート p6 の先にある。

ここから得た情報に基づき，新 FW と LB 間のユニキャスト通信に対応するエントリを Flow-Mod（2）メッセージで登録する。そのエントリが，表 5「図 4 中の Flow-Mod（2）によって登録されるエントリ」で示されている。

このアドレス解決が完了した後，SYN パケット⑬が新 FW から LB 宛てに送信される。

ここまで理解できれば，解を導くことができる。

実際に，表 5 のエントリが，新 FW と LB のユニキャスト通信に対応していることを，エントリ 2 から確認できる。

エントリ 2 のパケット識別条件を見ると，ETH_DST（宛先 MAC アドレス）が m2（LB）であり，ETH_SRC（送信元 MAC アドレス）が m1（新 FW）である。

IN_PORT（入力ポート）は，送信元の新 FW が接続しているポートなので p7 である。p7 はトランク接続しているため，このポートから VLAN タグフレームを受信する。DMZ 内の ARP シーケンスから得られた情報であることを考慮すると，VLAN_VID は「v2」（DMZ）となる。

それゆえ，新 FW から LB 宛てのユニキャスト通信に対応していることが確認できた。

エントリ 1 は，エントリ 2 と逆方向の通信に対応している。すなわち，LB から新 FW 宛てのユニキャスト通信である。本問が問うているのは，この MF だ。

その内容は，ETH_DST と ETH_SRC を入れ替え，IN_PORT が ETH_SRC の接続ポートに変更したものになっている。

この ETH_DST の値は，「**m1**」（LB）となる。これが空欄**た**の解となる。

この ETH_SRC の値は，「**m2**」（新 FW）となる。これが空欄**ち**の解となる。

この IN_PORT の値は，送信元の LB が接続しているポートなので「**p6**」となる。これが空欄**せ**の解となる。

この VLAN_VID の値は，p6 がトランク接続していないことから，「**なし**」となる。これが空欄**そ**の解となる。

(6)

解答例

Push-VLAN，Set-Field VLAN_VID ＝ v2，Output（p7）

本問は，表 5 中のエントリ 1 の Action を問うている。

設問 2（4）で解説したとおり，表 5 のエントリ 1 は，LB から新 FW 宛てのユニキャスト通信に対応している。

この Action に登録する内容は，「LB からのパケットを新 FW に向けてフレームを出力する」というものである。

具体的に言うと，次のような処理が必要となる。

- VLAN タグの挿入
  LB はトランク接続されていないため，OFS に入力されるのは通常のイーサネットフレームである。一方，新 FW は OFS1 とトランク接続していることから，出力時に VLAN タグを挿入する必要がある。
- パケットの出力
  新 FW はポート p7 の先にあるため，ここから出力する。

この内容を，表 2「MF と Action の例」に列挙された Action 名を使って記述すればよい。

解を導くに当たり，参考になる Action は，表 4 中のエントリ 1 である。なぜなら，同じように，トランク接続されていないノードからのパケットを，トランク接続された新 FW に向けて出力しているからだ。具体的に指定する値が異なるだけで，Action に登録する内容は同じものになるはずである。

まず，VLAN タグの挿入について考察しよう。

表 4 のエントリ 1 を見ると，「Push-VLAN」「Set-Field VLAN_VID=v1」と記述されている。表 4 は外部 NW 内の通信なので VLAN_VID の値が v1 になっている。この VLAN_VID の値を，表 5 のエントリ 1 に合うように置き換えればよい。

表 5 の方は DMZ 内の通信なので，VLAN_VID は「v2」となる。

したがって，登録する Action は，「Push-VLAN」「Set-Field VLAN_VID=v2」となる。

次に，パケットの出力について考察しよう。

表 4 のエントリ 1 を見ると，「Output（p7）」と記述されている。表 4 は新 FW に向

けて出力しているので，Output の引数である出力ポート ID が「p7」になっている。この出力ポートの値を，表 5 のエントリ 1 に合うように置き換えればよい。

表 5 の方は出力先が新 FW なので，出力ポートは同じ「p7」でよい。

したがって，登録する Action は，「Output（p7）」となる。

以上をまとめると，正解は解答例に示したとおりとなる。

■設問 3

設問 3 は〔クラウドサービス利用拡大の検討〕について出題している。

本設問を首尾よく解くには，B 社 CDN と B 社 ISP を利用した NW の概要，及び，機械が Web アクセスする際の，DNS 通信と HTTP 通信の流れを理解しておく必要がある。そこで，これらの点についてまずは解説する。

● B 社 CDN と B 社 ISP を利用した NW の概要

同見出しの第 1 段落の箇条書きは，この NW の概要を説明している。

1 番目から 3 番目までの箇条書きは，通常の本運用環境に関する説明である。以下，これを「通常の本運用環境」と呼ぶことにしよう。

4 番目の箇条書きは，B 社の CDN を適用したときの説明である。以下，これを「CDN 適用時の本運用環境」と呼ぶことにしよう。

CDN を適用するのは高負荷が予想されるときである。CDN の適用は，B 社 API サービスを使って，必要な期間だけ行う。

4 番目の箇条書きに「世界中に設置されている B 社の CDN エッジサーバが，指定された B 社の IaaS 環境内の Web サーバ（以下，オリジンサーバという）の処理を代行する」とある。ここに「代行」とあることから，アクセスするサーバは，通常時はオリジンサーバとなり，CDN 適用時は CDN エッジサーバとなることが分かる。

しかし，クライアントである機械から見ると，通常であるか CDN 適用時であるかに関わりなく，同じ要領で本運用環境にアクセスしている。この点については，後ほど，「●機械が Web アクセスする際の，DNS 通信と HTTP 通信の流れ」の中で解説する。

2 種類ある本運用環境について，箇条書きに書かれている内容を整理すると，次のようにまとめることができる。

・通常時の本運用環境

- 本運用環境の Web-B へのアクセスは，B 社 ISP を経由する。
- 機械から Web-B へのアクセスは，FQDN“weblive.asha.example.com”を使っ

て行う。

- FQDN を Web-B 社のグローバルアドレス（図 1 中の i6）に変換する。

・CDN 適用時の本運用環境

- Web-B をオリジンサーバに指定する。
- B 社 CDN のエッジサーバが，オリジンサーバの処理を代行する。
- B 社 CDN を適用する場合には，B 社から割り当てられる FQDN“webasha.bshacdn.example.net”を使ってアクセスする。

●機械が Web アクセスする際の，DNS 通信と HTTP 通信の流れ

第 4 段落の 1 番目の箇条書きには，「機械の動作には，試行モードと本運用モードがある」と記述されている。

試行モードは，2 番目の箇条書きにあるとおり，「機械から Web-A」へのアクセスである。つまり，試行環境（Web-A）へのアクセスである。

本運用モードは，3 番目の箇条書きにあるとおり，「機械から Web-B」へのアクセスである。つまり，本運用環境（Web-B）へのアクセスである。

この本運用環境へのアクセスは，通常時と CDN 適用時によって経路が異なる。

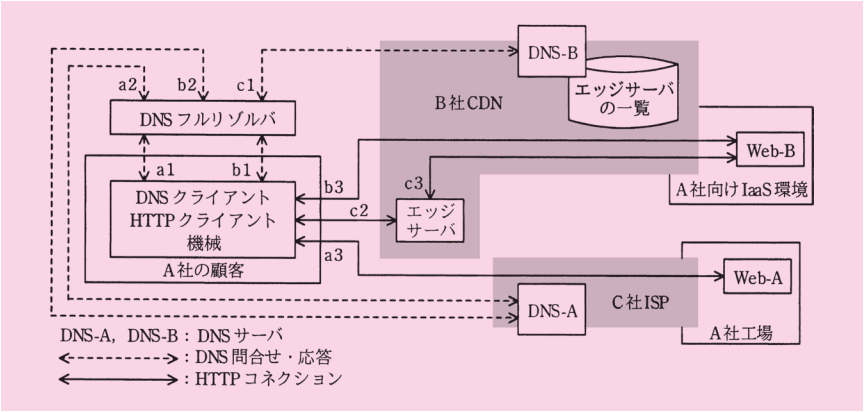
3 番目の箇条書きは，通常時のアクセスを説明している。

4 番目の箇条書きは，「本運用モードにおいて高負荷が予想される期間」とあるとおり，CDN 適用時のアクセスを説明している。続く 5 番目の箇条書きに「エッジサーバを選択（する）」とあるとおり，CDN 適用時は，Web-B をオリジンとするエッジサーバへアクセスする。

ここまでの内容を整理すると，機械が Web アクセスする経路は，次の 3 種類があることが分かる。2 ～ 4 番目の箇条書きに記された，図 5 中のアクセス経路も併せて掲載しておこう。

表：機械が Web アクセスする経路

アクセスの種類	モード	図 5 中のアクセス経路
試行環境（Web-A）へのアクセス	試行モード	a1，a2，a3
通常時の本運用環境（Web-B）へのアクセス	本運用モード	b1，b2，b3
CDN 適用時の本運用環境（エッジサーバ）へのアクセス	本運用モード	b1，b2，c1，c2，c3

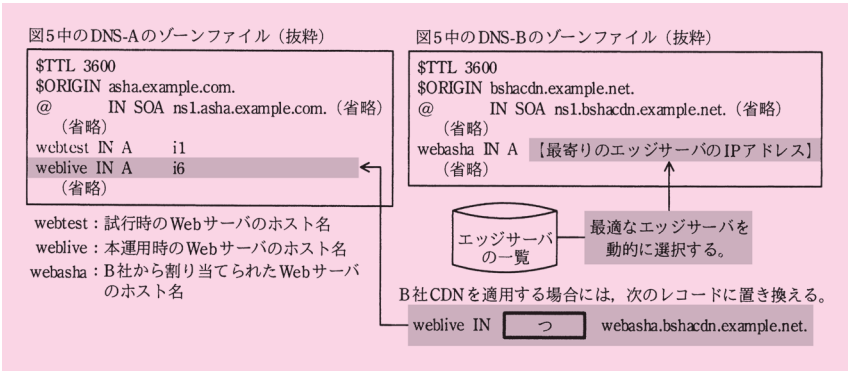


図：B 社 CDN を A 社に適用したときの概念図（図 5 の抜粋）

第 3 段落に「B 社 CDN を適用する場合には，図 5 中の DNS-A のゾーンファイルを書き換え，機械からのアクセスを，Web-B からエッジサーバへ切り換える」とある。その切換え方法を示したのが図 6 である。

試行環境へのアクセス，通常時の本運用環境へのアクセスは，DNS-A のゾーンファイルを用いて名前解決する。

一方，CDN 適用時の本運用環境へのアクセスは，図 6 に示す方法で DNS-A のゾーンファイルを書き換えたものを用いて，名前解決する。



図：D 君が考えたエッジサーバへの切り替え方法（図 6 の抜粋）

ここまで理解できれば，設問 3 を解く準備は整った。

3 種類のアクセス経路について，具体的な内容をまだ詳しく述べていないが，小問の解説を通して徐々に明らかにしていこう。

それでは，いよいよ小問の解説に移ろう。

(1)

解答例

つ：CNAME

つ

問題文は，「図 6 中の［　つ　］に入れる適切な字句を答えよ」と記述されている。

空欄つは，図 6 中の「B 社 CDN を適用する場合には，次のレコードに置き換える」と記述された，リソースレコードの中にある。そのリソースレコードを次に示す。

weblive IN ［　つ　］ webasha.bshacdn.example.net.

これによって置き換わるのは，DNS-A の中にある次のリソースレコードである。

weblive IN A i6

どちらのリソースレコードも，名前解決の対象となるホスト名は「weblive」である。図 6 を見ると，このホスト名について，「本運用時の Web サーバのホスト名」であると注記されている。

通常時は，機械が「weblive」の名前解決を問い合わせると，この A レコードが使われて「i6」が応答される。

設問 3 全体の解説で述べたとおり，通常時の本運用環境へのアクセスは，FQDN “weblive.asha.example.com” を使う（第 1 段落，2 番目の箇条書き）。「weblive」の FQDN は，ゾーンファイルの $ORIGIN の値で補完すると，「weblive.asha.example.com」となる。

この DNS 問合せ･応答を，図 5 のアクセス経路に当てはめると，「b1，b2」となる。名前解決の後，図 5 の「b3」のアクセス，すなわち，Web-B への HTTP アクセスが行われる。

CDN 適用時も，相変わらず「weblive」の名前解決を問い合わせる。このとき，先

ほどの A レコードは，空欄つを含むリソースレコードに置き換えられている。それゆえ，「webasha.bshacdn.example.net」が応答される。

要するにこのリソースレコードは，ホスト名を問い合わせたときに，別のホスト名を応答しているわけだ。このような応答をするリソースレコードは CNAME レコードである。

ここから，空欄つの解が導かれる。正解は「**CNAME**」となる。

●参考：CDN 適用時のアクセス経路

正解は導いたが，この CNAME レコードを使ってどのように名前解決が行われるのだろうか。図 5 を見ると CDN 適用時のアクセス経路はこの後も続くので，さらに解説しよう。

これまで明らかにしたアクセス経路について，いったん整理しておこう。

CDN 適用時，「weblive」の名前解決を DNS-A に問い合わせる。そこで応答されるのが，CNAME レコードに定義された内容だったわけだ。

この問合せを，図 5 のアクセス経路に当てはめると，「b1，b2」となる。

今分かっているのは，ここまでだ。その次にどうなるかを，これから解説しよう。

b2 で応答された FQDN「webasha.bshacdn.example.net」は，設問 3 全体の解説で述べたとおり，CDN 適用時の本運用環境へのアクセスで使われる（第 1 段落，4 番目の箇条書き）。

この FQDN のホスト名は「webasha」であり，ゾーン名は「bshacdn.example.net」である。図 6 を見ると，このホスト名に対応する IP アドレスの登録は，DNS-B のゾーンファイルで行われている。

そのゾーンファイルには，次の A レコードが登録されている。

webasha IN A【最寄りのエッジサーバの IP アドレス】

ホスト名「webasha」の名前解決をするため，DNS-B にアクセスする。このとき，DNS-B の A レコードが使われ，最寄りのエッジサーバの IP アドレスが応答される。

この DNS-B への問合せを，図 5 のアクセス経路に当てはめると，「c1」となる。

名前解決の後，図 5 の「c2」のアクセス，すなわち，エッジサーバへの HTTP アクセスが行われる。

エッジサーバへの HTTP アクセスが GET リクエスト（ダウンロード）であり，かつ，エッジサーバがダウンロード用コンテンツをキャッシュしているとき，この c2 でアクセスはお終いになる。

一方，ダウンロード用コンテンツをキャッシュしていないとき，あるいは，HTTP アクセスが POST リクエスト（アップロード）であるとき，エッジサーバは「プロキシ」の動作をする（第 1 段落，4 番目の箇条書き）。そのとき，図 5 の「c3」のアクセス，すなわち，オリジンサーバ Web-B への HTTP アクセスが行われる。

(2)

解答例

webtest.asha.example.com

問題文は，「図 6 中のゾーンファイルの定義内容を参考にして，図 5 中の a1 によって名前解決される FQDN を答えよ」と記述されている。

設問 3 全体の解説で述べたとおり，図 5 中の「a1」は，試行環境（Web-A）へアクセスする経路に含まれている（第 4 段落，2 番目の箇条書き）。

したがって，本問は，試行環境にアクセスする際の名前解決について問うている。

この a1 は，機械から DNS フルリゾルバへの DNS 問合せ・応答である。

DNS フルリゾルバとは，DNS クライアントから再帰的問合せを受け付け，世界中の DNS サーバに対し反復的な問合せを行う DNS サーバのことである。

機械から a1 の問合せを受けた DNS フルリゾルバは，a1 の結果が得られるまで，世界中の DNS サーバに問い合わせる。その際，ルート DNS サーバから開始し，順々にゾーンを下りながら，権威 DNS サーバに問い合わせていく。これが反復的問合せだ。

この反復的な問合せの最後にたどり着いた権威 DNS サーバが DNS-A であり，このアクセスが図 5 の「a2」で表されている。

したがって，DNS フルリゾルバへの DNS 問合せ･応答（a1）は，次にその DNS フルリゾルバが行う問合せ･応答（a2）と，同じものである。つまり，本問は，「図 5 中の a2 によって名前解決される FQDN」を問うているのと，実質同じだ。

それでは，試行環境（Web-A）にアクセスするとき，名前解決される FQDN は何であろうか。

図 6 を見ると，ホスト名「webtest」について，「試行時の Web サーバのホスト名」であると注記されている。このホスト名の FQDN は，ゾーンファイルの $ORIGIN の値で補完すると，「webtest.asha.example.com」である。

したがって，これが，試行時に機械が問い合わせる FQDN となる。本問が問うているのはこの FQDN だ。

よって，正解は「webtest.asha.example.com」となる。

(3)

解答例

weblive.asha.example.com

問題文は，「図 6 中のゾーンファイルの定義内容を参考にして，図 5 中の b1 によって名前解決される FQDN を答えよ」と記述されている。

図 5 中の「b1」は，通常時又は CDN 適用時の本運用環境へアクセスする経路に含まれている（第 4 段落，3 ～ 4 番目の箇条書き）。

したがって，本問は，本運用環境にアクセスする際の名前解決について問うている。

この b1 は，機械から DNS フルリゾルバへの DNS 問合せ・応答である。

設問 3（2）の解説で述べたとおり，DNS フルリゾルバへの DNS 問合せ･応答（b1）は，次にその DNS が行う DNS 問合せ・応答（b2）と同じである。つまり，本問は，「図 5 中の b2 によって名前解決される FQDN」を問うているのと，実質同じだ。

ここまで理解できれば，本問の解を導くことができる。

通常時又は CDN 適用時の本運用環境へのアクセスについて，設問 3（1）の解説で既に述べている。本運用時に機械が問い合わせる FQDN は，「weblive.asha.example.com」である（第 1 段落，2 番目の箇条書き）。これが求める解となる。

よって，正解は「weblive.asha.example.com」となる。

(4)

解答例

D	N	S	ク	ラ	イ	ア	ン	ト	と	D	N	S	フ	ル	リ	ゾ	ル	バ	が	,	ネ	ッ	ト	ワ	ー	ク
上	で	離	れ	た	位	置	に	あ	る	場	合															

（39字）

問題文は，「本文中の下線（iv）について，より適したエッジサーバが選択される場合を，……述べよ」と記述されている。

下線（iv）は，〔クラウドサービスの利用拡大の検討〕の第 4 段落，5 番目の箇条書きにある。そこには，次のように記述されている。

・c1 において，DNS-B は，DNS メッセージの送信元 IP アドレスを基に，最適なエッジサーバを選択し，その IP アドレスを返す。（iv）EDNS-Client-Subnet（RFC7871）を使って DNS クライアントの情報が通知された場合には，その情報も利用し，より適したエッジサーバを選択する。

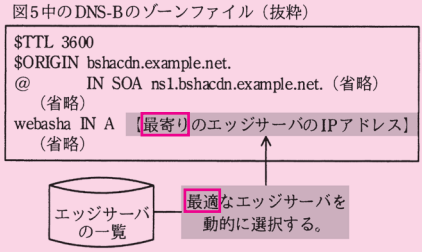
本問は，一般的な知識から解を導く。

本問の解を導くには，CDN が「最適」なエッジサーバを選択する方法，及び，下線（iv）に記された「EDNS-Client-Subnet」を理解する必要がある。そこで，まずはこの技術について解説し，次いで解を導こう。

● CDN が最適なエッジサーバを選択する方法

CDN 適用時の名前解決において，権威 DNS サーバは，問合せを受けた FQDN に対し，適切なエッジサーバの IP アドレスを応答する。それでは，何をもって「最適」と判断しているのだろうか。

その答えは，図 6 にある。あくまで本事例の B 社 CDN の場合であるが，次のように記述されている。



図：B 社 CDN が選択する，「最適」なエッジサーバ

ここに記されているとおり，「最適」なエッジサーバとは，「最寄り」のエッジサーバである。ここで言う「最寄り」とは，「クライアントから見てネットワーク的に最も近い位置にある」という意味である。

ここで幾つか疑問が湧いてくる。

1. ネットワーク的に近いエッジサーバが，なぜ最適であると判断できるのか。
2. ネットワーク的に近いエッジサーバを，どのように選択しているのか。

ネットワークの性能について学習する良い機会となるので，一般的な知識も含めて解説しよう。

●ネットワーク的に近いエッジサーバが，なぜ最適であると判断できるのか

あらかじめ断っておくが，この疑問に対する答えは，本文中で明確に与えられているわけではない。これから解説することは，一般的な知識に基づくものである。

CDN を適用するのは，高負荷時である。それゆえ，端的な答えは「性能を向上できるからである」と言えよう。では，もう少し掘り下げて，ネットワークの性能向上と，ネットワーク的な近さとは，どのような関係があるのだろうか。

一般的に言って，ネットワーク経由でやり取りするクライアント／サーバ間の通信品質に求められることは，応答性能である。本事例において，クライアントは機械であり，サーバは Web-B（本運用時）である。

この通信品質は，レスポンスタイムやターンアラウンドタイムなどの品質指標を用いて定量化される。

レスポンスタイムは，サービス時間と待ち時間の合計である。また，レスポンスタイムへの影響は，ネットワークに起因するものとサーバに起因するものがある。

この点を整理すると，次の表のようになる。

表：レスポンスタイムに影響するもの

	サービス時間	待ち時間
ネットワーク	①シリアル化遅延 ② RTT	④輻輳による遅延
サーバ	③処理の実行	⑤アクセス集中による遅延

結論から言おう。CDN 適用によって改善されるのは，「② RTT」「⑤アクセス集中による遅延」である。

このうち，「最寄り」のエッジサーバ選択によってもたらされる改善は，「② RTT」である。それゆえ，前述の疑問に対する答えは，「ネットワーク的に近いエッジサーバは，クライアントとサーバ間の RTT が短いので，レスポンスタイムが短い。それゆえ，最適であると判断できる」となる。要するに，「最適」の判断基準を RTT の短さにしているわけだ。

それでは，以下，手短に①～⑤の概要を解説しよう。

・①シリアル化遅延

「①シリアル化遅延」は，コンテンツの伝送時間である。これは，コンテンツのサイズが大きければ長くなり，ネットワークの帯域が太ければ短くなる。

CDN サービスを利用しても，コンテンツのサイズが変化するわけではないし，端末側の ISP 接続回線の帯域が変化するわけではない。

インターネットバックボーンは広帯域であるが，それに比べると端末側の ISP 接続回線の帯域は狭い。シリアル化遅延時間に関して問題視されるのは，端末側の帯域である。

したがって，CDN サーバにより最寄りのエッジサーバが選択されても，これを改善することはできない。

・② RTT

「② RTT」（Round Trip Time）は，パケットの往復時間である。これは，ネットワーク的に近ければ短くなる。

RTT は回線を通過するたびに発生する遅延時間なので，クライアントとサーバ間のやり取りが多いと，往復するたびに RTT がレスポンスタイムに加わってしまう。大容量のコンテンツであれば，当然ながらパケット数は大量になるので，RTT の合算値は無視できなくなるはずだ。

CDN サービスは，最寄りのエッジサーバを選択することにより，できる限り RTT を短くしようとしているのである。

・③処理の実行

「③処理の実行」は，クライアントが要求した処理をエッジサーバが実行する時間である。したがって，処理が軽く，サーバのスペックが高ければ，実行時間は短くなる。

とはいえ，これは，CDN サービスを利用しているか否かに関わりがない。

・④輻輳による遅延

「④輻輳による遅延」は，他の通信が同時に行われているため，ネットワークのどこかで待ち時間が発生していることを意味している。

この輻輳が，端末側の環境（ISP 接続回線やイントラネット）で発生しているならば，CDN サービスを利用しても制御することはできない。

したがって，CDN サーバにより最寄りのエッジサーバが選択されても，これを改善することはできない。

なお，インターネットのバックボーンは広帯域なので輻輳は発生しにくいと考えられるが，仮にどこかで発生した場合，最寄りのエッジサーバを選択することで回避できる可能性はある。

・⑤アクセス集中による遅延

「⑤アクセス集中による遅延」は，他の通信が同時に行われているため，エッジサーバで待ち時間が発生していることを意味している。

CDN サービスを利用すると，たくさんのエッジサーバで負荷分散できるので，「⑤アクセス集中による遅延」を改善できる。

とはいえ，これは「多数」のエッジサーバを用意することによってもたらされる改善であって，「最寄り」のエッジサーバを選択することによってもたらされるものではない。

もしかすると，「最寄りのエッジサーバ」を単純に選択するだけであれば，エッジサーバ間で負荷の偏りが生じるかもしれない。

以上をまとめると，最寄りのエッジサーバを選択する理由は，クライアントとサーバ間の RTT が短くなるため，その分だけ，高速性（低遅延）を実現できるからである。

●ネットワーク的に近いエッジサーバを，どのように選択しているのか

B 社の権威サーバ DNS-B は，DNS フルリゾルバから「weblive」の名前解決の問合せを受けたとき，「最寄り」のエッジサーバの IP アドレスを応答する。

この点を念頭に置き，下線（iv）を含む箇条書き（第 4 段落，5 番目の箇条書き）を振り返ってみよう。そこには，「c1 において，DNS-B は，DNS メッセージの送信元 IP アドレスを基に，最適なエッジサーバを選択し，その IP アドレスを返す」と記述されている。

つまり，DNS-B は，DNS フルリゾルバが送信した DNS メッセージ（問合せの IP パケット）から，送信元 IP アドレスを取得し，この IP アドレスを基に「ネットワーク的に近いエッジサーバ」を選択しているわけだ。

厳密に言うと，DNS フルリゾルバではなく，クライアント（機械）から見て，ネットワーク的に近いものを選択するべきである。しかし，従来の DNS 問合せでは，権威サーバは，直に問い合わせをしてきた DNS フルリゾルバの IP アドレスしか入手できない。

もっとも，ほとんどのケースでは，これで問題はないと言える。

通常，クライアントは，自分とネットワーク的に近い DNS サーバを DNS フルリゾルバに指定するからだ。例えば，会社の PC が自社の DNS サーバを DNS フルリゾルバに指定したり，自宅の PC が契約先 ISP の DNS サーバを DNS フルリゾルバに指定したりするケースが，これに該当する。

通常はこのケースに該当するので，DNS フルリゾルバの IP アドレスに基づく選択が，最適のものとなる。

しかしながら，例外はあり得る。DNS クライアントは，必ずしも自分とネットワーク的に近いわけではない DNS サーバ（Google Public DNS サーバ，Open DNS サーバ，等の公開キャッシュサーバ）を，DNS フルリゾルバに指定するかもしれないのだ。

こちらのケースに該当する場合，先ほど述べた方法で選択されたエッジサーバは，必ずしも最適とは言えなくなる。

この問題に対処するため，EDNS-Client-Subnet が登場した。

それでは，次にこの技術について解説しよう。

● EDNS-Client-Subnet

EDNS-Client-Subnet は，DNS クライアントが DNS フルリゾルバに名前解決を問い合わせる際，DNS クライアントのアドレスブロック（サブネット）を通知する技術である。

この問合せには，DNS 拡張プロトコルである EDNS0 を用いる仕様になっている。

DNS フルリゾルバは，反復的問合せを実施する際，問合せ先の権威 DNS サーバに対して，DNS クライアントのアドレスブロック（サブネット）を通知する。

この技術を使えば，権威 DNS サーバは，問合せを受けた FQDN について，真の意味で，クライアントとネットワーク的に近いエッジサーバを選択できるようになる。

●解の導出

本問は，EDNS-Client-Subnet（RFC7871）を使って DNS クライアントの情報が通知された際に，より適したエッジサーバが選択されるのはどのような場合であるかを問うている。

前述のとおり，EDNS-Client-Subnet を使用しなければ，ただ単に DNS フルリゾルバから見て近いエッジサーバを選択する。一方，これを使用すれば，真の意味で，クライアント（機械）から見て近いエッジサーバを選択する。

したがって，もしも DNS クライアントが，「自分とネットワーク的に近いわけではない DNS サーバを，DNS フルリゾルバに指定した場合」には，EDNS-Client-Subnet を使用すると，「より適した」エッジサーバを選択できるわけだ。

この点を字数に収まるように解答すればよい。

よって，正解は「**DNS クライアントと DNS フルリゾルバが，ネットワーク上で離れた位置にある場合**」となる。

(5)

解答例

W	e	b	-	B	の	サ	ー	バ	処	理	能	力	不	足	（15字）
機	械	と	W	e	b	-	B	間	の	通	信	遅	延		（14字）

問題文は，「本文中の下線（ｖ）の場合に，B 社 CDN の適用によって解消される TAT 悪化の要因を二つ挙げ（よ）」と記述されている。

下線（ｖ）は，〔クラウドサービスの利用拡大の検討〕の第 4 段落，6 番目の箇条書きにある。そこには，「機械から本運用環境への二つのアクセス（b3，c2）を比較したとき，（ｖ）HTTP の GET リクエストを使うファームウェアの一斉更新の場合に，B 社 CDN 適用による TAT（Turn Around Time）の改善が期待できる」と記述されている。

図 5 のアクセス「b3」は，通常時の本運用環境（Web-B）への HTTP アクセスである。「c2」は，CDN 適用時の本運用環境（エッジサーバ）への HTTP アクセスである。

それゆえ，下線（ｖ）は，「HTTP の GET リクエストを使う一斉更新の場合，CDN 適用時のエッジサーバへアクセスする方が，通常時の Web-B へアクセスするより，TAT の改善が期待できる」と述べているわけだ。

本問が問うているのは，この CDN の適用によって解消される「TAT 悪化の要因」である。つまり，通常時の Web-B へのアクセスで生じていた「TAT 悪化の要因」のうち，CDN 適用時のエッジサーバへのアクセスによって解消されるものを問うている。

Web-B へのアクセスと，エッジサーバへのアクセスを比べると，相違点が二つある。

一つ目は，HTTP アクセスに応じるサーバの台数である。

二つ目は，ネットワーク的な距離である。

まず，一つ目の相違点について解説する。

Web-B へのアクセスの場合，A 社向け IaaS 環境に用意された，Web-B1，Web-B2 の 2 台である。LB を使うことで，2 台で負荷分散して HTTP アクセスに応じている。

これに対し，エッジサーバへのアクセスの場合，エッジサーバは「世界中に設置されている」（第 1 段落，4 番目の箇条書き）。何台あるか定かではないが，かなりの台

数で負荷分散して HTTP アクセスに応じることができるに違いない。

したがって，ファームウェアの一斉更新が行われたとき，負荷分散する Web サーバが 2 台しかない Web-B では，Web-B のサーバ処理性能不足による TAT 悪化が懸念される。このとき，CDN を適用すれば，負荷分散する台数が増えるため，TAT の改善を期待できる。よって，ここに述べた TAT 悪化の要因が，一つ目の解となる。

次に，二つ目の相違点について解説する。

Web-B へのアクセスの場合，A 社向け IaaS 環境が設置されているのは，B 社拠点（国内）である。「国内外の多数の機械」からのアクセスに対応する必要があるが（［目的 2］），国外の機械から見て，B 社拠点（国内）はネットワーク的に遠い位置にあり，通信遅延の懸念がある。

これに対し，エッジサーバへのアクセスの場合，最寄りのエッジサーバ（ネットワーク的に近い位置にあるエッジサーバ）の選択を期待できる。EDNS-Client-Subnet が使用されていれば，確実にそのような選択が行われる。使用されていなくても，多くの場合は機械と DNS フルリゾルバはネットワーク的に近い位置にあるだろうから，そのような選択を期待できる。

したがって，国内外の様々なところにある機械から一斉にアクセスが行われたとき，B 社拠点（国内）の 1 か所にのみ存在する Web-B では，機械と Web-B 間の通信遅延による TAT 悪化が懸念される。このとき CDN を適用すれば，各々の機械から見て最寄りのエッジサーバが応答するため，TAT の改善を期待できる。よって，ここに述べた TAT 悪化の要因が，二つ目の解となる。

以上をまとめると，正解は，「**Web-B のサーバ処理能力不足**」「**機械と Web-B 間の通信遅延**」となる。

■設問 4

設問 4 は〔A 社向け IaaS 環境のバックアップの検討〕について出題している。

これを検討するに至った理由について，第 1 段落は，「A 社向け IaaS 環境へのサーバ移行を順次進めており，A 社向け IaaS 環境が存在する B 社拠点（国内）が長時間使えないリスクを想定し，そのバックアップ対策（以下，DR という）を運用マニュアルに盛り込むことにしている」と述べている。

「DR」は，「Disaster Recovery」の略であり，災害復旧という意味である。つまり，ここに記されている「長時間使えないリスク」とは，国内拠点が広域災害に見舞われて長時間使えなくなるリスクを指している。

DR の前提条件について，〔A 社向け IaaS 環境のバックアップの検討〕の第 2 段落には，次のように記述されている。

DR の前提条件

自社の運用要員だけで対応できること

この前提条件に基づき，次の 2 案について「それぞれの DR 案に必要な NW に関する準備」を検討することとなった（第 2 段落）。

DR 案

（1）自社設備利用 DR 案

（2）B 社拠点（国外）利用 DR 案

第 2 段落には，案ごとに副見出しが設けられ，「NW に関する準備」について説明されている。

ここで言う「準備」は，どの時点で実施するものを指しているのだろうか。長時間使えなくなるというリスクが顕在化する前（平時），あるいは，顕在化した後（災害発生後の切換え時）のどちらだろうか。

本設問の小問は，この準備作業について具体的に問うている。作業時点を正確に見極めた上で，解答を作文しなければならない。

本文を注意深く読むと，平時の準備作業を指していることが分かる。

この点を裏付ける記述を本文から確認してみよう。

まず，「（1）“自社設備利用 DR 案”と NW に関する準備」の 3 番目の箇条書きを取り上げる。そこでは，DNS ゾーンファイルのリソースレコードの置換えについて説明しており，「そのための手順を用意する」と述べている。明らかに，手順の用意は平時に行うべきことだ。

次に，2 番目の箇条書きを取り上げよう。こちらは少々分かりづらいのだが，平時の作業と読める。そこでは，新工場 LAN の構成変更について説明しており，「OFC の管理ソフトウェアに，新工場 LAN の構成変更に関する定義を登録する」と述べている。「定義を登録する」とあるが，これは「平時にあらかじめ定義のみをしておいて，その内容を管理ソフトウェアに保存しておく」という意味である。

手間と時間のかかる作業をなるべく平時に行っておくことで，作業内容の正確性を確保でき，かつ，災害発生後の切換え作業を迅速化できる。

DR 案について概観したところで，それでは，いよいよ設問の解説に移ろう。

（1）

解答例

転用後の業務サーバのIPアドレスを，LBの振り分け先に追加しておく。（34字）

問題文は，「本文中の下線（vi）の準備作業を……述べよ」と記述されている。

下線（vi）は，〔A 社向け IaaS 環境のバックアップの検討〕，「（1）“自社設備利用 DR 案”と NW に関する準備」の第 1 段落の 1 番目の箇条書きにある。

「（1）“自社設備利用 DR 案”と NW に関する準備」の第 1 段落は，この案について，「工場の Web-A を使い，A 社向け IaaS 環境の Web-B を代替する。Web-A の性能不足に備え，工場内の重要度が低い業務サーバを Web サーバに転用し，Web-A をスケールアウトする」と述べている。

スケールアウトとは，システムの処理性能を向上させるため，サーバの台数を増やして負荷分散させることを言う。システムが参照系の処理を実施している場合，スケールアウトは有効な手段となる。参照させたいコンテンツを多数のサーバに配置することで，サーバ 1 台当たりの処理負荷が軽くなり，結果として応答性能の向上が見込まれるからだ。

本事例において行われる処理は，「ファームウェアの一斉更新」（ダウンロード），「稼働状況の定期収集」（アップロード）である（［目的 2］）。前者が参照系，後者が更新系だ。それゆえ，前者の処理の性能向上にスケールアウトは効果的である。

Web サーバなので，ここで実施しているのは参照系の処理となる。それゆえ，「Web-A の性能不足」対策としてスケールアウトは有効であると言える。

Web-A は，LB と 2 台の Web サーバ（Web-A1，Web-A2）から構成されたシステムである。これをスケールアウトする方法は，「工場内の重要度が低い業務サーバを Web サーバに転用」すること，すなわち，LB の振り分け対象に業務サーバを加え，Web サーバの台数を増やして負荷分散することである。

この点を踏まえて，下線（vi）が引かれた 1 番目の箇条書きに目を向けよう。そこには，「（vi）転用後の業務サーバの IP アドレスを決め，それを用いて準備作業を行う」と記述されている。

本問で問うているのは，転用後の業務サーバの IP アドレスを決めた後に行う，準備作業である。設問 4 全体の解説で述べたとおり，この作業は平時に行うものである。

平時にできることは幾つもある。切換え時の手順やバックアップ運用時の体制など

を確立しておくことができるし，災害発生後の切換え作業を迅速化するために設定を保存しておくこともできる。どの観点に立って解を導いたらよいだろうか。

その手掛かりは，下線（vi）の中に与えられている。そこには，「転用後の業務サーバの IP アドレス」を用いて準備作業を行うとある。したがって，後者の観点，すなわち，具体的な設定を保存しておく作業を指していると推論できる。

業務サーバを Web サーバに転用することを見越し，あらかじめ保存できる設定として，様々なものが思いつくだろう。とはいえ，ここで問われているのは「転用後の業務サーバの IP アドレス」を用いた設定であるから，この点を考慮するとかなり絞り込まれる。

さらに，文脈を考慮するなら，「Web-A の性能不足に備え，工場内の重要度が低い業務サーバを Web サーバに転用（する）」というスケールアウト案に深く関係する準備作業が，ここでは主に検討されているはずだ。

このように本文の記述と照らし合わせることで，解が導かれていく。

前述のとおり，Web-A のスケールアウトは，LB の振り分け先となる Web サーバの台数を増やすことによって達成されるものである。スケールアウトするには，LB の振り分け先として，転用後の業務サーバの IP アドレスを LB に設定しておく必要がある。したがって，平時の準備作業として，LB にこの設定を保存しておくことができる。

よって，正解は，「**転用後の業務サーバの IP アドレスを，LB の振り分け先に追加しておく**」となる。

なお，試験センターの解答例は「LB の振り分け先に追加しておく」とある。これは，「平時から振り分け先として設定済みにしておく」と読める文章だ。

実際にそのように設定しても差し支えはない。

そのように言える理由は，LB は，振り分け対象のサーバの稼働状況をチェックしているからである（序文の第 5 段落，4 番目の箇条書き）。業務サーバ転用時の IP アドレスは，災害発生後のバックアップ運用時のみ使用する。平時は未使用であるため，この IP アドレスは，稼働状況チェックによって振り分け先の対象から外されるだけである。

このような，バックアップ運用時の設定を平時から適用することは，LB だからできる芸当だと言えよう。一般的に考えると，LB にせよ何にせよ，平時とバックアップ運用時の設定は分けておくべきだろう。

(2)

解答例

置換え前：weblive IN A i6
置換え後：weblive IN A i1

問題文は，「本文中の下線（vii）について，置換え前と置換え後のリソースレコードを，それぞれ答えよ。ここで，B 社 CDN は適用していないものとする」と記述されている。

下線（vii）は，〔A 社向け IaaS 環境のバックアップの検討〕の第 2 段落の中，「(1) “自社設備利用 DR 案” と NW に関する準備」の第 1 段落の 3 番目の箇条書きにある。そこには，「(vii) 図 6 中の DNS-A のゾーンファイルのリソースレコードを置き換えて，機械の本運用モードのアクセスを Web-A に切り換える」と記述されている。

下線（vii）によると，機械のモードは本運用モードになっている。それゆえ，機械が名前解決の問合せをするホスト名は，図 6 より「weblive」であることが分かる。

問題文に「B 社 CDN は適用していないものとする」とある。したがって，置換え前のリソースレコードは次のとおりである。

```
weblive  IN  A  i6
```

下線（vii）は「本運用モードのアクセスを Web-A に切り換える」と述べている。したがって，バックアップ運用時には，「weblive」の名前解決の問合せに対し，Web-A の IP アドレスを応答するようにリソースレコードを置き換えることが分かる。

Web-A へのアクセスは，試行モード時に行われる。そこで，試行モード時の名前解決で使われるリソースレコードから，Web-A のグローバルアドレスの値が分かる。

図 6 の DNS-A ゾーンファイルを見ると，試行時にアクセスするときのホスト名は「webtest」であり，これに対応する IP アドレスが「i1」である。

なお，この i1 は，図 1 の FW の外部 NW 側インタフェースに割り当てられたアドレスである（設問 1 空欄**あ**の解説の中で，この i1 がグローバルアドレスであることを述べている）。

したがって，バックアップ運用時には，weblive の名前解決の問合せに対し，i1 を応答するよう，先ほどのリソースレコードを置き換えればよい。

置換え後のリソースレコードは次のようになる。

weblive IN A i1

よって，ここに導いた，置換え前と置換え後のリソースレコードを解答すればよい。

参考までに，本文に書かれている準備作業は，このWeb-Aへの切換えの「手順」を用意することである。言うまでもなく，リソースレコードの置換えは平時に行うことではない。平時にできるのは，その手順を確立しておくことだ。

(3)

解答例

①転用する業務サーバに関する物理配線の変更が不要になる。
（27字）

②管理ソフトウェアを用いて，社内要員だけで対応できる。
（26字）

問題文は，「新工場LANを使った自社設備利用DR案について，現行の工場内LANを使った自社設備利用DR案と比較して，障害復旧時間（RTO）が短縮できる要因を二つ挙げ（よ）」と記述されている。

ここで障害復旧時間と書かれているRTO（Recovery Time Objective）は，災害復旧時の品質指標としてよく用いられている。これは，災害が発生してからシステムが再開するまでの時間である。

ハードウェアの部位が故障するといった局所的な障害の場合，フェールオーバなどの高信頼性技術を活用し，迅速な再開が可能だ。

しかし，災害などの広域的な障害の場合，復旧自体が大掛かりな作業となるし，ときには人手を介した作業が必要になることもあるため，再開までに時間がかかってしまう。

こうした点を念頭に置いて，新工場LANを使った自社設備利用DR案と，現行の工場内LANを使った自社設備利用DR案を比較してみよう。

2案の比較に当たり，押さえておくべき点がある。

それは，どちらの案を採用するにせよ，バックアップ運用時のWebサーバのNW構成は同じだということである。そのNW構成とは，〔A社向けIaaS環境のバックアップの検討〕の第2段落の中，「(1)“自社設備利用DR案”とNWに関する準備」の第1段落にあるとおり，「工場のWeb-Aを使い，A社向けIaaS環境のWeb-Bを代替する」

というものだ。

他にも，特に明記されていない事柄（障害検知，切換え後のテスト実施，等）は，どちらの案も基本的に同じだと考えることにする。

したがって，解を導くには，あくまでも 2 案の相違点に着目した上で，RTO を比較しなければならない。

その相違点は，SDN 技術の導入である。今回の NW 拡張の目的の一つであり，冒頭の解説の中で，［目的 1］として整理した点だ。

改めてこの［目的 1］を確認しておこう。

それは，序文の第 4 段落，1 番目の箇条書きに記されている。

そこには，「工場 LAN の SDN 化」というタイトルが掲げられており，次のように記述されている。「SDN 技術を用いて，現在の工場 LAN を，ビジネス変化に対応できる柔軟性と拡張性を備えた新たな工場 LAN（以下，新工場 LAN という）に刷新する。新工場 LAN では，物理配線の変更なしに，自社要員だけで構成変更ができるようにする」。

言うまでもなく，SDN 技術は，ビジネス変化による構成変更だけでなく，災害発生時の構成変更にも柔軟に対応できる。

ここに記述されている内容を整理すると，SDN 技術は，次の二つの点で優れていることが分かる。

1. 物理配線の変更なしに構成変更ができること
2. 自社要員だけで構成変更ができること

まず，一つ目の「物理配線の変更なしに構成変更できること」について考察しよう。

通常，物理配線の変更とその確認には手間と時間がかかる。NW の構成変更時にこれを削減できるのは大きな利点だ。本問が問うている RTO の短縮に寄与するのは明らかである。

次に，二つ目の「自社要員だけで構成変更ができること」について考察しよう。

「現行の工場内 LAN を使った自社設備利用 DR 案」では，自社要員だけで構成変更ができるのだろうか。

この点について，〔A 社向け IaaS 環境のバックアップの検討〕の第 2 段落に，「A 社では，サーバ，LB，DNS-A の運用は自社の運用要員が行い，それ以外の NW 機器の運用は，ベンダに委託している。NW 拡張後は，自社の運用要員が，OFC の管理ソフトウェアを使って新工場 LAN の構成を変更（するようになる）」と記述されている。それゆえ，ルータ，L2SW，FW を含む構成変更は，現行では自社要員で行えることに

限界がありそうだ。

広域災害の発生時に，この構成変更をベンダに委託するとしたら，どうなるだろうか。仮に平時であっても現地に出向くための時間がかかるのに，広域災害の混乱時となれば通常以上に時間がかかることだろう。

したがって，自社要員だけで構成変更を行えることは，こうした時間を削減できるわけだから，RTO の短縮に寄与すると言える。

ここに挙げた 2 点以外に，SDN 技術は別の点でも優れている。全てをソフトウェアで定義する技術なので，次の三つ目を挙げることができる。

3. バックアップ運用時の NW 構成をあらかじめ平時に定義して保存し，災害発生後の構成変更時にこれを適用できること

この点について，〔A 社向け IaaS 環境のバックアップの検討〕，「(1)“自社設備利用 DR 案”と NW に関する準備」の 2 番目の箇条書きに，「OFC の管理ソフトウェアに，新工場 LAN の構成変更に関する定義を登録する」と記述されている。設問 4 全体の解説で述べたとおり，この箇条書きが言わんとしているのは，「平時にあらかじめ定義のみしておいて，その内容を管理ソフトウェアに保存しておく」ということだ。

これは，平時に時間をかけて慎重に定義することで正確性を確保できること，保存した定義内容をすぐさま適用することでバックアップ運用環境への切換え時間を短縮できること，といった利点をもたらす。特に後者は，本問が問うている RTO の短縮に寄与する。

それでは，ここまでに述べたことを整理しよう。

新工場 LAN を使った自社設備利用 DR 案と，現行の工場内 LAN を使った自社設備利用 DR 案を比較すると，前者は SDN 技術を導入している点が異なっている。

この SDN 技術という相違点に着目して 2 案を比較すると，RTO に差が出てくることが分かる。次の三つの要因から，前者の方が短いという結論を導ける。

一つ目は，物理配線の変更なしに構成変更を行えることだ。

二つ目は，自社要員だけで構成変更を行えることだ。

三つ目は，管理ソフトウェアに保存した定義内容を適用して構成変更を行えることだ。

本問が求めているのは，前者の RTO が短縮できる要因を二つ挙げることである。

それでは最後に，ここに挙げた三つの点を二つにまとめてみよう。

ここから先は，答案をいかに仕上げるかの話になる。試験に合格するには大事なプロセスだ。

ここで，本小問の解説の中で引用した，〔A 社向け IaaS 環境のバックアップの検討〕の第 2 段落の記述を思い起こしてみよう。そこには，「NW 拡張後は，自社の運用要員が OFC の管理ソフトウェアを使って新工場 LAN の構成を変更（する）」と記述されている。

この言い回しを使って作文したら，二つ目と三つ目を一緒にできそうだ。「管理ソフトウェアを用いて，自社要員だけで対応できる」といった文案が思い浮かぶ。

よって，正解は解答例に示したとおり，次のようになる。

①転用する業務サーバに関する物理配線の変更が不要になる。

②管理ソフトウェアを用いて，社内要員だけで対応できる。

●参考：二つ目の解答について

本書の序章「0.3.5」で，「2. 本文より一歩掘り下げて，できるだけ具体的に解答する」という解答テクニックを紹介した。稀なケースであるが，本小問の二つ目の解答は，本文の〔A 社向け IaaS 環境のバックアップの検討〕の第 2 段落の記述を，ほぼ引用したものになっている。

とはいえ，この解答テクニックが役立たないという意味ではないことを申し添えておこう。

この解答テクニックで著者が主張したかったことは，「技術者でなければ導けないような解答が求められている」ということである。

そのように考えると，ここで問われている「RTO 短縮の要因」に対し，本文の「自社の運用要員が OFC の管理ソフトウェアを使って新工場 LAN の構成を変更（する）」を解として導き出すには，技術のバックグラウンドが必要である。

情報処理技術者試験は，国語力は求められているものの，現代国語の試験のように，本文から答えを論理的に導き出すわけではない。問いから答えを導くためには，本文中の手掛かりを前提に，技術者の知識と経験を駆使して推論を「補強」する必要がある。この補強された推論を首尾よく行えるかどうかで技術力が評価されているわけだ。

通常は，その「補強」が解答にも反映され，結果として本文より一歩掘り下げた表現になるものだと心得ていただきたい。

(4)

解答例

CDN，ISP，IaaS環境の構築と切替えに関する，
APIサービスとDNSを使った手順の確立　（46字）

問題文は，「B 社拠点（国外）利用 DR 案の NW に関する準備を，……述べよ」と記述されている。

B 社拠点（国外）利用 DR 案の内容は，〔A 社向け IaaS 環境のバックアップの検討〕の第 2 段落の中，「(2)“B 社拠点（国外）利用 DR 案”とその準備」の第 1 段落に記述されている。そこには，「B 社 API サービスを使って，B 社拠点（国外）の A 社向け IaaS 環境も利用できるので，そこに Web-B のバックアップを作成する」とある。

つまり，当案は，B 社拠点（国外）に A 社向け IaaS 環境のバックアップを作成する，というものである。B 社 API サービスを使えば，自社要員だけで作成することができる。

その具体的な準備作業は，本文では省略されている。本問はこれを問うている。

設問 4 全体の解説で述べたとおり，この準備作業は平時に行うものである。つまり，災害発生後に B 社拠点（国外）にバックアップを作成するわけだから，これに備えて平時に行うことを問うているのだ。

解を導く上で参考になる表現が，「(1)“自社設備利用 DR 案”と NW に関する準備」の 3 番目の箇条書きにある。そこでは DNS の切換えについて説明しているが，肝心の準備作業は「**手順**を用意する」となっている。DNS の切換えは災害時に行うわけだから，平時に準備できるのは「手順」を確立することである。

本問も，これと同じように考えればよい。災害発生時のバックアップ作成に備えて，「何かの手順を確立する」という内容が答えになる。

それでは，B 社拠点（国外）にバックアップを作成する手順には，具体的に何があるだろうか。例えば，次のものが思い浮かぶ。

［IaaS 環境の構築］
- API サービスを用い，IaaS 環境のバックアップを作成する手順
- API サービスを用い，バックアップのサーバにデータを移行する手順

［IaaS 環境への切換え］

- C 社 ISP の DNS-A ゾーンファイルに登録された，ホスト名「weblive」に対応する IP アドレスを，バックアップの Web-B のものに置き換える手順
- API サービスを用い，B 社 CDN のオリジンサーバを，バックアップの Web-B に置き換える手順

見てのとおり，複雑かつ大量の作業内容だ。平時にじっくり検討し，手順を確立しておくべきである。

この内容をまとめたものが，本問の解となる。

答案には，次に示すようなキーワードを含めておくとよいだろう。

- IaaS 環境の構築
- CDN の切換え
- C 社 ISP の DNS の切換え
- API サービスの使用
- 前記の手順の確立

(5)

解答例

①国外を利用するので国内の広域災害の影響を回避できる。
（26字）

②B社CDNなどを使い通常時と同じ品質を保つことができる。
（28字）

問題文は，「B 社拠点（国外）利用 DR 案について，自社設備利用 DR 案と比べたときの利点を二つ挙げ（よ）」と記述されている。

自社設備利用 DR 案と比較したときの相違点は，次のとおりである。

1. 国外に設置していること
2. B 社の設備を使用していること

一つ目の相違点がもたらす利点は，国内の広域災害の影響を回避できることである。

ここでは DR 案を検討しているわけだから，広域災害というリスクを想定する必要があるので，これを利点として挙げておくべきだ。この解答は一般的な知識から導くことができる。

二つ目の相違点がもたらす利点は，本文の記述に基づいて解を導かなくてはならない。

B 社クラウドサービスの特徴は，API サービスで環境を構築できること，API サービスで B 社 ISP 利用時の通信速度を指定できること，CDN を利用できること，である。

まず，API サービスで環境を構築できることは，B 社に限らずクラウドサービス全般に言えることでもある。机上の操作でオンデマンドに NW を調達できることは，一般的にクラウドサービスが有する，オンプレミスと比較したときの利点となる。

とはいえ，ここで問われているのは，一般的なオンプレミスとの比較ではなく，自社設備利用 DR 案との比較である。こちらは SDN の管理ソフトウェアを使用し，同じように机上の操作で NW を構築できる。それゆえ，本事例においては大きな差異にはならない。つまり，API サービスで環境を構築できることは，利点にはならない。

次に，API サービスで B 社 ISP 利用時の通信速度を指定できることについては，シリアル化遅延時間を短くできるのは利点だと言えよう。ただし，国外拠点となるのが気になる点である。国内の機械から見たらネットワーク的に遠くなるからだ。これに対処するために RTT の改善が求められている。

最後に，CDN を利用できることについては，どのように言えるだろうか。

もしもバックアップ運用時に，ファームウェアの一斉更新が行われた場合，CDN を適用すれば本運用時と変わらない通信品質を保つことができる。

これに対し，自社設備利用 DR 案では，国内外の機械が A 社工場 1 か所に集中してアクセスしてくるため，通信遅延の懸念が生じることだろう。転用する業務サーバの台数が十分でないならば，サーバ処理性能不足の懸念も生じるだろう。

したがって，B 社拠点（国外）利用 DR 案は，自社設備利用 DR 案と比較したとき，CDN を利用できることが大きな利点となる。

以上を整理すると，B 社拠点（国外）利用 DR 案が有する，自社設備利用 DR 案と比べたときの利点は，「国外に設置しているため，国内の広域災害の影響を回避できる」「CDN を利用できるため，本運用時と変わらない通信品質を保つことができる」の二つとなる。

この点を字数に収め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。

問 2

出題趣旨

IEEE 802.11ac によって，無線 LAN でも G ビット／秒の高速通信が可能になった。無線 LAN は PC の使用場所を固定化しないので，柔軟性に富んだ PC 利用環境が提供される。しかし，電波を通信に利用することによって，通信の傍受が容易になることから，有線 LAN では考慮しなかった箇所でのセキュリティ対策が求められる。

本問では，無線 LAN を導入してオフィスをフリーアドレスにする事例を取り上げた。この中で，無線 LAN 技術の状況，無線 LAN で利用されている暗号化と認証方式，アクセスポイントの配置設計，ディジタル証明書の運用方法などについて解説した。

本問では，無線 LAN の導入に当たって必要となる技術面と運用面の課題を題材にして，受験者が，ネットワークの設計・構築・運用などの業務をとおして修得した能力が，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，無線 LAN を題材として，IEEE 802.11ac 規格の無線 LAN システムを導入してオフィスをフリーアドレスにする事例を取り上げた。その中で，無線 LAN の基本技術，無線 LAN で利用されている暗号化と認証方式，アクセスポイント関連技術，ディジタル証明書の配布と運用方法などについて出題した。

設問 1 では，a，b，c とも正答率は高かったが，e の正答率が低かった。IEEE 802.11i は，幅広く利用されている無線 LAN のセキュリティ規格なので，是非，知っておいてほしい。

設問 2 では，暗号化と認証について問うた。(2)の正答率は高かったが，(1)の正答率が低かった。暗号化と認証は，IPsec，TLS などでも行われている重要な技術なので，ネットワーク技術者も理解しておいてほしい。

設問 3 では，アクセスポイントの設置方法に関連する技術について問うた。全体的に正答率は高かったが，その中で，(5)の正答率が低かった。PoE ＋の呼称は技術者間の会話で使われるので，相互理解のためにも知っておいてほしい。

設問 4 では，ディジタル証明書を使った認証及びディジタル証明書の配布について問うた。(1)の正答率が低かった。ディジタル証明書を使った認証は，通信においては不可欠な技術であるので，認証の仕組みや認証時に必要となる情報について，十分理解しておいてほしい。

設問 5 は，既設 LAN への無線 LAN の接続構成について問うた。(1)では，オーセンティケータとなる機器の正答率が低かった。オーセンティケータは，認証処理を行うものである。本文中の記述から，無線 LAN コントローラ（以下，WLC という）が RADIUS サーバに問い合わせて，その結果を基に認証の可否の処理を行うことが分かるので，正答が導き出せたはずである。(5)の“理由”も正答率が低かった。本文中に，WPA2 で暗号鍵の基になる PMK（Pairwise Master Key）の保存方法が規定され，ハンドオーバ時の再生成が不要になったことが 記述されている。この記述と WLC の機能を基に考え，正答を導き出してほしかった。一方，(2)，(6)の正答率は高かった。(2)の結果から，無線 LAN のパーソナルモードの設定情報についてはよく理解できていることがうかがわれた。また，(6)の結果から，無線 LAN 導入後の通信パケットの流れについても，よく理解できていることがうかがわれた。

設問		解答例・解答の要点		備考
設問 1		a	2.4	
		b	5	
		c	any	
		d	共通	
		e	802.11i	
設問 2	(1)	f	ストリーム	
		g	同一	
		h	認証サーバ	
		i	MAC アドレス	
		j	認証	
	(2)	カウンタ値 c を AES で暗号化した結果と，暗号文ブロック e1 を XOR する。		
設問 3	(1)	**周波数帯域幅**	80	
		アンテナ本数	2	
	(2)	① ②	・WLC に通信の負荷が集中するのを抑制することができる。 ・認証後に WLC に障害が発生しても，その無線 LAN 端末の通信は継続できる。	
	(3)	電波干渉によって，通信障害が発生する。		
	(4)	**周波数帯のグループの数**	4	
		目的	・ハンドオーバをスムーズに行わせるため ・AP の負荷分散を行わせるため	
	(5)	**呼称**	PoE＋	
		最小供給電力	216	
設問 4	(1)	① ②	・CA の自己証明書 ・クライアントの秘密鍵	
	(2)	ダウンロードサーバの認証情報が漏えいすると，来訪者もクライアント証明書などがダウンロードできてしまう。		
	(3)	・クライアント証明書の有効期限を切らせた営業員 ・無線 LAN 導入後に営業部に配属された営業員		
設問 5	(1)	**サプリカントとなる機器**	NPC	
		オーセンティケータとなる機器	WLC	
	(2)	① ②	・ESSID ・PSK	
	(3)	㋑		
	(4)	ルータ 2 への接続ポートだけに，VLAN200 のポート VLAN を設定する。		
	(5)	**問題**	ハンドオーバができなくなる。	
		理由	NPC に配布した PMK と認証関連情報が WLC で保持されているから	
	(6)	AP → L2SW5 → L3SW → FW → L2SW1 →プロキシサーバ→ L2SW1 → FW →ルータ 1		

本問は，クライアント証明書による認証方式を採用した，無線 LAN システムの導入事例を取り上げている。

本問は，無線 LAN の暗号化方式と認証方式，AP の設置方法，ディジタル証明書の配布方法，既設有線 LAN への接続方法について問うている。

●本問の全体像

本事例に登場する Y 社は，オフィスビルの 2 フロアを使用している本社と，複数の営業所を拠点にもつ。

営業員にはノート PC（以下，NPC という）の他にモバイル Wi-Fi ルータ（以下，Wi-Fi ルータという）が貸与されている。社内では NPC を有線 LAN に接続して営業業務を行っている。

現在，営業部が抱えている課題が，〔営業部の課題と対策〕の第 1，第 2 段落の中で説明されている。その内容をまとめると，次のとおりである。

［課題 1］取引先の増加に伴って，接客エリアが不足している（第 1 段落）。
［課題 2］Wi-Fi ルータを持たない来訪者から，インターネット接続環境を提供してほしいとの要望が挙がっている（第 2 段落）。

折しも，Y 社では「書類の電子化を推進した結果，……保管している書類が半減し，机上の書類も一掃された。そこで，営業部の座席をフリーアドレスにしてオフィスエリアを縮小し，接客エリアを拡大することにした」（第 3 段落）。つまり，電子化の推進に伴って，課題 1 の解決の目途がついたわけだ。

続く第 4 段落には，「これらを実現する目的で，営業部フロアに無線 LAN システムを導入することに決め（た）」と記述されている。「これらを実現」とあるので，文脈を踏まえて考察すると，具体的に設定している目的は次の 2 点だと言える。

［目的 1］営業部のフリーアドレス化と接客エリアの拡大を実現し，課題 1 を解決すること
［目的 2］来訪者へインターネット接続環境の提供を実現し，課題 2 を解決すること

この目的を達成し，無線 LAN システムを導入するため，情報システム部（以下，情シスという）にプロジェクトが発足した。

無線 LAN システムの導入に向けて，技術的な調査と選定，設計に備えた検討を幾つ

か実施し，無線 LAN の設計を行う。

これら一連の作業は，本文の見出しに対応している。整理すると，次のようになる。

表：無線 LAN の設計

フェーズ	作業（本文の見出し）	主な内容
調査	無線 LAN 技術の調査と選定	アクセス制御方式と暗号化方式の調査
		IEEE802.11ac と 11n の選定
検討	暗号化方式と認証方式の検討	WPA2 の選定
		営業員の利用者認証にエンタープライズモードの EAP-TLS 認証を選定
	AP の設置方法の検討	WLC（無線 LAN コントローラ）製品の選定
		AP の設置場所の決定
	ディジタル証明書の配布方法の検討	RADIUS 製品の選定
		ダウンロードサーバの設置
設計	既設 LAN への無線 LAN の接続構成の設計	来訪者の利用者認証にパーソナルモードを選定
		営業員向け VLAN と来訪者向け VLAN の設定

・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
なし（序文）	• 現在の LAN 構成 • 図 1　本社の現在の LAN 構成	—	—
営業部の課題と対策	• 接客エリア拡大と無線 LAN 導入のプロジェクト発足	—	—
無線 LAN 技術の調査と選定	• 暗号化方式（WEP，WPA，WPA2）の比較検討 • 認証方式（パーソナル，エンタープライズ）の比較検討 • 図 2　カウンタモードによる暗号化手順	1	空欄 a ～ e
暗号化方式と認証方式の検討		2	(1) ～ (2)
AP の設置方法の検討	• AP の導入台数 • WLC による AP の管理 • AP の設置場所と電源供給 • 図 3　営業部フロアへの AP の設置イメージ	3	(1) ～ (5)

（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
ディジタル証明書の配布方法の検討	• ダウンロードサーバの機能とクライアント証明書の運用について検討 • ダウンロードサーバの設置場所	4	(1) ～ (3)
既設 LAN への無線 LAN の接続構成の設計	• 営業員 NPC 向けの VLAN 割当てと無線 LAN 接続方法 • 来訪者 NPC 向けの VLAN 割当てと無線 LAN 接続方法 • 図 4　既設 LAN に無線 LAN システムを導入したときの LAN 構成	5	(1) ～ (6)

それでは，いよいよ設問の解説に移ろう。

■設問 1

解答例

a：2.4
b：5
c：any
d：共通
e：802.11i

本問は空欄 a ～ e に入れる適切な字句又は数値を問うている。
この空欄は，〔無線 LAN 技術の調査と選定〕の表 1 ～表 3 の中にある。
順番に解説しよう。

a ，b

空欄 a，b は，表 1「IEEE 802.11 で使用される周波数帯」の中にある。
IEEE802.11n の周波数帯は 2.4GHz と 5GHz の 2 種類である。
これに対し，IEEE802.11ac の周波数帯は 5GHz の 1 種類である。
この数値を表 1 中の空欄に当てはめればよい。
よって，空欄 a の正解は「2.4」となり，空欄 b の正解は「5」となる。

c

空欄 c は，表 2「無線 LAN のアクセス制御方式」の中にある。

AP は，無線 LAN 端末間の通信を中継したり，無線 LAN セグメントと有線 LAN セグメントを中継したりするなど，無線 LAN 通信で重要な役割を果たしている。

ただ，1 台の AP だけでは電波の到達距離に限界がある。そこで，多数の無線 LAN 端末を収容する目的で，複数の AP からなる大規模な無線 LAN セグメントを構成するのが一般的である。この無線 LAN セグメントを ESS（Extended Service Set）という。

この ESS を識別するのが，ESSID である。一般的には，ESSID を SSID（Service Set ID）と呼ぶことが多い。この文脈でも SSID と表記しているので，以降の解説もそれに倣う。

通常は，無線 LAN 端末が通信を開始する際，接続したい ESS の SSID を指定した上で，AP に接続する。その AP は，当該端末と同じ ESS に属していなければならない。

その AP を介して，当該端末は，同一の ESS に収容された他の無線 LAN 端末と通信できる。さらに，その AP に接続された有線 LAN の端末とも通信できる。

ここで，前記の説明で，「通常は」と断りを入れたことに注目していただきたい。

実を言うと，SSID を明示的に指定して AP に接続する方法が，唯一規定されたものではない。

無線 LAN 端末は，SSID を指定せずに，通信状態が最も良い AP との接続を試みることができる。この方法による接続を「ANY 接続」という。

この ANY 接続を無線 LAN 端末が試みた場合，AP がこの接続を許可したときは，当該端末はその AP の ESS に収容された上で通信ができる。一方，AP がこの接続を拒否したときは，当然ながらその AP を介した通信ができないので，適切な SSID に設定し直してから接続を試みなければならない。

無線 LAN 端末上で ANY 接続を設定する際のユーザインタフェースは，多くの場合，SSID のフィールドを空白にしたり，あるいは「ANY 接続」である旨の設定をしたりする。

この点を踏まえて，空欄 c を含む表 2 に目を向けてみよう。そこには，次のように記述されている。

表：無線 LAN のアクセス制御方式（表 2 の抜粋）

方式	機能
c 接続拒否	SSID が空白又は c での接続要求を拒否する機能

機能欄に「SSID が空白」とあるので，ANY 接続を指していることが分かる。機能欄の文全体を見ると，ここでは，ANY 接続を拒否する機能を述べている。

したがって，その方式名は「ANY 接続拒否」となる。

よって，空欄 c の正解は「**ANY**」（又は小文字で「**any**」）となる。

d

空欄 d は，表 3「無線 LAN のデータ暗号化方式」の中にある。

空欄 d を含む文は，「RC4 と呼ばれる暗号化アリゴリズムを使用した［ d ］鍵暗号方式」と記述されている。

文脈上，RC4 という暗号化アルゴリズムがどの方式に分類できるかを述べていることが分かる。特定のアルゴリズムを，「鍵」と名の付く方式で分けるとしたら，「共通鍵暗号方式」と「公開鍵暗号方式」の 2 種類のうち，どちらかに入れることができる。

このうち，RC4 は共通鍵暗号方式に分類される暗号化アルゴリズムである。

よって，空欄 d の正解は「**共通**」となる。

e

空欄 e は，表 3「無線 LAN のデータ暗号化方式」の中にある。

無線 LAN のデータ暗号化方式は，この表に示されているとおり，WEP，WPA，WPA2 の 3 種類がある。

当初規定された WEP には脆弱性が見つかったため，IEEE802.11i が標準化された。ただし，この標準化には時間がかかったため，無線 LAN 機器ベンダの業界団体「Wi-Fi Alliance」が，WPA（Wireless Protected Access）という仕様を発表した。

この WPA では，暗号化方式と利用者認証方式の二つが規定されている。

Wi-Fi Alliance はその後，WPA の暗号化方式をより強固なものにした WPA2 という仕様を発表した。この WPA2 は，前述の IEEE802.11i の最終版を参考にしたものである。

WPA2 は，IEEE802.11i と完全に一致しているわけではないため，「IEEE802.11i 準拠」と言える存在だ。

この点を踏まえて，空欄 e を含む表 3 に目を向けてみよう。そこには，次のように記述されている。

表：無線 LAN のデータ暗号化方式（表 3 の抜粋）

方式	説明
WPA2 （Wi-Fi Protected Aceeess 2）	暗号化アルゴリズムは AES に対応し，暗号化プロトコルに CCMP（Counter-mode with CBC-MAC Protocol）を使用した，WPA よりも堅牢（ろう）な IEEE［ e ］準拠の方式

説明欄に，「WPA よりも堅牢（ろう）な IEEE［　e　］準拠の方式」とある。
よって，空欄 e の正解は「802.11i」となる。

前述のとおり，WPA2 は，暗号化方式と利用者認証方式を規定している。
暗号化アルゴリズムは，表 3 にあるとおり，AES を使用する。
利用者認証方式は，パーソナルモード（事前鍵共有を用いた方式）又はエンタープライズモード（認証サーバを用いた方式）が規定されており，この 2 種類の中からどちらかを選ぶことができる。エンタープライズモードの認証シーケンスには IEEE802.1X を利用する。
空欄 e の解を導く際には，これら二つの規格，「802.11i」と「802.1X」を混同しないように気を付けたい。
ここに IEEE802.1X が当てはまらないと言える理由は，空欄 e を含む文は，利用者認証を説明したものではないからである。
この表 3 は全体として暗号化方式を掲載したものであるが，空欄 e の文脈では，WPA2 そのものが準拠している規格について語っている。それゆえ，ここに当てはまる最も適切な規格名は IEEE802.11i となる。

■設問 2

(1)

解答例

f：ストリーム
g：同一
h：認証サーバ
i：MAC アドレス
j：認証

著者解答例

h（1 番目）：認証サーバ
h（2 番目）：AP

本問は空欄 f ～ j に入れる適切な字句又は数値を問うている。

この空欄**は**，〔暗号化方式と認証方式の検討〕の中にある。

順番に解説しよう。

f

空欄 f は，第 1 段落の（1）の中にある。そこには，「1 バイト単位の［ f ］暗号である RC4」と記述されている。

文脈上，RC4 という暗号化アルゴリズムがどの方式に分類できるかを述べていることが分かる。

暗号化アルゴリズムの方式を分類する方法には幾つか種類がある。その代表的な分類と，それぞれの方式に含まれるアルゴリズムの例を挙げる。

表：暗号化アルゴリズムの分類

分類		アルゴリズムの例
共通鍵暗号方式	ストリーム暗号方式	RC4
	ブロック暗号方式	AES
公開鍵暗号方式		RSA，DSA

こうした分類方法を念頭に置き，文脈に基づいて，空欄 f に入れる適切な字句を考察してみよう。

空欄 f を含む第 1 段落の（1）は，WEP が採用している暗号化アルゴリズムについて詳しく説明している。

- 1 バイト単位の［ f ］暗号である RC4 を使用している。
- 一つの AP と複数の無線 LAN 端末間で WEP キーを共有する。
- WEP キーと IV（Initialization Vector）を基に，暗号鍵であるキーストリームを生成する。

ここにある「キーストリームを生成する」という記述は，ストリーム暗号方式の処理内容を具体的に説明したものである。キーストリームを用いて「1 バイト単位」で暗号化することは，ストリーム暗号方式の大きな特徴である。

さらに，続く（2）は WPA について，（3）は WPA2 について，同様の詳しい説明が述べられている。例えば WPA2 が採用している暗号化アルゴリズムの AES について，次のように述べられている。

- AES はブロック暗号なので，暗号化するメッセージを一定サイズのブロック単位に分割して処理する必要がある。

ここにある「一定サイズのブロック単位に分割して処理する」という記述は，ブロック暗号方式の処理内容を具体的に説明したものである。このブロックの大きさは，AES の場合，16，24 及び 32 バイトの 3 通りある。このように，ブロック単位で暗号化すること（言い換えると，1 バイト単位で暗号化できないこと）は，ブロック暗号方式の大きな特徴である。

このように文脈を考慮すると，ここではストリーム又はブロック暗号方式の処理内容を取り上げて具体的な説明を述べていること，AES という暗号化アルゴリズムに対して「ブロック暗号方式」を当てはめていることが分かる。

したがって，RC4 という暗号化アルゴリズムの暗号方式について述べた空欄 f は，その二つの方式のいずれかであると推論できる。

RC4 はストリーム暗号方式に分類されるので，空欄 f の正解は「**ストリーム**」となる。

なお，RC4 は共通鍵暗号方式にも分類されるが，こちらは正解にならないだろうか。

そうならないと言える根拠は，本問が問うているのが「適切」な字句だからである。

これまで解説したとおり，文脈に照らすと，「ストリーム暗号方式」は具体性の度合いからして適切である。一方，「共通鍵暗号方式」では粗すぎるため不適切だ。

蛇足ながら，試験テクニックの観点からも，適切とは言い難い。

設問 1 空欄 d で RC4 に当てはまる暗号方式を出題しているが，この正解は「共通鍵暗号方式」である。試験では，何かしら明確な出題意図がない限り，通常は，同じ字句が当てはまる空欄には同じ記号を用いている。異なる空欄に同じ字句を入れる設問では，同じ字句を繰り返し用いてもよい旨，断り書きがある。

それゆえ，試験テクニックとして，「同じ RC4 について出題しているのに，わざわざ二つの空欄 d，f を設けている以上，それぞれ異なる暗号方式を問うているはずだ」と判断すべきだろう。

g

空欄 g は第 1 段落の（1）の中にある。

（1）は WEP について説明している。

WEP は，無線 LAN 通信が普及し始めた頃（2000 年前後）に用いられていた暗号化方式である。

WEP は，共通鍵暗号方式を採用している。この点について，第 1 段落には，「WEP は，一つの AP と複数の無線 LAN 端末間で WEP キーを共有（する）」「WEP キーと IV

を基に，暗号鍵であるキーストリームを生成する」と記述されている。

暗号化する通信の区間は，無線 LAN 端末と AP 間である。共通鍵であるキーストリームを生成する基となる WEP キーを，無線 LAN 端末と AP の双方に登録しておく必要がある。

この WEP キーを頻繁に変更することは，運用上の負担となる。このため，結果として同一の WEP キーが使われ続けることとなってしまい，WEP キーが漏えいすると通信の秘匿性を保てなくなってしまう。

この点を踏まえ，空欄 g を含む文を見てみよう。

そこには，「WEP は，［ g ］の WEP キーが使用され続けることに加え，暗号化アルゴリズムも複雑ではないことから，短時間での暗号解読が可能になっているので採用しない」と記述されている。

ここでは，WEP 暗号化方式の問題点を指摘している。空欄 g は WEP キーにまつわる問題である。それは，同一の WEP キーが使用され続けることだ。

よって，空欄 g の正解は，「**同一**」となる。

この第 1 段落で説明されているとおり，WEP 暗号化方式は幾つか問題点を抱えていた。そのため，より強力な暗号方式が望まれるようになり，WPA，WPA2 が登場した。

［ h ］

空欄 h は（2）の中に二つある。

（2）は WPA について説明している。

WPA は，WEP の脆弱性を解消するために登場した暗号化方式である。無線 LAN 通信の利用が拡大した当初から（2000 年頃），WEP の脆弱性が明るみに出て，その対応が急務となっていた。

WPA は，既に市中に普及していた AP や無線 LAN カードの買換えを必要とせず，ファームウェアのアップグレードだけで対応できることを目指して開発された。そのために採用した暗号化アルゴリズムは，TKIP（Temporal Key Integrity Protocol）である。

端的に言うと，TKIP の正体は，WEP の改良版である。暗号化アルゴリズムは WEP と同じ RC4 を使用するが，WEP よりも複雑な仕組みを用いて，共通鍵であるキーストリームを生成する。（2）には，そのキーストリーム生成手順の複雑さについての説明が述べられている。

TKIP の大きな特徴は，エンタープライズモードを使用することで，WEP が抱えていた「同一の WEP キーを使用し続ける」という問題を解消できることだ。このモードでは，無線 LAN に接続するたびに動的に生成する暗号鍵を使用するのである。

エンタープライズモードは，認証サーバを用いて無線 LAN 端末の利用者認証を行

う。無線 LAN 端末と認証サーバ間で，IEEE802.1X を利用した認証用の通信を行う。

なお，無線 LAN 端末は無線 LAN セグメントにあり，認証サーバは有線 LAN セグメントにある場合，無線 LAN と有線 LAN セグメントを接続しているのは AP となる。つまり，AP は両者の通信を中継する役割を担う。

利用者認証に成功した後，認証サーバと無線 LAN 端末は，256 ビットの PMK（Pairwise Master Key）を動的に生成する。その後，両者の通信を中継する AP にもこれは配布される（安全な方法で配布される）。

その後，無線 LAN 端末と AP 間で鍵生成のやり取りが行われ，PMK から一時鍵を生成する。この一時鍵は，実際の暗号化通信で使用される共通鍵の基となるものだ。

この点を踏まえ，空欄 h を含む文を見てみよう。空欄 h は（2）中に 2 か所ある。

実を言うと，著者は，1 番目と 2 番目の空欄 h に入る適切な字句が異なっていると判断している。試験としては「解なし」だ。

そこで，1 番目と 2 番目を分けて解説しよう。

●1 番目の空欄 h の解

1 番目の空欄 h を含む記述は，「IEEE 802.1X の認証成功後に［ h ］で動的に生成されてクライアントに配布される PMK」である。

よって，1 番目の空欄 h の正解は，「**認証サーバ**」となる。

より正確に言うと，PMK は認証サーバから無線 LAN 端末に配布されるわけではない。IEEE802.1X を使用した利用者認証を通し，認証サーバと無線 LAN 端末は，PMK の基となる「乱数」を共有する。

例えば，IEEE802.1X の認証方式として，EAP-TLS が指定されているとしよう（本事例はそうなっている）。EAP-TLS の認証に成功したとき，認証サーバと無線 LAN 端末は TLS のプレマスタシークレットを共有する。これが PMK の基となる「乱数」の正体だ。両者はそれぞれ，この乱数から PMK を生成する。

●2 番目の空欄の解

2 番目の空欄 h を含む文から，解を導くのに必要なところだけをピックアップしよう。その記述は，「一時鍵は，……PMK（Pairwise Master Key）を基に，無線 LAN 端末及び［ h ］の両者で生成される」である。

よって，2 番目の空欄 h の正解は，「**AP**」となる。

IEEE802.1X 認証，及び，認証サーバの PMK 配布について，詳しくは本書の第 8 章「8.4.3　IEEE802.1X」を参照していただきたい。

i

空欄 i は（2）の中にある。

（2）は WPA について説明している。空欄 i の文脈では，特に，WPA が採用している TKIP について説明している。

TKIP は，最終的な暗号化処理では，WEP と同じく RC4 を使用する。RC4 の共通鍵であるキーストリームの生成を，TKIP では WEP よりも複雑化している。これにより暗号の強度を高めている。

そのキーストリーム生成について説明しているのが，空欄 i を含む文章である。

キーストリーム生成は 2 段階で行われる。

第 1 段階目では，一時鍵，IV（48 ビット中の上位 32 ビット），無線 LAN 端末の MAC アドレスの三つを混合して生成する。このとき生成されるのがキーストリーム 1 である。

第 2 段階目は，キーストリーム 1 及び IV（48 ビット中の下位 16 ビット）を混合して生成する。このとき生成されるのがキーストリーム 2 である。

IV とキーストリーム 2 から，最終的なキーストリーム，すなわち共通鍵が生成される仕組みになっている。

IV はパケットを送信するたびにインクリメントされる。つまり，毎回変化する。前述の仕組みで生成されるキーストリームも，毎回，かなり複雑に変化するわけだ。

この点を踏まえ，空欄 i を含む文を見てみよう。

そこには，「TKIP では，フェーズ 1 で，一時鍵，IV 及び無線 LAN 端末の［ i ］の三つを混合してキーストリーム 1 を生成する」とある。

よって，空欄 i の正解は，「**MAC アドレス**」となる。

j

空欄 j は（3）の中にある。

この解を導くには，エンタープライズモードを用いた無線 LAN 通信の接続手順，並びに，WPA2 が規定している事前認証及び PMK キャッシュについて理解しておく必要がある。その点をまず解説し，次いで解を導こう。

●エンタープライズモードを用いた無線 LAN 通信の接続手順

エンタープライズモードでは，利用者認証に IEEE802.1X を用いる。

IEEE802.1X は，認証手順を定めているが，認証方式を固定化しているわけではない。EAP-TLS や EAP-PEAP 等の様々な認証方式を選ぶことができる仕組みになっている。

本事例では EAP-TLS が用いられているため，これを踏まえた説明を述べよう。

EAP-TLS では，ディジタル証明書を使用したサーバ認証とクライアント認証が行わ

れる。ここで言うサーバとクライアントを，無線 LAN 接続に当てはめると，サーバは認証サーバであり，クライアントは無線 LAN 端末である。

認証と接続の手順は次のとおりである。

①アソシエーション確立

IEEE802.11i 規格は，IEEE802.1X 規格の認証に先立ち，この段階でオープンシステム認証を行うこと（AP が実質的な端末認証を行わないこと）を定めている。

②IEEE802.1X 認証

無線 LAN 端末と認証サーバの間の主体認証である。

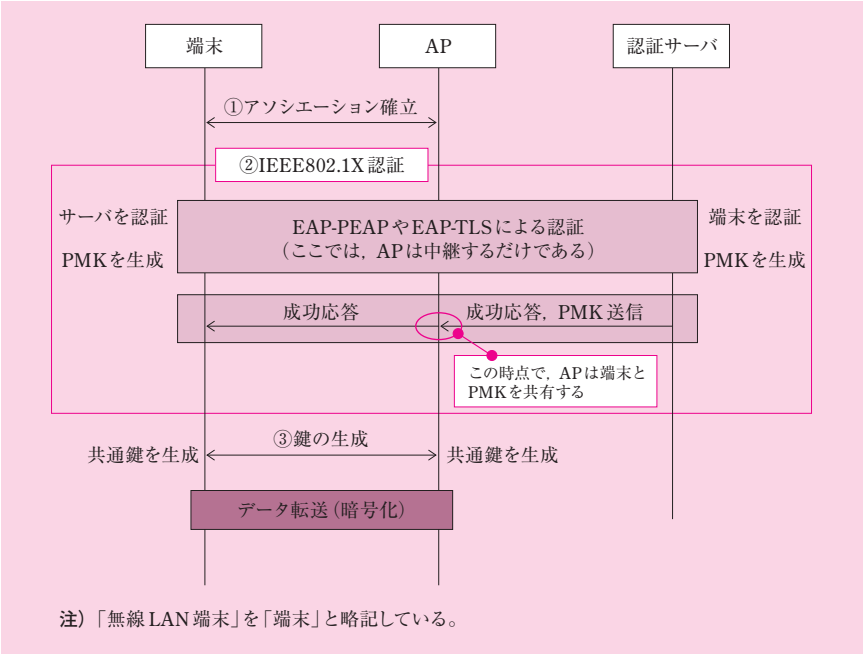
EAP-TLS を用いている場合，このやり取りは TLS で暗号化されている。

この認証に成功すると，無線 LAN 端末と認証サーバの間で PMK を共有する。

PMK を生成した後，認証サーバは AP に PMK を送信する。

③鍵の生成

空欄 h で解説した「一時鍵」が生成される。



図：エンタープライズモードを用いた無線 LAN 接続の手順

「①アソシエーションの確立」「② IEEE802.1X 認証」「③鍵の生成」を経て，ようやくデータ転送が行われる。このうち，最も時間がかかる手順は，「② IEEE802.1X 認証」である。

さて，この後すぐに解説する PMK キャッシュの布石として，ここで注目しておきたい点がある。

それは，手順②の中で，認証成功時に，認証サーバが AP に PMK を送信していることだ。認証サーバは，有線 LAN を通じ，安全な方法で PMK を AP に転送する。

この PMK は無線 LAN 通信の暗号鍵の生成に用いられるので，これを必要としているのは無線 LAN 端末と AP である。

無線 LAN 端末は，手順②の中でこれ生成済みだ。一方，AP は，手順②の TLS 暗号化通信を中継しているだけなので，これをもっていない。そこで，手順②の最終段階で，認証サーバから AP に PMK が転送されるわけだ。

●事前認証

複数の AP を備えた ESS 内で，無線 LAN 端末が AP 間を移動することがしばしば発生する。これをハンドオーバと呼んだり，ローミングと呼んだりする。

事前認証とは，このハンドオーバに備えて，近隣 AP との間で，IEEE802.1X 認証を事前に行っておくことである。

事前認証が済んでいれば，当該近隣 AP に移動した直後に行うことは，「①アソシエーションの確立」と「③鍵の生成」となる。したがって，最も時間のかかる「② IEEE802.1X」が不要となり，ハンドオーバに伴う通信の切断時間を大幅に削減できる。

無線 LAN 端末は，現 AP との無線 LAN 通信を行っている間，近隣 AP の電波も感知している。無線 LAN 端末は，電波状態等を考慮して，近隣 AP との間でいつでも事前認証を実行できる（事前認証をいつ行うかの判定方法は，実装依存である）。このようにしてハンドオーバに備えているわけだ。

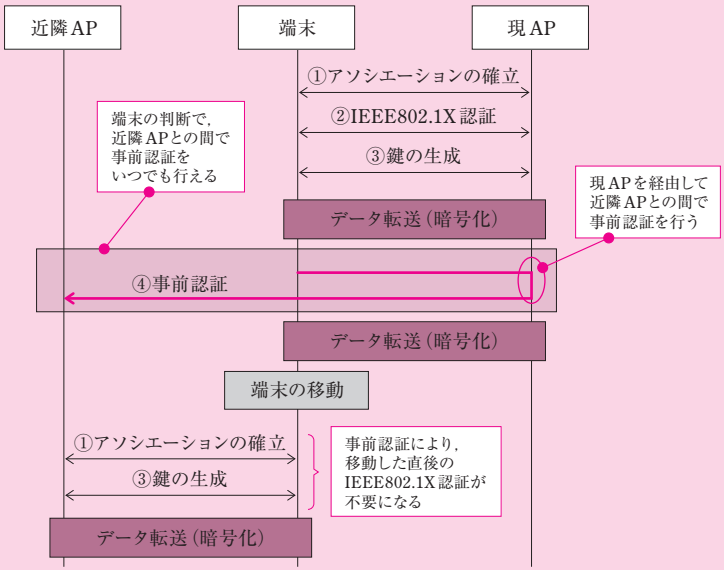
事前認証を行うには，幾つかの条件がある。

一つ目は，前述のとおりハンドオーバに備えるための条件である。無線 LAN 端末は，現 AP のセル（電波がカバーするエリア）と近隣 AP のセルが重なり合っている領域に，存在していなければならない。

二つ目は，AP 間で事前認証のやり取りを行うための条件である。アソシエーションは同時に 1 個の AP との間でのみ確立できるので，近隣 AP と通信するには，現 AP を経由する必要がある。したがって，現 AP と近隣 AP が有線 LAN で接続されており，現 AP を経由して無線 LAN 端末と近隣 AP 間で通信できなければならない。

事前認証の手順を次の図に示す。事前認証を行っているタイミングは，図中の「④

事前認証」である。



注）「無線 LAN 端末」を「端末」と略記している。この図では，認証サーバを省略している。

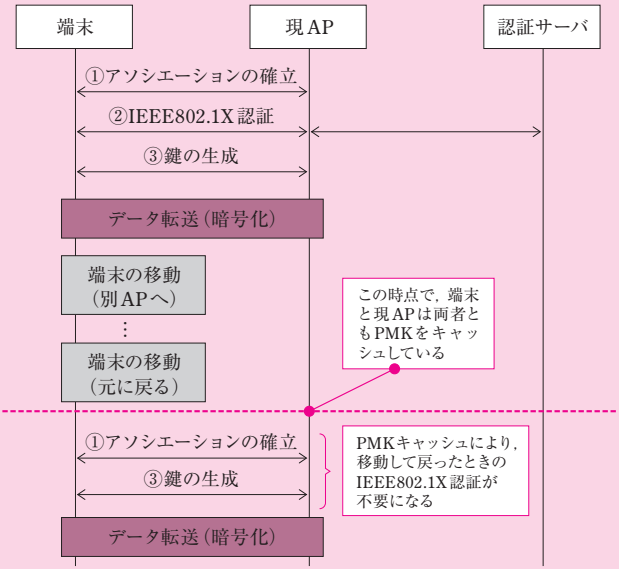
図：事前認証の手順

● PMK キャッシュ

PMK キャッシュとは，無線 LAN 端末と AP がそれぞれ PMK をキャッシュしておくことである。無線 LAN 端末は，現 AP から別の AP へ移動した後，元の AP のところへ戻ってくることがある。PMK をキャッシュしておけば，元の AP へ移動した直後に行うことは，「①アソシエーションの確立」と「③鍵の生成」となる。したがって，「② IEEE802.1X 認証」が不要となるわけだ。

このように，PMK キャッシュは，IEEE802.1X 認証を省くことができるという特徴をもつ。事前認証は，ハンドオーバ直後に IEEE802.1X 認証を行わないというだけであって，IEEE802.1X 認証そのものは AP ごとにあらかじめ行っておく必要がある。

PMK キャッシュの手順を次の図に示す。この図で，無線 LAN 端末は現 AP との間で接続した後，いったん別の AP に移動している。そして，再び元の AP に戻っている。このとき，PMK がキャッシュされているため，「② IEEE802.1X 認証」を省くことができる。



注）「無線 LAN 端末」を「端末」と略記している。この図では，別 AP へ移動する際の事前認証を省略している。

図：PMK キャッシュの手順

参考までに，無線 LAN コントローラの中には，無線 LAN 端末と認証サーバが生成した PMK を一元管理して，AP 間で PMK キャッシュを共有する機能をもつものがある。こうすれば，無線 LAN 端末が近隣 AP に移動するときにも同じ PMK キャッシュを使用できる。この結果，初回の一度だけ，IEEE802.1X 認証を行えばよい。

●解の導出

この点を踏まえ，空欄 j を見てみよう。

そこには，「WPA2 では，事前［　j　］の方法及び PMK の保持方法が規定されている。これらによって，無線 LAN 端末が AP 間を移動（以下，ハンドオーバという）するタイミングでの認証や認証済みの AP に戻ってきたときの PMK の再生成が不要になることから，ハンドオーバ時間が短縮される」と記述されている。

前述のとおり，事前認証によって，ハンドオーバ前に IEEE802.1X 認証が済んでいるため，「ハンドオーバするタイミングでの認証」が不要になる。

PMK キャッシュによって，「認証済みの AP に戻ってきたときの PMK の再生成」が

不要になる。

よって，空欄 j の正解は，「**認証**」となる。

(2)

解答例

カ	ウ	ン	タ	値	c	を	A	E	S	で	暗	号	化	し	た	結	果	と	,	暗	号	文	ブ	ロ
ッ	ク	e	1	を	X	O	R	す	る	。														

（36字）

問題文は，「本文中の下線①について，図 2 中の暗号文ブロック e1 を平文ブロック m1 に復号する手順を，……述べよ」と記述されている。

下線①及び図 2 は，〔暗号化方式と認証方式の検討〕の（3）の中にある。

（3）では，WPA2 が採用している暗号化アルゴリズムである，「AES をベースにした CCMP」について説明している。

（3）内の第 3 段落には次のように記述されている。

> AES はブロック暗号なので，暗号化するメッセージを一定サイズのブロック単位に分割して処理する必要がある。……CCMP ではカウンタモードが採用されている。カウンタモードでは，暗号化するメッセージをダイレクトに暗号化するのではなく，ブロックサイズと同じバイト数のカウンタ値を暗号化して，暗号化したカウンタ値と暗号化するメッセージとを XOR（排他的論理和）して暗号文を生成する。カウンタモードによる暗号化手順を図 2 に示す。

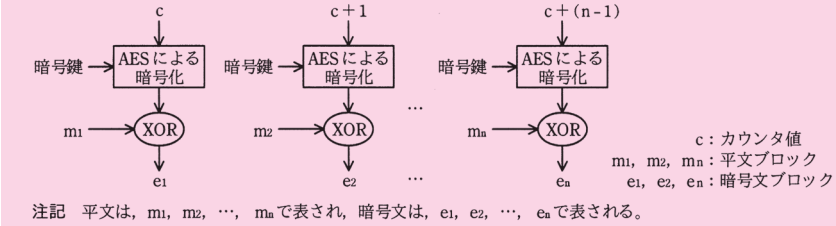


図 2　カウンタモードによる暗号化手順

> CCMP では，①暗号化と復号は同じ手順で行われ，復号時も AES が使用される。

図 2 を見ると，ブロックごとに，次の要領で暗号化手順を実施していることが分かる。ここで，カウンタ値 c，c + 1，……を暗号化したものを「暗号化カウンタ値」と呼ぶことにし，記号 d で表す。XOR 演算を記号⊕で表す。

【カウンタモードの暗号化手順】

$e_1 = d_0 \oplus m_1$
$e_2 = d_1 \oplus m_2$
$e_n = d_{n-1} \oplus m_n$

d の下付き添え字は，カウンタ値 c との差分とする。例えば，c の暗号化カウンタ値は d_0 となる。

カウンタモードの暗号化は，暗号化カウンタ値 d と平文 m から，暗号文 e を取得する処理である。したがって，この復号は，暗号化カウンタ値 d と暗号文 e から，平文 m を取得する処理であることが分かる。

一般的に言って，共通鍵暗号方式では，暗号化と復号を次に示す要領で実施している。ここで，k は共通鍵である。

【共通鍵暗号方式の暗号化手順】

$e = k \oplus m$ （式 1）

【共通鍵暗号方式の復号手順】

$m = k \oplus e$ （式 2）

念の為，式 2 を展開し，正しく復号できることを確認してみよう。

$$
\begin{aligned}
m &= k \oplus e \\
&= k \oplus (k \oplus m) \\
&= (k \oplus k) \oplus m \\
&= 0 \oplus m \\
&= m
\end{aligned}
$$

カウンタモードの暗号化手順では，上の式 1 の「k」に相当するのが，暗号化カウンタ値「d」となる。それゆえ，復号手順でも，「k」を「d」に読み替えればよい。

したがって，次の要領で復号手順を実施すればよいことが分かる。

【カウンタモードの復号手順】

$m_1 = d_0 \quad \oplus e_1$

$m_2 = d_1 \quad \oplus e_2$

$m_n = d_{n-1} \quad \oplus e_n$

本問はこの復号手順を問うている。

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

■設問 3

(1)

解答例

周波数帯域幅：80
アンテナ本数：2

問題文は，「本文中の下線②について，検討している AP 製品で最大 867M ビット／秒の通信速度を得るのに，最低限必要な周波数帯域幅とアンテナ本数を，それぞれ答えよ」と記述されている。

下線②は，〔AP の設置方法の検討〕の第 3 段落の中にある。

第 3 段落は，IEEE802.11ac 規格のチャネルボンディングと MIMO（Mutiple Input Mutiple Output）について説明している。

そこには次のように記述されている。

> IEEE 802.11ac 規格では，八つのチャネルを束ねる 8 チャネルボンディング（160MHz の帯域幅）を行えば，アンテナ 1 本当たり最大約 867M ビット／秒の通信が可能である。8チャネルボンディングと8本のアンテナによるMIMO（Mutiple Input Mutiple Output）で 8 ストリームの同時伝送を行えば，理論上最大約 6.93G ビット／秒で通信できる。②検討している AP 製品は，4 チャネルボンディング（80MHz の帯域幅）まで行え，3 本のアンテナが搭載されているので，1G ビット／秒の通信速度が達成できる。

チャネルボンディングとは，隣り合う帯域幅 20MHz のチャネルを複数束ねること

によって物理層の帯域幅を倍増する技術である。帯域幅が増えれば，その分だけ通信は高速化される。そのため，理論上は，束ねるチャネル数に比例して通信速度が増加する。例えば，2 チャネルを束ねれば，通信速度は 2 倍となる。

MIMO とは，送信側と受信側の双方で複数のアンテナを使うことによって物理層を高速化し，伝送速度を倍増する技術である。MIMO は，送信データを複数のストリーム（信号）に分割し，各ストリームをそれぞれ異なるアンテナを使って同時に送信する仕組みになっている。そのため，理論上は，アンテナ本数（ストリーム数）に比例して通信速度が増加する。例えば，2 本のアンテナを立てれば，通信速度は 2 倍となる。

したがって，チャネルボンディングと MIMO を使用したとき，理論上の通信速度は次式で求まる。

通信速度 = チャネルボンディング使用時の帯域幅 × アンテナ本数

チャネルボンディングするチャネル数は，IEEE802.11n では 2 チャネルまでであったが，IEEE802.11ac では 4 チャネルと 8 チャネルが可能となった。

本文によると，「八つのチャネルを束ねる 8 チャネルボンディング（160MHz の帯域幅）を行えば，アンテナ 1 本当たり最大約 867M ビット／秒の通信が可能である」。

本問は，下線②に示された AP 製品で，最大 867M ビット／秒の通信速度を得るための，周波数帯域幅とアンテナ数を問うている。求める周波数帯域幅は，チャネルボンディングするチャネル数に，1 チャネル当たりの周波数帯域幅 20MHz を乗じたものとなる。

下線②より，検討している AP 製品は 4 チャネルボンディグ（80MHz）まで行うことができ，アンテナの本数は 3 本まで用いることができる。それゆえ，通信速度を 867M ビット／秒にするには，周波数帯域を 80MHz にし，アンテナの本数を 2 本にする必要がある。

これが求める解となる。

よって，最低限必要な周波数帯域幅は「**80**」MHz となり，アンテナ本数は「**2**」本となる。

(2)

解答例

①WLCに通信の負荷が集中するのを抑制することができる。（27字）

②認証後にWLCに障害が発生しても，その無線LAN端末の通信は継続できる。（36字）

問題文は，「本文中の下線③の方式について，無線 LAN 端末による通信が WLC を経由する方式と比較したときの利点を二つ挙げ（よ）」と記述されている。

下線③は，〔AP の設置方法の検討〕の第 6 段落の中にある。

第 6 段落は，本事例で選定する無線 LAN コントローラ（以下，WLC という）について説明している。

そこには次のように記述されている。

> WLC は分散処理方式で，通信データの暗号化と復号を AP に任せるものである。WLC で EAP-TLS を利用するときは，AP と WLC 間でトンネルが設定され，無線 LAN 端末と WLC 間で認証情報の交換が行われる。WLC は，利用者認証を行った後，利用者 ID に対応した VLAN を AP に設定する認証 VLAN 機能をもっている。③認証後に行われる無線 LAN 端末による通信は，WLC を経由しない。

WLC は利用者認証に関与しているが，無線 LAN と AP 間の通信を中継する役割まで担っているわけではない。この点について，第 6 段落の初めに「WLC は分散処理方式で，通信データの暗号化と復号を AP に任せる」とある。

仮に，暗号化処理を WLC が実行していたら，無線 LAN と AP 間の通信は WLC を経由することになっただろう。しかし，ここを見ると，暗号化処理は各 AP に任せていることが分かる。本文はこれを「分散処理方式」と呼んでいる。

本問が問うているのは，認証後に行われる無線 LAN 端末と AP 間の通信について，WLC を経由しない方式（本事例の方式）と経由する方式を比較したとき，前者が有する利点である。

その答えは，先ほどの「分散処理方式」という記述をヒントにすれば，すぐに見つかるはずだ。前者の方式は，通信処理を AP に分散させる方式である。後者の方式は，通信処理を WLC に集中させる方式である。

分散と集中は，どちらも代表的な処理方式の形態である。

一般的に言って，分散型が有する利点は，主に二つある。

一つ目は高性能の利点であり，トラフィックや処理の負荷集中に起因する性能劣化を回避できることだ。二つ目は高信頼性の利点であり，処理を分散させるべく配置した機器同士で，冗長構成を実現できることだ。もっとも，二つ目の利点は，技術上，冗長化が実現可能である場合に限った話である。

それぞれの利点を，本事例の WLC に当てはめてみよう。

まず，一つ目の高性能の利点について考察する。

本事例の無線 LAN 端末は数十台に上る。第 4 段落には「最大で約 66 名の営業員（の端末）が同時」に無線 LAN に接続する可能性が示唆されている。これほど多数の端末の通信全てが WLC を経由するならば，WLC に通信が集中し，性能劣化が生じる可能性がある。

したがって，WLC を経由させないことの利点の一つ目は，WLC に通信の負荷が集中するのを抑制できることである。

次に，二つ目の高信頼性の利点について考察する。

先ほど「処理を分散させるべく配置した機器同士で，冗長構成を実現できる」と述べたが，このことが本事例の WLC に当てはまるだろうか。

繰り返しになるが，本事例の WLC は「通信処理を AP に分散させる方式」を採っている。つまり，「処理を分散させるべく配置した機器」とは，AP である。

本事例では，合計 12 台の AP を設置する（第 4 段落）。要するに，フロア内の無線 LAN 通信処理を，この 12 台の AP で分散処理するわけだ。このうち 1 台の AP が機能停止しても，フロア内で他の AP の電波が届く範囲に無線 LAN 端末を移動すれば，通信処理を継続できる。したがって，本事例の WLC では，通信処理の冗長化を実現できることが分かる。

この点を踏まえて，本事例の方式と WLC に処理を集中させる方式を比較すれば，前者の利点が明らかになる。前者は，WLC の障害発生時でも無線 LAN 端末の通信が継続できる。一方，後者は WLC が単一障害点となるため，同様の障害発生時に無線 LAN 端末の通信が途絶してしまう。それゆえ，前者は高信頼性の利点を有していると言える。

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

(3)

解答例

電波干渉によって，通信障害が発生する。（19字）

問題文は，「本文中の下線④の悪影響の内容を，……述べよ」と記述されている。

下線④は，〔AP の設置方法の検討〕の第 8 段落の中にある。そこには，「AP の設置場所は，営業フロアでの電波伝搬状態を測定してから決める。このとき，④外来電波による悪影響が発生する可能性があるかどうかを調査（する）」と記述されている。

これは，一般的な知識から解を導く。

自社の無線 LAN セグメントに，外来電波（別所の無線 LAN からの電波など）が入り込むと，電波が干渉してしまう。その結果，期待した通信速度が得られなくなるといった通信障害が発生する。

よって，正解は，「**電波干渉によって，通信障害が発生する**」となる。

(4)

解答例

周波数帯のグループの数：4
目的：ハンドオーバをスムーズに行わせるため（18字）
又はAPの負荷分散を行わせるため（14字）

問題文は，「図 3 の構成で AP を設置して，チャネルボンディングした周波数帯が重ならないようにするためには，少なくとも幾つの周波数帯のグループが必要になるかを答えよ。また，各 AP のセルを重ねる目的を，……述べよ」と記述されている。

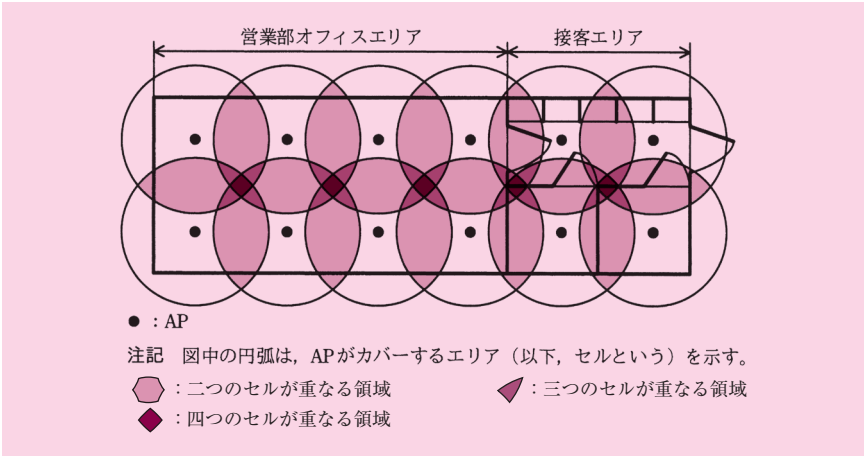
本小問は二つのことを問うている。

一つ目は，図 3 の構成で AP を設置したときの周波数帯のグループ数である。

二つ目は，図 3 の構成で各 AP のセルを重ねる目的である。

図 3 は，〔AP の設置方法の検討〕の第 7 段落の中にある。

図中の円弧は，AP がカバーするエリア（以下，セルという）を示している。この図を見ると，セルが重なっていることが分かる。その重なる部分を色づけした上で，ここに掲載しておこう。



図：営業部フロアへの AP の設置イメージ（図 3 に色を加えている）

この図を基に，以下，一つずつ解を導くことにしよう。

●一つ目の解：周波数帯のグループ数

ここでは，周波数帯のグループ数を問うている。

無線 LAN セグメントに AP を設置する際，AP にチャネルを設定する。チャネルごとに周波数帯が割り当てられているので，ここで問われているグループ数とは，AP に設定するチャネル数と同じである。

AP にチャネルを設定するとき，セルが重なる領域ができてしまう。この領域で電波干渉が発生すると通信障害に見舞われてしまう。

電波干渉の原因は，1 か所の領域に伝搬してくる複数の AP からの電波が，同じチャネル（周波数帯）に設定されているためである。したがって，重なり合うセルのチャネルがそれぞれ異なっていれば，電波干渉は発生しない。

この点を踏まえ，図 3 を見てみよう。

この図には，セルの重なる領域がかなりの部分を占めている。その重なり具合は様々であるが，セルの重なる数は最大で四つである。つまり，この領域で異なるチャネルが設定されていればよい。

したがって，チャネル数は 4 個必要となる。よって，正解は「**4**」となる。

●二つ目の解：各 AP のセルを重ねる目的

本事例では多数の AP を設置し，それら AP を WLC で管理している。

本小問の解を導くに当たり，WLC の機能を確認しておこう。

その点について，〔AP の設置方法の検討〕の第 4 段落の中で，次のように記述されている。

> WLC には複数の方式があったが，次の三つの主要機能をもつ製品を選定することにした。
> ・有線 LAN 経由での複数の AP に対する設定変更，ファームウェアのアップデータなどの一括処理機能
> ・AP の負荷分散制御，PMK の保持などによるハンドオーバ制御機能
> ・利用者認証，認証 VLAN などのセキュリティ対策

ここで着目すべき機能は，2 番目の箇条書きにある，AP 負荷分散制御，ハンドオーバ制御である。

結論から言うと，これら二つの機能を有効に働かせることが，各 AP のセルを重ねる目的であると言える。つまり，本小問の正解は二つ考えられるわけだ。

そこで，一つずつ機能を取り上げて，それぞれの解を導こう。

・AP 負荷分散制御に基づく解

AP 負荷分散とは，AP のセルが重なり合う領域において，無線 LAN 端末の接続先 AP を分散させ，AP の通信負荷を平準化する機能である。

無線 LAN 端末が AP とアソシエーションを確立する際，当該端末に電波の届く AP が複数あるとしよう。つまり，当該端末は，セルの重なり合う領域にいるわけだ。このとき，通信負荷が軽い方の AP が，このアソシエーション確立に応対する。

この機能が有効に働くには，セルの重なり合う領域を大きくとるとよい。

したがって，各 AP のセルを重ねる目的は，「**AP の負荷分散を行わせるため**」である。

これが一つ目の解となる。

・ハンドオーバ制御に基づく解

ハンドオーバ制御について，本文は「PMK の保持などによる」と補足している。

設問 2（1）空欄 j で解説したとおり，WPA2 が規定している事前認証機能と PMK キャッシュ機能により，ハンドオーバ時間の短縮が図られる。

簡潔に振り返ろう。事前認証機能は，セルが重なり合う領域に無線 LAN 端末が存在しているときに働く。これは，ハンドオーバに備えて，時間のかかる処理である IEEE802.1X 認証だけを事前に済ませておく機能だ。

PMK キャッシュ機能は，移動先 AP に，PMK がキャッシュされているときに働く。PMK を再利用できるので，ハンドオーバする際に本来必要となる IEEE802.1X の認証が，一切不要となる。

事前認証と PMK キャッシュにより，無線 LAN 端末が移動したとき，認証等に起因する通信の中断時間が短縮又は削減され，スムーズなハンドオーバが可能となる。

本事例の WLC は PMK を保持する機能を有している。これにより，ハンドオーバの移動先となる AP に対し，あらかじめ PMK を配布することができる。つまり，無線 LAN 端末から見ると，どの AP にも PMK がキャッシュされている状態になっているわけだ。

もちろん，WLC は PMK を保持しているとはいえ，管理下にある全 AP に PMK を一斉配信するわけではない。ハンドオーバに備えて，無線 LAN 端末の近隣にある AP を選んで配布している。その詳細は実装依存であるが，例えば，セルの重なり合う領域に無線 LAN 端末が移動してきたときに，そこをカバーしている AP が無線 LAN 端末を感知することにより，その AP を選んで配布するといった方法が考えられるだろう。

無線 LAN 端末がフロア内を移動しているとき，セルが重なり合う領域が大きければ，移動先方向にある AP がいち早く無線 LAN 端末を感知するため，移動前に PMK がキャッシュされやすくなるはずである。この結果，スムーズなハンドオーバが可能となる。

したがって，各 AP のセルを重ねる目的は，「**ハンドオーバをスムーズに行わせるため**」である。

これが二つ目の解となる。

・解の導出（まとめ）

以上より，各 AP のセルを重ねる目的が導かれた。

ここでは目的が二つ考えられるので，どちらか一つを答えればよい。

よって，正解は解答例に示したとおりとなる。

(5)

解答例

呼称：PoE ＋
最小供給電力：216

問題文は，「本文中の下線⑤について，IEEE 802.3at 規格の PoE 機能の呼称，及び当該 L2SW で今回必要になる最小供給電力を，それぞれ答えよ」と記述されている。

下線⑤は，〔AP の設置方法の検討〕の第 10 段落の中にある。そこには，「選定した AP 製品の消費電力は最大 18W なので，IEEE 802.3af 規格では供給電力が不足することが分かった。そこで，⑤ IEEE 802.3at 対応の L2SW を 1 台導入することにした」と記述されている。

本小問は二つのことを問うている。

一つ目は，IEEE802.3at 規格の PoE 機能の呼称である。

二つ目は，今回必要になる最小供給電力である。

以下，一つずつ解を導いてゆこう。

●一つ目の解：IEEE802.3at 規格の PoE 機能の呼称

これは，一般的な知識から解を導く。

まず，本小問で問われている PoE の概要を解説する。

PoE（Power over Ethernet）とは，イーサネットの LAN ケーブルを介して，あるネットワーク機器から別のネットワーク機器に電力を供給する技術である。

給電側のネットワーク機器を PSE（Power Source Equipment）と呼び，受電側のネットワーク機器を PD（Powered Device）という。あるネットワーク機器が PSE に接続されると，PSE はまず検出用の弱電圧をかけて電気抵抗を計測し，当該機器が PoE に対応しているか否かを確認する仕組みになっている。

PD として製品化されているネットワーク機器は低消費電力のものに限られるが，無線 LAN のアクセスポイント，IP 電話機，Web カメラなど，その種類は多岐にわたる。LAN ケーブルを敷設するだけで電力を供給できるという導入容易性から，無線 LAN や IP 電話網の普及とともに，PoE 対応機器の導入も広がりを見せている。

2003 年に策定された IEEE802.3af 規格は，カテゴリ 3 以上の LAN ケーブルを用い，1 ポート当たり最大 15.4W の電力を 100m まで供給できる。2009 年に策定された IEEE802.3at 規格では，カテゴリ 5E 以上の LAN ケーブルを用い，1 ポート当たり最大 30W の電力を 100m まで供給できる。

両規格の供給電力が異なっていることを鑑み，両者を容易に区別するための簡便な呼称が用いられている。IEEE802.3af 規格を PoE，IEEE802.3at 規格を PoE+ と呼ぶ。

PoE+ は，PoE の上位互換となっている。すなわち，PoE+ の PSE は，PoE+ 又は PoE の PD に電力を供給できる。一方，PoE の PSE は，PoE の PD にしか電力を供給できない。

それでは，PoE の概要を理解できたところで，いよいよ解を導こう。

IEEE802.3at 規格の PoE 機能の呼称は，前述のとおり，「**PoE+**」である。
よって，これが正解となる。

●二つ目の解：今回必要になる最小供給電力

PSE の供給電力は，次式から求まる。ここで，PD は同一の機種とする。

PSE の供給電力 ＝ PD の消費電力 × PSE に接続する PD の台数

今回の PD は，AP である。この消費電力について，下線⑤がある第 10 段落に「最大 18W」とある。AP の台数について，第 4 段落に「合計 12 台」とある。
したがって，PSE の供給電力は，次のとおりとなる。

PSE の供給電力 ＝ PD の消費電力 × PSE に接続する PD の台数
＝ 18W × 12 台
＝ 216W

本問は，給電側 L2SW に求められる最小供給電力を問うているので，この値を解答すればよい。よって，正解は「**216W**」となる。
余談であるが，試験センターの解答例は「216」となっている。常識的に見れば，PoE のような低電力機器で消費される電力の単位は W でよいだろう。とはいえ，国家試験である以上，こうした計算問題の出題に当たっては，単位を W（ワット）に定める旨の断り書きがあってしかるべきだろうと著者は考える。

■設問 4

設問 4 は〔ディジタル証明書の配布方法の検討〕について出題している。
本事例では，無線 LAN の利用者認証の方式として，EAP-TLS を採用する。
EAP-TLS は，TLS ハンドシェークプロトコルの手順に従って実施される。その真正性を確認するため，サーバ認証，クライアント認証の双方とも，ディジタル証明書が使用される。
エンタープライズモードで EAP-TLS を実施する場合，TLS のサーバに相当するのが「認証サーバ」となり，クライアントに相当するのが「無線 LAN 端末」となる。
EAP-TLS の実施に当たって，主に次に示す準備が必要となる。

1. ディジタル証明書の発行

サーバの公開鍵と秘密鍵を生成し，サーバの公開鍵のディジタル証明書（サーバ証明書）を発行する。

同様に，クライアントの公開鍵と秘密鍵を生成し，クライアントの公開鍵のディジタル証明書（クライアント証明書）を発行する。

2. サーバ証明書のセットアップ

サーバ証明書とサーバ秘密鍵を認証サーバにセットアップする。

3. クライアント証明書のセットアップ

クライアント証明書とクライアント秘密鍵を無線 LAN 端末へセットアップする。

このうち，十分な検討を要するのが，3 番目に示したクライアント証明書に関係するものである。設問 4 が問うているのは，まさにこの部分についてである。

これらの準備について，本文の記述を概観しておこう。

1 番目のディジタル証明書の発行について，第 2 段落には，「RADIUS サーバ製品は，EAP-TLS で必要になるディジタル証明書（サーバ証明書又はクライアント証明書）を発行する CA（Certification Authority）機能をもっている。サーバ証明書とクライアント証明書は，RADIUS サーバの CA 機能を使って発行する」と記述されている。

RADIUS サーバは，EAP-TLS の認証手順における「認証サーバ」に他ならない。要するに，認証サーバでディジタル証明書を発行することが分かる。

ちなみに，ここ第 2 段落では，公開鍵のディジタル証明書のことを述べているが，公開鍵の対となる秘密鍵のことを何も述べていない。なぜならば，まさにこの秘密鍵を小問（1）で問うているので，ここでは意図的に伏せているのだ。

2 番目のサーバ証明書のセットアップについては，認証サーバで発行した際，そのままセットアップすればよい。この点は特に本文で触れられていない。あえて言及しなくても，文脈から分かるからだ。

3 番目のクライアント証明書のセットアップに関し，「十分な検討を要する」と先ほど述べた。その理由が第 3 段落から読み取れる。

そこには，「情シスの担当者が本社の営業員の NPC に直接インストールすれば安全であるが，情シスの負担が大きい」とある。営業員は 110 名に達するため，いくら安全であっても負担がかかる方法は採用できない。それゆえ，安全性を確保しつつ，負担がかからない方法を検討する必要があるわけだ。

そこで見出した答えが，ダウンロードサーバを設置するというものである。

その点について，同じく第 3 段落の中で，次のように記述されている。

> 本社 LAN に，クライアント証明書を NPC にダウンロードさせるサーバ（以下，ダウンロードサーバという）を新規に構築して，LAN 経由でクライアント証明書を配布すれば情シスの負担が抑えられる。

営業員各自は，自分の NPC にクライアント証明書をダウンロードした後，インストールまで行う。その点について，第 4 段落の中で，次のように記述されている。

> ダウンロードサーバによるクライアント証明書の配布案内は，無線 LAN 導入後に，情シスから全営業員宛てに一斉メールで通知する。案内文には，ダウンロードサーバの導入目的，利用方法，ダウンロードサーバの URL などを記載する。その後，各営業員に，ダウンロードサーバ利用のための利用者 ID とパスワードを個別に連絡する。営業員は，情シスからの案内を基に，クライアント証明書のインストールを行う。

この方法を採用すれば，情シスの負担は確かに抑えられる。

しかしながら，情シスの担当者が直接関与していないことから，新たに検討すべき懸念事項が生じる。

それは，セキュリティを確保することであったり，営業員がダウンロードを行えないという事態を想定しておくことであったりする。

これらの点が，設問 4 の小問（2），（3）で取り上げられている。小問の解説の中で詳しく説明することにしよう。

それでは，いよいよ小問の解説に移ろう。

（1）

解答例

①CAの自己証明書　（8字）
②クライアントの秘密鍵（10字）

問題文は，「本文中の下線⑥について，NPC で必要になる情報を二つ挙げ（よ）」と記述されている。

下線⑥は，〔ディジタル証明書の配布方法の検討〕の第 5 段落，「（1）クライアント

証明書の管理機能」の中にある。そこには，「ダウンロードサーバは，RADIUS サーバで生成されたクライアント証明書と⑥その他に NPC で必要となる情報を RADIUS サーバからコピーし，RFC 7292 で規定されている PKCS #12 形式のファイルに変換して管理する」と記述されている。

問われている二つの情報は，クライアント証明書とともに，RADIUS サーバからコピーしたものである。したがって，RADIUS サーバが生成したものであることが分かる。

この点を踏まえて，解を導く必要がある。

結論から言うと，この二つの情報は次のものである。

1. RADIUS サーバの CA の自己証明書
2. クライアントの秘密鍵

以下，一つずつ解説しよう。

●一つ目の解：RADIUS サーバの CA の自己証明書

設問 4 全体の解説で先ほど述べたとおり，ディジタル証明書は RADIUS サーバで発行する。

本文では詳しく説明されていないが，この発行には，次の事柄が含まれている。先ほどの解説を改めて掲載しよう。大事なところを下線で強調しておいた。

> サーバの公開鍵と秘密鍵を生成し，**サーバの公開鍵のディジタル証明書**（サーバ証明書）**を発行**する。
> 同様に，クライアントの公開鍵と秘密鍵を生成し，クライアントの公開鍵のディジタル証明書（クライアント証明書）を発行する。

第 2 段落に「サーバ証明書とクライアント証明書は，RADIUS サーバの CA 機能を使って発行する」とあることから，ここで発行したディジタル証明書に署名するときに用いる署名鍵は，RADIUS サーバの秘密鍵である。言い換えると，これに署名した CA は，RADIUS サーバの CA である。

この秘密鍵（署名鍵）と対となる公開鍵（検証鍵）は，RADIUS サーバのディジタル証明書（以下，RADIUS サーバ証明書という）から取得しなければならない。それゆえ，サーバ証明書とクライアント証明書に付与された署名を検証するために，RADIUS サーバ証明書が別途必要となる。実はこれが，一つ目の「必要な情報」である。

ここで一つの疑問が浮かび上がる。

この RADIUS サーバ証明書は，どの CA が発行したものなのだろうか。

これを発行した CA を，「発行元 CA」と呼ぶことにしよう。

大きく分けて，発行元 CA の選択肢は 2 種類考えられる。「自分自身」（RADIUS サーバの CA）であるか，「自分以外」であるかのいずれかだ。

ディジタル証明書の発行には署名が必要である。署名の暗号化処理には発行元 CA の秘密鍵が必要である。ゆえに，RADIUS サーバ証明書の発行は，発行元 CA のサイトで秘密裏に行わなければならない。

下線⑤とこれに続く記述を見ると，「必要な情報」である RADIUS サーバ証明書の発行元が明らかになる。そこには，「必要な情報を RADIUS からコピー（する）」とあるのだ。

したがって，発行元 CA は，RADIUS サーバ自身であることが分かる。このような CA を「プライベート CA」という。

RADIUS サーバ証明書は，発行元 CA である自分自身が署名している。このようなディジタル証明書を「自己証明書」という。

以上より，一つ目の正解は，「**CA の自己証明書**」となる。

参考までに，RADIUS サーバの CA は，世間一般で信頼された「パブリック CA」ではない。それゆえ，TLS ハンドシェークプロトコルの手順に従ってサーバ認証を実施した場合，サーバ証明書の署名を検証した時点でクライアントのブラウザが警告を発してしまう。これを抑制するには，RADIUS サーバの CA の自己証明書を，ブラウザの「信頼された認証局」のリストに加えておく必要がある。

●二つ目の解：クライアントの秘密鍵

設問 4 全体の解説で述べた，RADIUS サーバのディジタル証明書発行について，再び掲載しよう。大事なところを下線で強調しておいた。

> サーバの公開鍵と秘密鍵を生成し，サーバの公開鍵のディジタル証明書（サーバ証明書）を発行する。
> 同様に，クライアントの公開鍵と**秘密鍵**を生成し，クライアントの公開鍵のディジタル証明書（クライアント証明書）を発行する。

TLS のクライアント認証は，「正当な利用者がもっているもの」を確認することによって行われる。それは，クライアントの端末にインストールされた，次の二つのものだ。

- クライアント証明書（クライアントの公開鍵のディジタル証明書）
- その公開鍵の対となる秘密鍵

この存在を確かめるために必要な手順が，次に示す三つである。これらは，TLS ハンドシェークプロトコルに従ってやり取りされる。

表：クライアント認証の手順

項番	手順の内容	ハンドシェークプロトコルのメッセージ名
手順 1	サーバは，クライアント証明書の送信を，クライアントに要求する	Certificate Request
手順 2	クライアントは，クライアント証明書を送信する	Certificate
手順 3	クライアントは，クライアント署名を送信する	Certificate Verify

前記の手順 1，2 は，「正当な利用者がもっているもの」の一部であるクライアント証明書に関する，要求と応答のやり取りである。

もっとも，クライアント証明書（ここに格納された公開鍵）は，正当な利用者だけがもっているわけではない。公開されており，誰もが入手可能だ。もしかすると，何者かがクライアントになりすまし，手順 2 でクライアント証明書を応答しているかもしれない。

その懸念を払拭するために，手順 3 が必要となる。

手順 3 で送信しているのは，これまでのハンドシェークプロトコルの手順でやり取りしたメッセージに対して，クライアントが自分の秘密鍵（署名鍵）で署名したものである。サーバは，クライアントの公開鍵（検証鍵）でこの署名の検証に成功したとき，公開鍵の対となる秘密鍵をクライアントがもっていることを確認できる。

ここまで理解できれば，二つ目の解を導くことができる。

RADIUS サーバは，クライアントの公開鍵と秘密鍵を生成し，クライアント証明書を発行する。TLS のクライアント認証に成功するため，このクライアント証明書と秘密鍵をクライアント端末にインストールする必要がある。

よって，二つ目の正解は，「**クライアントの秘密鍵**」となる。

参考までに，第 5 段落によれば，「PKCS #12」形式，クライアント証明書と秘密鍵を一体化したファイルに変換する。

実際，これはよく行われている方法だ。ファイル変換時にパスワードで保護できる

形式となっているため，インストール時にパスワードを入力させることで正当な利用者だけが入手でき，安全性が確保される。

(2)

解答例

ダウンロードサーバの認証情報が漏えいすると，来訪者も
クライアント証明書などがダウンロードできてしまう。（51字）

問題文は，「本文中の下線⑦の問題を，……述べよ」と記述されている。

下線⑦は，〔ディジタル証明書の配布方法の検討〕の第 7 段落の中にある。そこには，次のように記述されている。

> 無線 LAN 経由でダウンロードサーバにアクセスさせる方法を検討した。この方法では，NPC にクライアント証明書がインストールされていないので，認証エラーになる。そこで，認証エラー時に WLC の認証 VLAN 機能によって，特別な VLAN を AP に設定し，この VLAN にダウンロードサーバを設置することを考えた。しかし，その場所にダウンロードサーバを設置すると，⑦クライアント証明書の配布に関してセキュリティ上問題がある。

この問題を解決するために，別のアクセス方法が採用された。その点が，第 7 段落の続く文章に記述されている。

> そこで，営業部オフィスエリアの有線 LAN 接続でアクセスできる場所にダウンロードサーバを設置することにした。

下線⑦に「セキュリティ上問題」とあるが，やや漠然としている。

そこで，解法の糸口をつかむため，「そもそも情報セキュリティにはどのような要素が含まれているか」を思い巡らしてみよう（付録 PDF「午後問題の解答テクニック」の「0.3.6　問題を解く②：応用テクニック」の「4. 出題の意図を汲み取れないときは，出題分野の重要トピックを思い巡らしてみる」を参照されたい）。

情報セキュリティの 3 要素は，「機密性」「完全性」「可用性」である。

それでは，各要素の観点に立ち，「セキュリティ上の問題」が発生するかを考察しよう。

その際，文脈にある「有線 LAN に設置する」という解決策も併せて考慮する。出題者が意図している，下線⑦の「セキュリティ上問題」は，これで解決できる内容だからだ。

三つの要素をそれぞれ考察した後，下線⑦で本質的に問題視されていることに基づいて，解を導こう。

●機密性の観点

まず，「機密性」について考察する。

機密性とは，簡単に言うと，「アクセスを許可されている者だけがアクセスできること」である。これに抵触する問題が発生し得るだろうか。

この点を明らかにするために，時間軸を整理する必要がある。

本小問で問うているダウンロードサーバの無線 LAN 経由でのアクセスは，営業部オフィスエリアのフリーアドレス化がまだ実現していない時点の話である。これは，下線⑦の先を読み進めていくと，「無線 LAN に移行した後」の話題に移ることから理解できる。だから，下線⑦の文脈上の時間は，その移行前となるわけだ。

この時点で，来訪者には自社の無線 LAN を開放していない。来訪者は，持参した Wi-Fi ルータを使って LTE 回線経由でインターネットにアクセスする。ただし，Wi-Fi ルータは，敷設された無線 LAN の AP が発する電波を拾うことができる。

将来的に無線 LAN システムが導入されると，堅牢な利用者認証が実施される。営業員はエンタープライズモードで，来訪者はパーソナルモードで，それぞれ無線 LAN に接続する。それぞれのモードに応じた利用者権限を付与することでアクセス制限を課し，機密性を確保しようとしている。とはいえ，残念ながら，まだその仕組みが導入されていないのである。

したがって，下線⑦の時点においては，機密性の観点から考えると，来訪者が無線 LAN に不正アクセスする可能性がある。

もちろん，来訪者が営業員になりすましてエンタープライズモードで無線 LAN に接続しようとしても，クライアント証明書を所有していないので，利用者認証に失敗してしまう。

しかしながら，営業員についても，ダウンロードサーバからクライアント証明書をダウンロードするまで，エンタープライズモードによる利用者認証を行えない。つまり，来訪者と同様，利用者認証に失敗してしまうのだ。

この点を念頭において，先ほど引用した第 7 段落を見てみると，この利用者認証の「失敗」を契機に，ダウンロードサーバからクライアント証明書をダウンロードするように誘導していることが分かる。「認証エラー時に WLC の認証 VLAN 機能によって，

特別な VLAN を AP に設定し，この VLAN にダウンロードサーバを設置することを考えた」とあるからだ。

それでは，敷設した無線 LAN のエンタープライズモード認証に関する情報が来訪者に漏えいし，来訪者がその認証を試みたならば，どうなるだろうか。

当然ながら認証エラーとなるが，これを契機に「特別な VLAN」に接続されるので，ダウンロードサーバにアクセスできてしまうのである。

本文には，ダウンロードサーバでパスワード認証等のアクセスコントロールを実施している旨は特に述べられていない。したがって，特別な VLAN に接続できた時点で，ダウンロードサーバからクライアント証明書などをダウンロードできると考えられる。

これは由々しき問題だ。

それでは，この機密性の問題は，「有線 LAN 接続でアクセスできる場所にダウンロードサーバを設置する」ことで解決できるだろうか。つまり，文脈上，これが出題者の意図した問題であると言えるだろうか。

確かにそのように言える。なぜなら，そもそも来訪者の NPC を有線 LAN に接続させないので，ダウンロードサーバに物理的にアクセスできないからだ。

ゆえに，これこそ，下線⑦にある「セキュリティ上問題」であるに違いない。

したがって，これまで解説した内容をまとめて，解を導けばよい。答案の作文は，本小問の解説の最後に行うことにする。

●完全性，可用性の観点

念の為，情報セキュリティの別の要素についても考察しておこう。

それは，「完全性」「可用性」である。

完全性とは，簡単に言うと，「情報とその処理方法のどちらも，正確であり，かつ，完全である（改ざんされていない）こと」である。

本事例のダウンロードサーバに適用するとしたら，クライアント証明書の改ざん，マルウェア感染による不正な処理の実行などが，完全性の問題であると言えよう。

しかし，こうした完全性を損なうインシデントは，そもそもダウンロードサーバへの不正アクセスが可能になって初めて生じ得る，二次的なものに過ぎない。機密性の問題を解決すれば，同時に解消される。

したがって，完全性の観点は，ここで問われているものではない。

可用性とは，簡単に言うと，「必要なときに情報を利用できること」である。

本事例のダウンロードサーバに適用するとしたら，ダウンロードサーバの障害，ダウンロードサーバに至る通信経路の障害などが，可用性の問題であると言えよう。

しかし，こうした可用性を損なうインシデントは，そもそもこの文脈では想定され

ていない。そのように言える理由は，下線⑦の「セキュリティ上問題」を踏まえた解決策が，可用性向上とは無関係の内容だからである。具体的に言うと，それは「有線 LAN 接続でアクセスできる場所にダウンロードサーバを設置する」ことであり，サーバやネットワークを冗長構成にしているわけではないのだ（第 7 段落）。

したがって，可用性の観点も，ここで問われているものではない。

●解の導出

以上より，本小問で問われているのは，機密性の観点であることが分かる。

まとめると，認証情報が漏えいした場合，ダウンロードサーバからクライアント証明書などをダウンロードできることが，下線⑦で問題視されていることである。

よって，正解は解答例に示したとおりとなる。

(3)

解答例

クライアント証明書の有効期限を切らせた営業員（22字）
又は
無線 LAN 導入後に営業部に配属された営業員（21字）

問題文は，「本文中の下線⑧について，ダウンロードできない本社の営業員を，……答えよ。ただし，NPC の紛失，故障などで新たに貸与されるケースは除く」と記述されている。

下線⑧は，〔ディジタル証明書の配布方法の検討〕の第 7 段落の中にある。そこには，「無線 LAN に移行した後，営業部オフィスエリアをフリーアドレスにして NPC 接続用の有線 LAN は撤去するが，クライアント証明書の更新は無線 LAN 経由で可能である。しかし，⑧状況によっては，クライアント証明書をダウンロードできない本社の営業員も出てくる。その営業員には，情シスの担当者がクライアント証明書などの必要な情報を NPC にインストールして，当該営業員に渡す」と記述されている。

まずは時間軸を整理しておこう。先の小問 (2) とは話題となっている時期が異なっているので，留意しておきたい。

先ほど引用した本文に「無線 LAN に移行した後」とあるので，無線 LAN システムが導入された後の時期であることが分かる。

この時点で，営業員はエンタープライズモードの EAP-TLS 認証で無線 LAN に接続

している。この時期にダウンロードサーバにアクセスする理由として，本文が挙げているのは，「クライアント証明書の更新」である。

クライアント証明書のダウンロードに失敗したときの解決策は，「クライアント証明書などの必要な情報を NPC にインストール（する）」ことである。

これで解決できることから，ダウンロードできるのは，「クライアント証明書などをもっている営業員」という条件を満たしている人だと分かる。

以下，これを「アクセス条件」と呼ぶことにしよう。

本小問で問われている営業員は，要するにこの大事な条件を満たしていないわけだ。

それでは，このアクセス条件を満たしていない営業員は，いったいどのような状況に置かれているのだろうか。これを具体的に指摘することが，本問の出題意図である。求める解は，「（そのような状況に置かれた）営業員」となる。

●具体性に欠けるが，論理的に導けること

先ほど述べたアクセス条件は，次のとおりである。

クライアント証明書などをもっている社員

ここから推論すると，次に示す状況に置かれた営業員は，この条件を満たしていないと言える。

1. クライアント証明書などをもっているが，それが不完全である営業員
2. クライアント証明書などをもっていない営業員

どちらも条件を満たしていないことに変わりはないが，程度の違いに着目している。これにより，異なる解が導かれる可能性があるためだ。

なお，このままではまだ具体性に欠けるので，出題者の意図する答えには至らない。

この内容を，本事例の状況に照らして具体的に述べることができれば，解が求まったことになる。

それでは，一つずつ解を導いてゆこう

●一つ目の解の導出

まず，「クライアント証明書などをもっているが，それが不完全である営業員」を考察しよう。

不完全なクライアント証明書とは，具体的にどのようなものであろうか。

そのヒントとなるが，ダウンロードサーバにアクセスする理由として本文が挙げている，「クライアント証明書の更新」である。

クライアント証明書を更新する必要があるのは，証明書に有効期限が設定されているからである。当然ながら，その更新は，有効期限が切れる前に行っておく必要がある。さもないと，ダウンロードしようとして無線 LAN に接続した時点で，エンタープライズモードの認証に失敗してしまう。それゆえ，有効期限が切れた証明書は，他の体裁がいくら整っていようとも，認証に成功するには不完全なものである。

したがって，有効期限が切れたクライアント証明書を NPC にインストールしている営業員は，「クライアント証明書などをもっているが，それが不完全である営業員」だと言えよう。

よって，正解は，「**クライアント証明書の有効期限を切らせた営業員**」となる。

●二つ目の解の導出

次に，「クライアント証明書などをもっていない営業員」を考察しよう。

下線⑧の時期は，無線 LAN が導入された後である。導入時点で在籍していた営業員は全員，適切なクライアント証明書をもっている。

それでは，無線 LAN の導入後に営業部に配属された営業員はどうだろうか。

クライアント証明書が NPC にインストールされていない限り，エンタープライズモードの認証に失敗するので，無線 LAN に接続できないことは明らかだ。当然，ダウンロードサーバへのアクセスもままならない。

したがって，クライアント証明書が NPC にインストールされていない，無線 LAN の導入後に営業部に配属されたばかりの営業員は，「クライアント証明書などをもっていない営業員」だと言えよう。

よって，正解は，「**無線 LAN 導入後に営業部に配属された営業員**」となる。

■設問 5

設問 5 は〔既設 LAN への無線 LAN の接続構成の設計〕について出題している。

様々な調査，検討を踏まえ，この見出しの中で設計を行っている。

ここで，冒頭の解説で述べた，無線 LAN 導入の目的を思い起こしてみよう。

［目的 1］営業部のフリーアドレス化と接客エリアの拡大を実現し，課題 1 を解決策すること

［目的 2］来訪者へインターネット接続環境の提供を実現し，課題 2 を解決すること

これを実現するには，無線 LAN に接続する利用者を，2 種類考える必要がある。

［目的 1］に照らし，一つ目の利用者は，営業員である。

［目的 2］に照らし，二つ目の利用者は，来訪者である。

当然ながら，それぞれの利用者はアクセス範囲が異なっている。そこで，本事例の無線 LAN システムは，次の内容を採り入れた設計を行う。

● **ESS の設定**

営業員向けの ESS，来訪者向けの ESS を設ける。

● **VLAN の設定**

ESS ごとに異なる VLAN を設定する。

営業員向けの VLAN を，VLAN100 とする。

来訪者向けの VLAN を，VLAN200 とする。

● **VLAN のアクセス範囲の設定**

L2SW のポート VLAN 設定で，VLAN の範囲を設定する。

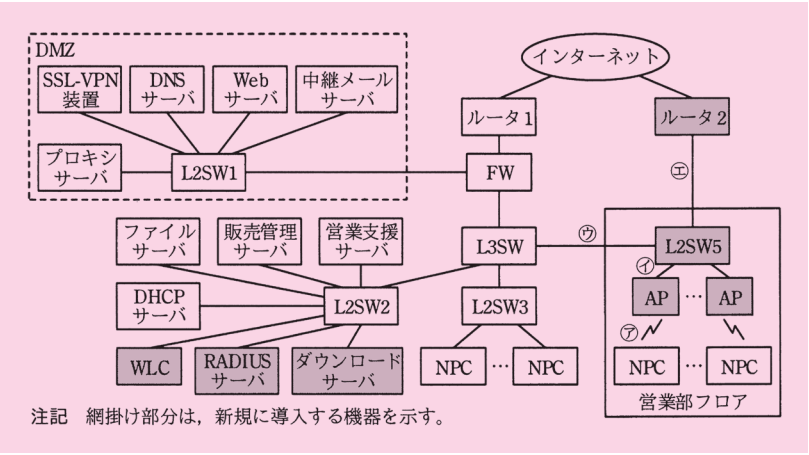
営業員向けの VLAN は，既設の有線 LAN に接続する。

来訪者向けの VLAN は，既設の有線 LAN に接続しないが，インターネットに接続する。

● **利用者認証の実施**

営業員はエンタープライズモードの EAP-TLS 認証を実施する。

来訪者はパーソナルモードの認証を実施する。



図：既設 LAN に無線 LAN システムを導入したときの LAN 構成（図 4 の抜粋）

設計の概要が理解できたところで，それでは，いよいよ小問の解説に移ろう。

(1)

解答例

サプリカントとなる機器：NPC
オーセンティケータとなる機器：WLC

問題文は，「図 4 中で，IEEE 802.1X のサプリカントとなる機器及びオーセンティケータとなる機器を，図 4 中の機器名でそれぞれ答えよ」と記述されている。

本問の解を導くには，IEEE802.1X の用語である，サプリカント，オーセンティケータについて理解する必要がある。その後，解を導こう。

● IEEE802.1X のサプリカント，オーセンティケータ

IEEE802.1X は，認証に成功した端末だけが特定の VLAN に接続できるようにする技術である。

この技術は，当初は有線 LAN のスイッチで使われていた。スイッチのポートに端末が接続すると，この認証が実行される。認証に成否に応じて，端末収容ポートの VLAN を切り替える。このような機能を有するスイッチを，認証スイッチという。

この技術が，後に無線 LAN の AP でも使われるようになった。無線 LAN で，スイッチと端末のケーブル接続に相当するのが，AP と端末のアソシエーション確立となる。

一般的に言えば，IEEE802.1X 認証を導入している無線 LAN 環境では，有線 LAN の認証スイッチの役割を，無線 LAN の AP が担っている。

しかし，本事例では，AP を管理する WLC が使われている。認証スイッチの役割を，AP と WLC で分担している可能性がある。その役割分担を具体的に見極めるには，本文を注意深く読む必要がある。

そこで，IEEE802.1X そのものを理解するため，いったん本事例から距離を置き，あえて有線 LAN を題材に取り上げることにする。一般的なサプリカントとオーセンティケータについて，まずは解説しよう。

IEE802.1X の認証と接続は，次の手順に従って行われる。

ここで，認証に成功する前の VLAN を「認証用 VLAN」，成功した後の VLAN を「接続許可 VLAN」を呼ぶことにする。

①端末が認証スイッチのポートに接続されると，認証サーバは端末を認証する。端末収容ポートが所属する VLAN は，この時点では認証用 VLAN である。
②認証に成功すると，認証サーバは，接続許可 VLAN の VLAN ID を認証スイッチに送信する。
③認証スイッチは，端末収容ポートが所属する VLAN を，接続許可 VLAN に動的に切り替える。

ここに登場する認証サーバは，RADIUS サーバである。

手順①から明らかであるが，端末が認証用 VLAN に収容されている間，RADIUS サーバと端末間の RADIUS 通信は，認証スイッチによって転送されている。

認証スイッチの役割は，単なる転送に留まらない。手順②，③から分かるとおり，認証スイッチは認証サーバの指示に従ってポートの VLAN を切り替える。こうして，ポート単位でアクセス制御を実現している。

このような機能を装備した認証スイッチのことを，オーセンティケータという。

認証対象となる端末（又は，端末にインストールされた認証用ソフトウェア）のことをサプリカントという。

●解の導出：サプリカント

本小問は，図 4 中のサプリカントとなる機器及びオーセンティケータとなる機器を問うている。

サプリカントは，端末に該当する機器を答えればよい。

この点について，本事例では特に難しく考える必要はない。無線 LAN 端末がそれである。

よって，サプリカントの正解は，「**NPC**」となる。

●解の導出：オーセンティケータ

オーセンティケータは，認証スイッチに該当する機器を答えればよい。

この点について，本事例では，AP を管理する WLC が使われている。

この解を導くには，認証スイッチの役割を，AP と WLC がどのように担っているかを見極める必要がある。

WLC の機能について，〔AP の設置方法の検討〕の第 4 ～第 6 段落を見ると，幾つか記述されている。内容を要約すると，次のとおりとなる。

- 主要な機能の一つは，利用者認証，認証 VLAN などのセキュリティ対策機能で

ある（第 4 段落）。

- WLC で EAP-TLS を利用するときは，AP と WLC 間でトンネルが設定される。無線 LAN 端末と WLC 間で認証情報の交換が行われる。利用者認証を行った後，利用者 ID に対応した VLAN を AP に設定する（第 6 段落）。
- 認証後に行われる無線 LAN 端末の通信は WLC を経由しない。通信データの暗号化と復号は AP が行う（第 6 段落）

ここから，WLC は，認証スイッチの役割を全面的に果たしていることが分かる。

これに対し，AP は，認証スイッチの単なる「ポート」と同等の存在に過ぎない。これが果たす役割は，端末との間でアソシエーションを確立すること，WLC の指示に従って VLAN を設定すること，認証後の通信を行うことである。

よって，オーセンティケータの正解は，「**WLC**」となる。

(2)

解答例

① ESSID
② PSK

問題文は，「本文中の下線⑨について，来訪者に教える情報を二つ挙げ（よ）」と記述されている。

下線⑨は，〔既設 LAN への無線 LAN の接続構成の設計〕の第 4 段落の中にある。そこには，「NPC を持参した来訪者には，Y 社の担当者が，⑨ WPA2 又は WPA のパーソナルモードで無線 LAN に接続するための情報を教える」と記述されている。

本事例では，営業員が接続する VLAN と，来訪者が接続する VLAN を別々にしている。来訪者に割り当てる VLAN について，続く文章は，「来訪者の NPC には，AP が ESSID に対応した来訪者向けの VLAN（VLAN200）を割り当てる」と記述されている。

ここから，VLAN ごとに ESS を分けていることが分かる。一つ目は営業員用の ESS であり，二つ目は来訪者用の ESS である。

来訪者が Y 社の接客エリアで Wi-Fi ルータを立ち上げると，Y 社の AP から通知される ESSID は二つ見える。したがって，このどちらを使えばよいのかを来訪者に教える必要がある。

よって，一つ目の情報は，「**ESSID**」となる。

来訪者用の ESS に接続すると，パーソナルモードの利用者認証が求められる。

パーソナルモードでは，AP と無線 LAN 端末が，同じ PSK（Pre-Shared Key，事前共有鍵）を設定しているときに限り，認証に成功する。

この PSK を知らされない限り，無線 LAN に接続することはできない。したがって，これを来訪者に教える必要がある。

よって，二つ目の情報は，「PSK」となる。

(3)

解答例

㋑

問題文は，「図 4 中で，今回新たにタグ VLAN が設定される箇所を，図 4 中の㋐～㋓から選び，記号で答えよ」と記述されている。

本小問が問うているタグ VLAN の範囲を導くには，無線 LAN システムに設定される VLAN とその範囲を見極める必要がある。

タグ VLAN を設定する箇所は，物理的に 1 本のリンクの中に，複数の VLAN が重なり合っているところである。

設問 5 全体の解説で述べたとおり，無線 LAN システムに設定する VLAN は，2 種類ある。

一つ目は営業員向けのものであり，二つ目は来訪者向けのものである。

まず，営業員向けの VLAN について，〔既設 LAN への無線 LAN の接続構成の設計〕の第 3 段落には次のように記述されている。

> EAP-TLS で認証を受けた本社の営業員の NPC には，営業員向けの VLAN（VLAN100）を割り当て，既設の有線 LAN 使用時と同じ作業ができるようにする。

ここに「既設の有線 LAN 使用時と同じ作業ができる」とあるので，営業員向けの VLAN は，既設の有線 LAN に接続できることが分かる。

営業員向けの VLAN の範囲は，営業員の NPC からアクセスできる機器の範囲と一致する。営業員の NPC から既設有線 LAN にアクセスできるので，その経路全域が VLAN の範囲となる。

これを図 4 の記号で表すと，次のようになる。NPC から L3SW までの経路を示そう。

NPC →㋐→ AP →㋑→ L2SW5 →㋒→ L3SW……（以下略）

次に，来訪者向けの VLAN について，第 4 段落には次のように記述されている。

> 来訪者の NPC には，……来訪者向けの VLAN（VLAN200）を割り当てる。VLAN200 が割り当てられることによって，来訪者の NPC は，無線 LAN へのアソシエーション後に，ルータ 2 がもつ DHCP 機能でネットワーク情報が付与され，インターネットアクセスだけができるようになる。

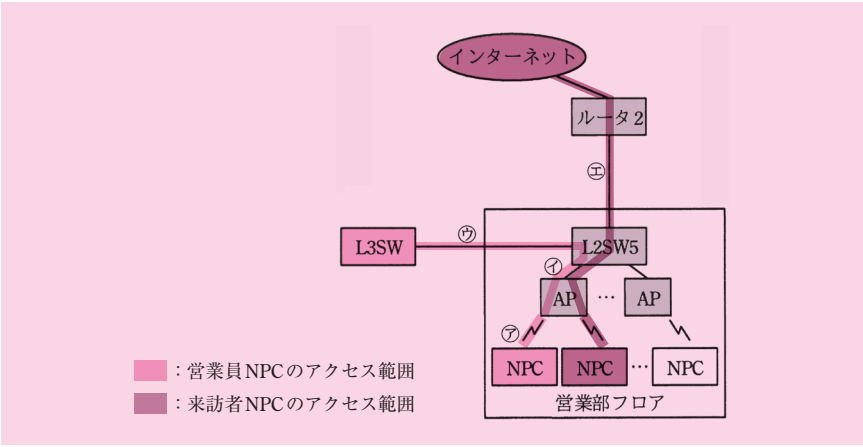
ここに「インターネットアクセスだけができるようになる」とあるので，来訪者向けの VLAN は，ルータ 2 経由でインターネットに接続できることが分かる。これにより，冒頭の解説の［目的 2］で述べた，「来訪者へインターネット接続環境の提供を実現し，課題 2 を解決すること」が実現される。

来訪者向けの VLAN の範囲は，来訪者の NPC からアクセスできる機器の範囲と一致する。来訪者の NPC からインターネットにアクセスできるので，その経路全域が VLAN の範囲となる。

これを図 4 の記号で表すと，次のようになる。

NPC →㋐→ AP →㋑→ L2SW5 →㋓→ルータ 2 →インターネット

二つの経路を図示したものを，次に示す。



図：営業員 NPC と来訪者 NPC のアクセス範囲

したがって，複数の VLAN が重なり合う物理リンクは，㋐と㋑である。

まず，リンク㋐について考察しよう。

これは無線 LAN の区間に当たるが，営業員の NPC は営業員向けの ESS を指定して接続している。同様に，来訪者の NPC は来訪者向けの ESS を指定して接続している。

ESS が異なっていれば，独立した無線 LAN セグメントになる。つまり，営業員の NPC と来訪者の NPC は，無線 LAN 上は，別々の区間に存在しているわけだ。

その各々の ESS の中で，VLAN はただ一つしか存在していない。

したがって，この区間の無線 LAN フレームにタグ VLAN が挿入されることはない。つまり，タグ VLAN が設置されるリンクではない。

次に，リンク㋑について考察しよう。

これは有線 LAN の区間に当たるが，1 本の物理リンクの中で，営業員向け VLAN と，来訪者向けの VLAN が重なり合っている。

したがって，この区間のイーサネットフレームにタグ VLAN を挿入し，二つの VLAN の通信が論理的に区別される必要がある。つまり，ここが，タグ VLAN が設置されるリンクである。

よって，正解は「㋑」となる。

(4)

解答例

ルータ2への接続ポートだけに，VLAN200のポートVLANを設定する。（36字）

問題文は，「図 4 の構成で，来訪者の NPC にインターネットアクセスだけを可能にするための，L2SW5 への VLAN 設定内容を，……述べよ」と記述されている。

L2SW5 に接続しているリンクは，㋑，㋒及び㋓である。

小問（3）で解説した図「営業員 NPC と来訪者 NPC のアクセス範囲」を見ると，リンクに設定する VLAN が明らかになる。その内容をまとめたものを次の表に示す。

表：リンクに設定する VLAN

リンク	接続先	VLAN の名称	VLAN ID
㋑	AP	営業員向け VLAN	100
		来訪者向け VLAN	200

（表は次ページに続く）

リンク	接続先	VLAN の名称	VLAN ID
㋒	L3SW	営業員向け VLAN	100
㋓	ルータ 2	来訪者向け VLAN	200

本小問が問うているのは，特に，「来訪者の NPC にインターネットアクセスだけを可能にするための，……VLAN 設定内容」である。

それゆえ，来訪者向け VLAN に着目して解を導けばよい。ここでは「VLAN 設定内容」を解として求めているので，「どのポートにどの VLAN を設定するか」を答えるように留意するとよい。

よって，正解は「**ルータ 2 の接続ポートだけに，VLAN200 のポート VLAN を設定する**」となる。

なお，これと多少表現が異なっていても，内容が合っていればもちろん正解である。

(5)

解答例

問題： ハンドオーバができなくなる。（14 字）

理由： NPCに配布したPMKと認証関連情報がWLCで保持されているから（32 字）

問題文は，「図 4 中の NPC が認証された後に WLC に障害が発生した場合，当該 NPC で発生する問題を，……答えよ。また，その理由を，……述べよ」と記述されている。

本小問の解を導くに当たり，WLC の機能を確認しておこう。

その点について，〔AP の設置方法の検討〕の第 4 段落の中で，次のように記述されている。

> WLC には複数の方式があったが，次の三つの主要機能をもつ製品を選定することにした。
> ・有線 LAN 経由での複数の AP に対する設定変更，ファームウェアのアップデータなどの一括処理機能
> ・AP の負荷分散制御，PMK の保持などによるハンドオーバ制御機能
> ・利用者認証，認証 VLAN などのセキュリティ対策機能

着目すべきは，2 番目の箇条書きにある，「PMK の保持などによるハンドオーバ制御機能」である。

WLC のハンドオーバ制御については，設問 3（4）で既に解説している。今ここで，その内容を簡潔に振り返ろう。

事前認証機能は，セルが重なり合う領域に無線 LAN 端末が存在しているときに働く。これは，ハンドオーバに備えて，時間のかかる処理である IEEE802.1X 認証だけを事前に済ませておく機能だ。

PMK キャッシュ機能は，移動先 AP に，PMK がキャッシュされているときに働く。これは，PMK を再利用できる機能だ。これにより，ハンドオーバする際に本来必要となる IEEE802.1X の認証が，一切不要となる。

この点を踏まえて，本小問が問うている「NPC が認証された後に WLC に障害が発生した場合」を想定してみよう。

WLC の障害発生により，ここにキャッシュされていた PMK は失われる。

それゆえ，ハンドオーバの際，無線 LAN 端末は PMK を改めて生成するため，IEEE802.1X 認証のやり取りが必要となる。

ここで改めて，先ほど引用した WLC の機能に目を向けよう。

注目すべきは，3 番目の箇条書きにある，「利用者認証，認証 VLAN などのセキュリティ対策機能」である。

WLC のセキュリティ対策機能については，設問 5（1）で既に解説している。内容を要約すると，この機能の意味するところは，「WLC がオーセンティケータである」ということだ。

しかしながら，WLC に障害が発生するならば，IEEE802.1X 認証を行えなくなる。

したがって，この状況下でハンドオーバしたら，通信が途絶えてしまうことが分かる。要するに，ハンドオーバできなくなるわけだ。

このような問題に陥る理由は，WLC で保持されている PMK が失われるからである。

よって，正解は解答例に示したとおりとなる。

●参考：試験センターの解答例に関する補足

試験センターの解答例「理由」を見ると，「NPC に配布した PMK と認証関連情報が WLC で保持されているから」となっている。

「PMK と認証関連情報」とあるが，「認証関連情報」とはいったい何であろうか。

念のため，この点を補足しておこう。

その具体的な内容は本文中に特に書かれていないので，一般的な知識から推察してみる。

この認証関連情報とは，おそらく，「この PMK はこの NPC が保持しているものである」という PMK と NPC の紐づけ情報であったり，認証成功後に AP に動的に設定した VLAN の情報であったりするのだろう。あるいは，実装依存の何らかの情報を示唆しているのかもしれない。

いろいろと思いつくが，さほど深い意味があるわけではない。仮に「認証関連情報」を答案に書いていなかったとしても正解として扱われるはずだ。

(6)

解答例

AP → L2SW5 → L3SW → FW → L2SW1 →プロキシサーバ→ L2SW1 → FW →ルータ 1

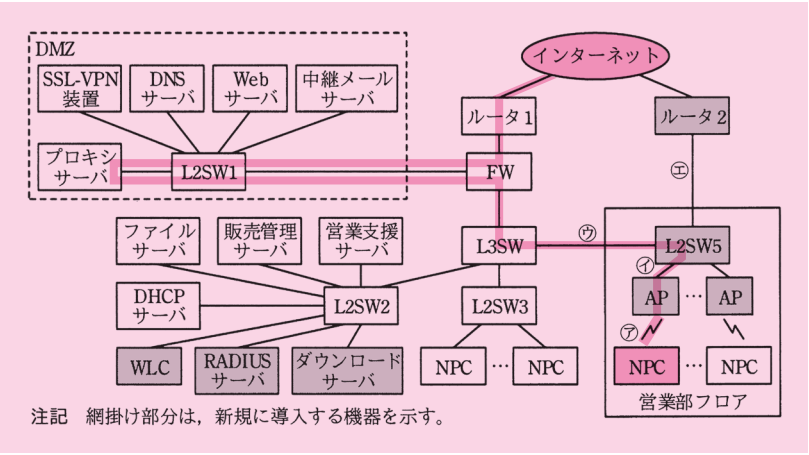
問題文は，「図 4 中で，認証後の営業員の NPC によるインターネットアクセスにおいて，経由する機器名又はサーバ名を，【転送経路】の表記法に従い，経由する順に全て列挙せよ」と記述されている。

認証に成功すると，営業員の NPC は営業員向け VLAN に収容される。このとき，営業員は，既設の有線 LAN 使用時と同じ作業ができる（〔既設 LAN への無線 LAN の接続構成の設計〕の第 3 段落）。

既設の有線 LAN におけるインターネットアクセスについて，序文の第 1 段落には「インターネットアクセスは，本社 DMZ のプロキシサーバ経由で行われている」と記述されている。それゆえ，認証後の NPC も，インターネットアクセスするときはプロキシサーバを経由することが分かる。

したがって，その経路は次に示すとおりとなる。

NPC → AP → L2SW5 → L3SW → FW → L2SW1 →プロキシサーバ→ L2SW1 → FW →ルータ 1 →インターネット



図：営業員の NPC からインターネットへのアクセス経路

解答に際しては，始点の「NPC」，終点の「インターネット」を除いた機器を列挙すればよい。よって，正解は解答例に示したとおりとなる。