

# 目 次

## まえがき

### 第1部 ネットワークスペシャリスト試験の出題ポイント

- 第1章 出題傾向分析 ..... 8
- 第2章 学習方法 ..... 17
- 第3章 本書の使い方 ..... 20

### 第2部 午前II（専門知識）試験の対策ポイント ..... 23

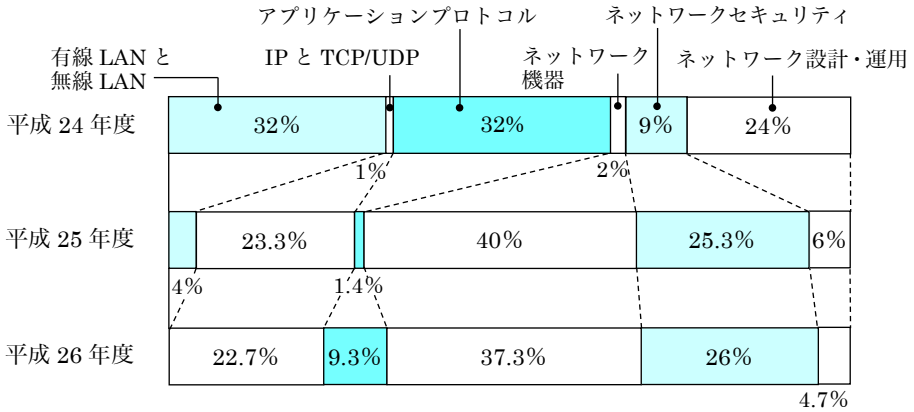
### 第3部 午後問題の重点対策

- 第1章 午後試験に対する取組み方 ..... 36
  - 1.1 試験問題への対応方法 ..... 36
  - 1.2 答案の作成方法 ..... 39
  - 1.3 答案作成の具体例 ..... 40
  - 1.4 午後II試験問題の解き方 ..... 57
- 第2章 LANの方式 ..... 81
  - 2.1 伝送媒体とアクセス制御方式 ..... 81
  - 2.2 無線LAN (IEEE 802.11) ..... 86
  - 2.3 ADSLとFTTH ..... 94
  - 2.4 PPPとPPPoE ..... 98
- 第3章 IPルーティング ..... 130
  - 3.1 IPアドレスとルーティングテーブル ..... 130
  - 3.2 アドレス変換 ..... 140
  - 3.3 IPマルチキャスト ..... 144
  - 3.4 DHCP ..... 147
  - 3.5 VRRP ..... 149
  - 3.6 IPv6 ..... 152
- 第4章 TCPとUDP ..... 184

■ 第 5 章	アプリケーションプロトコル	205
5.1	HTTP とクッキー情報	205
5.2	FTP	212
5.3	SNMP	215
5.4	NTP	218
■ 第 6 章	DNS の仕組み	235
■ 第 7 章	電子メールの仕組み	262
■ 第 8 章	VoIP	290
■ 第 9 章	ネットワーク機器	330
9.1	ブリッジとルータ	330
9.2	ルーティングプロトコル	334
9.3	LAN スイッチ	341
9.4	NAS と SAN	354
9.5	IP-VPN と広域イーサネット	357
■ 第 10 章	ネットワークセキュリティ	438
10.1	暗号化技術	438
10.2	認証技術	440
10.3	ファイアウォールと IDS	448
10.4	IPsec	455
10.5	SSL	462
10.6	その他のセキュリティプロトコル	467
■ 第 11 章	ネットワークの設計構築	531
■ 第 12 章	ネットワークの運用管理	557
索 引		585

商標表示

各社の登録商標及び商標、製品名に対しては、特に注記のない場合でも、これを十分に尊重いたします。



分野	技術内容
有線 LAN と無線 LAN	CSMA/CD, MAC フレーム, CSMA/CA, WEP, TKIP, CCMP, WPA, SONET, リング構成, 伝送媒体など
IP と TCP/UDP	IP アドレス, CIDR, ルーティングテーブル, アドレス変換, ICMP (ping 試験の方法など), IP マルチキャスト, DHCP, VRRP, TCP, UDP など
アプリケーションプロトコル	HTTP, クッキー, プロキシサーバ, 負荷分散方法, DNS の仕組み (キャッシュ, DNS サーバの信頼性対策など), 電子メール配送の仕組み, 電子メールのセキュリティ, 迷惑メール対策, VoIP (SIP, RTP, 優先制御など), SNMP, NTP など
ネットワーク機器	LAN スイッチ (スイッチングハブ) の機能・動作, 仮想スイッチ, 仮想 NIC, スパニングツリー, VLAN, ルータの機能・動作, ルーティングプロトコル (RIP, OSPF, BGP-4), TRILL, NAS, FC-SAN, IP-SAN, FCoE, ネットワーク仮想化, SDN (オーバーレイ方式, ホップバイホップ方式, OpenFlow) など
ネットワークセキュリティ	暗号化技術, 認証技術 (デジタル署名, ワンタイムパスワード, 時刻認証, メッセージ認証など), 電子証明書の検証方法, ファイアウォールの設定, IPsec, SSL, VPN, IEEE 802.1X/EAP, RADIUS など
ネットワーク設計・運用	ネットワークにおけるボトルネックやバックアップの考え方, ネットワーク構成法, 必要帯域の検討, 故障切分け, 保守運用のノウハウなど
計算問題, 情報処理技術一般	トラフィック計算, 回線速度 (必要帯域), データ転送量, データベースの整合性, システム構成など

注 出題比率は、設問ごとに配点を予想し、集計したものを総配点で割って求めたもの。また、技術区分は上記の表に従って分類した。

図 1-1 午後 I 問題の技術分野別出題比率

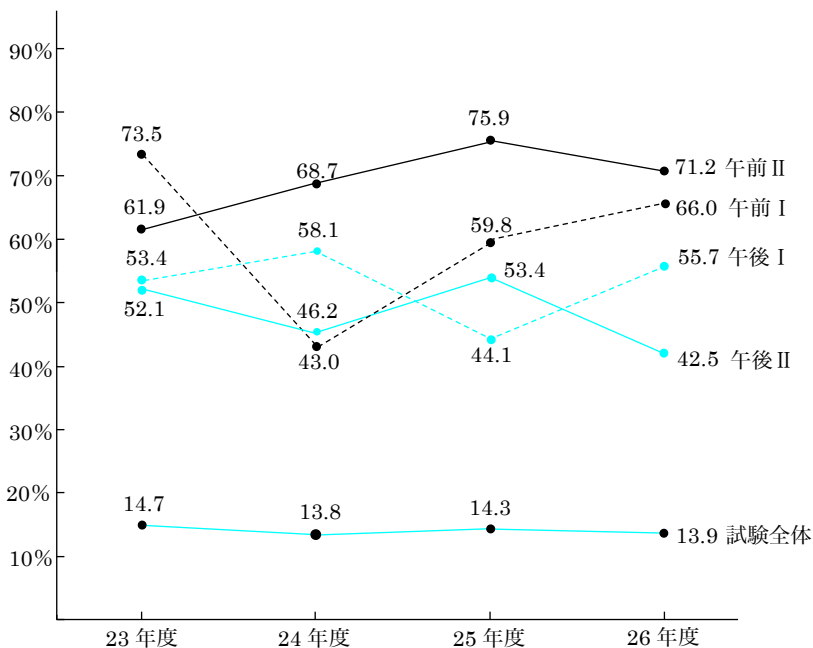


図 1-2 試験区分ごとの合格率の推移

の技術レベルが向上していると考えられます。その半面、午後II試験の合格率は、前回（53.4%）よりも、約 11 ポイント低下し 42.5%になりました。これは、過去 4 回の試験でも、最も低いものです。午後II試験の間1は、SPFのほか、プロキシサーバで復号機能をもたせた場合のセキュリティ対策、パケットフィルタリングの設定など、標準レベルの問題が多いと思われましたが、ネットワークセキュリティ問題に対する準備が十分に行われていなかった結果ではないでしょうか。一方、間2は、平成24年度以降、全く出題のなかったSIPやRTPなどの音声パケットに関するものや、仮想スイッチの動作に関するものでした。このため、合格基準点をクリアすることはかなり難しく、間2に限ればほぼ妥当な結果と考えられます。

## 第2章

## 学習方法

ネットワークスペシャリスト試験で合格基準点をクリアするには、TCP/IP やその応用プロトコル、LAN スイッチやルータといったネットワーク構成機器などに関する基本技術をしっかりと把握していくことが必要です。そして、できるだけ多くの問題を解いて、問題文の読み方、記述式的答案作成に慣れておくことが必要です。

### (1) 基本技術を理解すること

ネットワークスペシャリスト試験においてマスターすべき基本技術は、TCP/IP 通信の仕組みです。TCP/IP 通信では、TCP セグメント、IP パケット、MAC フレームなどに順次、カプセル化され、様々な情報が運ばれていきます。そして、これらのプロトコルがもつヘッダ情報によってデータ転送におけるすべての制御が行われます。つまり、TCP/IP ネットワークにおける制御は、すべてヘッダ情報に基づいて行われ、ヘッダ情報にないことは制御することができません。これが TCP/IP 通信の基本原則です。また、ヘッダ情報は、アプリケーション層、TCP/UDP 層、IP 層、MAC 層といった各層ごとに内容が決められています。アプリケーション層におけるヘッダ情報は、TCP/IP ネットワーク内の転送途中において参照されることはありません。例えば、電子メールの SMTP ヘッダにある To や From フィールドの情報は、電子メールの転送に当たっては参照されることはありません。つまり、To や From フィールドの情報は、封筒の中に書き込まれた情報ですから、電子メールの転送途中では参照されません。それらは、あて先のメールボックスにメールが書き込まれた後に参照される情報です。

ヘッダ情報のもつ意味を理解していけば、インターネットへのアクセスはどのような仕組みによって実現されているのか、電子メールはどのようにして通信相手に届けられるかなどについて、正しく把握できるようになります。また、IP ルーティングについては、IP パケットが LAN 内で転送される際には、MAC フレームにカプセル化されるので、IP アドレスから MAC アドレスへの変換が必要になることや、TCP/IP のプロトコルスタックにおいて、上位と下位のプロトコル間における情報の引渡し方などの関係を明確に考えることができます。このよう

## 第3章

## 本書の使い方

本書は、ネットワークスペシャリスト試験の午後問題を解いていくための技術知識がどれだけ身に付いているかなど、午後対策に重点を置いた構成にしています。

**(1) 本書の構成**

本書は、第1部から第3部までの3部構成になっています。第1部は、ネットワークスペシャリスト試験の出題傾向分析と学習方法などについて紹介しています。第2部では、午前II（専門知識）試験の出題パターンを体系化し、それぞれの取組み方を簡単に述べています。そして、第3部が本書の中心です。第3部では、これまでの試験問題を基に出題された技術分野を、テーマ別に体系化し、分類しました。つまり、試験で必要になる技術は、これらの技術テーマが中心であり、こうした技術内容の問題を十分に理解していくことによって、解答を作成できるようになると思います。

第3部の各章は〔要点チェック〕、〔要点解説〕、〔演習問題〕という構成にしています。まず、要点チェックで、それぞれの技術に関し、その知識を保有しているかどうかを確認するようにしてください。よく知らない事項などについては、要点解説で、その内容をしっかり把握しましょう。ポイントを絞った解説にしていますから、十分に理解できないときなどは、「高度専門 ネットワーク技術」やWeb検索などによって、自らの知識としてしっかり身に付けるようにしてください。基本的に各章の要点が理解できたら、演習問題を解いて、さらに実践的な技術知識を身に付けるようにしましょう。

演習問題は、本試験の午後問題の関連する技術項目ごとに切り出すようにしています。午後Iや午後IIの問題は、それ自体が長文ですから、問題を読むこと自体も結構、大変です。そこで、本書の演習問題は、問題文の長さをできるだけ短くし、手軽に問題に取り組めるように工夫しました。また、その方が技術単位にまとめることができるので、知識の整理にも役立つはずです。



## 演習問題

## Exercise

問1 IPv6 が利用できるネットワークに接続した PC において、二つの IPv6 アドレスが割り当てられていた。

(H26 秋 NW 午前II問1)

(1) 2001:db8::b083:ba94:60c7:7c36

(2) fe80::200:c0ff:fea8:2

このうち、(2)はリンクローカルユニキャストアドレスである。この説明として適切なものはどれか。

ア 下位のビットにこの PC の IPv4 アドレスを埋め込み、IPv6 アドレスと IPv4 アドレスを関連付けて管理を容易にするアドレスである。

イ グローバルユニキャストアドレスが取得できなかったときだけに有効なアドレスである。

ウ このアドレスを使った場合、パケットはネットワークには送信されず、自分自身の PC 内で動作しているプログラムとだけ通信できる。

エ このアドレスをもつネットワークインタフェースからルータを介さずに直接接続できる相手との通信にだけ使用できるアドレスである。

## 【解説】

この問題は、適切な記述を選択する問題の例ですが、(1)、(2)の二つの IPv6 アドレスが記載されています。このため、この二つを同時に考えてしまいがちですが、この問題では(2)のリンクローカルユニキャストアドレスの説明として適切なものが問われていますので、(2)に限定して考えていきましょう。

リンクローカルユニキャストアドレスは、同一リンク内の通信、つまり、ルータを介さずに直接接続できる相手との通信に限って使用できるものです。したがって、正解は (エ) です。

なお、(1)の 2001:db8::b083:ba94:60c7:7c36 は、IPv6 グローバルユニキャストアドレスを示しますが、これは 2001:db8::/32 というプレフィックスをもつことから、文書記述用の IPv6 アドレス、つまり、設定のサンプル用として用いられています (このアドレスを実際の通信に用いることはできません)。ちなみに、2001:db8::/32 というプレフィックスの使用方法は、RFC 3849 (IPv6 Address Prefix Reserved for Document) で規定されています。

## 第1章

## 午後試験に対する取り組み方

## 1.1 試験問題への対応方法

ネットワークスペシャリスト試験で合格するには、午前Ⅰ、午前Ⅱ試験で合格基準点をクリアした上で、さらに午後Ⅰ、午後Ⅱ試験とも 60 点以上の点数を確保することが必要です。

午前Ⅰ、午前Ⅱの試験は、四肢択一の選択問題ですから、ある程度の技術知識があれば比較的容易にクリアできます。しかし、午後の試験は、数十字で解答する記述式の問題が大半を占めるので、午後Ⅰ、午後Ⅱの試験で合格基準点をクリアすることは並大抵のことではありません。TCP/IP や仮想化技術、ネットワークセキュリティなどをはじめ、ネットワーク関連の詳細な技術知識を十分に身に付けた上で、しかも、問題の記述内容を正しく把握して、設問で問われていることに合致した答案を作成していくことなどが要求されます。こうした作業をうまく行うには、幾つかのポイントがあります。

ここでは、午後試験の問題に取り組むときの注意点などを紹介することにします。

## (1) 決してあせらない

ネットワークに関する基本的な技術知識をしっかりと身に付けて試験に臨めば、午後試験においても合格基準点に達することは、それほど難しいというわけではありません。そこで、どのような問題が出題されても落ち着いて問題に取り組んでいくようにしましょう。また、記述式の問題は、思うように得点できないので、少し気楽に考えることも必要です。

午後Ⅰ、午後Ⅱ試験は、午前試験と違って過去問題と同じ問題は出題されません。このため、問題にさっと目を通すと、どれも難しそうな問題ばかりに見えます。しかし、この時点であせってしまうと、冷静に問題に取り組むことができなくなります。午後Ⅰ試験は 3 問の中から 2 問を、午後Ⅱ試験は 2 問の中から 1 問を選択すればよいので、得意分野の問題を選択するようにしましょう。そして、落ち着いて問題に取り組んでいけば、徐々に正解を思いついたり、正解を導いた



## 第3章

## IP ルーティング

## 3.1 IP アドレスとルーティングテーブル



## 要点チェック

## Check

- IP アドレスの種類とその意味
- CIDR による IP アドレスの表示方法とその特徴
- IP アドレスとサブネットマスク、デフォルトゲートウェイの関係
- ルーティングテーブルの検索方法
- IP アドレスと MAC アドレスの関係
- ARP の仕組み
- モバイル IP



## 要点解説

## Study

## 1. IP アドレスの種類とその意味

- (1) IP アドレスについては、32 ビット長の IPv4 と、128 ビット長の IPv6 の二つがあります。これまでのネットワーク試験の午後問題では、IPv4 に関する問題しか出題されていませんでした。しかし、初めて平成 24 年度の午後 II 問 2 の一部として出題されたので、IPv6 についても、理解を深めていくようにしましょう。
- (2) IPv4 のアドレス空間は、図 3-1 のように定義されていて、クラス A～E という分類がされています。クラス A～C については、クラスという概念を外した CIDR (Classless Inter-Domain Routing) という割当て方式が主流になります。なお、クラス D はマルチキャスト用のアドレスです。

一方、IPv6 のアドレスは、ユニキャストアドレス (この中には、リンクローカルアドレス、グローバルアドレス、ユニークローカルアドレスがあります)、エニーキャストアドレス、マルチキャストアドレスという 3 種類が定義されて

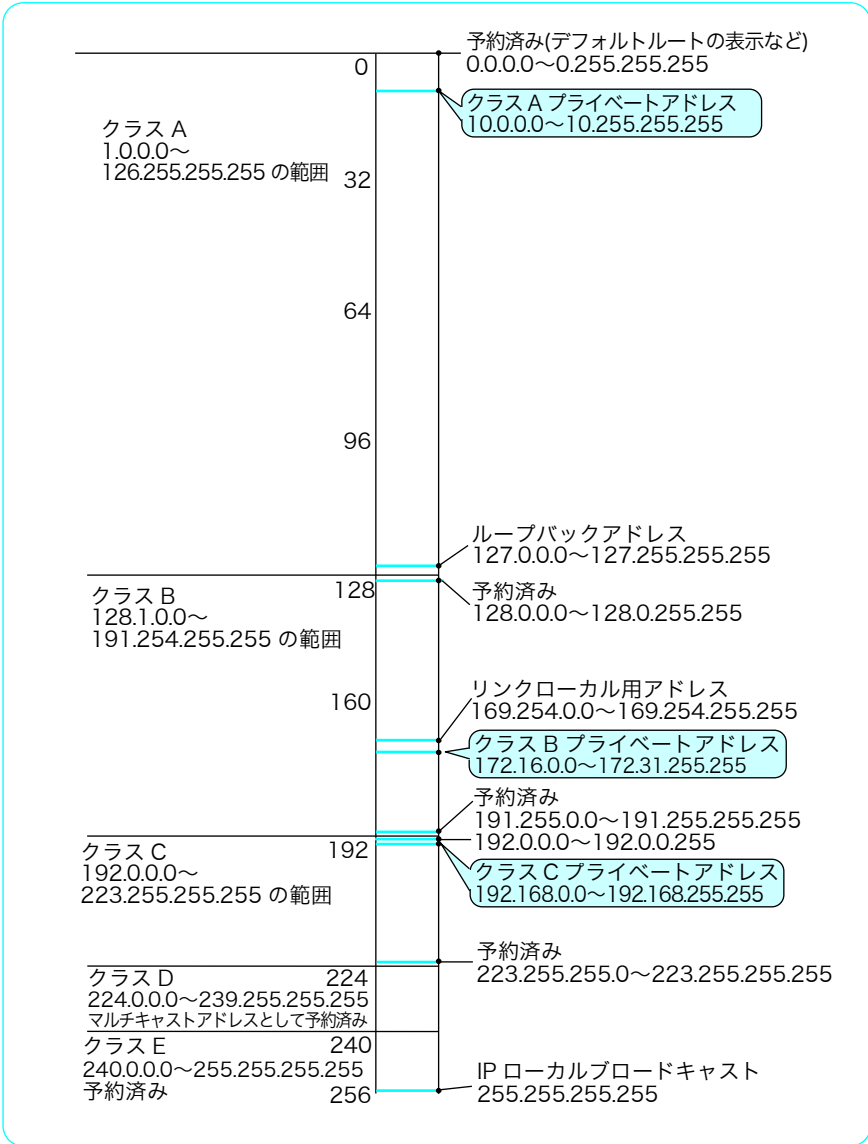


図 3-1 IPv4 のアドレス空間

います。

(3) IPv4 のアドレス空間における一部のアドレスには、組織内で自由に使用でき



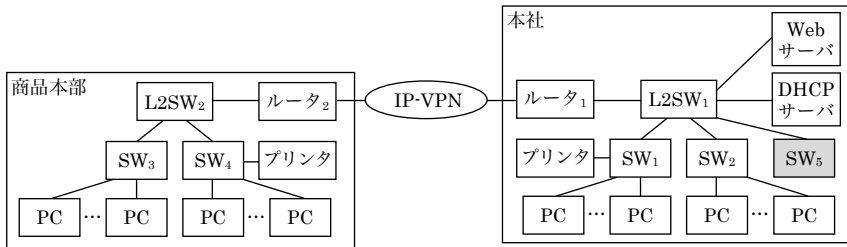
## 演習問題

## Exercise

問1 端末の管理強化に関する次の記述を読んで、設問1～3に答えよ。

(H25秋-NW 午後1問2)

Z社は、生活雑貨の企画、製造及び販売を行う企業である。本社は東京にあり、商品の製造と配送を行う商品本部が山梨にある。ネットワーク管理は、本社の情報管理課が行っている。Z社の現在のネットワーク構成を、図1に示す。



L2SW：レイヤ2スイッチ

SW：アクセス用レイヤ2スイッチ

注記 SW<sub>5</sub>は、増設予定のSWである。

図1 Z社の現在のネットワーク構成（抜粋）

[IPアドレス割当ての仕組みと経緯]

Z社では、全ての機器のIPアドレスを固定で割り当てていた。しかし、近年はPCの増設、入替えが頻繁になり、IPアドレス管理業務が煩雑になってきた。また、①情報管理課の許可を得ずにPCのIPアドレスを割り当て、他のPCの通信に障害が発生したことがあった。そこで、DHCPを用いたIPアドレス自動割当てに切り替えた。現在、全社のPCのIPアドレスは、本社にあるDHCPサーバで一元管理し、ルータ<sub>2</sub>でDHCP  を動作させて商品本部での割当てに対応させている。

IPアドレス自動割当ては、PC使用者の利便性が高まる反面、ネットワーク障害の調査では支障を来すことがあった。例えば、ウイルスに感染し、不正なパケットを送信しているPCを特定するには、ルータ又はWebサーバの  テーブルからIPアドレスとMACアドレスの対応を調べ、MACアドレスからSWのポートを特定し、更に配線図面を見てケーブルをたどる必要があった。また、商品本部で行った、  GHz帯の電波を使用するIEEE 802.11a規格の商品管理端末の導入試験では、不正なDHCPサーバの接続によって、PCに不正

とが分かった。作業3で起きた障害は、SW<sub>5</sub>の増設によってSWの不具合が表面化したものであった。

U君は、L2SW<sub>1</sub>の設定の誤りを修正して、DHCPスヌーピング機能の動作を検証した。L2SW<sub>1</sub>は、DHCPサーバの接続ポート以外から受信したDHCPOFFER及びDHCPACKを破棄するので、SW<sub>5</sub>を接続しても障害が発生しないことが分かった。

U君から検証結果の報告を受けたO主任は、SWの不具合があっても運用に影響しないと判断し、端末の管理強化策を導入することにした。

翌営業日、本社では、PC使用者からの苦情もなく1日の業務は無事終了した。ただし、O主任は、U君が休日の作業を行ったときに発生した障害から、現在のネットワーク構成の弱点を特定し、③本社及び商品本部のL2SWの代わりにレイヤ3スイッチを使用する構成を検討するよう、U君に指示した。

情報管理課は、端末の管理強化策の暫定運用中に各部門の協力を得て準備を完了し、本社での本運用を開始した。続いて、商品本部にも導入・運用を拡大し、PC使用者に大きな負担を掛けることもなく、端末の管理強化を達成することができた。

設問1 本文中の  ～  に入れる適切な字句を答えよ。

ア		イ	
ウ		エ	
オ			

設問2 [IPアドレス割当ての仕組みと経緯]について、(1)～(3)に答えよ。

(1) 本文中の  に入れる適切な数値を答えよ。

a	
---	--

(2) 本文中の下線①では、何が起きたことで通信に障害が発生したのか。15字以内で答えよ。

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

(3) 本文中の下線②では、BBルータのポートのうち、SWに接続したポートは何を接続すべきポートであったのか。15字以内で答えよ。

構成は、L2SW の配下に複数の SW を接続する構成であることから、SW の増設が、ほかの SW に影響を及ぼしたことが分かります。SW 間でこのような影響が発生しないようにするには、SW 単位で異なるネットワーク、つまり、SW 単位に VLAN を設定し、ブロードキャストフレームがそれぞれの VLAN 単位に閉じ込められるようにします。なお、従来の L2SW を用いたネットワーク構成では、本社内、商品本部内とも同一のネットワークセグメントとして接続できる構成だったので、レイヤ 3 スイッチで SW 単位に VLAN を設定すると、基本的に SW 間の通信ができなくなります。そこで、レイヤ 3 スイッチで VLAN 間の接続ができるように経路制御を行うことが必要です。さらに、SW に接続された PC がレイヤ 3 スイッチの各ポートに接続されるので、それぞれの VLAN に応じた IP アドレスを割り当てる必要があります。従来、本社では PC と DHCP サーバが同じブロードキャストドメイン内に存在していたので、DHCP リレーをさせる必要はなかったが、レイヤ 3 スイッチを用いると、レイヤ 3 スイッチに DHCP リレーを行わせるようにする必要があります。また、商品本部では、従来、ルータ<sub>2</sub>が DHCP リレーを行っていたが、レイヤ 3 スイッチを使用する構成にすると、レイヤ 3 スイッチが DHCP リレーを行う必要があります。以上のことを取りまとめ、O 主任が下線③で実現しようとしているネットワーク構成としては、「SW 単位に VLAN を設定し、VLAN 間経路制御と DHCP リレーを行う構成」などのように答えるとよいでしょう。

## 解答例

[設問 1] ア：リレーエージェント    イ：ARP    ウ：製造者  
エ：ミラー    オ：DHCPDISCOVER

[設問 2] (1) a : 5  
(2) IP アドレスの重複割当て  
(3) PC を接続すべきポート

[設問 3] (1) b : 24    c : 6  
(2) 固定 IP アドレスの割当て：MAC アドレスに対応付けた IP アドレスを割り当てる。  
暫定運用中の対処：MAC アドレスが未登録でも IP アドレスを割り当てる。  
(3) SW<sub>1</sub> と SW<sub>2</sub> の間でのブロードキャストフレームの折り返し  
(4) SW 単位に VLAN を設定し、VLAN 間経路制御と DHCP リレーを行う構成

## 索引

## 数字

3 ウェイハンドシェイク	184
4B/5B 変換	82
6to4	154
8B/10B 変換	82

## A

A レコード	237
AAAA レコード	237
ABR	335
ACE	241
ACK ビット	448
ADSL	94
AH	456
anonymous FTP	212
ARP	136
ARP キャッシュ	135
ARP テーブル	135
AS	332
ASBR	335
AS_PATH 属性	337
AS 境界ルータ	335
AS パスプリペンド	337
Auto MDI/MDI-X	85

## B

BGP-4	336
BGP スピーカ	336
BPDU	348
BSS	89
BSS-ID	89

## C

CA	444
CA 証明書	444
CBC	465
CCK	86
CCMP	92
CE ルータ	358
CHAP	99
CIDR	130
CIFS	354
Cookie	209
CoS	298
CRL	445
CSMA/CA	87
CSMA/CD	83

## D

DATA	264
DHCP	147
DHCP スヌーピング	343
DHCP リレーエージェント	148, 332
Diffie-Hellman	455
dig	558
DKIM	270
DMT	95
DNS	235
DNS amplification 攻撃	243
DNS reflection 攻撃	243
DNSSEC	244
DNS キャッシュポイズニング攻撃	243
DNS サーバ	236
DNS ラウンドロビン	241, 533
DoS 攻撃	185
DS	297
DSL	95