NW

令和６年度　春期
ネットワークスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2 時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. 答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。
4. 問題は，次の表に従って解答してください。

問題番号	問１，問２
選択方法	１問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (2) 受験番号欄に受験番号を，生年月日欄に受験票の生年月日を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) 選択した問題については，次の例に従って，選択欄の問題番号を○印で囲んでください。○印がない場合は，採点されません。2 問とも○印で囲んだ場合は，はじめの 1 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問２を選択した場合の例〕

選択欄	
１問選択	問１
	問２

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　データセンターのネットワークの検討に関する次の記述を読んで，設問に答えよ。

K 社は国内にデータセンターを所有する大手 EC 事業者である。データセンターのネットワークには，VXLAN（Virtual eXtensible Local Area Network）を利用している。K 社の情報システム部は，ネットワークの拡張性を向上させるために EVPN（Ethernet VPN）の適用を計画しており，EVPN を用いた VXLAN の技術検証を行うことを検討している。

〔VXLAN の概要〕

RFC 7348 で規定された VXLAN では，VXLAN ヘッダー内の［　a　］ビットの VNI（VXLAN Network Identifier）を用いて，約 1,677 万個のレイヤー2 のオーバーレイネットワークをレイヤー［　b　］のネットワーク上に構成できる。VXLAN トンネルの端点である VTEP（VXLAN Tunnel End Point）は，VXLAN のカプセル化及びカプセル化の解除を行う。VTEP 及び VXLAN トンネルの構成例を図 1 に示す。

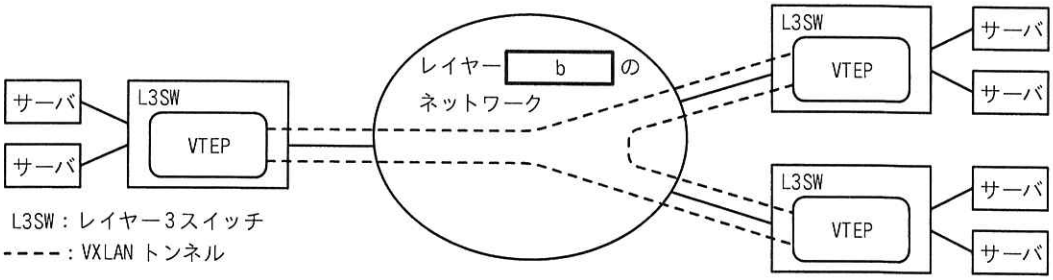


図 1　VTEP 及び VXLAN トンネルの構成例

図 1 中の L3SW の VTEP は，サーバから受信したイーサネットフレームに，VXLAN ヘッダー，［　c　］ヘッダー及び IPv4 ヘッダーを付加した IP パケット（以下，VXLAN パケットという）を，宛先の VTEP（以下，リモート VTEP という）に転送する。転送される VXLAN パケットの送信元及び宛先には，各 VTEP に割り当てられた IP アドレスを利用する。VXLAN パケットの構造を図 2 に示す。

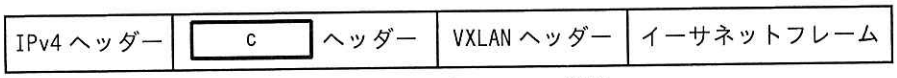


図 2　VXLAN パケットの構造

VTEP は，イーサネットフレームの宛先に応じて VXLAN パケットの宛先を決定するための情報として，リモート VTEP から受信した VXLAN パケットから次の情報を組み合わせて学習する。

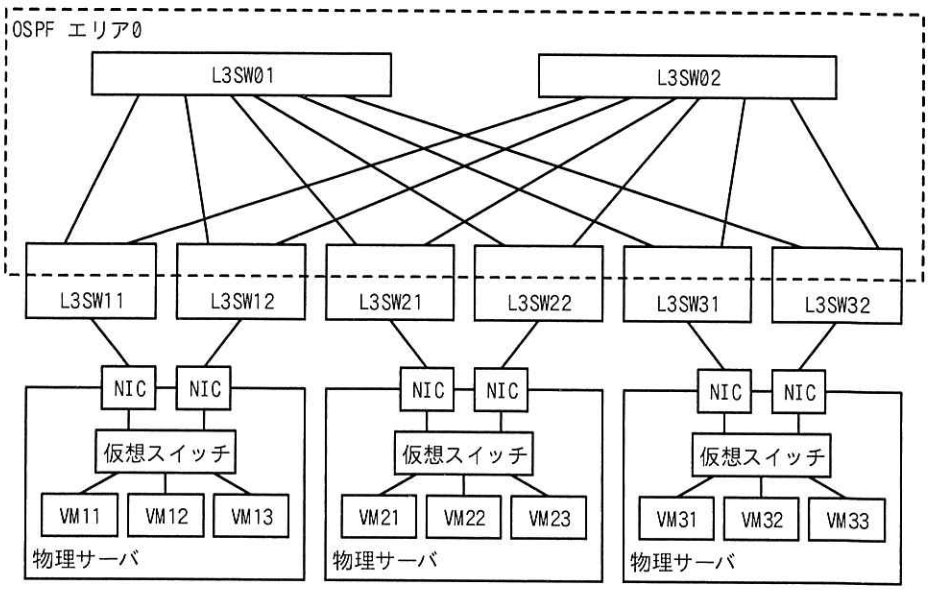
・①リモート VTEP に接続されたサーバの MAC アドレス
・② VXLAN トンネルの VNI
・③リモート VTEP の IP アドレス

K 社の現行のネットワークでは，VTEP は，自身に接続されたサーバからリモート VTEP に接続されたサーバ宛てのイーサネットフレームを，次の方式を選択して転送する。

・イーサネットフレームが，VTEP によって学習されているサーバ宛てのユニキャストの場合には，図 2 中の IPv4 ヘッダーの宛先 IP アドレスに，リモート VTEP の IP アドレスをセットして転送する。
・④イーサネットフレームが，BUM（Broadcast，Unknown Unicast，Multicast）フレームの場合には，図 2 中の IPv4 ヘッダーの宛先 IP アドレスに，IP マルチキャストのグループアドレスをセットして転送する。

〔現行の検証ネットワーク〕

K 社は，現行のネットワークの維持管理のために，検証ネットワーク（以下，検証 NW という）を構築している。現行の検証 NW を図 3 に示す。



L3SW のループバックインタフェースの IP アドレス

機器名	IP アドレス/プレフィックス長
L3SW01	10.0.0.1/32
L3SW02	10.0.0.2/32
L3SW11	10.0.0.11/32
L3SW12	10.0.0.12/32
L3SW21	10.0.0.21/32
L3SW22	10.0.0.22/32
L3SW31	10.0.0.31/32
L3SW32	10.0.0.32/32

図 3　現行の検証 NW（抜粋）

図 3 の概要を次に示す。

・物理サーバに接続する L3SW のポートには，タグ VLAN を設定している。

・物理サーバの二つの NIC はアクティブ／スタンバイ構成であり，L3SW11，L3SW21 及び L3SW31 に接続する NIC をアクティブにしている。

・L3SW の経路制御には OSPF を用いている。

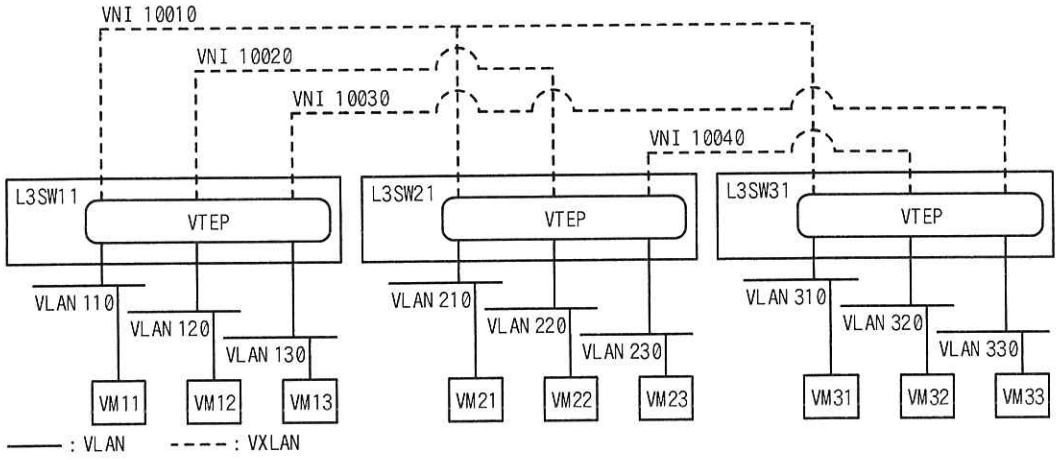
・L3SW は，OSPF で交換する LSA（Link State Advertisement）の情報から［　d　］というデータベースを作成する。次に，［　d　］を基に，それぞれの L3SW を根とする［　e　］ツリーを作成して，ルーティングテーブルに経路情報を登録する。

・⑤LSA に含まれるルータ ID には，それぞれの L3SW のループバックインタフェースに割り当てた IP アドレスを使用している。

・⑥ OSPF の ECMP（Equal-Cost Multipath）によって，トラフィックを負荷分散している。

・PIM-SM（Protocol Independent Multicast - Sparse Mode）による IP マルチキャストルーティングを用いており，L3SW01 及び L3SW02 に IP マルチキャストのランデブーポイントを設定している。

現行の検証 NW の VLAN，VXLAN 及び VTEP を図 4 に示す。



注記　L3SW12，L3SW22 及び L3SW32 の VTEP に係る構成は省略している。

VM の IP アドレスと VLAN ID

VM 名	IP アドレス/プレフィックス長	VLAN ID
VM11	192.168.1.1/24	110
VM12	192.168.1.1/24	120
VM13	192.168.1.1/24	130
VM21	192.168.1.2/24	210
VM22	192.168.1.2/24	220
VM23	192.168.1.2/24	230
VM31	192.168.1.3/24	310
VM32	192.168.1.3/24	320
VM33	192.168.1.3/24	330

VXLAN のカプセル化に用いる対応表

機器名	VLAN ID	VNI	グループアドレス
L3SW11	110	10010	239.0.0.1
	120	10020	239.0.0.2
	130	10030	239.0.0.3
L3SW21	210	10010	239.0.0.1
	220	10020	239.0.0.2
	230	10040	239.0.0.4
L3SW31	310	10010	239.0.0.1
	320	10040	239.0.0.4
	330	10030	239.0.0.3

図 4　現行の検証 NW の VLAN，VXLAN 及び VTEP（抜粋）

図4の概要を次に示す。

・図3の物理ネットワーク上に，VXLANトンネルを論理的に構成している。

・L3SW11，L3SW12，L3SW21，L3SW22，L3SW31及びL3SW32にVTEPを設定している。

・⑦VTEPのIPアドレスには，それぞれのL3SWのループバックインタフェースに割り当てたIPアドレスを使用している。

・VTEPのBUMフレームの転送には，IPマルチキャストを用いる設定にしている。

・VTEPでは，図4中の“VXLANのカプセル化に用いる対応表”に示す次の三つの情報を対応させてカプセル化を行っている。

- 受信したイーサネットフレームの“VLAN ID”
- VXLANトンネルの“VNI”
- BUMフレームを転送するときに使うIPマルチキャストの“グループアドレス”

レイヤー2のネットワークにおけるVM11及びVM23と各VMの通信可否を表1に示す。

表1　レイヤー2のネットワークにおけるVM11及びVM23と各VMの通信可否（抜粋）

通信先 / 通信元	VM11	VM12	VM13	…	VM31	VM32	VM33
VM11	－	×	×	…	○	×	×
VM23	ア	イ	ウ	…	エ	オ	カ

○：通信可　　×：通信不可　　－：通信元と通信先が同じ

〔現行の検証NWにおけるVTEPの動作〕

図4中のVM11とVM31のARP通信におけるVTEPの動作を，次に示す。

(1)　L3SW11のVTEPでは，⑧VM11から受信したVM31のMACアドレスを問い合わせるARP要求フレームに対してVXLANのカプセル化を行い，IPマルチキャストのグループアドレスを宛先にして，グループに参加する全てのリモートVTEPに転送する。

(2)　L3SW12，L3SW21，L3SW22，L3SW31及びL3SW32のVTEPでは，受信したVXLANパケットのカプセル化を解除して，対応するVLANにARP要求フレームをブロードキャストする。

(3)　L3SW31のVTEPでは，⑨VM31から受信したARP応答フレームに対して，VXLAN

のカプセル化を行い，L3SW11 の VTEP 宛てに転送する。

(4) L3SW11 の VTEP では，受信した VXLAN パケットのカプセル化を解除して，VM11 宛てに ARP 応答フレームを転送する。

(1)～(4)の動作完了後に確認できる，L3SW11 及び L3SW31 が学習した VXLAN についての情報を，表 2 に示す。

表 2 L3SW11 及び L3SW31 が学習した VXLAN についての情報

機器名	VM の MAC アドレス	VNI	リモート VTEP の IP アドレス
L3SW11	AC-αβ-F1-00-00-31	キ	ク
L3SW31	AC-αβ-F1-00-00-11	ケ	コ

注記 1 AC-αβ- F1-00-00-11 は，VM11 の MAC アドレスである。
注記 2 AC-αβ- F1-00-00-31 は，VM31 の MAC アドレスである。

〔EVPN の概要〕

K 社の情報システム部では，S 課長から指示を受けた Q 主任が，EVPN を用いた VXLAN の技術検証を検討することになった。Q 主任が調査した EVPN の概要を示す。

RFC 7432 及び RFC 8365 で規定された EVPN は，RFC 4760 で規定された MP-BGP (Multiprotocol Extensions for BGP-4) を用いて，オーバーレイネットワークを制御するための情報を交換する。VXLAN のネットワークに EVPN を適用した場合，コントロールプレーンに EVPN を用いてオーバーレイネットワークを制御して，データプレーンに VXLAN を用いてイーサネットフレームを転送する。

図 1 の構成例に対して EVPN を適用した場合の EVPN の主な機能について，Q 主任が K 社の現行のネットワークと比較して確認した内容を次に示す。

機能 1：リモート VTEP に関する情報の学習について

現行のネットワークでは，VTEP は受信した VXLAN パケットからリモート VTEP の情報を学習する。EVPN を適用した場合，VTEP は MP-BGP を用いて，リモート VTEP の IP アドレス及び VNI などの情報をあらかじめ学習する。

機能 2：リモート VTEP に接続されたサーバに関する情報の学習について

現行のネットワークでは，VTEP は受信した VXLAN パケットから，リモート VTEP に接続されたサーバの MAC アドレス，VNI 及びリモート VTEP の IP ア

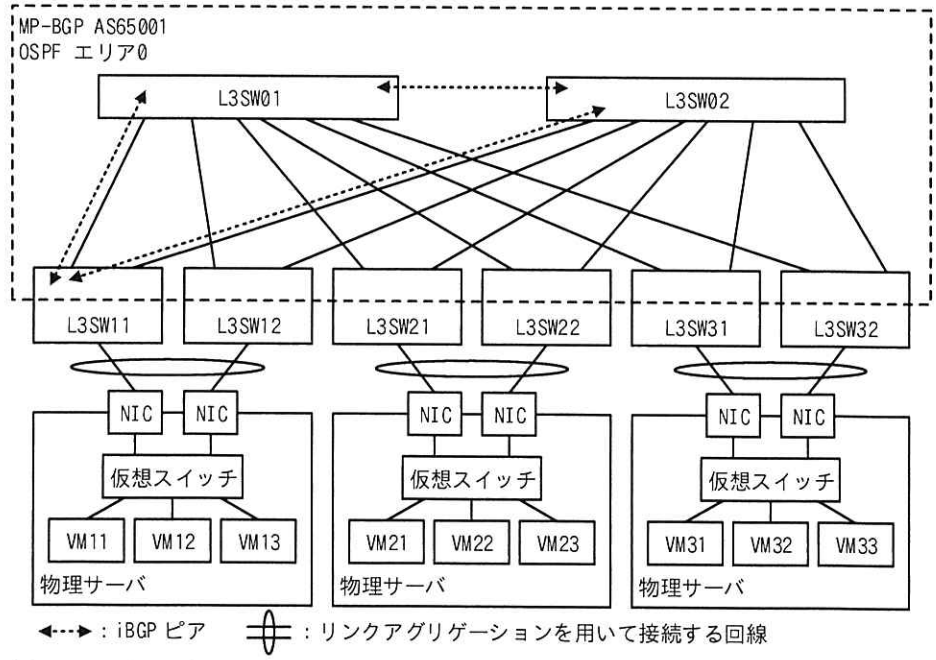
ドレスの情報を学習する。EVPN を適用した場合，VTEP は MP-BGP を用いて，リモート VTEP に接続されたサーバの MAC アドレス，VNI 及びリモート VTEP の IP アドレスなどの情報をあらかじめ学習する。

機能 3：サーバとの接続について

現行のネットワークでは，複数の VTEP とサーバの接続にリンクアグリゲーションを利用できない。EVPN を適用した場合，VTEP は MP-BGP を用いて，自身に接続されたサーバを識別する ESI（Ethernet Segment Identifier）という識別子を交換できるようになる。同じ ESI を設定した論理インタフェースをもつ複数の VTEP は，サーバとの接続にリンクアグリゲーションを利用できる。

〔新検証 NW の設計〕

Q 主任は，現行の検証 NW を基に，EVPN を用いた VXLAN を検証するためのネットワーク（以下，新検証 NW という）を設計することにした。新検証 NW を図 5 に示す。



注記　iBGP ピアのうち，L3SW01 と L3SW02 との間，L3SW01 と L3SW11 との間及び L3SW02 と L3SW11 との間を例として図示している。

図 5　新検証 NW（抜粋）

現行の検証NWから新検証NWに流用される設計を次に示す。

・新検証NWのL3SW及びVMには，図3及び図4中のIPアドレス及びVLAN IDと同じ値を割り当てる。
・物理サーバに接続するL3SWのポートには，タグVLANを設定する。
・L3SWの経路制御にOSPFを用いて，現行の検証NWと同じ設定にする。
・新検証NWのVLAN，VXLAN及びVTEPを図4と同じ論理構成にする。
・L3SW11，L3SW12，L3SW21，L3SW22，L3SW31及びL3SW32にVTEPを設定する。
・VTEPには，それぞれのL3SWのループバックインタフェースに割り当てるIPアドレスを使用する。

新検証NWに追加されるEVPNについての設計を次に示す。

・L3SWのEVPNを有効にする。
・L3SWにMP-BGPを設定して，ASを65001にする。
・⑩L3SW01及びL3SW02をMP-BGPのルートリフレクタにして，L3SW01とL3SW02との間でiBGPピアリングを行う。
・L3SW11，L3SW12，L3SW21，L3SW22，L3SW31及びL3SW32をルートリフレクタのクライアントにして，L3SW01及びL3SW02とiBGPピアリングを行う。
・iBGPのピアリングに使用するIPアドレスには，それぞれのL3SWのループバックインタフェースに割り当てるIPアドレスを使用する。

新検証NWにおける，現行の検証NWから変更される設計を次に示す。

・現行の検証NWで用いていたIPマルチキャストルーティングについては，利用しない。
・VTEPのBUMフレームの転送には，IPユニキャストを用いる設定にする。
・物理サーバの二つのNICをアクティブ／アクティブ構成にして，リンクアグリゲーションを用いてL3SWに接続する。

Q主任は，EVPNの機能1～3，図3～5を参照して，新検証NWの設計及びEVPNの機能を，上司のS課長に説明した。2人の会話を次に示す。

Q主任：EVPNの技術検証を行うための新検証NWを設計しました。図5のとおり，L3SW

に MP-BGP を設定して，EVPN を用いた VXLAN を構成するための物理ネットワークを構築します。VLAN，VXLAN 及び VTEP については，図 4 と同じ論理構成を組みます。

S 課長：新検証 NW で EVPN をどのように利用するのか教えてください。

Q 主任：EVPN の“機能 1”では，L3SW の VTEP は MP-BGP を利用して，リモート VTEP の情報をあらかじめ学習します。BUM フレームを受信した VTEP は，学習したリモート VTEP の情報を参照して，VLAN ID に対応する VNI をもつ各リモート VTEP を宛先に転送できるようになります。VTEP の BUM フレームの転送には，IP ユニキャストを用いる設定にします。

S 課長：IP マルチキャストルーティングを利用できないネットワークであっても拡張できるようになるのですね。ほかの機能についても説明してください。

Q 主任：EVPN の“機能 2”では，VTEP は MP-BGP を利用して，リモート VTEP に接続された VM の MAC アドレス，VNI 及びリモート VTEP の IP アドレスをあらかじめ学習します。VTEP は，リモート VTEP に接続された VM 宛てのイーサネットフレームを，学習した情報を参照して転送します。“機能 2”によって，BUM フレームのうちの［ f ］によるフラッディングの発生を低減できます。

S 課長：ネットワーク負荷の軽減を期待できそうですね。ところで，図 5 中の物理サーバと L3SW の接続方法は，図 3 中の接続方法と異なるのですか。

Q 主任：物理サーバと L3SW との間は，⑪ EVPN の“機能 3”によって，リンクアグリゲーションを用いて接続します。同一の物理サーバに接続する 2 台の L3SW に作成するリンクアグリゲーションの論理インタフェースには，同一の物理サーバに接続されていることを識別させるために，同じ［ g ］を設定します。

S 課長：新検証 NW を使ってどのようなテストを実施するのか教えてください。

Q 主任：VM 同士の通信可否を確認します。

S 課長：現行の検証 NW から設定を変更する BUM フレームの転送についても，動作を確認してください。

Q 主任：分かりました。⑫ ARP 要求フレームをカプセル化した全ての VXLAN パケットをキャプチャして，宛先 IP アドレスを確認します。

Q 主任が検討した新検証 NW の設計及びテスト内容は，情報システム部で承認された。Q 主任は EVPN の技術検証の実施のため，新検証 NW の構築に着手した。

設問１　〔VXLAN の概要〕について答えよ。

(1)　本文，図 1 及び図 2 中の［ a ］～［ c ］に入れる適切な字句又は数値を答えよ。

(2)　本文中の下線①～③について，それぞれの情報が図 2 中のどのヘッダー又はイーサネットフレームに含まれるか。図 2 中の字句を用いて答えよ。

(3)　本文中の下線④について，宛先 IP アドレスを IP マルチキャストのグループアドレスにして転送する目的を，45 字以内で答えよ。

設問２　〔現行の検証ネットワーク〕について答えよ。

(1)　本文中の［ d ］，［ e ］に入れる適切な字句を答えよ。

(2)　本文中の下線⑤について，K 社においてルータ ID は，OSPF のネットワーク内で何を識別するものか。20 字以内で答えよ。

(3)　本文中の下線⑥について，ECMP を用いるために必要となる設計を，“経路”と“コスト”という字句を用いて 45 字以内で答えよ。

(4)　本文中の下線⑦について，VTEP の IP アドレスに物理インタフェースの IP アドレスではなく，ループバックインタフェースの IP アドレスを使用するのはなぜか。45 字以内で答えよ。

(5)　表 1 中の［ ア ］～［ カ ］に入れる適切な通信可否を，表 1 の凡例に倣い“○”又は“×”で答えよ。

設問３　〔現行の検証 NW における VTEP の動作〕について答えよ。

(1)　本文中の下線⑧について，VXLAN パケットの宛先 IP アドレスを答えよ。

(2)　本文中の下線⑨の動作について，L3SW31 が L3SW11 の VTEP 宛てに転送するために，L3SW11 から ARP 要求フレームを含む VXLAN パケットを受信したときに学習する情報を，45 字以内で答えよ。

(3)　表 2 中の［ キ ］～［ コ ］に入れる適切な字句を，図 3 及び図 4 中の字句を用いて答えよ。

設問４　〔新検証 NW の設計〕について答えよ。

(1)　本文中の下線⑩について，ルートリフレクタを用いる利点を“iBGP”とい

う字句を用いて 25 字以内で答えよ。また，図 5 中の L3SW01 及び L3SW02 をルートリフレクタとして冗長化するときに，ループを防止するために設定する ID の名称を答えよ。

(2) 本文中の［ f ］，［ g ］に入れる適切な字句を，本文中の字句を用いて答えよ。

(3) 本文中の下線⑪について，現行の検証 NW と比較したときの利点を 25 字以内で答えよ。

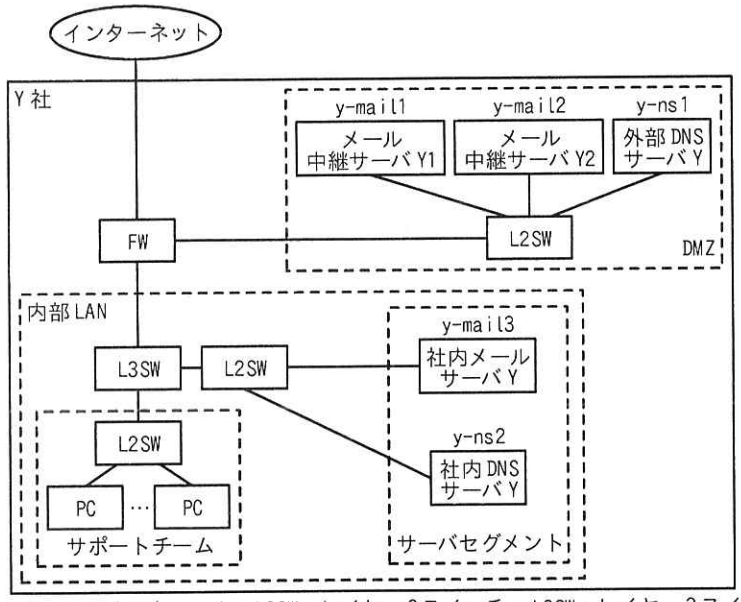
(4) 本文中の下線⑫について，VTEP は宛先 IP アドレスにセットするリモート VTEP の IP アドレスをどのように学習するか。20 字以内で答えよ。

(5) 本文中の下線⑫について，ある VLAN ID をセットされた ARP 要求フレームは，VTEP によってどのようなリモート VTEP に転送されるか。“VNI” という字句を用いて 40 字以内で答えよ。

問2　電子メールを用いた製品サポートに関する次の記述を読んで，設問に答えよ。

Y 社は，企業向けに IT 製品を販売する会社であり，電子メール（以下，メールという）を使用して，販売した製品のサポートを行っている。Y 社では，取扱製品の増加に伴って，サポート体制の強化が必要になってきた。そこで，サポート業務の一部を，サポートサービス専門会社の Z 社に委託することを決定し，Y 社の情報システム部の X 主任が，委託時のメールの運用方法を検討することになった。

Y 社のネットワーク構成を図 1 に，外部 DNS サーバ Y が管理するゾーン情報を図 2 に，社内 DNS サーバ Y が管理するゾーン情報を図 3 に示す。



FW：ファイアウォール　L2SW：レイヤー2スイッチ　L3SW：レイヤー3スイッチ

注記　y-ns1，y-ns2，y-mail1，y-mail2，及び y-mail3 はホスト名である。

図 1　Y 社のネットワーク構成（抜粋）

$TTL　172800				
y-sha.com.	IN	MX	20	y-mail1.y-sha.com.
y-sha.com.	IN	MX	1	y-mail2.y-sha.com.
y-mail1.y-sha.com.	IN	A		200.a.b.1
y-mail2.y-sha.com.	IN	A		200.a.b.2

注記　200.a.b.1 及び 200.a.b.2 はグローバル IP アドレスである。

図 2　外部 DNS サーバ Y が管理するゾーン情報（抜粋）

```
$TTL    172800
y-mail3.y-sha.lan.              IN      A       192.168.1.1
mail.y-sha.lan.         60      IN      A       192.168.0.1
mail.y-sha.lan.         60      IN      A       192.168.0.2
y-mail1.y-sha.lan.              IN      A       192.168.0.1
y-mail2.y-sha.lan.              IN      A       192.168.0.2
```

図3　社内DNSサーバYが管理するゾーン情報（抜粋）

Y社では，サポート契約を締結した顧客企業の担当者（以下，顧客という）からの製品サポート依頼を，社内メールサーバYに設定された問合せ窓口のメールアドレスである，support@y-sha.com で受け付けている。このメールアドレスはグループアドレスであり，support@y-sha.com 宛てのメールは，Y社のサポート担当者のメールアドレスに配信される。サポート担当者は，送信元メールアドレスが support@y-sha.com にセットされた製品サポートのメール（以下，サポートメールという）を，社内メールサーバYを使用して顧客に返信している。

〔Y社のネットワーク構成とセキュリティ対策の背景〕

Y社のネットワーク構成とメールのなりすまし防止などの情報セキュリティ対策の背景について次に示す。

・サポート担当者が送信したサポートメールが①社内メールサーバYからメール中継サーバに転送されるとき，②DNSラウンドロビンによってメール中継サーバY1又はY2に振り分けられる。

・転送先のメール中継サーバが障害などで応答しないとき，社内メールサーバYは，他方のメール中継サーバ宛てに転送する機能をもつ。

・顧客が送信したサポートメールがメール中継サーバに転送されるときは，外部DNSサーバYに登録されたMXレコードの［　a　］値によって，平常時は，ホスト名が［　b　］のメール中継サーバが選択される。

・FWには，インターネットからDMZのサーバ宛ての通信に対して，静的NATが設定されている。

FW に設定されている静的 NAT を表 1 に示す。

表 1　FW に設定されている静的 NAT（抜粋）

宛先のホスト	宛先 IP アドレス	変換後の IP アドレス
y-mail1.y-sha.com	ア	イ
y-mail2.y-sha.com	省略	省略

送信元メールアドレスの詐称の有無に対しては，DNS の［　c　］と呼ばれる名前解決によって，送信元メールサーバの IP アドレスからメールサーバの FQDN を取得し，その FQDN と送信元メールアドレスのドメイン名が一致した場合，詐称されていないと判定する検査方法が考えられる。しかし，③攻撃者は，自身が管理する DNS サーバの PTR レコードに不正な情報を登録することができるので，ドメイン名が一致しても詐称されているおそれがあることから，検査方法としては不十分である。このような背景から，受信側のメールサーバが送信元メールアドレスの詐称の有無を正しく判定できるようにする手法として，送信ドメイン認証が生まれた。

送信ドメイン認証の技術には，送信元 IP アドレスを基に，正規のサーバから送られたかどうかを検証する SPF（Sender Policy Framework）や，送られたメールのヘッダーに挿入された電子署名の真正性を検証する DKIM（DomainKeys Identified Mail）などがある。Y 社では SPF 及び DKIM の両方を導入している。

〔Y 社が導入している SPF の概要〕

SPF では，送信者のなりすましの有無を受信者が検証できるようにするために，送信者のドメインのゾーン情報を管理する権威 DNS サーバに，SPF で利用する情報(以下，SPF レコードという)を登録する。Y 社では，外部 DNS サーバ Y に SPF レコードを TXT レコードとして登録している。

Y 社が登録している SPF レコードを図 4 に示す。

```
y-sha.com.    IN    TXT    "v=spf1 +ip4: [ ウ ] +ip4: [ エ ] -all "
```

図 4　Y 社が登録している SPF レコード

Y社が導入しているSPFによる送信ドメイン認証の流れを次に示す。

(i) サポート担当者は，送信元メールアドレスがsupport@y-sha.comにセットされたサポートメールを，顧客宛てに送信する。

(ii) サポートメールは，社内メールサーバYからメール中継サーバY1又はY2を経由して，顧客のメールサーバに転送される。

(iii) 顧客のメールサーバは，メール中継サーバY1又はY2から，メール転送プロトコルである［ d ］の［ e ］コマンドで指定されたメールアドレスのドメイン名の［ f ］を入手する。顧客のメールサーバは，DNSを利用して，［ f ］ドメインのゾーン情報を管理する外部DNSサーバYに登録されているSPFレコードを取得する。

(iv) 顧客のメールサーバは，④取得したSPFレコードに登録された情報を基に，送信元のメールサーバの正当性を検査する。

(v) 正当なメールサーバから送信されたメールなので，なりすましメールではないと判断してメールを受信する。なお，正当でないメールサーバから送信されたメールは，なりすましメールと判断して，受信したメールの隔離又は廃棄などを行う。

〔Y社が導入しているDKIMの概要〕

DKIMは，送信側のメールサーバでメールに電子署名を付与し，受信側のメールサーバで電子署名の真正性を検証することで，送信者のドメイン認証を行う。電子署名のデータは，メールの［ g ］及び本文を基に生成される。

DKIMでは，送信者のドメインのゾーン情報を管理する権威DNSサーバを利用して，電子署名の真正性の検証に使用する鍵を公開する。鍵長は，2,048ビットより大きな鍵を利用することも可能である。しかし，DNSをトランスポートプロトコルである［ h ］で利用する場合は，DNSメッセージの最大長が［ i ］バイトという制限があるので，［ i ］バイトに収まる鍵長として，一般に2,048ビットの鍵が利用される。

DKIMの電子署名には，第三者認証局（以下，CAという）が発行した電子証明書を利用せずに，各サイトの管理者が生成する鍵が利用できる。

Y社では，Y社のネットワーク運用管理者が生成した鍵などのDKIMで利用する情報

（以下，DKIM レコードという）を，外部 DNS サーバ Y に TXT レコードとして登録している。

Y 社が登録している DKIM レコードを図 5 に，DKIM レコード中のタグの説明を表 2 に示す。

```
sel.ysha._domainkey.y-sha.com.    IN    TXT    "v=DKIM1; k=rsa; t=s; p=（省略）"
```

注記　sel.ysha は，y-sha.com で運用するセレクター名を示し，y-sha.com.は，電子署名を行うドメイン名を示す。

図 5　Y 社が登録している DKIM レコード

表 2　DKIM レコード中のタグの説明（抜粋）

タグ	説明
v	バージョン番号を示す。指定する場合は“DKIM1”とする。
k	電子署名の作成の際に利用する鍵の形式を指定する。
t	DKIM の運用状態が本番運用モードの場合は“s”を指定する。
p	Base64 でエンコードした［　オ　］のデータを指定する。

DKIM における送信側は，電子署名データなどを登録した DKIM-Signature ヘッダーを作成して送信するメールに付加する処理（以下，DKIM 処理という）を行う。DKIM では，一つのドメイン中に複数のセレクターを設定することができ，セレクターごとに異なる鍵が使用できる。セレクターは，DNS サーバに登録された DKIM レコードを識別するためのキーとして利用される。

DKIM-Signature ヘッダー中のタグの説明を表 3 に示す。ここで，DKIM-Signature ヘッダーの構成図は省略する。

表 3　DKIM-Signature ヘッダー中のタグの説明（抜粋）

タグ	説明
b	Base64 でエンコードした電子署名データ
d	電子署名を行ったドメイン名
s	複数の DKIM レコードの中から鍵を取得する際に，検索キーとして利用するセレクター名

Y 社は，顧客宛てのサポートメールに対する DKIM 処理を，メール中継サーバ Y1 及

び Y2 で行っている。Y 社では，ドメイン名が y-sha.com でセレクター名が sel.ysha のセレクターを設定している。Y 社が送信するメールの DKIM-Signature ヘッダー中の s タグには，図 5 中に示したセレクター名の sel.ysha が登録されている。

Y 社が導入している DKIM による送信ドメイン認証の流れを次に示す。

（ｉ） サポート担当者は，送信元メールアドレスが support@y-sha.com にセットされたサポートメールを，顧客宛てに送信する。

（ii） サポートメールは，社内メールサーバ Y からメール中継サーバ Y1 又は Y2 を経由して，顧客のメールサーバに転送される。

（iii） メール中継サーバ Y1 又は Y2 は，サポートメールに付加する DKIM-Signature ヘッダー中に電子署名データなどを登録して，顧客のメールサーバに転送する。

（iv） 顧客のメールサーバは，DKIM-Signature ヘッダー中の d タグに登録されたドメイン名である y-sha.com と s タグに登録されたセレクター名を基に，DNS を利用して，当該ドメインのゾーン情報を管理する外部 DNS サーバ Y に登録されている DKIM レコードを取得する。

（v） 顧客のメールサーバは，⑤取得した DKIM レコードに登録された情報を基に，電子署名の真正性を検査する。

（vi） 正当なメールサーバから送信されたメールなので，なりすましメールではないと判断してメールを受信する。なお，正当でないメールサーバから送信されたメールは，なりすましメールと判断して，受信したメールの隔離又は廃棄などを行う。

〔Z 社に委託するメールの運用方法の検討〕

まず，X 主任は，自社のメールシステムのセキュリティ運用規程に，次の規定があることを確認した。

（あ） 社内メールサーバ Y には，Y 社に勤務する従業員以外のメールボックスは設定しないこと

（い） 社内の PC によるメール送受信は，社内メールサーバ Y を介して行うこと

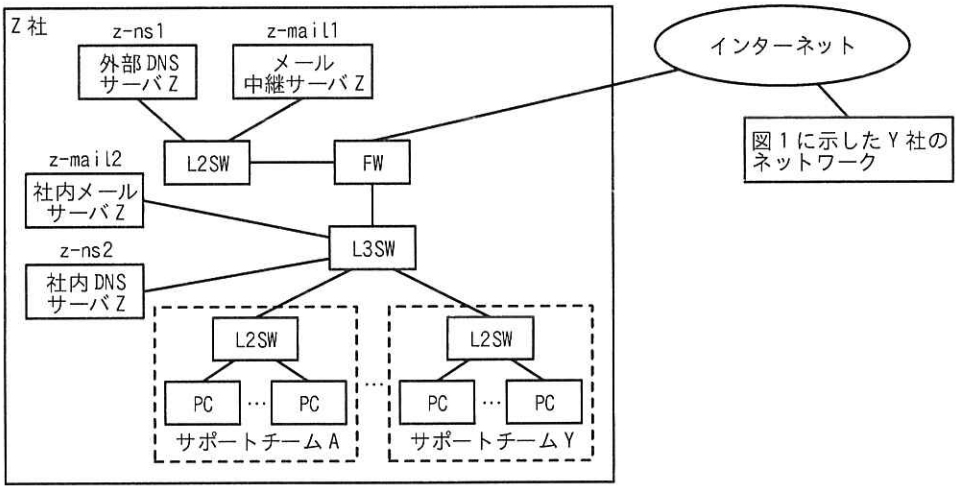
（う） メール中継サーバ Y1 及び Y2 にはメールボックスは設定せず，社内メールサーバ Y から社外宛て，及び社外から社内メールサーバ Y 宛てのメールだけを中継す

ること

（え） Y 社のドメインを利用するメールには，なりすまし防止などの情報セキュリティ対策を講じること

次に，メールの運用方法の検討に当たって，X 主任は，Z 社のネットワーク構成とサポート体制を調査した。

Z 社のネットワーク構成を図 6 に，外部 DNS サーバ Z が管理するゾーン情報を図 7 に示す。



注記 1　z-ns1，z-ns2，z-mail1 及び z-mail2 はホスト名である。
注記 2　サポートチーム A は，A 社向けのサポート業務を行い，サポートチーム Y は，Y 社向けのサポート業務を行うチームである。

図 6　Z 社のネットワーク構成（抜粋）

z-sha.co.jp.	IN	MX	10	z-mail1.z-sha.co.jp.
z-mail1.z-sha.co.jp.	IN	A		222.c.d.1

注記　222.c.d.1 はグローバル IP アドレスである。

図 7　外部 DNS サーバ Z が管理するゾーン情報（抜粋）

Z 社は，複数の企業から受託したメールを用いたサポート業務を，チームを編成して対応している。

X 主任は，Z 社のネットワーク構成，サポート体制及び Y 社のメールシステムのセキュリティ運用規程を基に，Z 社に委託するメールによるサポート方法を，次のようにまとめた。

・Z 社のサポートチーム Y のサポート担当者は，現在使用している問合せ窓口のメールアドレス support@y-sha.com でサポート業務を行う。
・support@y-sha.com 宛てのメール中から，Z 社に委託した製品のサポート依頼メール及びサポート途中のメールが抽出されて，Z 社のサポートチーム Y のグループアドレス宛てに転送されるようにする。
・サポートチーム Y のサポート担当者は，送信元メールアドレスが support@y-sha.com にセットされたサポートメールを，社内メールサーバ Z を使用して Y 社の顧客宛てに送信する。

次に，セキュリティ運用規程の(え)に対応するために，Z 社に委託するサポートメールへの SPF と DKIM の導入方法を検討した。

SPF には，⑥ DNS サーバに SPF で利用する情報を登録することで対応できると考えた。

DKIM には，図 6 中のメール中継サーバ Z で，送信元メールアドレスが support@y-sha.com のメールに対して DKIM 処理を行うことで対応できると考えた。このとき，顧客のメールサーバが，外部 DNS サーバ Y を使用して DKIM の検査を行うことができるように，DKIM-Signature ヘッダー中の d タグで指定するドメイン名には［ j ］を登録し，⑦ s タグで指定するセレクター名は sel.zsha として，Y 社と異なる鍵を電子署名に利用できるようにする。また，外部 DNS サーバ Y に，sel.zsha セレクター用の DKIM レコードを追加登録する。

委託時のメールの運用方法がまとまったので，検討結果を上司の W 課長に説明したところ，⑧ “Z 社のサポートチーム Y 以外の部署の従業員が，送信元メールアドレスに support@y-sha.com をセットしてサポート担当者になりすました場合，顧客のメールサーバでは，なりすましを検知できない”，との指摘を受けた。そこで，X 主任は，追加で実施する対策について調査した結果，S/MIME（Secure/MIME）の導入が有効であることが分かった。

〔S/MIME の調査と実施策〕

S/MIME では，受信者の MUA（Mail User Agent）によるメールに付与された電子署名の真正性の検証で，なりすましやメール内容の改ざんが検知できる。

MUA による電子署名の付与及び電子署名の検証の手順を表 4 に示す。

表4　MUAによる電子署名の付与及び電子署名の検証の手順

処理MUA	手順	処理内容
送信者のMUA	1	ハッシュ関数hによってメール内容のハッシュ値aを生成する。
	2	⑨ハッシュ値aを基に，電子署名データを作成する。
	3	送信者の電子証明書と電子署名付きのメールを送信する。
受信者のMUA	4	⑩受信したメール中の電子署名データからハッシュ値aを取り出す。
	5	ハッシュ関数hによってメール内容のハッシュ値bを生成する。
	6	⑪ハッシュ値を比較する。

X主任は，S/MIME導入に当たってY社とZ社が実施すべき事項について検討し，次の四つの実施事項をまとめた。

・Y社のホームページ上で，サポートメールへのS/MIMEの導入をアナウンスし，なりすまし防止対策を強化することを顧客に周知する。
・取得した電子証明書は，Z社にも秘密鍵と併せて提供する。
・Y社のサポート担当者及びZ社のサポートチームYのサポート担当者は，自身のPCに電子証明書と秘密鍵をインストールする。
・Y社及びZ社のサポート担当者は，送信するメールに電子署名を付与する。

X主任は，サポートメールにSPFとDKIMだけでなく新たにS/MIMEも導入したメールの運用方法と，サポート委託を開始するまでにY社及びZ社で実施すべき事項をW課長に報告した。報告内容が承認されたので，X主任は，委託時のメールの運用を開始するまでの手順書の作成，及びZ社の窓口担当者との調整に取り掛かった。

設問1　〔Y社のネットワーク構成とセキュリティ対策の背景〕について答えよ。

(1)　本文中の下線①について，転送先のメール中継サーバのFQDNを答えよ。

(2)　本文中の下線②について，社内メールサーバYからメール中継サーバY1又はY2へのメール転送時に，振分けの偏りを小さくするために実施している方策を，25字以内で答えよ。

(3)　本文中の［a］～［c］に入れる適切な字句を答えよ。

(4)　表1中の［ア］，［イ］に入れる適切なIPアドレスを答えよ。

(5)　本文中の下線③について，攻撃者がPTRレコードに対して行う不正な操作

の内容を，次に示す図8を参照して45字以内で答えよ。

ホストのIPアドレス	IN	PTR	ホストのFQDN

図8　PTRレコードの形式（抜粋）

設問2　〔Y社が導入しているSPFの概要〕について答えよ。

(1)　図4中の［ウ］，［エ］に入れる適切なIPアドレスを答えよ。

(2)　本文中の［d］～［f］に入れる適切な字句を答えよ。

(3)　本文中の下線④について，正当性の確認方法を，50字以内で答えよ。

設問3　〔Y社が導入しているDKIMの概要〕について答えよ。

(1)　本文中の［g］～［i］に入れる適切な字句又は数値を答えよ。

(2)　図5のDKIMレコードで指定されている暗号化方式のアルゴリズム名，及び表2中の［オ］に入れる適切な鍵名を答えよ。

(3)　本文中の下線⑤について，電子署名の真正性の検査によって送信者がなりすまされていないことが分かる理由を，50字以内で答えよ。

設問4　〔Z社に委託するメールの運用方法の検討〕について答えよ。

(1)　本文中の下線⑥について，登録するDNSサーバ名及びDNSサーバに登録する情報を，それぞれ，図1又は図6中の字句を用いて答えよ。

(2)　本文中の［j］に入れる適切な字句を答えよ。

(3)　本文中の下線⑦について，異なる鍵を利用することによる，Y社におけるセキュリティ面の利点を，50字以内で答えよ。

(4)　本文中の下線⑧について，顧客のメールサーバでは，なりすましを検知できない理由を，40字以内で答えよ。

設問5　〔S/MIMEの調査と実施策〕について答えよ。

(1)　表4中の下線⑨の電子署名データの作成方法を，25字以内で答えよ。

(2)　表4中の下線⑩のハッシュ値aを取り出す方法を，20字以内で答えよ。

(3)　表4中の下線⑪について，どのような状態になれば改ざんされていないと判断できるかを，25字以内で答えよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. 問題に関する質問にはお答えできません。文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。