NW

令和３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（○）

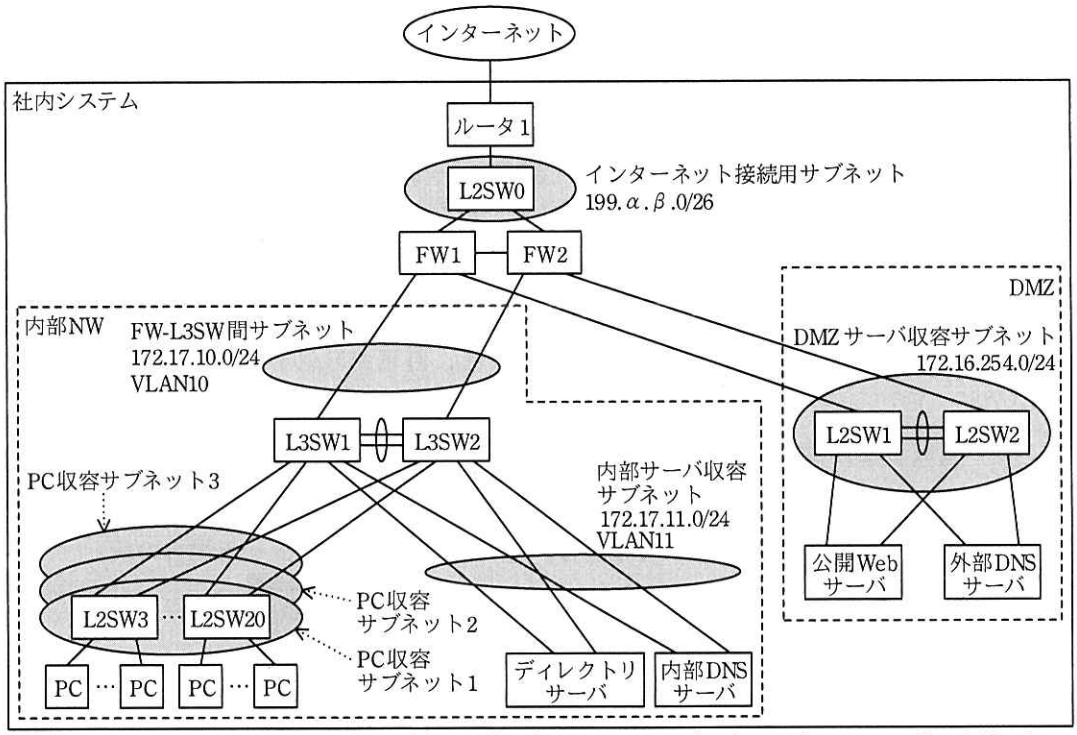
注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　社内システムの更改に関する次の記述を読んで，設問1～6に答えよ。

G社は，都内に本社を構える従業員600名の建設会社である。G社の従業員は，情報システム部が管理する社内システムを業務に利用している。情報システム部は，残り1年でリース期間の満了を迎える，サーバ，ネットワーク機器及びPCの更改を検討している。

〔社内システムの概要〕

G社の社内システムの構成を図1に示す。



L2SW：レイヤ2スイッチ　　L3SW：レイヤ3スイッチ　　FW：ファイアウォール　　NW：ネットワーク

：リンクアグリゲーションを用いて接続している回線

注記1　199.α.β.0/26は，グローバルIPアドレスを示す。
注記2　PC収容サブネット1のIPアドレスブロックは172.17.101.0/24，VLAN IDは101である。
注記3　PC収容サブネット2のIPアドレスブロックは172.17.102.0/24，VLAN IDは102である。
注記4　PC収容サブネット3のIPアドレスブロックは172.17.103.0/24，VLAN IDは103である。
注記5　L2SW3～L2SW20は，PC収容サブネット1～PC収容サブネット3を構成している。

図1　G社の社内システムの構成（抜粋）

G 社の社内システムの概要は，次のとおりである。

・外部 DNS サーバは，DMZ のドメインに関するゾーンファイルを管理する権威サーバであり，インターネットから受信する名前解決要求に応答する。

・内部 DNS サーバは，社内システムのドメインに関するゾーンファイルを管理する権威サーバであり，PC 及びサーバから送信された名前解決要求に応答する。

・内部 DNS サーバは，DNS［ a ］であり，PC 及びサーバから送信された社外のドメインに関する名前解決要求を，ISP が提供するフルサービスリゾルバに転送する。

・全てのサーバに二つの NIC を実装し，アクティブ／スタンバイのチーミングを設定している。

・L3SW1 及び L3SW2 で VRRP を構成し，L3SW1 の［ b ］を大きく設定して，マスタルータにしている。

・L3SW1 と L3SW2 間のポートを，VLAN10，VLAN11 及び VLAN101 ～ VLAN103 を通すトランクポートにしている。

・L2SW3 ～ L2SW20 と L3SW 間のポートを，VLAN101 ～ VLAN103 を通すトランクポートにしている。

・内部 NW のスイッチは，IEEE 802.1D で規定されている STP（Spanning Tree Protocol）を用いて，経路を冗長化している。

・内部 DNS サーバは DHCP サーバ機能をもち，PC に割り当てる IP アドレス，サブネットマスク，デフォルトゲートウェイの IP アドレス，及び①名前解決要求先の IP アドレスの情報を，PC に通知している。

・FW1 及び FW2 は，アクティブ／スタンバイのクラスタ構成である。

・FW1 及び FW2 に静的 NAT を設定し，インターネットから受信したパケットの宛先 IP アドレスを，公開 Web サーバ及び外部 DNS サーバのプライベート IP アドレスに変換している。

・FW1 及び FW2 に NAPT を設定し，サーバ及び PC からインターネット向けに送信されるパケットの送信元 IP アドレス及び送信元ポート番号を，それぞれ変換している。

G 社のサーバ及び PC の設定を表 1 に，G 社のネットワーク機器に設定する静的経

路情報を表2に，それぞれ示す。

表1　G社のサーバ及びPCの設定（抜粋）

機器名	IPアドレスの割当範囲	デフォルトゲートウェイ		所属VLAN
		機器名	IPアドレス	
公開Webサーバ	172.16.254.10 ～ 172.16.254.100	FW1，FW2	172.16.254.1 1)	なし
外部DNSサーバ				
ディレクトリサーバ	172.17.11.10 ～ 172.17.11.100	L3SW1，L3SW2	172.17.11.1 2)	11
内部DNSサーバ				
PC	172.17.101.10 ～ 172.17.101.254	L3SW1，L3SW2	172.17.101.1 2)	101
	172.17.102.10 ～ 172.17.102.254	L3SW1，L3SW2	172.17.102.1 2)	102
	172.17.103.10 ～ 172.17.103.254	L3SW1，L3SW2	172.17.103.1 2)	103

注 1)　FW1とFW2が共有する仮想IPアドレスである。
　 2)　L3SW1とL3SW2が共有する仮想IPアドレスである。

表2　G社のネットワーク機器に設定する静的経路情報（抜粋）

機器名	宛先ネットワークアドレス	サブネットマスク	ネクストホップ	
			機器名	IPアドレス
FW1，FW2	172.17.11.0	255.255.255.0	L3SW1，L3SW2	172.17.10.4 1)
	172.17.101.0	255.255.255.0	L3SW1，L3SW2	172.17.10.4 1)
	172.17.102.0	255.255.255.0	L3SW1，L3SW2	172.17.10.4 1)
	172.17.103.0	255.255.255.0	L3SW1，L3SW2	172.17.10.4 1)
	0.0.0.0	0.0.0.0	ルータ1	199.α.β.1
L3SW1，L3SW2	0.0.0.0	0.0.0.0	FW1，FW2	172.17.10.1 2)

注 1)　L3SW1とL3SW2が共有する仮想IPアドレスである。
　 2)　FW1とFW2が共有する仮想IPアドレスである。

情報システム部のJ主任が社内システムの更改と移行を担当することになった。更改と移行に当たって，上司であるM課長から指示された内容は，次のとおりである。

(1)　内部NWを見直して，障害発生時の業務への影響の更なる低減を図ること

(2)　業務への影響を極力少なくした移行計画を立案すること

〔現行の内部NW調査〕

J主任は，まず，現行の内部NWの設計について再確認した。内部NWのスイッチは，一つのツリー型トポロジをSTPによって構成し，全てのVLANのループを防止している。②L3SW1に最も小さいブリッジプライオリティ値を，L3SW2に2番目に

小さいブリッジプライオリティ値を設定し，L3SW1 をルートブリッジにしている。

ルートブリッジに選出された L3SW1 は，STP によって構成されるツリー型トポロジの最上位のスイッチである。L3SW1 はパスコストを 0 に設定した BPDU（Bridge Protocol Data Unit）を，接続先機器に送信する。BPDU を受信した L3SW2 及び L2SW3 ～ L2SW20（以下，L3SW2 及び L2SW3 ～ L2SW20 を非ルートブリッジという）は，設定されたパスコストを加算した BPDU を，受信したポート以外のポートから送信する。非ルートブリッジの L3SW 及び L2SW の全てのポートのパスコストに，同じ値を設定している。

STP を設定したスイッチは，各ポートに，ルートポート，指定ポート及び非指定ポートのいずれかの役割を決定する。ルートブリッジである L3SW1 では，全てのポートが［ c ］ポートとなる。非ルートブリッジでは，パスコストやブリッジプライオリティ値に基づきポートの役割を決定する。例えば，L2SW3 において，L3SW2 に接続するポートは，［ d ］ポートである。

STP のネットワークでトポロジの変更が必要になると，スイッチはポートの状態遷移を開始し，［ e ］テーブルをクリアする。

ポートをフォワーディングの状態にするときの，スイッチが行うポートの状態遷移は，次のとおりである。

(1) リスニングの状態に遷移させる。

(2) 転送遅延に設定した待ち時間が経過したら，ラーニングの状態に遷移させる。

(3) 転送遅延に設定した待ち時間が経過したら，フォワーディングの状態に遷移させる。

J 主任は，内部 NW の STP を用いているネットワークに障害が発生したときの復旧を早くするために，IEEE 802.1D-2004 で規定されている RSTP（Rapid Spanning Tree Protocol）を用いる方式と，スイッチのスタック機能を用いる方式を検討することにした。

〔RSTP を用いる方式〕

J 主任は，トポロジの再構成に掛かる時間を短縮したプロトコルである RSTP について調査した。RSTP では，STP の非指定ポートの代わりに，代替ポートとバックア

ップポートの二つの役割が追加されている。RSTP で追加されたポートの役割を，表3に示す。

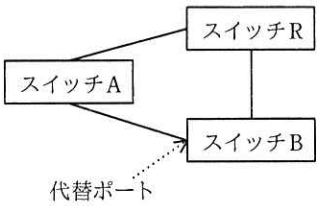
表3　RSTP で追加されたポートの役割

役割	説明
代替ポート	通常，ディスカーディングの状態であり，ルートポートのダウンを検知したら，すぐにルートポートになり，フォワーディングの状態になるポート
バックアップポート	通常，ディスカーディングの状態であり，指定ポートのダウンを検知したら，すぐに指定ポートになり，フォワーディングの状態になるポート

注記　ディスカーディングの状態は，MAC アドレスを学習せず，フレームを破棄する。

RSTP では，プロポーザルフラグをセットした BPDU（以下，プロポーザルという）及びアグリーメントフラグをセットした BPDU（以下，アグリーメントという）を使って，ポートの役割決定と状態遷移を行う。

調査のために，J 主任が作成した RSTP のネットワーク図を図2に示す。



注記1　全てのスイッチに RSTP を用いる。
注記2　スイッチ R がルートブリッジである。

図2　J 主任が作成した RSTP のネットワーク図

スイッチ A において，スイッチ R に接続するポートのダウンを検知したときに，スイッチ A とスイッチ B が行うポートの状態遷移は，次のとおりである。

(1) スイッチ A は，トポロジチェンジフラグをセットした BPDU をスイッチ B に送信する。

(2) スイッチ B は，スイッチ A にプロポーザルを送信する。

(3) スイッチ A は，受信したプロポーザル内のブリッジプライオリティ値やパスコストと，自身がもつブリッジプライオリティ値やパスコストを比較する。比較結果から，スイッチ A は，スイッチ B が RSTP によって構成されるトポロジにおいて［　f　］であると判定し，スイッチ B にアグリーメントを送信し，指定ポー

トをルートポートにする。

(4) アグリーメントを受信したスイッチ B は，代替ポートを指定ポートとして，フォワーディングの状態に遷移させる。

J 主任は，調査結果から，STP を RSTP に変更することで，③内部 NW に障害が発生したときの，トポロジの再構成に掛かる時間を短縮できることを確認した。

〔スイッチのスタック機能を用いる方式〕

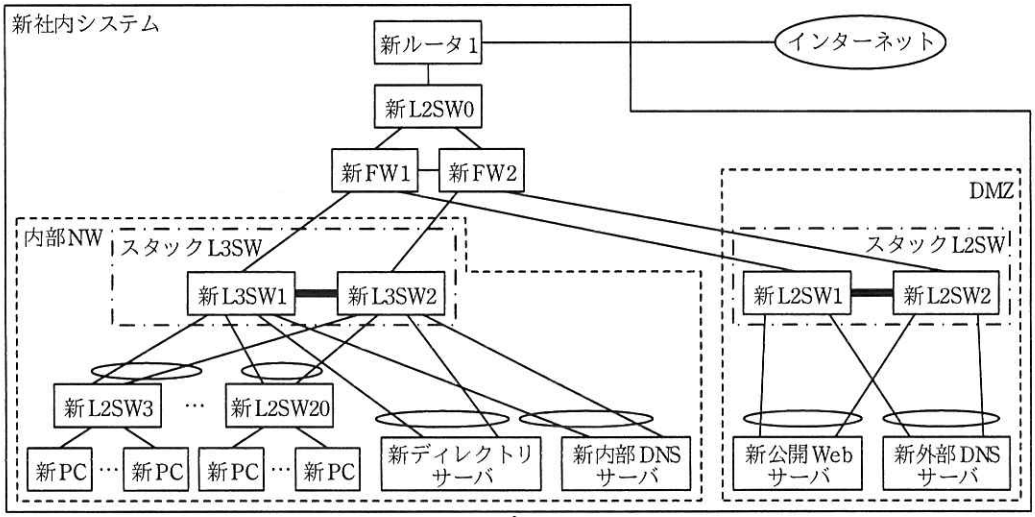
次に，J 主任は，ベンダから紹介された，新たな機器が実装するスタック機能を用いる方式を検討した。新たな機器を用いた社内システム（以下，新社内システムという）の内部 NW に関して，J 主任が検討した内容は次のとおりである。

・新 L3SW1 と新 L3SW2 をスタック用ケーブルで接続し，1 台の論理スイッチ（以下，スタック L3SW という）として動作させる。
・スタック L3SW と新 L2SW3～新 L2SW20 の間を，リンクアグリゲーションを用いて接続する。
・新ディレクトリサーバ及び新内部 DNS サーバに実装される二つの NIC に，アクティブ／アクティブのチーミングを設定し，スタック L3SW に接続する。

検討の内容を基に，J 主任は，スタック機能を用いることで，障害発生時の復旧を早く行えるだけでなく，④スイッチの情報収集や構成管理などの維持管理に係る運用負荷の軽減や，⑤回線帯域の有効利用を期待できると考えた。

〔新社内システムの構成設計〕

J 主任は，スイッチのスタック機能を用いる方式を採用し，STP 及び RSTP を用いない構成にすることにした。J 主任が設計した新社内システムの構成を，図 3 に示す。



注記　スタックL2SWは，新L2SW1と新L2SW2をスタック用ケーブルで接続した1台の論理スイッチである。

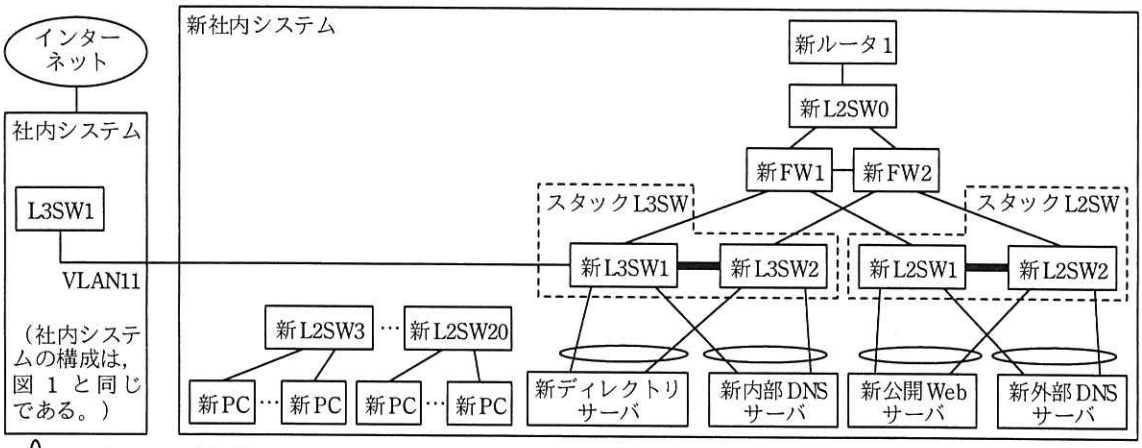
図3　新社内システムの構成（抜粋）

〔新社内システムへの移行の検討〕

J主任は，現行の社内システムから新社内システムへの移行に当たって，五つの作業ステップを設けることにした。移行における作業ステップを表4に，ステップ1完了時のネットワーク構成を図4に示す。ステップ1では，現行の社内システムと新社内システムの共存環境を構築する。

表4　移行における作業ステップ（抜粋）

作業ステップ	作業期間	説明
ステップ1	1か月	・図4中の新社内システムを構築し，現行の社内システムと接続する。
ステップ2	1か月	・⑥現行のディレクトリサーバから新ディレクトリサーバへデータを移行する。 ・⑦現行の社内システムに接続されたPCから，新公開Webサーバの動作確認を行う。
ステップ3	1日	・現行の社内システムから，新社内システムに切り替える。（表8参照）
ステップ4	1か月	・新社内システムの安定稼働を確認し，新サーバに不具合が見つかった場合には，速やかに現行のサーバに切り戻す。
ステップ5	1日	・現行の社内システムを切り離す。



注記 1　新 L2SW3～新 L2SW20 と新 L3SW1，新 L3SW2 間は接続されていない。
注記 2　スタック L3SW には，VLAN101～VLAN103 に関する設定を行わない。

図 4　ステップ 1 完了時のネットワーク構成（抜粋）

ステップ 1 完了時のネットワーク構成の概要は，次のとおりである。

・新ディレクトリサーバ及び新内部 DNS サーバに，172.17.11.0/24 の IP アドレスブロックから未使用の IP アドレスを割り当てる。

・⑧新公開 Web サーバ及び新外部 DNS サーバには，172.16.254.0/24 の IP アドレスブロックから未使用の IP アドレスを割り当てる。

・現行の L3SW1 と新 L3SW1 間を接続し，接続ポートを VLAN11 のアクセスポートにする。

・スタック L3SW の VLAN11 の VLAN インタフェースに，未使用の IP アドレスである 172.17.11.101 を，一時的に割り当てる。

・全ての新サーバについて，デフォルトゲートウェイの IP アドレスは，現行のサーバと同じ IP アドレスにする。

・新社内システムのインターネット接続用サブネットには，現行の社内システムと同じグローバル IP アドレスを使うので，新外部 DNS サーバのゾーンファイルに，現行の外部 DNS サーバと同じゾーン情報を登録する。

・現行の内部 DNS サーバ及び新内部 DNS サーバのゾーンファイルに，新サーバに関するゾーン情報を登録する。

・新 FW1 及び新 FW2 は，アクティブ／スタンバイのクラスタ構成にする。

・新 FW1 及び新 FW2 には，インターネットから受信したパケットの宛先 IP アドレスを，新公開 Web サーバ及び新外部 DNS サーバのプライベート IP アドレスに変換する静的 NAT を設定する。

・新 FW1 及び新 FW2 に NAPT を設定する。

・新サーバの設定を表 5 に，新 FW 及びスタック L3SW に設定する静的経路情報を表 6 に，FW 及び L3SW に追加する静的経路情報を表 7 に示す。

表 5　新サーバの設定（抜粋）

機器名	IP アドレスの割当範囲	デフォルトゲートウェイ		所属 VLAN
		機器名	IP アドレス	
新公開 Web サーバ	（設問のため省略）	新 FW1，新 FW2	172.16.254.1 [1)]	なし
新外部 DNS サーバ				
新ディレクトリサーバ	（省略）	L3SW1，L3SW2	172.17.11.1 [2)]	11
新内部 DNS サーバ				

注 [1)]　新 FW1 と新 FW2 が共有する仮想 IP アドレスである。
[2)]　L3SW1 と L3SW2 が共有する仮想 IP アドレスである。

表 6　新 FW 及びスタック L3SW に設定する静的経路情報（抜粋）

機器名	宛先ネットワークアドレス	サブネットマスク	ネクストホップ	
			機器名	IP アドレス
新 FW1，新 FW2	172.17.11.0	255.255.255.0	スタック L3SW	172.17.10.4
	172.17.101.0	255.255.255.0	スタック L3SW	172.17.10.4
	172.17.102.0	255.255.255.0	スタック L3SW	172.17.10.4
	172.17.103.0	255.255.255.0	スタック L3SW	172.17.10.4
	0.0.0.0	0.0.0.0	スタック L3SW	172.17.10.4
スタック L3SW	172.16.254.128	255.255.255.128	新 FW1，新 FW2	172.17.10.1 [1)]
	0.0.0.0	0.0.0.0	L3SW1，L3SW2	172.17.11.1 [2)]

注 [1)]　新 FW1 と新 FW2 が共有する仮想 IP アドレスである。
[2)]　L3SW1 と L3SW2 が共有する仮想 IP アドレスである。

表 7　FW 及び L3SW に追加する静的経路情報（抜粋）

機器名	宛先ネットワークアドレス	サブネットマスク	ネクストホップ	
			機器名	IP アドレス
FW1，FW2	172.16.254.128	255.255.255.128	L3SW1，L3SW2	172.17.10.4 [1)]
L3SW1，L3SW2	172.16.254.128	255.255.255.128	スタック L3SW	172.17.11.101

注 [1)]　L3SW1 と L3SW2 が共有する仮想 IP アドレスである。

次に，J主任は，ステップ3の現行の社内システムから新社内システムへの切替作業について検討した。J主任が作成したステップ3の作業手順を，表8に示す。

表8　ステップ3の作業手順（抜粋）

作業名	手順
インターネット接続回線の切替作業	・現行のルータ1に接続されているインターネット接続回線を，新ルータ1に接続する。
DMZのネットワーク構成変更作業	・新FW1及び新FW2に設定されているデフォルトルートのネクストホップを，新ルータ1のIPアドレスに変更する。 ・⑨現行のFW1とL2SW1間，及び現行のFW2とL2SW2間を接続しているLANケーブルを抜く。 ・⑩ステップ4で，新サーバに不具合が見つかったときの切戻しに掛かる作業量を減らすために，現行のL2SW1と新L2SW1間を接続する。 ・⑪インターネットから新公開Webサーバに接続できることを確認する。
内部NWのネットワーク構成変更作業	・現行のL3SW1及びL3SW2のVLANインタフェースに設定されている全てのIPアドレス，並びに静的経路情報を削除する。 ・スタックL3SWのVLAN11のVLANインタフェースに設定されているIPアドレスを，［ g ］に変更する。 ・スタックL3SWに設定されているデフォルトルートのネクストホップを新FW1と新FW2が共有する仮想IPアドレスに変更する。 ・スタックL3SWに設定されている宛先ネットワークアドレスが172.16.254.128/25の静的経路情報を削除する。
ディレクトリサーバの切替作業	・新ディレクトリサーバをマスタとして稼働させる。
DHCPサーバの切替作業	・現行の内部DNSサーバのDHCPサーバ機能を停止する。 ・新内部DNSサーバのDHCPサーバ機能を開始する。 ・⑫スタックL3SWにDHCPリレーエージェントを設定する。
新PCの接続作業	・スタックL3SWに，VLAN101～VLAN103のVLANインタフェースを作成し，IPアドレスを設定する。 ・新L2SW3～新L2SW20と新L3SW1，新L3SW2に，VLAN101～VLAN103を通すトランクポートを設定し，接続する。 ・新PCから新ディレクトリサーバに接続できることを確認する。

J主任が作成した移行計画はM課長に承認され，J主任は更改の準備に着手した。

設問1　〔社内システムの概要〕について，(1)，(2)に答えよ。

(1)　本文中の［ a ］，［ b ］に入れる適切な字句を答えよ。

(2)　本文中の下線①の名前解決要求先を，図1中の機器名で答えよ。

設問2　〔現行の内部NW調査〕について，(1)，(2)に答えよ。

(1) 本文中の下線②の設定を行わず，内部 NW の L2SW 及び L3SW に同じブリッジプライオリティ値を設定した場合に，L2SW 及び L3SW はブリッジ ID の何を比較してルートブリッジを決定するか。適切な字句を答えよ。また，L2SW3 がルートブリッジに選出された場合に，L3SW1 と L3SW2 が VRRP の情報を交換できなくなるサブネットを，図 1 中のサブネット名を用いて全て答えよ。

(2) 本文中の［ c ］～［ e ］に入れる適切な字句を答えよ。

設問３　〔RSTP を用いる方式〕について，(1)，(2) に答えよ。

(1) 本文中の［ f ］に入れる適切な字句を答えよ。

(2) 本文中の下線③について，トポロジの再構成に掛かる時間を短縮できる理由を二つ挙げ，それぞれ 30 字以内で述べよ。

設問４　〔スイッチのスタック機能を用いる方式〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，運用負荷を軽減できる理由を，30 字以内で述べよ。

(2) 本文中の下線⑤について，内部 NW で，スタック L3SW～新 L2SW 以外に回線帯域を有効利用できるようになる区間が二つある。二つの区間のうち一つの区間を，図 3 中の字句を用いて答えよ。

設問５　図 3 の構成について，STP 及び RSTP を不要にしている技術を二つ答えよ。また，STP 及び RSTP が不要になる理由を，15 字以内で述べよ。

設問６　〔新社内システムへの移行の検討〕について，(1)～(8) に答えよ。

(1) 表 4 中の下線⑥によって発生する現行のディレクトリサーバから新ディレクトリサーバ宛ての通信について，現行の L3SW1 とスタック L3SW 間を流れるイーサネットフレームをキャプチャしたときに確認できる送信元 MAC アドレス及び宛先 MAC アドレスをもつ機器をそれぞれ答えよ。

(2) 表 4 中の下線⑦によって発生する現行の PC から新公開 Web サーバ宛ての通信について，現行の L3SW1 とスタック L3SW 間を流れるイーサネットフレームをキャプチャしたときに確認できる送信元 MAC アドレス及び宛先 MAC アドレスをもつ機器をそれぞれ答えよ。

(3) 本文中の下線⑧について，新公開 Web サーバに割り当てることができる IP アドレスの範囲を，表 1 及び表 5～7 の設定内容を踏まえて答えよ。

(4) 表 8 中の下線⑨を行わないときに発生する問題を，30 字以内で述べよ。

(5) 表 8 中の下線⑩の作業後に，新公開 Web サーバに不具合が見つかり，現行の公開 Web サーバに切り替えるときには，新 FW1 及び新 FW2 の設定を変更する。変更内容を，70 字以内で述べよ。また，インターネットから現行の公開 Web サーバに接続するときに経由する機器名を，【転送経路】の表記法に従い，経由する順に全て列挙せよ。

【転送経路】

インターネット → [経由する順に全て列挙] → 公開 Web サーバ

(6) 表 8 中の下線⑪によって発生する通信について，新 FW の通信ログで確認できる通信を二つ答えよ。ここで，新公開 Web サーバに接続するための IP アドレスは，接続元が利用するフルサービスリゾルバのキャッシュに記録されていないものとする。

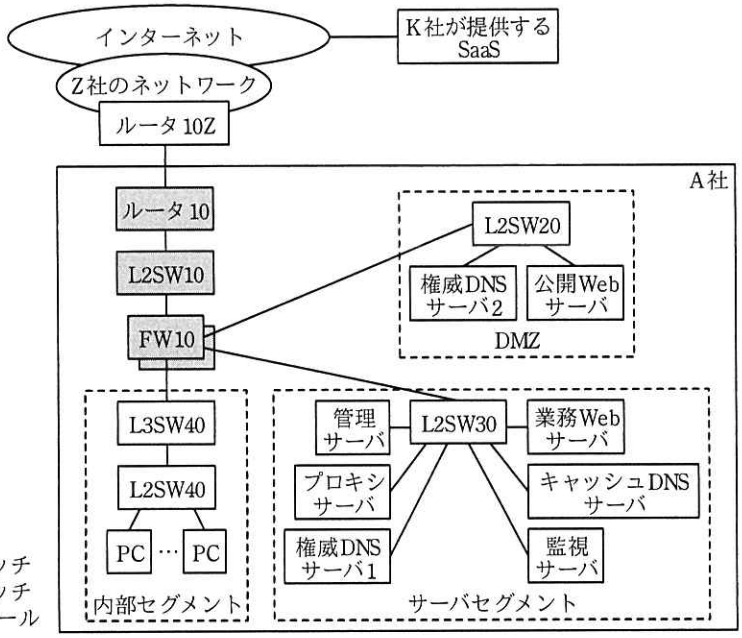
(7) 表 8 中の [g] に入れる適切な IP アドレスを答えよ。

(8) 表 8 中の下線⑫について，スタック L3SW は，PC から受信した DHCPDISCOVER メッセージの giaddr フィールドに，受信したインタフェースの IP アドレスを設定して，新内部 DNS サーバに転送する。DHCP サーバ機能を提供している新内部 DNS サーバは，giaddr フィールドの値を何のために使用するか。60 字以内で述べよ。

問2　インターネット接続環境の更改に関する次の記述を読んで，設問1～4に答えよ。

物品販売を主な事業とするA社は，近年，ネット通販に力を入れている。A社は，K社が提供するSaaSを利用して，顧客との電子メールやビジネスチャット，ファイル共有などを行っている。A社のシステム部では，老朽化に伴うA社インターネット接続環境の新しい機器への交換とインターネット接続の冗長化の検討を進めている。システム部門のB課長は，Cさんをインターネット接続環境の更改の担当者として任命した。

A社は，専用線を利用して，インターネットサービスプロバイダであるZ社を経由して，インターネットに接続している。現在のA社ネットワーク環境を図1に示す。



注記1　FWはクラスタ構成であり，物理的に2台のFWが論理的に1台のFWとして動作している。
注記2　□は，交換対象機器を示す。

図1　現在のA社ネットワーク環境（抜粋）

現在のA社ネットワーク環境の概要は次のとおりである。

・FWは，ステートフルパケットインスペクション機能をもつ。FWは，A社で必要な通信を許可し，必要のない通信を拒否している。

・FW は，許可又は拒否した情報を含む通信ログデータを管理サーバに SYSLOG で送信している。
・プロキシサーバは，従業員が利用する PC からインターネット向けの HTTP 通信及び HTTPS 通信をそれぞれ中継し，通信ログデータを管理サーバに SYSLOG で送信している。
・K 社が提供する SaaS との通信は全て HTTPS 通信である。
・管理サーバには，A 社のルータ，FW，L2SW 及び L3SW（以下，A 社 NW 機器という）から SNMP を用いて収集した通信量などの統計データ，FW とプロキシサーバの通信ログデータが保存されている。
・管理サーバは，通信ログデータを基に FW とプロキシサーバの通信ログ分析レポートを作成している。
・監視サーバは，A 社 NW 機器及びサーバを死活監視している。
・キャッシュ DNS サーバは，PC やサーバセグメントのサーバからの名前解決の問合せ要求に対して，他の DNS サーバへ問い合わせた結果，得られた情報を応答する。
・権威 DNS サーバ 1 は，A 社内の PC やサーバセグメントのサーバのホスト名などを管理し，名前解決の問合せ要求に対して PC やサーバセグメントのサーバなどに関する情報を応答する。
・サーバセグメントには，プライベート IP アドレスを付与している。
・サーバセグメントからインターネットに接続する際に，FW で NAPT による IP アドレスとポート番号の変換が行われる。
・内部セグメントには，プライベート IP アドレスを付与している。
・権威 DNS サーバ 2 は，A 社内の公開 Web サーバのホスト名などを管理し，名前解決の問合せ要求に対して公開 Web サーバなどに関する情報を応答する。
・DMZ には，グローバル IP アドレスを付与している。
・ルータ 10Z には，A 社が割当てを受けているグローバル IP アドレスの静的経路設定がされており，これを基に Z 社内部のルータに経路情報の広告を行っている。
・ルータ 10，FW10 及び L3SW40 の経路制御は静的経路制御を利用している。

C さんは，インターネット接続環境の更改の検討を進めるに当たり，まず，インタ

ーネット接続環境の利用状況を調査することにした。

〔インターネット接続環境の利用状況の調査〕

管理サーバは，SNMP を用いて，5 分ごとに A 社 NW 機器の情報を収集している。A 社 NW 機器のインタフェースの情報は，インタフェースに関する MIB によって取得できる。そのうち，インタフェースの通信量に関する MIB の説明を表 1 に示す。

表 1　インタフェースの通信量に関する MIB の説明（抜粋）

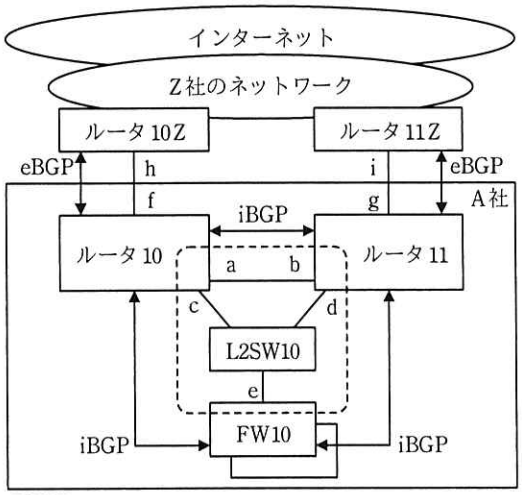
MIB の種類	説明
ifInOctets	インタフェースで受信したパケットの総オクテット数（32 ビットカウンタ）
ifOutOctets	インタフェースで送信したパケットの総オクテット数（32 ビットカウンタ）
ifHCInOctets	インタフェースで受信したパケットの総オクテット数（64 ビットカウンタ）
ifHCOutOctets	インタフェースで送信したパケットの総オクテット数（64 ビットカウンタ）

例えば，ifInOctets はカウンタ値で，電源投入によって機器が起動すると初期値の 0 から加算が開始され，インタフェースでパケットを受信した際にそのパケットのオクテット数が加算される。機器は，管理サーバから SNMP で問合せを受けると，その時点のカウンタ値を応答する。①管理サーバは，5 分ごとに SNMP でカウンタ値を取得し，単位時間当たりの通信量を計算し，統計データとして保存している。単位時間当たりの通信量の単位はビット／秒である。②カウンタ値が上限値を超える場合，初期値に戻って（以下，カウンタラップという）再びカウンタ値が加算される。通信量が多いとカウンタラップが頻繁に起きることから，インタフェースの通信量の情報を取得する場合には，32 ビットカウンタではなく，64 ビットカウンタを利用することが推奨されている。管理サーバに保存された統計データは，単位時間当たりの通信量の推移を示すトラフィックグラフとして参照できる。

統計データから，過去に何度か利用が増え，インターネットに接続する専用線に輻輳（ふくそう）が起きていたことが判明したので，専用線を増速する必要があると C さんは考えた。また，統計データと通信ログ分析レポートから交換対象機器の通信量や負荷の状態を確認した結果，ルータ 10 及び L2SW10 は同等性能の後継機種に交換し，FW10 は性能が向上した上位機種に交換すればよいと C さんは考えた。

〔インターネット接続の冗長化検討〕

C さんは，インターネット接続の冗長化方法について Z 社に提案を求めた。Z 社の提案は，動的経路制御の一つである BGP を用いた構成であった。Z 社の提案した構成を図 2 に示す。



各機器に付与されているアドレス一覧

機器名	インタフェース	IPアドレス/ネットマスク
ルータ10Z	h	α.β.γ.1/30
ルータ11Z	i	α.β.γ.5/30
ルータ10	a	α.β.γ.13/30
	c	α.β.γ.17/29
	f	α.β.γ.2/30
	ループバック	α.β.γ.8/32
ルータ11	b	α.β.γ.14/30
	d	α.β.γ.18/29
	g	α.β.γ.6/30
	ループバック	α.β.γ.9/32
FW10	e	α.β.γ.19/29

[- - -]：OSPFエリア
注記1　L2SWは冗長構成であるが，図では省略している。
注記2　a～iは，各機器の物理インタフェースを示す。
注記3　FWはクラスタ構成であり，物理的に2台のFWが論理的に1台のFWとして動作している。
注記4　表中のIPアドレスは，グローバルIPアドレスである。
注記5　◀――▶は，BGPピアを示す。

図 2　Z 社の提案した構成（抜粋）

Z 社の提案した構成の概要は次のとおりである。

・ルータ 10 側の専用線を増速する。また，新たに専用線を敷設して Z 社に接続する。新たに敷設する専用線を終端する機器として，ルータ 11 とルータ 11Z を設置する。ルータ 11 側の専用線の契約帯域幅は，ルータ 10 側の専用線と同じにする。

・平常時はルータ 10 側の専用線を利用し，障害などでルータ 10 側が利用できない場合は，ルータ 11 側を利用するように経路制御を行う。

・ルータ 10 とルータ 11 にはループバックインタフェースを作成し，これらに IP アドレスを設定する。

・a～e の各物理インタフェース及びループバックインタフェースでは，OSPF エリアを構成する。

・③ルータ 10 とルータ 11 はループバックインタフェースに設定した IP アドレスを利用し，FW10 は e に設定した IP アドレスを利用して，互いに iBGP のピアリングを行う。④ iBGP のピアリングでは，経路情報を広告する際に，BGP パスアトリビュートの一つである NEXT_HOP の IP アドレスを，自身の IP アドレスに書き換える設定を行う。

・ルータ 10 とルータ 10Z の間，及びルータ 11 とルータ 11Z の間では，eBGP のピアリングを行う。ピアリングには，f と h，及び g と i に設定した IP アドレスを利用する。

・eBGP のピアリングでは，A 社側はプライベート AS 番号である 64512 を，Z 社側はグローバル AS 番号である 64496 を利用する。

C さんは，Z 社の提案を受け，BGP の標準仕様について調査を行った。

BGP では，それぞれの経路情報に，パスアトリビュートの情報が付加される。BGP パスアトリビュートの一覧を表 2 に示す。

表 2　BGP パスアトリビュートの一覧（抜粋）

タイプコード	パスアトリビュート
2	AS_PATH
3	NEXT_HOP
4	MULTI_EXIT_DISC
5	LOCAL_PREF

AS_PATH は，経路情報がどの AS を経由してきたのかを示す AS 番号の並びである。eBGP ピアにおいて，隣接する AS に経路情報を広告する際に，AS_PATH に自身の AS 番号を追加する。また，⑤隣接する AS から経路情報を受信する際に，自身の AS 番号が含まれている場合はその経路情報を破棄する。

NEXT_HOP は，宛先ネットワークアドレスへのネクストホップの IP アドレスを示す。ネクストホップの IP アドレスは，ルータがパケットを転送する宛先を示す。eBGP ピアに経路情報を広告する際には，NEXT_HOP を自身の IP アドレスに書き換えて送信する。iBGP ピアに経路情報を広告する際には，NEXT_HOP を書き換えず，そのまま送信する。

MULTI_EXIT_DISC（以下，MED という）は，eBGP ピアに対して通知する，自身の AS 内に存在する宛先ネットワークアドレスの優先度である。MED はメトリックとも呼ばれる。

LOCAL_PREF は，iBGP ピアに対して通知する，外部の AS に存在する宛先ネットワークアドレスの優先度である。

BGP では，ピアリングで受信した経路情報を BGP テーブルとして構成する。この BGP テーブルに存在する，同じ宛先ネットワークアドレスの経路情報の中から，最適経路を一つだけ選択し，ルータのルーティングテーブルに反映する。A 社で利用している機器の最適経路選択アルゴリズムの仕様を表 3 に示す。

表 3　最適経路選択アルゴリズムの仕様

評価順	説明
1	LOCAL_PREF の値が最も大きい経路情報を選択する。
2	AS_PATH の長さが最も［　ア　］経路情報を選択する。
3	ORIGIN の値で IGP，EGP，Incomplete の順で選択する。
4	MED の値が最も［　イ　］経路情報を選択する。
5	eBGP ピアで受信した経路情報，iBGP ピアで受信した経路情報の順で選択する。
6	NEXT_HOP が最も近い経路情報を選択する。
7	ルータ ID が最も小さい経路情報を選択する。
8	ピアリングに使用する IP アドレスが最も小さい経路情報を選択する。

最適経路の選択は，表 3 中の評価順に行われる。例えば，同じ宛先ネットワークアドレスの経路情報が二つあった場合には，最初に，LOCAL_PREF の値を評価し，値に違いがあれば最も大きい値をもつ経路情報を選択し，評価を終了する。値に違いがなければ，次の AS_PATH の長さの評価に進む。

なお，ルータのルーティングテーブルに最適経路を反映するためには，NEXT_HOP の IP アドレスに対応する経路情報が，ルータのルーティングテーブルに存在し，ルータがパケット転送できる状態にある必要がある。

C さんは，以上の調査結果を基に Z 社の提案した構成を確認した。C さんと Z 社の担当者との会話は，次のとおりである。

C さん：専用線の経路制御はどのように行いますか。

担当者：今回は，LOCAL_PREF を利用して，図 2 中の各ルータ及び FW のパケット送信を制御します。ルータ 10Z とルータ 11Z が経路情報を受信した際に，LOCAL_PREF の値をそれぞれ設定し，Z 社内部の機器に経路情報の広告を行います。ルータ 10 とルータ 11 が経路情報を受信した際も同様に，LOCAL_PREF の値をそれぞれ設定し，A 社内部の機器に経路情報の広告を行ってください。

C さん：BGP で広告する経路情報はどのようなものですか。

担当者：ルータ 10Z とルータ 11Z はデフォルトルートの経路情報の広告を行います。ルータ 10 とルータ 11 は A 社が割当てを受けているグローバル IP アドレスの経路情報の広告を行ってください。平常時の FW10 の BGP テーブルは表 4 のように，ルーティングテーブルは表 5 のようになるはずです。

表 4　FW10 の BGP テーブル（抜粋）

宛先ネットワークアドレス	AS_PATH	MED	LOCAL_PREF	NEXT_HOP
0.0.0.0/0	64496	0	200	ウ
0.0.0.0/0	64496	0	100	エ

表 5　FW10 のルーティングテーブル（抜粋）

宛先ネットワークアドレス	ネクストホップ	インタフェース
0.0.0.0/0	$\alpha.\beta.\gamma.8$	e
$\alpha.\beta.\gamma.8/32$	オ	e
$\alpha.\beta.\gamma.9/32$	カ	e

C さん：分かりました。リンクダウンしないにもかかわらず，通信ができなくなるような専用線の障害時は，どのような動作になりますか。

担当者：BGP では，［　キ　］メッセージを定期的に送信します。専用線の障害時には，ルータが［　キ　］メッセージを受信しなくなることによって，ピアリングが切断され，AS 内の各機器の経路情報が更新されます。

C さん：分かりました。

担当者：ところで，⑥BGP の標準仕様ではトラフィックを分散する経路制御はできません。BGP マルチパスと呼ばれる技術を使うことで，平常時からルータ 10 側，ルータ 11 側両方の専用線を使って，トラフィックを分散する経路制御ができますがいかがですか。教えていただいた，今回利用を検討されている機器はどれも BGP マルチパスをサポートしています。BGP マルチパスを有効にすると，BGP テーブル内の LOCAL_PREF や AS_PATH，MED の値は同じで，NEXT_HOP だけが異なる複数の経路情報を，同時にルーティングテーブルに反映します。その結果，ECMP（Equal-Cost Multi-Path）によってトラフィックを分散することができます。

C さん：いいですね。では，BGP マルチパスを利用したいと思います。

担当者：承知しました。各機器の設定例を後ほどお渡ししますので参考にしてください。

C さん：ありがとうございます。

〔インターネット接続の冗長化手順〕

C さんは，冗長化作業中にインターネット利用に対する影響が最小限となる，インターネット接続の冗長化手順の検討を行った。C さんが検討した冗長化手順を表 6 に示す。

表 6　C さんが検討した冗長化手順

手順	作業対象機器	作業内容
手順 1	ルータ 11Z，ルータ 11	機器の設置
手順 2	ルータ 11Z，ルータ 11，ルータ 10，L2SW10	ケーブルの接続
手順 3	ルータ 11Z，ルータ 11，ルータ 10，L2SW10	物理インタフェースの設定，IP アドレスの設定及び疎通の確認
手順 4	ルータ 10，ルータ 11	ク
手順 5	ルータ 10，ルータ 11，FW10	ケ
手順 6	ルータ 10，ルータ 11，FW10	コ
手順 7	ルータ 10，ルータ 11，ルータ 10Z，ルータ 11Z	サ
手順 8	シ	静的経路の削除
手順 9	ルータ 10，L2SW10，FW10	後継機種又は上位機種に交換

手順 1，2 では，新たに導入する機器の設置及びケーブルの接続を行い，物理構成

を完成する。手順 3 では，作業対象機器の物理インタフェースの設定及び IP アドレスの設定を行い，機器間で疎通の確認を行う。疎通の確認では，ping を用いて，パケットロスが観測されないことを確認する。手順 4～7 で，BGP や OSPF を順次設定する。続いて，手順 8 を実施する。⑦A 社からインターネットへ向かう通信については，手順 8 の静的経路の削除が行われた時点で，動的経路による制御に切替えが行われ，冗長化が完成する。最後に，手順 9 では，インターネット利用に対する影響が最小限になるように機器を操作しながら，作業対象機器をあらかじめ設定を投入しておいた後継機種又は上位機種に交換する。例えば，ルータ 10 の交換に当たっては，⑧通信がルータ 10 を経由しないようにルータ 10 に対して操作を行った後に交換作業を実施する。

C さんは，これまでの検討結果をインターネット接続環境の更改案としてまとめ，B 課長に報告した。B 課長は，専用線に輻輳が発生していたこと，及び監視サーバで検知できなかったことを問題視した。想定外のネットワーク利用などによって突発的に発生した通信や輻輳を迅速に検知できるように，単位時間当たりの通信量の監視（以下，トラフィック監視という）について，C さんに検討するよう指示した。

〔トラフィック監視の導入〕

監視サーバの死活監視は，監視対象に対して，1 回につき ICMP のエコー要求を 3 パケット送信し，エコー応答を受信するかどうかを確認する。1 分おきに連続して 5 回，一つもエコー応答を受信しなかった場合に，アラートとして検知する。エコー要求のタイムアウト値は 1 秒である。C さんは，⑨専用線の輻輳を検知するために，監視サーバの監視対象として，ルータ 10Z とルータ 11Z を追加することを考えたが，問題があるため見送った。

そこで，C さんは，通信量のしきい値を定義し，上限値を上回ったり，下限値を下回ったりするとアラートとして検知する監視（以下，しきい値監視という）の利用を検討した。通信を均等に分散できると仮定すると，インターネット接続の冗長化導入によって利用できる帯域幅は専用線 2 回線分になる。どちらかの専用線に障害が発生すると，利用できる帯域幅は専用線 1 回線分になる。C さんは，どちらかの専用線に障害が発生した状況において，専用線に流れるトラフィックの輻輳の発生を避けるためには，平常時から，それぞれの専用線で利用できる帯域幅の

［　ス　］%を単位時間当たりの通信量の上限値としてしきい値監視すればよいと考えた。このしきい値監視でアラートを検知すると，トラフィック増の原因を調査して，必要であれば専用線の契約帯域幅の増速を検討する。

次に，C さんは，想定外のネットワーク利用などによって単位時間当たりの通信量が突発的に増えたり，A 社 NW 機器の故障などによって単位時間当たりの通信量が突発的に減ったりすること（以下，トラフィック異常という）を検知する監視の利用を検討した。C さんは機械学習を利用した監視（以下，機械学習監視という）の製品を調査した。

C さんが調査した製品は，過去に収集した時系列の実測値を用いて，傾向変動や周期性から近い将来の値を予測し，異常を検知することができる。例えば，単位時間当たりの通信量について，その予測値と新たに収集した実測値を基に，トラフィック異常を検知することができる。

C さんは，管理サーバに保存されている単位時間当たりの通信量の統計データを用いて，機械学習監視製品の試験導入を行った。C さんは，これまで検知できなかったトラフィック異常が検知できることを確認した。さらに，⑩管理サーバに保存されている，統計データとは別のデータについても，機械学習監視製品を用いて監視することで，トラフィック異常とは別の異常が検知できることを確認した。複数のデータを組み合わせて，機械学習監視製品を用いて監視することで，ネットワーク環境の状況を素早く，かつ，詳細に把握できることが分かった。

C さんは，機械学習監視製品の試験結果についてまとめ，B 課長に報告を行い，インターネット接続環境の更改に併せて，管理サーバにしきい値監視と機械学習監視製品を導入することが決まった。

その後，A 社では，C さんがまとめたインターネット接続環境の更改案を基に設備更改が実施され，また，しきい値監視と機械学習監視製品が導入された。

設問 1　〔インターネット接続環境の利用状況の調査〕について，(1)～(3) に答えよ。

(1) 本文中の下線①について，取得時刻 t におけるカウンタ値を X_t，取得時刻 t の 5 分前の時刻 t−1 におけるカウンタ値を X_{t-1} としたとき，t−1 と t の間における単位時間当たりの通信量（ビット／秒）を算出する計算式を答えよ。

ここで，1オクテットは8ビットとし，t−1とtの間でカウンタラップは発生していないものとする。

(2) 本文中の下線①について，利用状況の調査を目的として，単位時間当たりの通信量（ビット／秒）を求める際に時間平均することによる問題点を 35 字以内で述べよ。

(3) 本文中の下線②について，32 ビットカウンタでカウンタラップが発生した際に，通信量を正しく計算するためには，カウンタ値をどのように補正すればよいか。解答群の中から選び，記号で答えよ。ここで，取得時刻 t におけるカウンタ値を X_t，取得時刻 t の 5 分前の時刻 t−1 におけるカウンタ値を X_{t-1}，t−1 と t の間でカウンタラップが 1 回発生したとする。

解答群

ア　X_t を X_t+2^{32} に補正する。　　イ　X_t を $X_t+2^{32}-1$ に補正する。

ウ　X_{t-1} を $X_{t-1}+2^{32}$ に補正する。　　エ　X_{t-1} を $X_{t-1}+2^{32}-1$ に補正する。

設問2　〔インターネット接続の冗長化検討〕について，(1)〜(5)に答えよ。

(1) 本文中の下線③について，図 2 中のルータ 10 やルータ 11 にはループバックインタフェースを作成し，iBGP のピアリングにループバックインタフェースに設定した IP アドレスを利用するのはなぜか。FW10 とのインタフェースの数の違いに着目し，60 字以内で述べよ。

(2) FW10 のルーティングテーブルを表 7 に示す。本文中の下線④について，書き換える設定を行わない場合に，FW10 のルーティングテーブルに追加で必要になる情報はどのような内容か。表 5 を参考に，表 7 中の［ a ］，［ b ］に入れる適切な字句を答えよ。

表 7　FW10 のルーティングテーブル（抜粋）

宛先ネットワークアドレス	ネクストホップ	インタフェース
a	（設問のため省略）	e
b	（設問のため省略）	e

(3) 本文中の下線⑤について，経路情報を破棄する目的を 20 字以内で述べよ。

(4) 本文及び表 3〜5 中の［ ア ］〜［ キ ］に入れる適切な字句を答え

よ。

(5) 本文中の下線⑥について，BGP の標準仕様とはどのような内容か。本文中の字句を用いて 50 字以内で述べよ。

設問３　〔インターネット接続の冗長化手順〕について，(1)～(4) に答えよ。

(1) 表 6 中の［　ク　］～［　サ　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　eBGP の導入　　イ　iBGP の導入　　ウ　OSPF の導入

エ　ループバックインタフェースの作成と IP アドレスの設定

(2) 表 6 中の［　シ　］に入れる適切な機器名を，図 2 中の機器名で全て答えよ。

(3) 本文中の下線⑦について，静的経路の削除が行われた時点で，動的経路による制御に切替えが行われる理由を 40 字以内で述べよ。

(4) 本文中の下線⑧について，ルータ 10 に対して行う操作はどのような内容か。操作の内容を 20 字以内で述べよ。

設問４　〔トラフィック監視の導入〕について，(1)～(3) に答えよ。

(1) 本文中の下線⑨について，問題点を二つ挙げ，それぞれ 30 字以内で述べよ。

(2) 本文中の［　ス　］に入れる適切な数値を答えよ。

(3) 本文中の下線⑩について，統計データとは別のデータにはどのようなデータがあるか。本文中の字句を用いて 25 字以内で答えよ。また，そのデータを，機械学習監視製品を用いて監視することによって，どのようなトラフィック異常とは別の異常を検知できるようになるか。検知内容を 40 字以内で述べよ。

〔 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，マスク

   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。