問2　ネットワーク監視の改善に関する次の記述を読んで，設問1～4に答えよ。

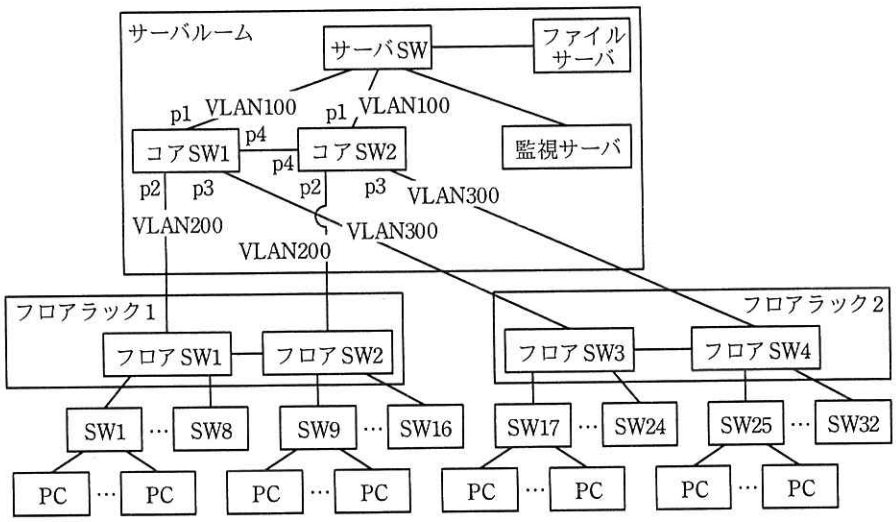
A社は従業員数200人の流通業者である。A社のシステム部門では，統合監視サーバ（以下，監視サーバという）を構築し，A社のサーバやLANの運用監視を行っている。

監視サーバは，pingによる死活監視（以下，ping監視という）とSYSLOGによる異常検知監視（以下，SYSLOG監視という）を行っている。現在定義されているLANに関するSYSLOG監視は，ポートのリンク状態遷移，STP（Spanning Tree Protocol）状態遷移及びVRRP（Virtual Router Redundancy Protocol）状態遷移の3種類である。

ある日，“従業員が使用するPCからファイルサーバを利用できない”という苦情が，システム部門に多数寄せられた。調査した結果，ケーブルの断線による障害と判明して対処したが，監視サーバで検知できなかったことが問題視された。

〔A社LANの概要〕

A社は，オフィスビルの1フロアを利用している。A社LANの構成を，図1に示す。




SW：スイッチ
注記1　コアSW1，コアSW2は，レイヤ3スイッチである。
注記2　フロアSW1～フロアSW4，サーバSW，SW1～SW32は，レイヤ2スイッチである。
注記3　p1～p4は，スイッチのポートを示す。
注記4　VLAN100，VLAN200，VLAN300は，スイッチのアクセスポートのVLAN IDを示す。

図1　A社LANの構成（抜粋）

コアSWには，サーバSWとフロアSWが接続されている。サーバSWは，監視サーバとファイルサーバを収容している。フロアSWには，従業員が使用するPCを収容するSWが接続されている。

A社LANは次のように設計されている。

・コアSWには，①VRRPが設定してあり，②正常時は，コアSW1がマスタルータで，コアSW2がバックアップルータとなるように設定している。

・A社LANは，ループ構成を含んでいる。例えば，コアSW1 - サーバSW - コアSW2 - コアSW1はループ構成の一つである。IEEE 802.1Dで規定されているSTPを用いて，レイヤ2ネットワークのループを防止している。正常時はコアSW1がルートブリッジとなるように設定している。

・コアSWのp1ポート，p2ポート及びp3ポートはアクセスポートで，③p4ポートをIEEE 802.1Qを用いたトランクポートに設定している。

〔監視サーバの概要〕

監視対象機器は，コアSW，サーバSW及びフロアSWである。

ping 監視には，RFC 792 で規定されているプロトコルである［　ア　］を利用する。echo request パケットの宛先として，監視対象機器には［　イ　］を割り当てる必要がある。

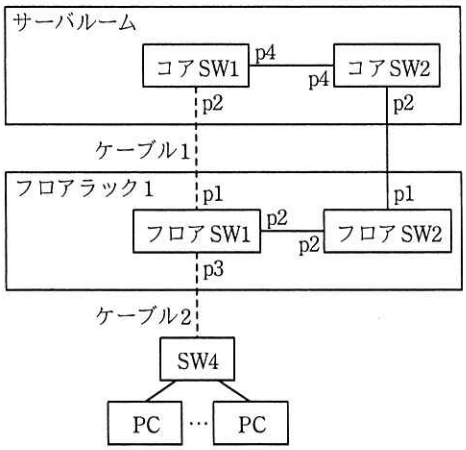
リンクダウンなどの異常が発生した機器は，監視サーバに対して直ちに SYSLOG メッセージを送信する。監視サーバは，受信した SYSLOG メッセージの分析を直ちに行い，定義に従って異常として検知する。SYSLOG は，トランスポートプロトコルとして RFC 768 で規定されている［　ウ　］を用いている。

〔監視サーバの問題〕

ネットワークに異常が発生した際に，監視サーバで検知できなかった問題について，システム部門の B 課長は，部下の C さんに障害発生時の状況確認とネットワーク監視の改善策の立案を指示した。

〔障害発生時の状況確認〕

ケーブルの断線による障害発生時の構成を，図 2 に示す。




注記　破線は，断線したケーブルを示す。

図 2　ケーブルの断線による障害発生時の構成（抜粋）

C さんが行った状況確認の結果は，次のとおりである。

・障害発生時，フロアラック 1 の近くでフロアのレイアウト変更が行われていた。その影響で，フロア SW1 の p1 ポートとコア SW1 の p2 ポートを接続するケーブル 1

が断線した。同時に，フロア SW1 の p3 ポートと SW4 を接続するケーブル 2 が断線した。

・ケーブル 1 の断線によって，④フロア SW2 の p1 ポートの STP のポート状態がブロッキングから，リスニング，ラーニングを経て，フォワーディングに遷移した。また，監視サーバでは，SYSLOG 監視によって，ケーブル 1 が接続されているポートのリンク状態遷移が発生したことを検知した。

・ケーブル 2 の断線に伴って⑤フロア SW1 が送信した，リンク状態遷移を示す SYSLOG メッセージが監視サーバに到達できなかった。その結果，監視サーバは，ケーブル 2 が接続されているポートのリンク状態遷移を検知できなかった。

〔ネットワーク監視の改善策の立案〕

C さんは，ネットワーク監視の改善策として，新たに SNMP（Simple Network Management Protocol）を使って監視することを検討した。C さんは，監視対象機器で利用可能な SNMPv2c について調査を行った。

SNMP は機器を管理するためのプロトコルで，⑥SNMP エージェントと SNMP マネージャで構成される。SNMP エージェントと SNMP マネージャは，同じグループであることを示す［　エ　］を用いて，機器の管理情報（以下，MIB という）を共有する。

SNMP の基本動作として，ポーリングとトラップがある。ポーリングは，SNMP マネージャが，SNMP エージェントに対して，例えば 5 分ごとといった定期的に MIB の問合せを行うことによって，機器の状態を取得できる。一方，トラップは，MIB に変化が起きた際に，SNMP エージェントが直ちにメッセージを送信し，SNMP マネージャがメッセージを受信することによって，機器の状態を取得できる。

C さんは，⑦5 分間隔のポーリング，又はトラップを使用して監視しても，今回発生したネットワークの異常においてはそれぞれ問題があることが分かった。しかし，SNMP のインフォームと呼ばれるイベント通知機能を利用すれば，これらの問題に対応できると考えた。

SNMP のインフォームでは，MIB に変化が起きた際に，SNMP エージェントが直ちにメッセージを送信し，SNMP マネージャからの確認応答を待つ。確認応答を受信できない場合，SNMP エージェントは，SNMP マネージャがメッセージを受信し

なかったと判断し，メッセージの再送信を行う。C さんは，⑧今回と同様なネットワークの異常が発生した場合に備えて，SNMP マネージャがインフォームの受信を行えるよう，SNMP エージェントの設定パラメタを考えた。

その後，C さんは SNMP のインフォームを用いたネットワーク監視の改善策を B 課長に報告し，その内容が承認された。

設問１　本文中の［　ア　］～［　エ　］に入れる適切な字句を答えよ。

設問２　〔A 社 LAN の概要〕について，(1)～(3) に答えよ。

(1) 本文中の下線①について，PC 及びサーバに設定する情報に着目して，VRRP による冗長化対象を 15 字以内で答えよ。

(2) 本文中の下線②について，バックアップルータはあるメッセージを受信しなくなったときにマスタルータに切り替わる。VRRP で規定されているメッセージ名を 15 字以内で答えよ。

(3) 本文中の下線③について，p4 ポートでトランクポートに設定する VLAN ID を全て答えよ。

設問３　〔障害発生時の状況確認〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，BPDU（Bridge Protocol Data Unit）を受信しなくなったフロア SW2 のポートを，図 2 中の字句を用いて答えよ。

(2) 本文中の下線⑤について，フロア SW1 が送信した SYSLOG メッセージが監視サーバに到達できなかったのはなぜか。“スパニングツリー”の字句を用いて 25 字以内で述べよ。

設問４　〔ネットワーク監視の改善策の立案〕について，(1)～(3) に答えよ。

(1) 本文中の下線⑥について，SNMP エージェントと SNMP マネージャに該当する機器名を，図 1 中の機器名を用いてそれぞれ一つ答えよ。

(2) 本文中の下線⑦について，ポーリングとトラップの問題を，それぞれ 35 字以内で述べよ。

(3) 本文中の下線⑧について，SNMP エージェントが満たすべき動作の内容を，40 字以内で述べよ。