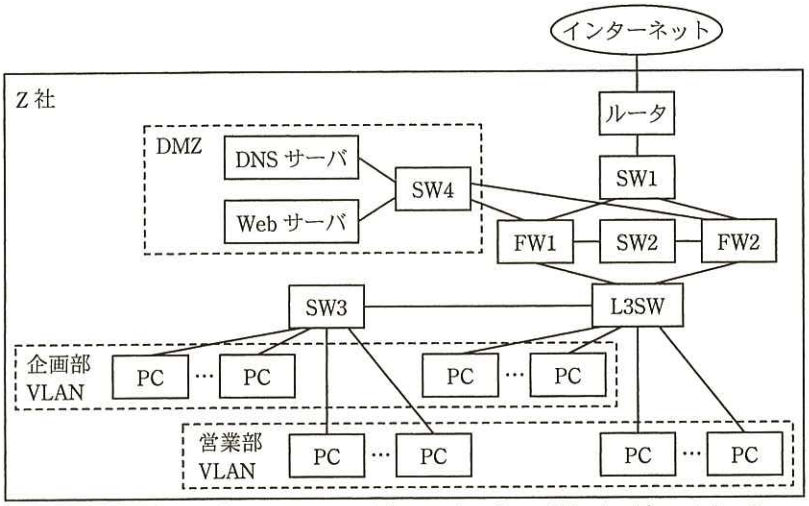
問2　ファイアウォールの障害対応に関する次の記述を読んで，設問1～3に答えよ。

Z社は，美容用品・健康用品を扱う企業である。Z社には企画部と営業部があり，各部のPCは部ごとのVLANに属している。ネットワークの管理は，企画部システム課のO主任とU君が行っている。Z社の現在のネットワーク構成を，図1に示す。



FW：ファイアウォール　L3SW：レイヤ3スイッチ　SW：レイヤ2スイッチ

図1　Z社の現在のネットワーク構成（抜粋）

〔FWの構成と交換作業〕

Z社では，FW1を主系に設定し，FW2を副系に設定したActive-Standby冗長構成を採用し，運用を行っている。通常時，FWは，必ず主系がActive動作になり，副系がStandby動作になる仕様である。

FWでは，［　ア　］と呼ばれる機能によって，ネットワークアドレス及びポート番号の変換を行っている。また，主系から副系にフェールオーバした後も通信を継続させるために，FWが通信の中継のために管理している情報（以下，管理情報という）を自動的に引き継ぐ［　イ　］フェールオーバ機能を動作させている。FWがフェールオーバした後に，多くのアプリケーションでデータの保全性が保たれて平常どおり通信できるのは，①トランスポート層のプロトコルの機能によるところが大きい。

FW1とFW2の間にはフェールオーバリンクと呼ばれる専用接続があり，設定情報の同期，管理情報の複製，及び対向FWの動作状態の識別に使用されている。フェー

ルオーバリンクには，ケーブル直結にする構成と SW を挟む構成があるが，Z 社では，②障害切分けのために SW2 を挟む構成を採用している。FW の冗長構成及びフェールオーバに関する動作は，次のとおりである。

・FW の冗長化機能は，仮想アドレスを使用する方式ではなく，主系の IP アドレス及び MAC アドレスを副系が引き継ぐ方式である。
・新たに Active 動作になった FW は，切り替わったことを通知するフレームを FW の各ポートから送信する。FW に接続しているスイッチは，このフレームを受信することで，③レイヤ 2 機能で用いるテーブルを適切に更新することができる。
・Active 動作の FW を副系から主系に切り戻すためには，手動操作が必要である。
・FW は，起動時にフェールオーバリンクによって，他の Active 動作中の FW を認識すると，主系又は副系であるかにかかわらず Standby 動作に入る。このとき，FW は自己の設定情報を無視して，Active 動作中の FW から設定情報を同期する。

Z 社では，数日前に FW1 が故障して，FW2 にフェールオーバした。U 君は，通信に影響を与えずに交換できると考え，代替機を入手次第，交換作業を行うことにした。

作業当日，U 君は，FW1 を工場出荷時の設定のままの代替機と交換し，配線後に電源を投入した。少したってから SW2 を見ると，FW1 接続ポートで，OSI 基本参照モデルの［　ウ　］層での正常接続を表すリンク LED が消灯していた。そこで，UTP のコネクタを強く押し込んだところ点灯した。その直後から，システム課に DMZ 及び社外へのアクセスができないとの苦情が相次いだ。慌てて，FW1 と FW2 を確認すると，両方とも Z 社用のフィルタリングルールを含む設定情報が失われていたので，直ちに FW1 の設定情報を復元し，FW2 に設定情報を同期させた。しかし，その後もアクセスできないとの苦情が続いた。U 君は，事故の原因を特定して通信を回復した後，今回の交換作業における事故では，次の二つが関係していることを確認した。

・FW1 は，電源投入後に FW2 を認識できず，Active 動作になった。
・フェールオーバリンク接続時に，FW1 が主系設定であったので，副系の FW2 は FW1 から設定情報の同期と管理情報の複製を行い，Standby 動作に切り替わった。

次は，今回の交換作業に関する O 主任と U 君の会話である。

O 主任：今回，FW1 の交換作業のミスは，U 君らしくなかったわ。

U君　：すみません。うかつでした。

O主任：FW1とFW2の設定復元後も，通信が回復しなかったのはなぜかしら。

U君　：FW1を代替機に交換した結果，FW1の各ポートのMACアドレスが変わったので，通信ができなかったのです。FWには，自ポートに設定されたIPアドレスの解決を要求する［　エ　］を用いて接続機器のARPテーブルを更新する機能がないので，手動操作が必要でした。このようなミスの再発防止のために，FW故障時の交換作業手順を整理しておきます。

O主任：お願いするわ。それから，FWの管理の都合上，フィルタリングルールを企画部と営業部で分けたいので，仮想FWを導入する案の検討をお願いできないかしら。

U君　：はい，分かりました。

U君は，FW故障時の交換作業手順を整理し，表1にまとめた。

表1　FW故障時の交換作業手順

故障機器	作業順序	作業内容
FW1	(1) 設定確認	代替機の主系設定が解除されていることを確認する。
	(2) 交換及び接続	代替機の電源を切断し，交換及び接続を行う。
	(3) 電源投入	Standby動作に入り，FW2から設定情報が同期されたことを確認する。
	(4) 主系への切戻し	FW1をActive動作に切り戻し，主系設定を行う。
	(5) ARPテーブル初期化	L3SW，［　a　］について初期化する。
	(6) 通信確認	DMZ及び社外との通信が可能であることを確認する。
FW2	(1) 設定確認	代替機の主系設定が解除されていることを確認する。
	(2) 交換及び接続	代替機の電源を切断し，交換及び接続を行う。
	(3) 電源投入	Standby動作に入り，［　b　］を確認する。
	(4) 通信確認	DMZ及び社外との通信が可能であることを確認する。

〔仮想FW導入案の検討〕

まず，U君は，仮想FWについて調査した。仮想FWとは，FW1及びFW2の中に論理的なFWの機能を複数定義できる機能である。フィルタリングルールは，仮想

FW ごとに独立して設定できる。仮想 FW には，FW の各ポート（フェールオーバリンク用ポートを除く）に相当する仮想ポートがあり，それぞれに IP アドレス及び VLAN 番号を割り当てる。仮想 FW との通信は，［　オ　］VLAN を使用して 1 本のリンクに複数の VLAN を収容する接続（以下，トランク接続という）を行い，VLAN 番号を合致させることで可能になる。

U 君は，企画部用の仮想 FW 及び営業部用の仮想 FW の両方を，それぞれ FW1 及び FW2 に定義する構成案を考えた。仮想 FW の導入に伴い，企画部と営業部の VLAN 間通信を廃止する。DNS サーバ及び Web サーバは現在のままとし，トランク接続を使用しない。新たに機器を購入せずに，④2 台のスイッチを相互に入れ替えて対処する。

さらに，仮想 FW について調査を進めると，Active-Active 冗長構成にした物理 FW（FW1 及び FW2）に，⑤Active 動作に設定した仮想 FW を適切に配置すると，物理 FW 間での負荷分散が可能であることが分かった。

U 君は，これらの調査結果を O 主任に報告し，仮想 FW の導入案は了承された。仮想 FW の導入作業は，翌月の法定点検による全館停電日に合わせて行うことになった。

設問 1　本文中の［　ア　］～［　オ　］に入れる適切な字句を答えよ。

設問 2　〔FW の構成と交換作業〕について，(1) ～ (5) に答えよ。

(1) 図 1 において，機器間がトランク接続でなければならない箇所はどこか。図 1 中の機器名を用いて答えよ。

(2) 本文中の下線①のプロトコルの機能を，10 字以内で答えよ。

(3) 本文中の下線②を採用する利点は何か。50 字以内で具体的に述べよ。

(4) 本文中の下線③のテーブル名を，15 字以内で答えよ。

(5) 表 1 中の［　a　］に入れる機器名を，図 1 中の機器名を用いて三つ答えよ。また，［　b　］に入れる確認内容を，20 字以内で答えよ。

設問 3　〔仮想 FW 導入案の検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線④の入れ替えを，図 1 中の機器名を用いて答えよ。ただし，各機器のポートには，余裕があるものとする。

(2) 本文中の下線⑤の配置を，50 字以内で具体的に述べよ。