問5　サブネットを活用したファイルの保護対策に関する次の記述を読んで，設問1～4に答えよ。

M社は，企業の研修用教材や雑誌などのコンテンツ制作を手掛ける，社員50名程度の企業である。顧客企業から依頼されたコンテンツ制作のために，対象とする企業分野ごとに三つの課を設けている。

社員はコンテンツの制作・編集業務（以下，業務という）のためにPCを利用し，業務で使用するファイルは全て各課のファイルサーバ（以下，FSという）に保管している。業務で使用するファイルはFS上で直接編集し，PCには残さない運用を行っている。PCからFSへのアクセスには，ファイル共有用のCIFS（Common Internet File System）プロトコル（TCPポート445を使用）を用いて，FS上で利用者IDとパスワードによる認証を行っている。

M社のネットワークは複数台のレイヤ2スイッチ（以下，L2SWという）を用いて構成され，PCにはDHCPで192.168.0.64～192.168.0.254の範囲のIPアドレスが付与される。M社のネットワーク構成を図1に示す。

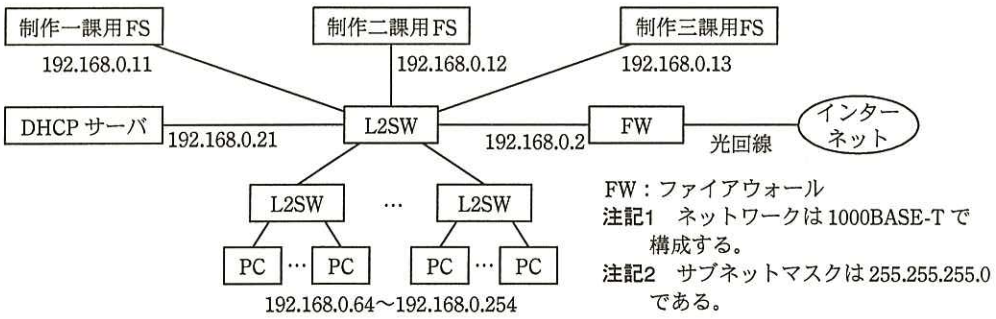


図1　M社のネットワーク構成

〔業務で使用するファイルの保護対策〕

M社では，情報セキュリティの重要性を考慮し，業務で使用するファイルのアクセス制御と，ファイル消失時における業務継続のために，次の保護対策を行うことにした。

・既存のL2SWを有効に活用しながら，新たにレイヤ3スイッチ（以下，L3SWという）を導入することによって，M社のネットワークを複数のサブネットに分割する。

各課の FS は 192.168.0.0/24，制作一課の PC は 192.168.1.0/24，制作二課の PC は 192.168.2.0/24，制作三課の PC は 192.168.3.0/24 のサブネットに配置する。各 PC には L3SW の DHCP サーバ機能によって，192.168.n.64～192.168.n.254 の IP アドレスを割り当てる。ここで，n には PC の配置に対応して，1～3 のいずれかの数値が入る。

・各課に配置された PC から FS へのアクセスについては，所属する課の FS だけにアクセスできるように制限する。

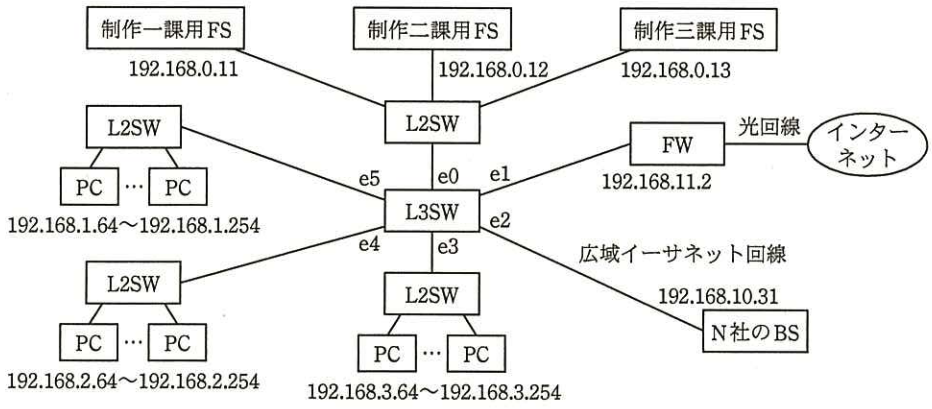
・PC から各課の FS へのアクセスは，従来どおり CIFS を使用し，FS 上で利用者 ID とパスワードによる認証を行う。

・各課の FS への通信は，FS の利用に必要な TCP ポートだけに限定し，その他の TCP/UDP ポートは遮断する。

・各課の FS 上のファイルは，広域イーサネット回線で接続された通信会社 N 社のバックアップサービス（以下，BS という）を利用して，全て遠隔地にバックアップされるようにする。

・各課の FS から N 社の BS へのファイル転送には，セキュアシェルの SCP（Secure Copy）コマンド（TCP ポート 22 を使用）を利用する。

ファイルの保護対策を行うために，M 社はネットワーク構成を変更した。変更後のネットワーク構成を図 2 に示す。



注記　e0～e5 は，L3SWのイーサネットインタフェースを示す。

図 2　変更後の M 社のネットワーク構成

〔L3SW のフィルタリングルールの設計〕

ネットワーク構成の変更とともに，L3SW のフィルタリングルールの設計を行った。

L3SW のフィルタリングルールの設計では，インタフェースに対して，双方向（IN/OUT）のルールを指定する。例えば，制作一課の PC を送信元，制作一課用 FS を宛先とするルールを設計する場合，インタフェース e5 と e0 に対して，L3SW に入る方向（IN）と出る方向（OUT）のルールを追加する必要がある。

設計した L3SW のフィルタリングルールを表 1 に示す。ここで，インタフェース e0 に関するルール及びインターネットアクセスに関するルールは，L3SW で適切に実装されているものとする。

表 1　L3SW のフィルタリングルール

インタフェース	方向	送信元 IP アドレス	宛先 IP アドレス	プロトコル	送信元ポート	宛先ポート	処理
e5	IN	192.168.1.0/24	192.168.0.11	TCP	ANY	445	許可
e5	OUT	192.168.0.11	192.168.1.0/24	TCP	445	ANY	許可
e4	IN	192.168.2.0/24	a	TCP	ANY	445	許可
e4	OUT	a	192.168.2.0/24	TCP	445	ANY	許可
e3	IN	192.168.3.0/24	192.168.0.13	TCP	ANY	445	許可
e3	OUT	192.168.0.13	192.168.3.0/24	TCP	445	ANY	許可
b	c	192.168.0.0/24	192.168.10.31	TCP	d	e	許可
b	f	192.168.10.31	192.168.0.0/24	TCP	e	d	許可
インタフェース e0 に関するルールは省略							
インターネットアクセスに関するルールは省略							
ANY	IN / OUT	ANY	ANY	TCP / UDP	ANY	ANY	遮断

注記 1　サブネットマスク長を指定しない IP アドレスはホスト IP アドレスを示す。
注記 2　ANY は対象が全てのインタフェース，IP アドレス，又はポートであることを示す。

〔保護対策の強化〕

〔業務で使用するファイルの保護対策〕で検討した内容についてレビューを行った。その結果，社内に不正な PC が持ち込まれて社内 LAN に接続された場合の備えが不足していると指摘された。

そこで，L3SW 及び L2SW に IEEE 802.1X 対応機種を選定し，PC にクライアント証明書を導入することによって，不正な PC の社内 LAN への接続を拒否することにした。

M社では，①図2のネットワーク構成に必要な構成要素を追加した。

〔N社のBSの利用〕

FSのファイルをバックアップするために，追加・変更があったファイルを当日の全作業終了後，翌日の作業開始前までに夜間バッチ処理でN社のBSに転送することにした。各課のFS上のログファイルなどの管理に必要なファイルは，毎日のバックアップとは別の時間帯に，週に1回バックアップする。また，ファイル削除による変更分は，削除から1週間以上経過したファイルを，週に1回バックアップから削除する。

各課のFSに格納されているファイルの総量と，ファイルの追加・変更によって毎日のバックアップが必要な最大量を表2に示す。

表2　各課のFSに格納されているファイルの総量と毎日のバックアップが必要な最大量

	格納されているファイルの総量	毎日のバックアップが必要な最大量
制作一課用FS	1,200Gバイト	10Gバイト
制作二課用FS	800Gバイト	5Gバイト
制作三課用FS	1,600Gバイト	15Gバイト

M社では，②夜間バッチ処理に利用可能な時間帯を考慮し，適切な帯域の広域イーサネット回線を用いてバックアップを行うことにした。

設問1　〔業務で使用するファイルの保護対策〕について，(1)，(2)に答えよ。

(1)　変更後のM社のネットワーク構成において，制作一課のPCにDHCPから割当て可能なIPアドレスの総数を答えよ。

(2)　実施するファイルの保護対策によって，対策実施前と比べて向上が期待される事項を解答群の中から選び，記号で答えよ。

解答群

ア　FSにアクセスする利用者を社員だけに限定できる。

イ　PCがマルウェアに感染してもFS上のファイルは保護される。

ウ　ファイルを社外に持ち出されても暗号化されているので復号できない。

エ　別の課のPCがFS上のファイルにアクセスすることを防ぐ。

設問2　〔L3SW のフィルタリングルールの設計〕について，表 1 中の［ a ］～［ f ］に入れる適切な字句を答えよ。

設問3　本文中の下線①について，図 2 に追加すべき構成要素名を 10 字以内で答えよ。

設問4　本文中の下線②について，夜間バッチ処理を 90 分以内に終了させたい場合，最低限必要な広域イーサネット回線の帯域を解答群の中から選び，記号で答えよ。ここで，通信に必要なパケットのヘッダなどのファイル転送プロトコルを含めた転送効率は 80％とする。1G バイトは 1,000M バイトとする。

解答群

ア　20M ビット／秒　　イ　40M ビット／秒

ウ　60M ビット／秒　　エ　80M ビット／秒