問３　LAN のセキュリティ対策に関する次の記述を読んで，設問 1～4 に答えよ。

E 社は，小売業を営む中堅企業である。E 社のネットワーク構成を，図 1 に示す。

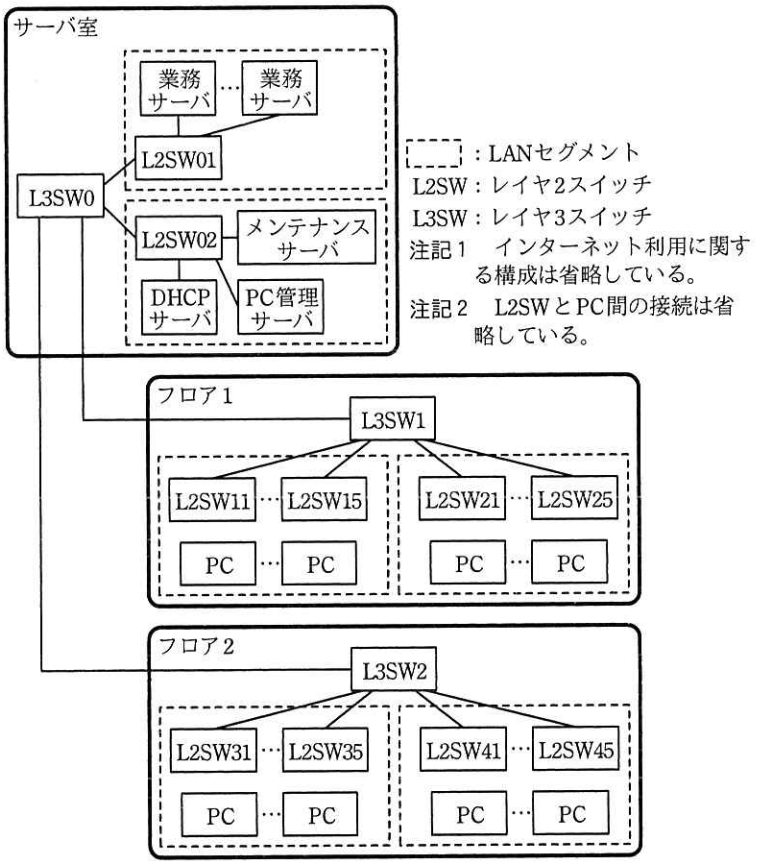

図 1　E 社のネットワーク構成（抜粋）

図 1 の概要，及び PC のセキュリティ対策について，次に示す。

・PC を接続する LAN は，各フロア二つ，計四つのセグメントに分かれている。

・ルーティング情報は，全てスタティックに定義してある。

・L3SW1，L3SW2 で設定されている VLAN は，全てポート VLAN である。

・<u>① PC の IP アドレスは，DHCP サーバによって割り当てられる</u>。

・PC はメンテナンスサーバを利用して，OS やアプリケーションプログラムのアップデート，ウイルス定義ファイルのアップデートなどを行う。

・PC には，E 社のセキュリティルールに従っているかどうかを検査するソフト（以

下，Sエージェントという）がインストールされている。

・Sエージェントは，検査結果をPC管理サーバに登録する。

E社では，情報システム部（以下，情シス部という）が，定期的にPC管理サーバを参照して，検査結果が不合格であるPCの利用者に，対処を指示している。しかし，対処をしないままPCを使用し続ける利用者が，少なからず存在する。また，無断で個人所有のPCをLANに接続することが，度々起きていた。そこでE社は，セキュリティルールに反したPCに対し，LANの利用を制限することにした。

〔LAN通信制限方法の検討〕

情シス部は，LAN通信制限の要件を次のとおり整理した。

・通信を許可するかしないかは，PC管理サーバ上の情報によって決定する。

・PC管理サーバ上の情報に応じて，PCを次の三つに区分する。

正常PC：Sエージェントの検査結果が合格のPC

不正PC：Sエージェントの検査結果が不合格のPC

未登録PC：PC管理サーバに登録がないPC（無断持込みのPCは，これに該当）

・正常PCは，通信を許可し，不正PCと未登録PC（以下，排除対象PCという）は，通信を許可しない。

情シス部は，LAN通信制限の実現策として，次の2案を検討した。

案1：DHCPサーバとL2SWによる通信制限

・正常PCだけにIPアドレスを付与するよう，DHCPサーバに機能追加する。

・②DHCPサーバからIPアドレスを取得したPCだけが通信可能となるように，各フロアのL2SWでDHCPスヌーピングを有効にする。

案2：専用機器による通信制限

・ARPスプーフィングの手法を使って，LAN上の通信を制限する機能をもつ機器（以下，通信制限装置という）を新たに導入し，排除対象PCによる通信を禁止する。

案 2 の通信制限装置は，セグメント内の ARP パケットを監視し，排除対象 PC が送信した ARP 要求を検出すると，排除対象 PC のパケット送信先が通信制限装置となるように偽装した ARP 応答を送信する。同時に，排除対象 PC 宛てパケットの送信先が通信制限装置となるように偽装した ARP 要求を送信する。これら各 ARP パケットのデータ部を，表 1 に示す。

表 1　各 ARP パケットのデータ部

フィールド名	排除対象 PC が送信した ARP 要求	通信制限装置が送信する ARP 応答	通信制限装置が送信する ARP 要求
送信元ハードウェアアドレス	排除対象 PC の MAC アドレス	a	c
送信元プロトコルアドレス	排除対象 PC の IP アドレス	b	d
送信先ハードウェアアドレス	00-00-00-00-00-00	排除対象 PC の MAC アドレス	00-00-00-00-00-00
送信先プロトコルアドレス	アドレス解決対象の IP アドレス	排除対象 PC の IP アドレス	アドレス解決対象の IP アドレス

なお，通信制限装置が送信する ARP 応答は 10 秒間隔で繰り返し送信され，あらかじめ設定された時間，又はオペレータによる所定の操作があるまで，継続する。

案 1，案 2 ともに，同等の LAN 通信制限ができるが，案 2 の通信制限装置には，PC 管理サーバとの連携を容易にする機能が存在する。そこで，情シス部は案 2 を採用することにした。

〔通信制限装置の導入〕

通信制限装置の LAN ポート数は 4 であり，各 LAN ポートの接続先は，全て異なるセグメントでなければならない。また，タグ VLAN に対応可能である。

通信制限装置の価格，セグメント数やタグ VLAN 対応に応じたライセンス料，フロア間配線の工事費用，既存機器の設定変更の工数などを勘案し，情シス部は，③タグ VLAN を使用せず，フロア間の配線も追加しない構成を選択した。また，④通信制限装置を接続するスイッチは，既設の L3SW とした。

〔運用の整備〕

新規に調達された PC は，PC 管理サーバに検査結果が登録されていないので，通信制限装置の排除対象になってしまう。そこで，新規の PC は，情シス部が PC 管理サーバに正常 PC として登録した後に，利用者に配布する運用にした。

また，不正 PC を正常 PC に復帰させる対処を行うために，不正 PC を接続するセグメント（以下，対処用セグメントという）を，フロア 1 とフロア 2 に追加することにした。⑤対処用セグメントから他セグメントの機器への通信は，L3SW1 及び L3SW2 のパケットフィルタリングによって必要最小限に制限する。

情シス部が作成した計画に基づいて，E 社は LAN のセキュリティ対策を導入し，運用を開始した。

設問 1　本文中の下線①について，DHCP サーバと PC のセグメントが異なっている場合に必要となる，スイッチの機能名を答えよ。また，その機能が有効になっているスイッチを，図 1 中の機器名で，全て答えよ。ただし，その機能が有効になっているスイッチは，台数が最少となるように選択すること。

設問 2　〔LAN 通信制限方法の検討〕について，(1)～(3) に答えよ。

(1) 案 1 において，本文中の下線②を実施しない場合に生じる問題を，35 字以内で述べよ。

(2) 図 1 中のフロア 1，フロア 2 の L2SW で，DHCP スヌーピングを有効にする際に，L3SW と接続するポートにだけ必要な設定を，25 字以内で述べよ。

(3) 表 1 中の［ a ］～［ d ］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　アドレス解決対象の IP アドレス

イ　アドレス解決対象の MAC アドレス

ウ　通信制限装置の IP アドレス

エ　通信制限装置の MAC アドレス

オ　排除対象 PC の IP アドレス

カ　排除対象 PC の MAC アドレス

設問３　〔通信制限装置の導入〕について，(1)，(2) に答えよ。

(1) 本文中の下線③の構成において，必要となる通信制限装置の最少台数を答えよ。ただし，サーバ室での不正 PC や未登録 PC の利用対策は，考慮しなくてよいものとする。

(2) 本文中の下線④について，導入する通信制限装置のうちの 1 台を対象として，その LAN ポート 1～4 の接続先を，図 1 中の機器名でそれぞれ答えよ。ただし，LAN ポート 1～4 は番号の小さい順に使用し，使用しないポートには“空き”と記入すること。

設問４　〔運用の整備〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑤について，対処用セグメントの PC の通信先として許可される他セグメントの機器を二つ挙げ，それぞれ図 1 中の機器名で答えよ。

(2) 対処用セグメントを追加する際に，L3SW1，L3SW2 以外に設定変更が必要な機器を二つ挙げ，それぞれ図 1 中の機器名で答えよ。また，それぞれの機器の変更内容を，30 字以内で述べよ。