

問9 検疫ネットワークに関する次の記述を読んで、設問1～3に答えよ。

W社は、食品の製造と販売を営む中堅の会社である。W社には営業部と製造部があり、それぞれの部の各社員にノートPC（以下、PCという）が1台ずつ配布されている。社員は、配布されたPCをW社社内ネットワーク（以下、社内ネットワークという）に接続して利用している。社内ネットワークでは、情報セキュリティ強化のための施策の一環として、IEEE 802.1x方式による認証VLANを用いた検疫ネットワークシステム（以下、検疫システムという）を導入している。

検疫システムは、セキュリティ対策の検査を行い、セキュリティ対策が不十分な端末を社内ネットワークに接続させず、隔離したり、必要なセキュリティ対策を施したりする機能をもつ。

社内ネットワークの構成は、図のとおりである。各種サーバ、レイヤ2スイッチ（L2SW）、レイヤ3スイッチ（L3SW）、ファイアウォール（FW）、ルータなどから構成される。設定されたVLAN一覧を表1に、サーバ一覧を表2に、ディレクトリサーバ上に格納されているユーザ情報（一部）を表3にそれぞれ示す。

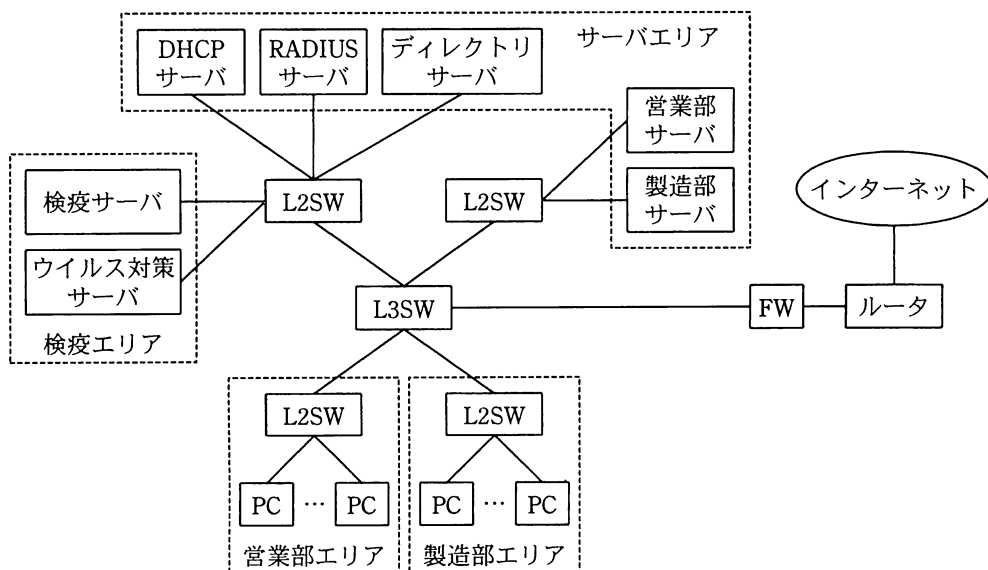


図 社内ネットワークの構成

表1 VLAN 一覧

VLAN ID	用途
VLAN 0	検疫用
VLAN 10	共通サーバ用
VLAN 20	営業部用
VLAN 30	製造部用
VLAN 40	インターネット接続用
VLAN 50	未使用（予備）

表2 サーバ一覧

サーバ名	所属 VLAN
検疫サーバ	VLAN 0
ウイルス対策サーバ	VLAN 0
DHCP サーバ	VLAN 10
RADIUS サーバ	VLAN 10
ディレクトリサーバ	VLAN 10
営業部サーバ	VLAN 20
製造部サーバ	VLAN 30

表3 ユーザ情報（一部）

ユーザ名	パスワード	所属 VLAN
AAA		VLAN 20
BBB		VLAN 20
CCC		VLAN 30
DDD		VLAN 30
EEE		VLAN 30

注 網掛けの部分は表示していない。

〔認証と検疫の処理の流れ〕

- (1) 所属 VLAN が設定されていない営業部エリアや製造部エリアの PC は、それぞれのエリア内の L2SW の空きポートに接続されると、L2SW や L3SW を介して、
a サーバと限定的に通信し、端末認証を受ける。
 PC から送られたユーザ名などの認証情報を a サーバが受信すると、
a サーバは、ユーザ情報を b サーバに問い合わせ、ユーザ認証を行う。
 ユーザ認証が c した PC は、引き続き、VLAN が設定されないままとなる。
- (2) ユーザ認証が d した PC の所属 VLAN を、検疫エリアに配置されたサーバと同じく e に設定して、その PC を隔離する。ここでは、所属 VLAN は、L2SW のポートごとに一つだけ設定される。
- (3) PC では、検疫サーバによって、セキュリティパッチが適用されているかどうか、ウイルスワクチンのパターンファイルが最新かどうか、スクリーンセーバなどの各種設定状況が適切かどうかを調べる検査が行われる。この検査が不合格となった PC

は、検査が合格となるまで、この に隔離され、検疫サーバによって、必要なセキュリティパッチの適用や各種設定の変更が強制的に行われる。さらにウイルス対策サーバによって、ウイルスチェックが行われる。

(4) 検査が合格となった PC は、 サーバに登録された所属 VLAN ID に従い、検疫システムによって、所属する VLAN が割り当てられる。

例えば、ユーザ名が CCC の場合、 サーバと同じ VLAN である が割り当てられる。

(5) 所属する VLAN を割り当てられた PC が、 サーバに IP アドレスを要求すると、 サーバは、VLAN ID に応じた IP アドレスを動的に割り当てる。

IP アドレスが割り当てられた PC は、社内ネットワークを利用することができる。

設問 1 本文中の ~ , , 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 DHCP | イ RADIUS | ウ インターネット |
| エ ウイルス対策 | オ 営業部 | カ 検疫 |
| キ 失敗 | ク 成功 | ケ 製造部 |
| コ ディレクトリ | サ ルータ | |

設問 2 本文中の , に入れる適切な VLAN ID を答えよ。

設問 3 〔認証と検疫の処理の流れ〕の(3)において、検査を隔離して行う理由を 25 字以内で述べよ。