問3　ネットワーク構成の見直しに関する次の記述を読んで，設問1～3に答えよ。

F 社は，中堅の輸入食品卸売会社であり，5 年前から営業支援システムを運用している。F 社における現在の営業支援システムのネットワーク構成を，図1に示す。

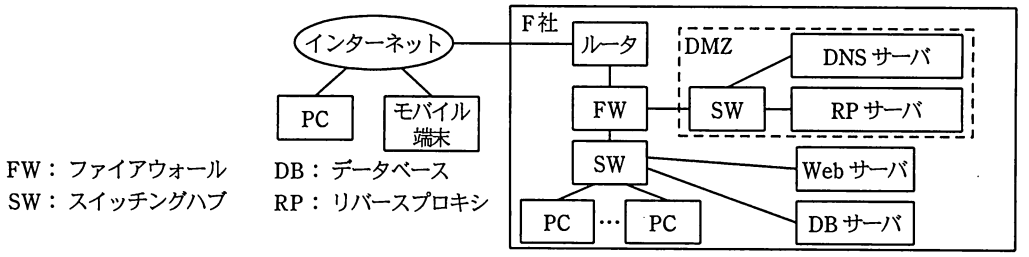

図1　現在の営業支援システムのネットワーク構成（抜粋）

F 社の営業部員は，社内では自席の PC を使い，社外ではモバイル端末を使って，営業支援システムにアクセスする。

営業支援システムが提供している主なサービスは，次のとおりである。

(1) 案件管理サービス

営業部員が Web 画面のメニューから，活動中の営業内容を DB に登録し，随時更新することで進捗状況を管理する，対話型のサービスである。自席の PC からは，社内のネットワークを通じて Web サーバにアクセスするが，モバイル端末からは SSL を実装した RP サーバを経由して，Web サーバにアクセスする。

(2) 商品検索サービス

Web 画面のメニューから，F 社で取り扱っている多種多様な商品を検索できる照会サービスである。営業部員だけでなく F 社の顧客を含めた一般の利用者も，インターネットに接続された PC などの端末を使って，RP サーバを経由してアクセスすることができる。

〔現在のネットワーク構成の問題点〕

最近になって，営業部員から情報システム部に対して，“外出先からアクセスしたとき，Web サーバのレスポンスが以前より悪くなった”とのクレームが寄せられた。そこで，FW のアクセスログを確認したところ，インターネットからのアクセスが 2～3 か月前から増大していることが判明した。営業部員数や業務量は以前と変わらず，一般の利用者からのアクセスが急増するような新商品の発売もなかったので，情報シス

テム部では，原因は不正なアクセスではないかと考え，ピーク時間帯における30分間のFWのアクセスログを分析し，表に示すあて先ポート別分析レポートをまとめた。

表　FWのアクセスログのあて先ポート別分析レポート（抜粋）

送信元IPアドレス	あて先IPアドレス	プロトコル	あて先ポート番号	受信件数	通過可否
（グローバル）	（RPサーバ）	TCP	1	151	否
（グローバル）	（RPサーバ）	TCP	2	150	否
（グローバル）	（RPサーバ）	TCP	3	152	否
⋮	⋮	⋮	⋮	⋮	⋮
（グローバル）	（RPサーバ）	TCP	80	8,976,340	可
（グローバル）	（RPサーバ）	TCP	81	150	否
⋮	⋮	⋮	⋮	⋮	⋮
（グローバル）	（RPサーバ）	TCP	443	638	可
⋮	⋮	⋮	⋮	⋮	⋮
（グローバル）	（RPサーバ）	TCP	65534	153	否
（グローバル）	（RPサーバ）	TCP	65535	152	否

注1　（グローバル）は，複数のグローバルIPアドレスの総称を指す。
注2　（RPサーバ）は，RPサーバのIPアドレスを指す。

分析レポートの内容を確認したところ，3か月前のレポートと比較して，正常なアクセスに加えて，インターネットの特定のグローバルIPアドレスからの不正と思われるアクセスが大量に記録されていた。このことによって，RPサーバの負荷が増大し，レスポンス悪化の原因となっていることが分かった。これを受け，情報システム部は，営業支援システムのセキュリティ向上のためのプロジェクトを立ち上げ，担当にはH君が任命された。

H君が営業支援システムのネットワーク構成を確認した結果，現在のFWには不正なアクセスに対する高度な検知機能がないことを確認した。また，FWは1台だけの構成となっており，故障が発生した場合の代替機がないことも確認した。そこでH君は，FWの機能に詳しいベンダE社のG氏に助言を求めた。

次は，FWの機能向上に関するH君とG氏の会話である。

H君：不要なポートをブロックするなど，パケットのTCPヘッダを参照して不正侵入を防ぐFWの機能を利用していましたが，今回のような攻撃は防御できていません。不正侵入を確実に防ぐには，どのような仕組みが必要でしょうか。

G氏：現在の構成では，FWで通過が許可されているパケットを使った不正侵入は防御できないので，より高度な機能をもった侵入検知システム（以下，IDSという）が必要です。IDSには，監視対象のネットワークに設置するネットワーク

型 IDS と，監視対象の Web サーバなどにインストールする［　ア　］型 IDS の 2 種類があります。また，侵入検知の仕組みとして，不正なパケットに関する一定のルールやパターンを使う［　イ　］型と，平常時のしきい値を超えるアクセスがあった場合に不正と見なすアノマリ型（異常検知型）の 2 種類があります。アノマリ型の場合，しきい値を高く設定したときだけでなく，①しきい値の設定が低すぎたときにも弊害が発生するので，注意が必要です。

H 君：なるほど。適切な設定が重要ですね。更に必要な対策はありますか。

G 氏：Web サーバへのアクセスを通じて不正な SQL が実行される［　ウ　］や，Web フォームに不正なスクリプトを埋め込んで送る［　エ　］など，TCP ヘッダのチェックやしきい値の設定では識別できないような Web サーバへの攻撃にも対応できる IDS の導入をお勧めします。もちろん，FW の冗長化についても考慮が必要です。

H 君：分かりました。では，ネットワーク構成の具体的な見直しについて，早速検討を開始します。

〔見直し後のネットワーク構成〕

G 氏の助言を受け，H 君は現在の FW を，IDS の機能をもった機種に置き換えることにした。また，FW の障害に備え，2 台による構成にした。

見直し後のネットワーク構成を図 2 に示す。

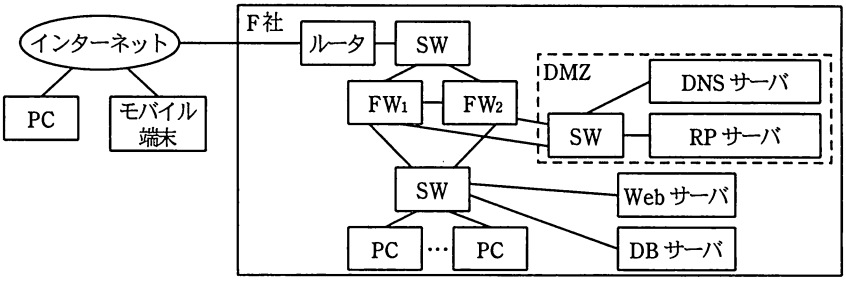

図 2　見直し後のネットワーク構成（抜粋）

新たに導入した FW は，通過パケットの TCP ヘッダの［　オ　］をセッションログとして保管しておき，パケットの到着順序に矛盾がないか確認する，ステートフルパケットインスペクションの機能をもっている。ステートフルパケットインスペクションでは，LAN 側から送信したパケットと WAN 側から到着したパケットが矛盾した

場合，パケットを遮断し，不正アクセスを防止する。さらに，このFWは，1台のFWが故障したときでも処理を中断させることなく，もう1台のFWで処理を継続させる，ステートフルフェールオーバの機能も備えている。

ステートフルフェールオーバを利用するため，2台のFWをネットワークに接続し，更にFW同士をケーブルで接続した。通常はFW_1だけが機能しているが，管理情報をFW_1からFW_2に一定間隔で複製し，FW_1に障害が発生した場合には，それまで稼働していないFW_2が自動的に処理を引き継ぐ設定とした。この設定によって，②営業部員は，FWが切り替わったことを意識せずに営業支援システムを継続利用できるようになった。ただし，FW_2からFW_1に管理情報を自動的に複製していないので，FWを切り戻すときは，手動の作業を必要とする設定にした。したがって，この切り戻し時，営業部員は営業支援システムを継続利用できないことになる。

F社では，H君の案に基づいてネットワーク構成を変更した後，テストのためにFW_1をシャットダウンしたところ，設定どおりFW_2への切替えが自動的に行われ，営業支援システムは継続利用できることを確認した。その後，FWの切り戻しを行って，元の状態に復旧させた。復旧後も営業支援システムは順調に稼働し，ネットワーク構成の見直しは完了した。

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　〔現在のネットワーク構成の問題点〕について，(1)～(3)に答えよ。

(1) FWで防御できない不正と思われるアクセスとは何か。表を参考にして，20字以内で述べよ。

(2) G氏が指摘した，TCPヘッダのチェックやしきい値の設定では識別できないようなWebサーバへの攻撃に対応するために，侵入検知の際に着目すべきパケットの部分を，15字以内で述べよ。

(3) 本文中の下線①について，発生する弊害を，40字以内で具体的に述べよ。

設問3　〔見直し後のネットワーク構成〕について，(1)～(3)に答えよ。

(1) FWの切替えが発生した場合に，FW_1からFW_2に引き継がれる情報を，OSI基本参照モデルの第3層以下から二つ挙げ，それぞれ10字以内で答えよ。

(2) 本文中の下線②の実現に必要な管理情報を，45字以内で具体的に述べよ。

(3) 実際にFWの故障による切替えが発生したとき，修理完了後にFW_2からFW_1に手動で切り戻す際に必要な運用上の留意点を，40字以内で述べよ。