問３　侵入検知・防御システムの導入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，自社で営業支援システムを運用している。

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。

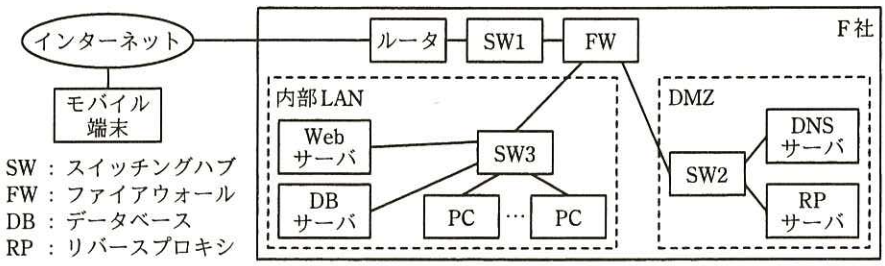

図 1　現在の営業支援システムのネットワーク構成（抜粋）

F 社の営業部員は，社内で営業支援システムにアクセスする場合には，自席の PC を使い，社外からは，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。営業支援システムで主なサービスを提供している Web サーバを社外から利用するには，SSL/TLS を実装した RP サーバを経由してアクセスする。社内の PC からインターネットへのアクセスは，RP サーバを経由しない。

F 社では数年前にネットワーク構成を見直し，侵入検知システム（IDS）の機能をもった FW を導入した。最近になって営業部員から，インターネットを通じたサービスのレスポンスがしばしば悪化していると，苦情が寄せられるようになった。F 社の情報システム部が調査した結果，現在の FW は IDS としての性能の限界に近づいており，これがレスポンス悪化の原因となっていると考えられた。IDS 機能を使わなければ FW は負荷が軽減され，今後も継続して利用できることが分かった。

また，最近発見された一部のサーバのミドルウェアの脆弱性を悪用する攻撃は，FW の IDS 機能では検出できないものであった。このときは，アプリケーションへの影響確認テストに時間が掛かり，当該サーバにセキュリティパッチを適用するまで，営業支援システムを数日間休止せざるを得なかった。

F 社の情報システム部は，インターネットを通じた様々なサイバー攻撃の増大が頻繁に報道されていることも考慮し，営業支援システムのセキュリティレベルを向

上させるために，プロジェクトを立ち上げた。プロジェクトのリーダには H 君が任命された。まず H 君は，IDS の見直しを開始した。

〔IDS の見直し〕

侵入検知の仕組みとしては，次の 2 種類がある。

一方はシグネチャ型と呼ばれ，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。原則として未知の攻撃には対応できないが，あらかじめ様々な種類のシグネチャが登録されている。

他方の［　ア　］型は，定義されたプロトコルの仕様などから逸脱したアクセスがあった場合に不正とみなす。シグネチャ型と比べて，未知の攻撃に対しては柔軟に対応できるが，正常と判断する基準によっては，正常なパケットを異常とみなすこともある。H 君は，それぞれの仕組みの特長を生かすために，両方の機能をもった IDS を採用することにした。

次に，H 君は，IDS のネットワークへの接続について検討した。

IDS は，監視対象のネットワークにある SW の［　イ　］ポートに接続し，IDS 側のネットワークポートを［　ウ　］モードにすることで，IDS 以外を宛先とする通信も取り込むことができる。また，IDS 側のネットワークポートに［　エ　］アドレスを割り当てなければ，IDS 自体が OSI 基本参照モデルの第 3 層レベルの攻撃を受けることを回避できる。

検出可能な通信は，IDS の接続箇所によって異なる。例えば，インターネットと DMZ 間の通信は，IDS を SW1 又は SW2 に接続した場合は検出可能だが，SW3 に接続した場合は検出できない。図 1 中の SW1～SW3 にそれぞれ IDS を接続した場合に，IDS で検出可能な通信を表 1 に示す。

表 1　IDS で検出可能な通信（接続箇所別）

通信の範囲	IDS の接続箇所		
	SW1	SW2	SW3
インターネット ⇔ DMZ	○	○	×
DMZ ⇔ DMZ	×	○	×
DMZ ⇔ 内部 LAN	×	○	○
内部 LAN ⇔ 内部 LAN	×	×	○
（設問のため，省略）			

○：検出可　　×：検出不可

H 君が調査した IDS には，検知した攻撃を遮断する機能を実装している機種があった。遮断機能のうちの一つは，①IDS と FW が連携することで，検知した送信元アドレスからの不正な接続を遮断するというものであった。

また，IDS が不正な TCP コネクションを検知した場合に，該当する通信を強制的に切断する目的で，送信元と宛先の双方の IP アドレス宛てに，TCP の RST フラグをオンにしたパケットを送る機能があった。検知した不正パケットが UDP の場合には，該当するパケットの送信元に，ICMP ヘッダのコードに port［　オ　］を設定したパケットを送って，更なる攻撃の抑止を試みることができる。しかし，H 君は，②この ICMP を使った攻撃抑止のためのパケットが，実際は攻撃者に届かないことがあること，又はこのパケット自体が他のサイトへの攻撃となることもあると考えた。

これまでの検討結果から，H 君は，より高度な侵入防御の仕組みが必要であると考え，ネットワークの重要な部分へは侵入防止システム（IPS）を追加することを検討した。

〔IPS の追加〕

IPS は，不正アクセスを監視するだけでなく，遮断する機能を強化したネットワーク機器である。例えば，SQL インジェクションのような，Web アプリケーションの脆弱性に対応する機能をもつもの，及び③防御対象のサーバに新たな脆弱性が発見された場合の一時的な運用に対応できるものがある。しかし，IPS は正常な通信を誤って不正と検知してしまうこと（フォールスポジティブ），又は不正な通信を見逃してしまうこと（フォールスネガティブ）があり，双方のバランスをとって効果的な侵入防御を実現することが重要である。

また，高度な機能をもつ IPS には高い負荷が掛かることが予想される。ネットワークの通信量が急激に増えた場合でも，営業支援システムのレスポンス悪化を避け，継続して利用できる状態にすることが重要であることから，H 君は IPS の障害対策について検討した。

IPS の障害対策には，並列に複数台導入する冗長化が考えられる。しかし，導入候補の IPS には，④IPS の機能の一部が故障した場合に備えた機能があった。費用対効果の観点と，IDS が併設されていることや，営業支援システムの継続利用を優

先することから，H 君は IPS を冗長化しないことにした。

以上の検討の結果，H 君は営業支援システムのネットワークに，IDS と IPS の両方を追加し，管理用 PC を接続した管理用 LAN を設けることを考えた。

H 君による，見直し後の営業支援システムのネットワーク構成案を，図 2 に示す。

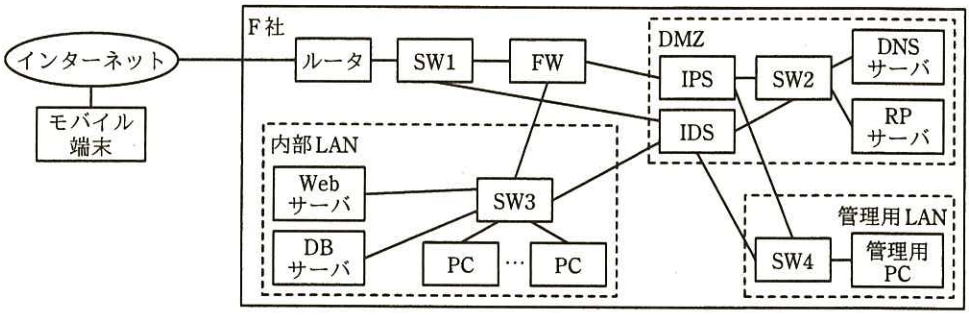

図 2　見直し後の営業支援システムのネットワーク構成案（抜粋）

H 君が考えたネットワーク構成案は承認され，営業支援システムの見直しプロジェクトが開始された。

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　〔IDS の見直し〕について，(1) ～ (3) に答えよ。

(1) IDS で検出可能な通信の範囲を追加して，表 1 を完成させよ。

(2) 本文中の下線 ① で，IDS と FW が連携することで不正な接続を遮断する仕組みとは，どのようなものか。40 字以内で具体的に述べよ。

(3) H 君が，本文中の下線 ② のように考えたのはなぜか。35 字以内で述べよ。

設問 3　〔IPS の追加〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線③で可能としている，一時的な運用を 50 字以内で述べよ。

(2) 本文中の下線 ④ の，IPS が実装している機能とは何か。25 字以内で述べよ。

(3) IDS と IPS の導入後に，セキュリティレベルの継続的な向上のために，管理用 PC を使ってどのようなことを行うか。35 字以内で具体的に述べよ。