問5　リモートアクセスに関する次の記述を読んで，設問1～3に答えよ。

T社は，東京に本社があり，都内に3か所の営業所をもつ，食料品販売会社である。本社と各営業所のLANは，インターネットVPNによって相互に接続され，T社のネットワークを構成している。インターネットVPNには，ファイアウォール（以下，FWという）に組み込まれているIPsec機能を使用している。

インターネットVPNの導入前から，営業員は，T社から1人に1台支給される携帯用PCから，公衆網を利用してT社ネットワークにリモートアクセスをしている。営業員は，リモートアクセスによって，メールサーバ，Webサーバ，データベースサーバ（以下，DBサーバという）へのアクセスなど，社内と同様の作業を行える。リモートアクセスには，本社に設置されたリモートアクセスサービスサーバ（以下，RASサーバという）にPHSで接続する方式を使用している。

図1に，T社ネットワークの構成を示す。社内LANでは，DHCPサーバが割り当てるローカルIPアドレスを使用している。

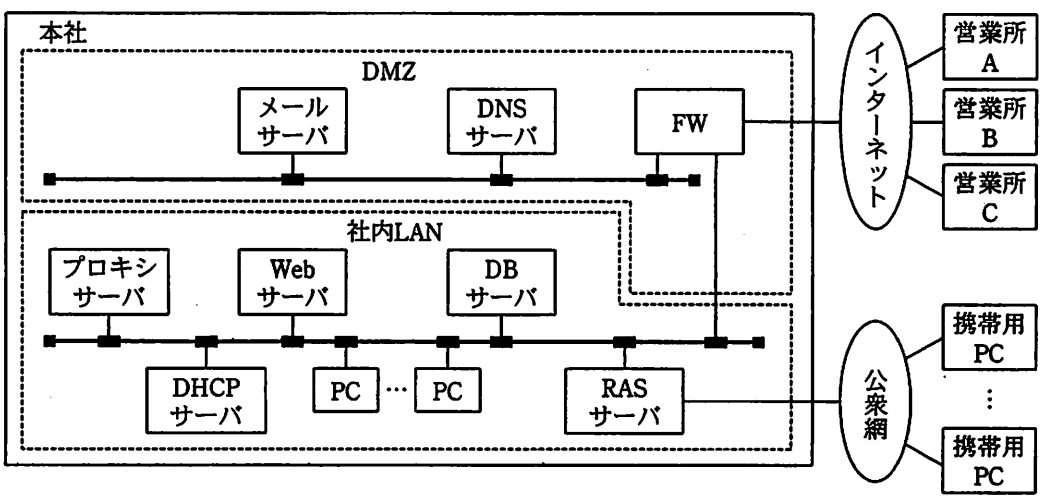

図1　T社ネットワークの構成

T社の事業拡張に伴い，携帯用PCのリモートアクセスに，次の問題が発生した。

・営業員の増加によってRASサーバへのアクセスが増し，回線がつながりにくくなり，業務に支障が出ている。

・営業地域が全国に拡大し，通信費が増大している。

問題解決のために，インターネット経由で携帯用 PC を接続する方法として，次の三つの案を検討した。

〔案 1〕

社内の RAS サーバの代わりに，通信事業者が提供する RAS サーバに，携帯用 PC からリモートアクセスする（図 2）。営業員は，最寄りの通信事業者の RAS サーバに，PHS で接続する。RAS サーバへの接続時のユーザ認証は，［ a ］や［ b ］などを利用して通信事業者が行う。

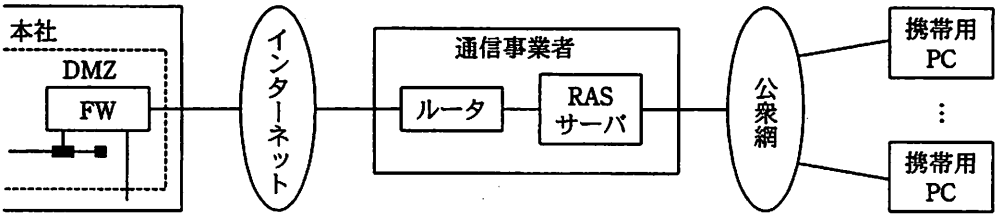

図 2　案 1 の構成

〔案 2〕

既存の FW による IPsec 機能とは別に，SSL-VPN 装置を導入し，SSL によって VPN を構成する（図 3）。携帯用 PC をインターネットに接続できる環境があれば，Web ブラウザを起動して，社内のアプリケーションを利用できる。

SSL-VPN 装置は，［ c ］が発行したサーバ証明書を携帯用 PC に送信して，自らをサーバ認証してもらう。逆に，クライアント証明書を受信して，クライアント認証を行うこともできる。

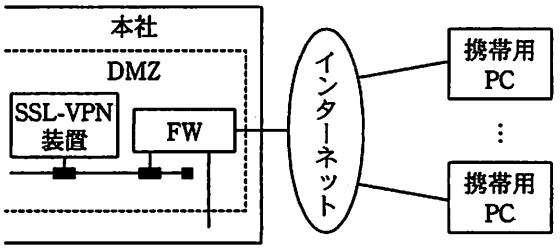

図 3　案 2 の構成

〔案3〕

既存のインターネットVPNを使用する（図4）。携帯用PCをインターネットに接続できる環境があれば，あらかじめインストールしておいたIPsecクライアント用ソフトウェアを使用して，社内のアプリケーションを利用できる。

セキュリティプロトコルには，データの暗号化機能を提供する［ d ］を使用する。通信モードには，IPヘッダとデータ部をまとめて暗号化するトンネルモードを使用する。

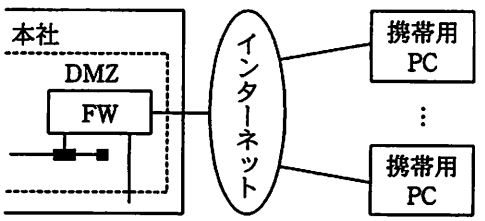

図4　案3の構成

〔案3の課題〕

案1～3の特徴を考慮して，案3を導入する方向で検討を進めた。営業員の利用環境を調査したところ，NAPTを利用している環境があったが，NAPTの利用に関連して発生することのある問題には対処できていることが確認できた。しかし，リモートアクセスを不可能にする別の課題があることが分かった。例えば，携帯用PCが，出張先のホテルにある［ e ］から，動的に［ f ］を取得する場合，T社ネットワーク内で［ f ］が重複してしまい，リモートアクセスができなくなるおそれがある。

この課題について更に調査し，恒久的な対策があることが分かった。

設問1　本文中の［ 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　AH	イ　CA	ウ　CHAP
エ　ESP	オ　ICMP	カ　IEEE
キ　ISO	ク　RADIUS	ケ　RFC

設問2　案1～3に関する記述として適切なものを解答群の中からそれぞれ一つ選び，記号で答えよ。

解答群

ア　HTTP以外のアプリケーションの通信プロトコルに対応できない。

イ　インターネット通信の暗号化を追加検討する必要がある。

ウ　クライアント認証の有無は，サーバ側で設定できる。

エ　事前共有鍵として，FWと携帯用PCに認証鍵を設定する。

オ　パケット転送に，ラベルスイッチング方式を用いている。

設問3　〔案3の課題〕について，(1)，(2)に答えよ。

(1)　本文中の［　e　］，［　f　］に入れる適切な字句を本文中から選んで答えよ。

(2)　本文中の下線部の恒久的な対策として適切なものを解答群の中から選び，記号で答えよ。

解答群

ア　本社DHCPサーバからIPsec専用のIPアドレスを携帯用PCに割り当てる。

イ　本社FWの通信ポート443番の通信を許可する。

ウ　本社と営業所の通信ポート番号の体系を変更する。

エ　本社と営業所のローカルIPアドレスの体系を変更する。

オ　本社プロキシサーバのNAPT機能を解除する。