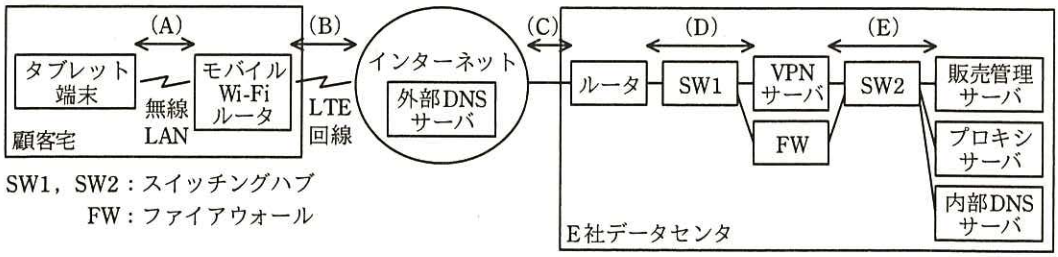
問２　モバイルネットワークの検討に関する次の記述を読んで，設問１～４に答えよ。

E 社は，中堅の運送業者である。E 社では，営業活動の効率向上を目的として，販売管理システム（以下，システムという）を導入することにした。システムでは，顧客宅を訪問した営業員が，支給されたタブレット端末とモバイル Wi-Fi ルータを用いて，サービス紹介などのプレゼンテーション，見積書の作成，及び車両・作業員の手配を行えるようにする。

〔モバイルネットワークの検討〕

システムの導入に当たり，社内プロジェクトチームが発足し，O 君がモバイルネットワークについて検討することになった。O 君が考えたモバイルネットワーク構成案を，図１に示す。



注記　(A)～(E) は，ネットワークセグメントを表す。

図１　モバイルネットワーク構成案

モバイルネットワーク構成案の概要は，次のとおりである。

・タブレット端末とモバイル Wi-Fi ルータの接続は，無線 LAN を用いる。
・モバイル Wi-Fi ルータとインターネットの接続は，通信事業者の LTE 回線を用いる。
・VPN サーバ及び FW とインターネットの接続は，SW1，ルータを介して行う。
・タブレット端末は，VPN サーバと VPN 接続を行い，VPN 接続後の名前解決は，内部 DNS サーバを用いて行う。
・タブレット端末から販売管理サーバ及びインターネット上のサーバへの通信は，VPN 接続を通して，プロキシサーバ経由で行う。

・タブレット端末から販売管理サーバへの通信には，HTTPS を用いる。
・プロキシサーバ及び内部 DNS サーバからインターネットへの通信は，FW を介して行う。
・販売管理サーバ，プロキシサーバ及び内部 DNS サーバには，プライベート IP アドレスを割り当てる。

〔無線 LAN 接続の検討〕

導入が検討されているモバイル Wi-Fi ルータでは，アクセスポイント保護のために次のセキュリティ対策機能が搭載されている。

・SSID の値を変更する機能
・SSID を隠ぺいする①ステルス機能
・MAC アドレスフィルタリング機能

②ステルス機能と MAC アドレスフィルタリング機能を用いたセキュリティ対策だけでは不十分なので，無線 LAN 通信の暗号化を行う。導入が検討されているタブレット端末及びモバイル Wi-Fi ルータは，WEP，WPA 及び WPA2 に対応しており，このうちの WPA2 を採用する。WPA2 は，無線LAN の暗号化アルゴリズムとして［　ア　］が初めて採用された方式である。認証方式には，あらかじめタブレット端末とモバイル Wi-Fi ルータに同じパスフレーズを設定する［　イ　］認証を用いる。このパスフレーズは一定以上の長さで十分に複雑な文字列とし，SSID と同様に，モバイル Wi-Fi ルータごとに異なる値を設定する。

タブレット端末が無線 LAN に接続すると，モバイル Wi-Fi ルータは，DHCP によってプライベート IP アドレスの配布を行う。③このプライベート IP アドレスは他のネットワークと重複しないように設計する。

〔LTE 回線を用いたインターネット接続の検討〕

モバイル Wi-Fi ルータには，通信事業者が契約者を識別する情報が記録されている［　ウ　］が挿入されている。モバイル Wi-Fi ルータには，利用者 ID やパスワードといった認証情報に加えて，LTE 回線からインターネットのようなネットワークへのゲートウェイの指定を意味する，［　エ　］の情報を設定する。

モバイル Wi-Fi ルータは，電源投入時に自動的にインターネット接続を開始し，グ

ローバル IP アドレスが割り当てられる。タブレット端末がインターネット上のサーバと通信を行う際に，モバイル Wi-Fi ルータでは［　オ　］による IP アドレスとポート番号の変換処理が行われる。

タブレット端末が，インターネットに接続できるようになると，営業員が業務に必要のない Web 閲覧を行うなど，不適切な利用が行われる可能性がある。その対策として，通信可能な接続先 IP アドレスを制限する LTE 回線のオプションサービスを利用し，モバイル Wi-Fi ルータからの通信が可能な範囲を，VPN サーバとその名前解決に用いる外部 DNS サーバに限定する。

〔VPN 接続の検討〕

導入が検討されているタブレット端末には，L2TP over IPsec を用いた VPN 接続機能が搭載されており，これを利用する。E 社データセンタの VPN サーバには，グローバル IP アドレスを割り当てる。

VPN サーバへの不正アクセスを防止するためのセキュリティ対策を行う。例えば，利用者 ID，固定パスワードを用いて利用者認証を行う場合，これらが漏えいすると，直ちにインターネットから不正アクセスが可能となり，危険である。その対策として，ハードウェアトークンを利用する。ハードウェアトークンでは，一定時間ごとに変化する数字が表示されるので，これをワンタイムパスワードとして利用する。

タブレット端末が VPN 接続を行うと，VPN サーバは，タブレット端末に対して図 1 中のネットワークセグメント（E）からプライベート IP アドレスを割り当てる。

訪問した顧客宅での利用が前提となるタブレット端末，モバイル Wi-Fi ルータ及びハードウェアトークンは，紛失する可能性がある。④営業員が，これらを紛失した際には，直ちにモバイルネットワーク管理者に報告するという運用ルールを策定する。不正アクセスが行われた際の影響を最小限にとどめるために，⑤ VPN 接続で許可する通信を必要最小限に設定する。

〔プロキシサーバの検討〕

プロキシサーバは，タブレット端末の通信ログを取得する目的で利用し，⑥プロキシサーバのログから各営業員を特定できるようにする。プロキシサーバは，HTTP プロキシと HTTPS プロキシの各機能をもつ。HTTP プロキシの場合，プロキシサー

バは，タブレット端末からのリクエストを受け付け，その内容を基に新たに HTTP サーバへリクエストを開始する。一方，HTTPS プロキシの場合，プロキシサーバは，タブレット端末からの［　カ　］要求によって HTTPS サーバへの TLS トンネルを中継し，その後のリクエストは，TLS トンネルの中をそのまま転送する。⑦HTTPS の場合は，HTTP と比較して取得できるログの内容が限られるが，システム運用上問題はない。

O 君は，以上の検討結果をまとめて，プロジェクトに提案した。その結果，O 君が考えたネットワーク構成案は，プロジェクトで採用され，システムが構築されることになった。

設問 1　本文中の［　ア　］～［　カ　］に入れる適切な字句を答えよ。

設問 2　〔無線 LAN 接続の検討〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線①について，ステルス機能の動作を 25 字以内で述べよ。

(2) 本文中の下線②について，SSID や MAC アドレスは容易に取得される危険性がある。その理由を，電波を用いて通信を行う無線 LAN の特性に着目して，30 字以内で述べよ。

(3) 本文中の下線③について，重複してはいけないセグメントを，図 1 中の (A) ～(E) から選べ。

設問 3　〔VPN 接続の検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線④について，報告を受けたモバイルネットワーク管理者が取るべき行動を，紛失した VPN 接続の利用者 ID に着目して，20 字以内で述べよ。

(2) 本文中の下線⑤で，許可するとしている通信を，図 1 中の字句を用いて 25 字以内で答えよ。

設問 4　〔プロキシサーバの検討〕について，(1)，(2) に答えよ。

(1) 本文中の下線⑥について，プロキシサーバに必要な機能名を 10 字以内で答えよ。また，営業員を特定するために必要な設定内容を 20 字以内で述べよ。

(2) 本文中の下線⑦について，HTTPS の Request-URI から取得できるログの内容を二つ挙げ，それぞれ 10 字以内で答えよ。