次の問1は必須問題です。必ず解答してください。

問1　営業支援サーバへのSSLの導入に関する次の記述を読んで，設問1～4に答えよ。

P社は，コンピュータ関連製品の販売会社である。P社では，営業支援システムと販売管理システムを運用している。営業支援システムでは，製品資料，顧客情報，プレゼンテーション資料などが参照できる。営業支援システムは，販売管理システムと連携しており，在庫数の確認や在庫の引当てもできる。各システムは，それぞれのサーバで稼働している。

P社では，全社員がノートPC（以下，PCという）を業務で使用している。営業員は，社内で営業支援サーバから各種資料をPCにダウンロードした後，PCを顧客先に持参して製品説明やプレゼンテーションなどを行っている。営業支援サーバへは，PCのブラウザを利用してアクセスしている。

P社のシステム構成を図1に示す。

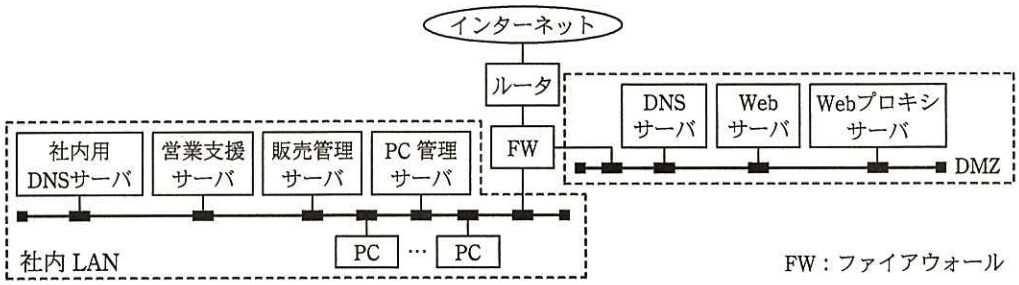


図1　P社のシステム構成（抜粋）

P社では，情報システム部が許可したアプリケーションプログラムだけを，PCにインストールさせている。PCは，社内LANに接続されたときにPC管理サーバにアクセスして，ウイルス対策ソフトの最新のパターンファイル，及びOSとアプリケーションプログラムのセキュリティパッチを適用する。

最近，営業員から，最新の在庫数の確認や在庫の引当てを社外からも行えるようにしてほしいとの要望が強くなった。そこで，情報システム部のQ課長は，営業支援システムをインターネット経由で利用できるようにするために，SSLの導入についての検討を，サーバ運用担当のR君に指示した。指示を受けたR君は，まず，SSLについて調査した。

〔SSL の機能概要〕

インターネットはオープンなネットワークなので，多くの脅威が存在する。これらの脅威に対応するために SSL が利用される。SSL では，［ a ］，なりすまし及び［ b ］に対する対応策が提供される。

［ a ］防止は，公開鍵暗号方式と共通鍵暗号方式を組み合わせて実現される。なりすまし防止は，サーバ認証とクライアント認証によって行われる。送受信されるメッセージの［ b ］検知は，メッセージの中に埋め込まれる，MAC（Message Authentication Code）を基に行われる。

R 君は，社外から営業支援サーバへのアクセスを SSL で行えば，営業支援システムの安全な利用が可能になると考え，営業支援サーバへの SSL の導入方法の検討を行うことにした。

〔クライアント認証の検討〕

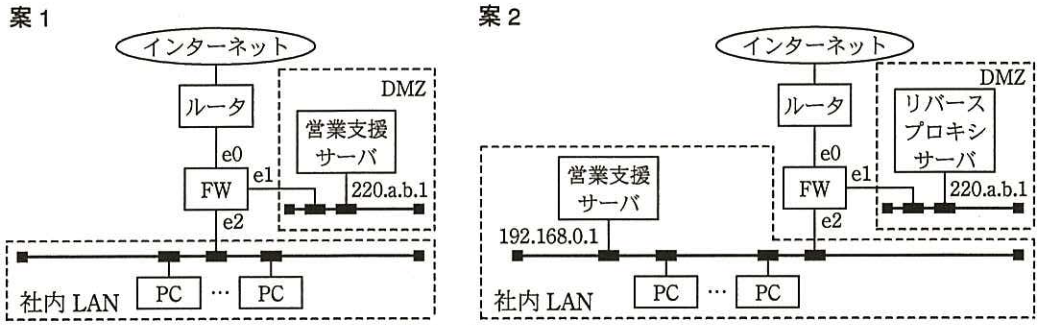
営業支援サーバには，信頼できる認証機関によって発行されたサーバ証明書を導入して，営業支援サーバの正当性を証明する。

営業支援サーバに SSL を導入しても，社外から営業支援サーバへのアクセスが不特定の PC によって行われると，新たなセキュリティリスクが発生してしまう。そこで，R 君は，社外から営業支援サーバにアクセスするときに，利用者 ID とパスワードによる認証に加えて，SSL がもつ，クライアント証明書を用いたクライアント認証機能も利用することを考えた。クライアント認証には，クライアント証明書をインストールした IC カードや USB トークンを利用することができるが，今回はこれらを利用せず，①クライアント証明書を PC 自体にインストールする方式を採用することにした。

〔営業支援サーバを社外に公開する構成〕

次に，R 君は，営業支援サーバを社外に公開する構成について検討した。

R 君が考えた営業支援サーバを社外に公開するための二つの構成案を図 2 に示す。案 1 は，営業支援サーバに SSL を導入して，DMZ に移設するものであり，案 2 は，SSL を導入したリバースプロキシサーバを，新規に DMZ に設置するものである。



注記1　図中に示されたサーバは，営業支援サーバの社外への公開に関連するものだけである。
注記2　e0，e1，e2 は，FWのイーサネットインタフェースを示す。
注記3　220.a.b.1 はグローバルIPアドレスを示す。

図2　営業支援サーバを社外に公開するための二つの構成案

二つの案について検討した結果，案 1 と案 2 には，それぞれ，次の対応が必要になることが分かった。

案 1 では，新たな機器の導入は不要だが，三つの作業が必要になる。一つ目は，営業支援サーバに SSL を導入する作業，二つ目は，営業支援サーバを DMZ に移設する作業，三つ目は，②営業支援サーバにアクセスする全ての PC に対する作業である。

案 2 では，二つの作業が必要になる。一つ目は，社外から営業支援サーバにアクセスする全ての PC に対する，案 1 と同様の作業であり，二つ目は，SSL を導入したリバースプロキシサーバを新規に構築して DMZ に設置する作業である。

また，案 1，案 2 ともに，インターネットからの DoS 攻撃によって，サービスの提供が不能になるリスクがあるが，③案 1 と比較すると案 2 の被害は限定的である。

R 君は，これらの検討結果を基に，案 2 を採用することにした。

案 2 を採用すると，FW で新たに通過を許可しなければならない通信が発生する。P 社が導入している FW は，ステートフルインスペクション機能をもつので，FW が最初に受信して通過させるパケットの内容の設定だけで済む。案 2 を採用する場合に，FW に追加が必要なフィルタリングルールを表 1 に示す。

表1　案2を採用する場合に，FWに追加が必要なフィルタリングルール

項番	方向	送信元 IP アドレス	宛先 IP アドレス	宛先ポート番号	処理
1	e0→e1	任意	220.a.b.1	443/TCP	許可
2	e1→e2	220.a.b.1	192.168.0.1	80/TCP	許可

R 君は，以上の検討結果を Q 課長に報告したところ，クライアント証明書の発行と運用についての追加検討を指示された。

〔クライアント証明書の発行と運用〕

クライアント証明書は，P 社内だけで使用するものなので，リバースプロキシサーバのディジタル証明書発行機能を利用して発行することにした。発行した証明書は，クライアント認証の目的を確実に達成するために，社外に持ち出して営業支援サーバにアクセスする全ての PC に，情報システム部の担当者が直接インストールすることにした。

R 君は，検討結果を Q 課長に報告したところ，証明書の有効期限の満了によって社外から営業支援システムが利用できなくなったり，④PC の盗難や紛失が発生したりすることがあるので，PC 管理台帳を作成して，間違いのない運用ができるようにしなければならないとの指摘があった。そこで，R 君は，PC 管理台帳で，証明書の発行日，有効期限，証明書の識別情報，使用者，インストールした PC の情報などに加えて，証明書が有効かどうかを示す情報も併せて管理することにした。

R 君は，以上の検討結果を基に，SSL 導入の実施策をまとめ，Q 課長に報告した。Q 課長は，実施策に問題がないことを確認できたので，具体的な作業を進めるよう R 君に指示した。

設問 1　本文中の［ a ］，［ b ］に入れる適切な字句を答えよ。

設問 2　本文中の下線①の方法によるクライアント認証の目的を，30 字以内で述べよ。

設問 3　〔営業支援サーバを社外に公開する構成〕について，(1)～(3)に答えよ。

(1)　本文中の下線②の作業内容を，20 字以内で答えよ。

(2)　本文中の下線③で，案 2 の方が営業支援サーバ利用における被害が限定的となる理由を，25 字以内で述べよ。

(3)　表 1 中の項番 1，2 において，各項番のフィルタリングルールで通過が許可されるパケットの TCP の上位層のプロトコルを答えよ。

設問 4　本文中の下線④が発生したとき，営業支援システムの不正利用を防ぐために，クライアント証明書に対して実施すべき対応策は何か。25 字以内で述べよ。