問8　Webサイトのセキュリティ強化策に関する次の記述を読んで，設問1～4に答えよ。

A社は，家庭向けのソフトウェアを製造販売する会社である。A社のWebサイトは，自社の会社情報や製品情報などを掲載しており，アクセスしてきた全ての人に同じ情報を提供する静的なページで構成されている。このたび，ユーザサポートの向上を目的としてWebサイトを更改し，Webサイト内に会員専用のサイトを設けることにした。会員専用サイトでは，ユーザIDとパスワードでユーザを認証し，ユーザが購入した製品や興味のある製品に関する詳細な技術情報を含むページを動的に生成するWebアプリケーションを用いる。

〔セキュリティの強化〕

A社のセキュリティ担当課長は，今回の更改に併せて，Webサイトのセキュリティを強化したいと考えている。想定する脅威としては，SQLインジェクション，Webサイトの改ざん，クロスサイトスクリプティング，認証情報の盗聴の四つを懸念している。これらの脅威に対応するセキュリティ強化策を検討した結果，セキュアプログラミングを意識してWebアプリケーションを開発することとし，さらに(1)～(3)の3点を実施することにした。

(1) 更改前は全てHTTPでアクセスさせるようになっていたWebサイトを，①暗号化されていないデータがそのままインターネット上に流れては問題がある部分では，HTTPSでアクセスさせるようにする。HTTPSでアクセスされるべきページにHTTPでアクセスされた場合は，クライアントにHTTPSのURLをリダイレクトで返し，自動的にHTTPSで再アクセスさせるようにする。

(2) 更改前はDMZに配置し，インターネットから直接アクセスさせていたWebサーバを，インターネットから直接アクセスできない内部のLANに移設する。DMZにはロードバランサと2台のリバースプロキシサーバを配置する。ロードバランサは，ユーザからのHTTP/HTTPSリクエストを，Cookieの情報を基にWebアプリケーションのセッションを維持するようにリバースプロキシサーバに振り分ける。各リバースプロキシサーバは，受け取ったリクエストを，対応するWebサーバに転送する。

(3) リバースプロキシサーバには，WAF（Web Application Firewall）の機能をもたせ，ブラックリストによる検査によって外部からの攻撃を防御する。ブラックリストに

は，Web アプリケーションの脆弱性を悪用した攻撃の特徴的なパターンを登録しておく。

更改後のA社Webサイトのシステム構成を図1に示す。

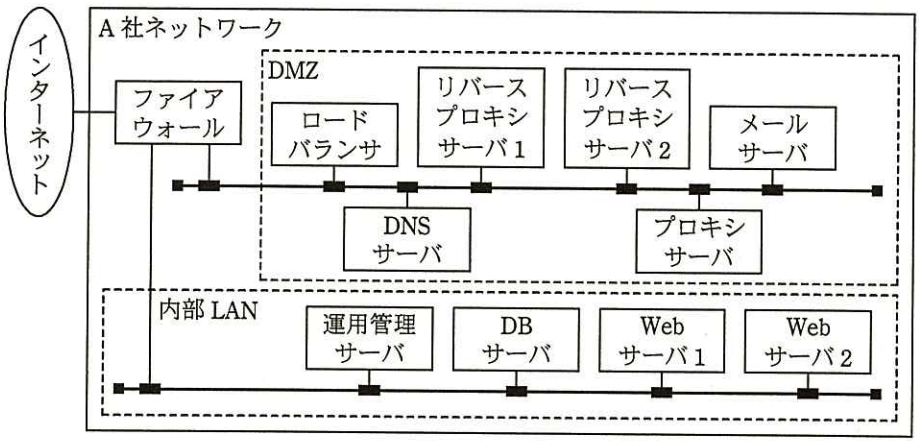

図1　更改後のA社Webサイトのシステム構成

〔Webサイトで HTTPS を使用するための準備〕

HTTPS を使って通信するためには，［ a ］を取得する必要がある。［ a ］の申請には，識別名（Distinguished Name）が必要になる。識別名は，国コード，都道府県名，市区町村名，組織名，部署名，コモンネーム（SSL 接続するサイトのFQDN）から構成される。A 社では，SSL 通信を行う Web サイトの URL を“https://www.a.co.jp/member/”とし，識別名を表1のように決定した。

表1　A社の識別名

識別名を構成する項目	値
国コード（Country）	JP
都道府県名（State）	Tokyo
市区町村名（Locality）	Bunkyo-ku
組織名（Organizational Name）	A Japan K.K.
部署名（Organizational Unit）	User Support
コモンネーム（Common Name）	［ b ］

A 社の Web サイト管理者は，識別名を決定し，コモンネームの重複がないことを確認した後，証明書署名要求（CSR：Certificate Signing Request）を生成し，認証局に申請することで［ a ］を取得した。証明書署名要求には，識別名と［ c ］が含まれており，認証局から取得した［ a ］を機器に導入する際には，［ c ］とペアを成す［ d ］が必要になる。［ a ］と［ d ］を機器に導入し，HTTPS でのアクセスが可能になるよう設定した。

〔セキュリティの警告〕

Web サイトの更改から 1 年ほど経過したころ，会員からサポート窓口に，「Web ブラウザから A 社の Web サイトにアクセスした際に，“セキュリティの警告”ダイアログボックスが表示された。どうすればいいのか。」との問合せが寄せられた。“セキュリティの警告”ダイアログボックスに含まれていたメッセージを図 2 に示す。

このサイトとの間で交換する情報は暗号化されているので，他の人から読み取られることはありません。しかし，このサイトは不正なセキュリティ証明書を使用しています。 ・このサイトのセキュリティ証明書は，信頼のおける認証機関が発行しています。 ・このサイトのセキュリティ証明書は，有効期間に問題があります。 ・このサイトのセキュリティ証明書に含まれている情報と，このページの名前は一致しています。

図 2　“セキュリティの警告”ダイアログボックスのメッセージ

サポート窓口担当者はセキュリティ担当課長に問合せに対する処置を依頼し，セキュリティ担当課長は，Web サイト管理者に対して，適切な対応をとるよう指示した。

設問1　本文中の下線①で，暗号化せずにインターネット上に流れては問題があるデータを二つ，本文中の字句を用いて答えよ。

設問2　〔セキュリティの強化〕で示した(1)～(3)のセキュリティ強化策は，セキュリティ担当課長が懸念している四つの脅威のうち，どの脅威に向けた強化策であるか。解答群の中から最も適切なものを選び，記号で答えよ。

解答群

ア　SQLインジェクション　　イ　Webサイトの改ざん

ウ　クロスサイトスクリプティング　　エ　認証情報の盗聴

オ　SQLインジェクション及びクロスサイトスクリプティング

カ　SQLインジェクション及び認証情報の盗聴

キ　クロスサイトスクリプティング及び認証情報の盗聴

設問3　本文及び表1中の［ a ］～［ d ］について，(1)～(3)に答えよ。

(1)　［ a ］，［ c ］，［ 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　SSLクライアント証明書　　イ　SSLサーバ証明書

ウ　SSLルート証明書　　エ　共通鍵

オ　公開鍵　　カ　秘密鍵

(2)　［ b ］に入れる適切な字句を答えよ。

(3)　A社のシステム構成のどの機器に［ a ］を導入する必要があるか。図1中のDMZ内の機器の名称で答えよ。また，その機器でなければならない理由を30字以内で述べよ。

設問4　図2の“セキュリティの警告”ダイアログボックスが表示されたことに対するWebサイト管理者の適切な対応を，20字以内で述べよ。