問3 Web アプリケーションファイアウォール（WAF）の導入に関する次の記述を読んで，設問1～4に答えよ。

R 社は従業員数 200 名の健康食品販売会社であり，消費者向けに電話受付による販売を行っており，5 年前からはインターネットを介した販売システムを利用した販売も行っている。

販売システムは，アウトソーシング事業者である Y 社のデータセンタに設置され，ルータ，ファイアウォール，負荷分散装置，Web サーバ，データベースサーバで構成されている。販売システムのネットワーク構成を図 1 に，販売システムの概略を図 2 に示す。

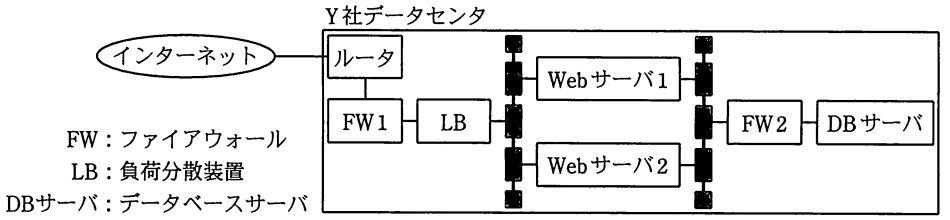

図1 R社の販売システムのネットワーク構成

(1) 利用者は，ブラウザでインターネットを介して Web サーバにアクセスし，販売システムを利用する。ブラウザからのアクセスは LB によって，Web サーバ 1 と Web サーバ 2 に負荷分散される。

(2) Web サーバ上では，HTTP による送受信を処理する Web サーバプログラム，ミドルウェア及びミドルウェア上で動作する Web アプリケーションが稼働している。Web アプリケーションは DB サーバと連携して動作する。

(3) Web アプリケーションの開発は，R 社のインターネット販売事業部で行っている。

(4) ルータ，FW 及び LB の管理，サーバのハードウェア保守，並びに OS のバージョン管理及び修正プログラム適用作業の運用は Y 社に業務委託している。

(5) FW は，パケットのヘッダ情報によってアクセスを制御するパケットフィルタリング型である。FW には，Web サーバへのアクセスを制御する FW1 と，DB サーバへのアクセスを制御する FW2 がある。

(6) 販売システムのログイン ID を保有している利用者は，Web アプリケーションのログイン画面で，ログイン ID とパスワードを入力することによってログインを行う。ログイン画面以降は，ブラウザと Web サーバ間で SSL 通信が行われる。また，ログイン時にミドルウェアがセッション ID を生成し，これをクッキーとして利用者のブラウザに格納することによってセッション管理を実現している。

(7) 販売システムのログイン ID を保有しない消費者向けに，R 社では電話による注文受付窓口を設置している。販売システムの商品紹介コンテンツは，ログイン ID を保有しない利用者でも閲覧できる。

図2 R社の販売システムの概略

〔脆弱性発見の情報〕

R 社は，情報セキュリティ専門会社からセキュリティ情報の提供を受けている。ある日，販売システムの Web サーバで稼働中のミドルウェアに脆弱性が発見されたとの情報が提供された。R 社インターネット販売事業部の S 主任がまとめた脆弱性の概要を図 3 に示す。

ミドルウェアによるセッション ID の生成に不備があり，利用者向けに発行されたセッション ID を第三者が推定できてしまう可能性がある。セッション ID は，利用者のログイン ID，ログインを行った年月日及び時刻の情報を基に生成される。この脆弱性によって，悪意のある第三者が，Web アプリケーションにログイン中のほかの利用者になりすまし，不正にアクセスできてしまう。

図 3　ミドルウェアで発見された脆弱性の概要

S 主任の調査の結果，ミドルウェアは開発元によるサポートが終了しており，修正プログラムが提供されないことが判明した。また，S 主任は，①販売システムの FW では，セッション ID の偽造を判別できないので，この脆弱性を悪用した攻撃を防御できないと判断した。

このミドルウェアを使用しないよう，販売システムを抜本的に改修するには，長期間を要する。そこで，R 社では，販売システムによる注文受付を一時的に停止し，注文は電話受付だけに限定する方針を決めた。また，インターネット販売事業部の P 課長は，脆弱性への早急な対策案の検討を S 主任に指示した。

〔WAF による対策の検討〕

S 主任は，図 3 の脆弱性への早急な対策案を，Y 社のセキュリティサービス担当の Q 氏に相談した。その結果，WAF の導入の提案を受けた。Q 氏が提案した WAF の主な機能を表に示す。

表　Q氏が提案したWAFの主な機能

機能の名称	機能の概要
シグネチャによる通信検査機能	HTTP による通信をシグネチャと比較し，一致した場合には攻撃として検知する。シグネチャには，脆弱性を悪用する攻撃に含まれる可能性の高い文字列が定義されている。シグネチャの更新情報は，WAF の開発元から定期的に配信される。シグネチャごとに有効化，無効化の選択ができ，有効化したシグネチャに対しては，検知時に通信を遮断するか，遮断は行わず通知だけを行うかを設定できる。独自のシグネチャも作成が可能である。
クッキーの暗号化機能	Web アプリケーションがブラウザに対してクッキーを発行した際，クッキーの値を暗号化して引き渡す。ブラウザからクッキーを受信した際，値を復号して，Web アプリケーションに引き渡す。
SSL アクセラレーション機能	SSL 通信の暗号化と復号を行う。
負荷分散機能	販売システムで利用中の LB と同等性能の負荷分散機能を有する。

次は，WAFによる対策の検討に関する，S主任とQ氏との会話である。

S主任：販売システムのミドルウェアで発見された脆弱性に対しては，WAF を使ってどのような対策が可能でしょうか。

Q氏　：②クッキーの暗号化機能によって，図 3 の脆弱性を悪用した攻撃への対策が可能です。この機能は WAF の導入後にすぐに利用を開始できるので，速やかに販売システムによる注文受付を再開できます。

S主任：分かりました。利用に際して，何か注意点はありますか。

Q氏　：③クッキーの暗号化では，クッキーに属性を付与している場合であっても，その属性の効果を維持できるように考慮されています。しかし，④ブラウザに格納されるクッキーが暗号化されたものになることから，Web アプリケーションによっては，動作に異常が生じる場合がありますので，販売システムでのクッキーの用途を事前に確認すべきです。

S主任：分かりました。確認しておきます。WAF にはシグネチャによる通信検査機能もあり，攻撃の遮断ができるようですが，どのような攻撃が遮断できるのでしょうか。また，この機能もすぐに利用が可能でしょうか。

Q氏　：クロスサイトスクリプティングや SQL インジェクションなど，既知の攻撃を検知して遮断することが可能です。シグネチャによる通信検査機能の利用に際しては，販売システムの可用性を維持するために，事前に十分な動作確認が必要です。販売システムを利用する上で必要な通信（以下，正常な通信と

いう）を WAF が攻撃として検知してしまうことで，利用者が販売システムを利用できなくならないよう，まずは［ a ］を減らすための検証期間を設けます。検証期間には，攻撃を検知しても通信の遮断は行わず，WAF 設定と Web アプリケーション設定のチューニングを行い，［ a ］が十分に減少した段階で，攻撃の遮断を開始します。ただし，チューニングに際しては，⑤正常な通信が攻撃と検知された場合であっても，不用意に，そのシグネチャを無効化するべきではありません。

S 主任 ：シグネチャによる通信検査機能によって，既知の攻撃を検知して遮断することが可能なので，安心して販売システムを運用できるのですね。

Q 氏 ：シグネチャによる通信検査機能では，攻撃がシグネチャに一致しなかった場合には，その攻撃を見逃してしまうので，必ずしも Web アプリケーションを防御できるとは限りません。

S 主任 ：なるほど。Web アプリケーションは，できるだけ脆弱性を除去して運用することが重要ですね。

Q 氏から説明を受けた S 主任は，販売システムでのクッキーの用途を確認した。その結果，WAF の機能によってクッキーを暗号化しても，販売システムの動作には異常が生じないことが分かった。そこで，S 主任は P 課長に WAF の導入を提案した。

〔WAF の導入〕

インターネット販売事業部では，S 主任の提案内容を検討した結果，販売システムへの WAF の導入を決定した。検討に際しては，クッキーの暗号化機能によって図 3 の脆弱性への対策が可能となる点に加えて，開発元によるサポートが終了したミドルウェアで，今後新たな脆弱性が発見された場合にも，シグネチャによる通信検査機能によって攻撃への防御を実現できる可能性がある点も評価された。

販売システムへの WAF の導入の際には，Web サーバへの負荷分散に WAF の負荷分散機能を利用することで，利用中の LB を WAF で置き換える方針とした。また，WAF の SSL アクセラレーション機能を利用し，⑥ブラウザからの SSL 通信は，WAF で終端させることにした。

インターネット販売事業部では，Q 氏の支援の下，WAF を販売システムに導入し，クッキーの暗号化機能を有効化した上で，販売システムによる注文受付を再開した。

その後，検証期間を終え，シグネチャによる通信検査機能の利用を開始した。そして，サポートの終了したミドルウェアを使用しないよう，販売システムの抜本的な改修に向けた検討を開始した。

設問1　本文中の［　a　］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　フェールセーフ　　イ　フェールソフト

ウ　フォールスネガティブ（偽陰性）　　エ　フォールスポジティブ（偽陽性）

設問2　本文中の下線①について，判別できないとS主任が考えた理由を，30字以内で述べよ。

設問3　〔WAFによる対策の検討〕について，(1)～(4)に答えよ。

(1) 本文中の下線②について，クッキーの値を暗号化することで，図3の脆弱性を悪用した攻撃への対策が可能とQ氏が判断した理由を，40字以内で述べよ。

(2) 本文中の下線③について，販売システムへのログイン時に，次のSet-Cookieヘッダを Web アプリケーションが送信した場合，WAF がそれを暗号化した結果の Set-Cookie ヘッダはどれか。解答群の中から選び，記号で答えよ。解答群の中の“☆☆”は，暗号化後の文字列を表す。

（Web アプリケーションが送信した Set-Cookie ヘッダ）

```
Set-Cookie: session_id=uid20101017143045; secure; path=/874045/
```

解答群

ア　`Set-Cookie: session_id=☆☆; path=/874045/`

イ　`Set-Cookie: session_id=☆☆; path=☆☆`

ウ　`Set-Cookie: session_id=☆☆; secure; path=/874045/`

エ　`Set-Cookie: session_id=☆☆; secure; path=☆☆`

(3) 本文中の下線④の動作に異常が生じる場合とは，クッキーがどのように用いられる場合か。30字以内で述べよ。

(4) 本文中の下線⑤について，シグネチャを無効化しても問題ないと判断するためには，何を確認することが望ましいか。“シグネチャ”と“脆弱性”という字句を用いて，60字以内で具体的に述べよ。

設問4　本文中の下線⑥について，この措置を行う理由を55字以内で述べよ。