問１　ソフトウェアの脆弱性への対応に関する次の記述を読んで，設問1～5に答えよ。

Q 社は従業員数 300 名の食品販売会社であり，消費者向けにインターネットを介して健康食品を販売している。

Q 社の社外向け情報システムは，販売システム（以下，E システムという）と広報システム（以下，F システムという）から成り，G 社のデータセンタに設置されている。E システムは Q 社の販売チャネルの大部分を担っており，保守のための時間帯を除き，常時稼働している。F システムは投資家などに対する財務情報・会社情報を提供している。両システムは，Q 社のシステム部が構築，運用している。

E システムは，E サーバ，待機サーバ，データベースサーバ（以下，DB サーバという）などから成る。E サーバは，E サーバ 1 と E サーバ 2 から成る冗長構成であり，ロードバランサ（以下，LB という）によって負荷分散を行っている。待機サーバは，E サーバ 1 及び E サーバ 2 がともに停止した際に，E システムの利用者に停止を告知するためのものである。Q 社の社外向け情報システムのネットワーク構成を図 1 に示す。

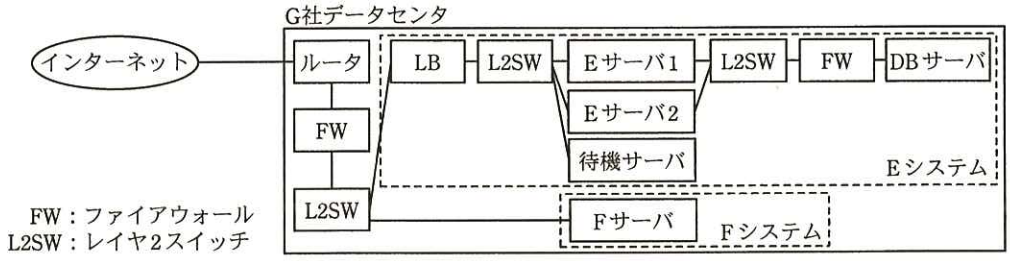

図１　社外向け情報システムのネットワーク構成

E サーバでは，HTTP サーバ，Web アプリケーションサーバ（以下，WAS という）及び Web アプリケーションソフトウェア（以下，Web アプリ E という）が稼働している。Web アプリ E は，オープンソースソフトウェアの Web アプリケーションフレームワーク（以下，WF という）を使用して開発された。Web アプリ E と WF は，WAS と同じ権限で動作する。また，HTTP サーバにはオープンソースソフトウェアの WAF が付属しており，HTTP サーバの一部として動作する。WAF にはルールを設定することができるが，現在は何も設定していない。Web アプリ E は，商品情報，購入者情報，購入履歴情報などが格納された DB サーバにアクセスする。E サーバの

ソフトウェア構成を表1に示す。

表1　Eサーバのソフトウェア構成

ソフトウェア	現在の動作権限設定	備考
OS	—	—
HTTPサーバ（WAF含む）	管理者権限	—
WAS	管理者権限	—
Webアプリ E（WF使用）	—	WASの動作権限と同一

注記　HTTPリクエストは，LB → HTTPサーバ（WAF含む） → WAS → Webアプリ Eの順に処理される。

Fシステムは，Fサーバ1台から成る。FサーバはHTTPサーバを搭載しており，静的なHTML コンテンツを公開している。F サーバには，WF，WAF を導入していない。Q社では，社外向け情報システムの開発検証用に図1中のEシステム，Fシステムと同一構成のシステムをそれぞれ別に用意している。

WAFのルールの記述形式を図2に，WAFの動作を図3に示す。

・ルールは，[検証対象]，[パターン]及び[動作]の三つを1行に記述する。
　（例：POST　abc¥.exe　検知）
・[検証対象]には，次のいずれかを指定する。
　GET　：GETメソッドのパラメタ名を検証対象とする。
　POST　：POSTメソッドのパラメタ名を検証対象とする。
　ANY　：任意のメソッドのパラメタ名を検証対象とする。
　COOKIE　：Cookieの名前を検証対象とする。
　Multipart　：Multipart/form-dataのフィールド名を検証対象とする。
・[パターン]には，次の要素で構成される正規表現を指定する。
　^　：文字列の先頭にマッチする。
　¥W　：任意の非英数字にマッチする。
　$x|y$　：x又はyにマッチする。
　$(x|y)z$　：xz又はyzにマッチする。
　$[xyz]$　：x，y又はzのいずれかにマッチする。
　.　：任意の文字とマッチする。
　¥.　：“.”とマッチする。
　*　：直前の要素と0回以上マッチする。
・[動作]には，次のいずれかを指定する。
　遮断：通信を遮断し，ログに記録する。
　検知：通信を通過させ，ログに記録する。
　許可：通信を通過させ，ログに記録しない。

図2　WAFのルールの記述形式

・WAF は，HTTP リクエストにおける[検証対象]に対して，[パターン]とのマッチングを行う。 ・設定されたルールを順に検証する。最初にマッチしたルールの[動作]に指定された処理を行い，残りのルールは検証しない。 ・どのルールにもマッチしなかった場合，その HTTP リクエストを通過させる。

注記　Multipart/form-data による HTTP リクエストは，[検証対象]に Multipart が指定されたときだけ[パターン]とのマッチングを行う。

図 3　WAF の動作

〔脆弱性の確認〕

ある日，システム開発担当の S 主任に別の部署の社員から WF の特定バージョン（以下，バージョン Z という）の脆弱性（以下，脆弱性 X という）が公表されたという連絡があった。S 主任が，Q 社での WF のバージョン Z の使用の有無を調査したところ，E サーバの WF が該当していた。早速，脆弱性 X への対応を S 主任と部下の T さんとで行うことになった。

T さんが確認したところ，次のことが分かった。

・脆弱性 X は，HTTP リクエストが適切に処理されないバグを突いて，ClassLoader を不正に操作できるというものである。

・攻撃者が“class.classLoader”という文字列を含む HTTP リクエストを送信することによって，任意のファイルへの書込みなど，WAS の動作権限で任意の攻撃コードを実行できる。

・攻撃方法及び攻撃コードが既にインターネットで公開されており，攻撃は容易である。

・修正モジュールが既に提供されている。

S 主任は脆弱性 X の確認結果を経営陣に報告し，E サーバ 1 及び E サーバ 2 を停止させるとともに，LB の設定を変えて待機サーバに切り替えた。次は，その後の S 主任と T さんの会話である。

S 主任：E サーバに対して，攻撃者が脆弱性 X をどのように悪用できるのか具体的に説明してくれるかな。

T さん：表 2 の攻撃コードの例を使って説明します。攻撃者は攻撃コードを表 2 の項番の順に E サーバに送ることで，任意のコマンド“XXXX”を実行できま

す。表 2 の攻撃コードの送信後，WAS のアクセスログ（以下，WAS ログという）のファイルが [a] に作成されます。

今回の脆弱性情報によると，GET メソッドに限らず POST メソッド，Multipart/form-data の POST メソッド，Cookie による攻撃の可能性もあります。さらに，攻撃者が WAS ログを細工する可能性もあります。

S 主任：それでは，攻撃の有無を確認するには，WAS ログだけでなく，社外向け情報システムの全サーバと FW のログも調査する必要があるね。

表 2　攻撃コードの例

項番	攻撃コード	説明
1	GET /app1/app.action?▲▲.directory=webapps/ROOT	WAS ログの出力先を公開ディレクトリ上に変更する。
2	GET /app1/app.action?▲▲.prefix=shell	WAS ログのファイル名を指定する。ファイル名のプレフィックスを“shell”という文字列にして，拡張子を jsp にする。
3	GET /app1/app.action?▲▲.suffix=.jsp	
4	GET /app1/app.action?▲▲.fileDateFormat=1	WAS ログの日付フォーマットの設定を“1”という文字にする。WAS ログのファイル名が，shell1.jsp となる。
5	GET /app1/app.action?a=<%Runtime.getRuntime().exec("XXXX");%>	任意のコマンド“XXXX”を実行させるためのコードが WAS ログに記録される。
6	GET /shell1.jsp	shell1.jsp を呼び出すことで，コマンド“XXXX”を WAS と同じ動作権限で実行する。

注記　▲▲は，“class.classLoader.resources.context.parent.pipeline.first”という文字列を示す。

S 主任と T さんは念のため，Q 社の社外向け情報システムの全サーバと FW のログを調査したが，不審な内容は見つからなかった。

〔脆弱性への対策〕

S 主任と T さんは，脆弱性 X への対策として，修正モジュールによる方法と WAF による方法の二つを比較検討した。Q 社では，ビジネス上の理由から，E システムを 5 日以内に再稼働させる必要がある。しかし，修正モジュール適用後の Web アプリ E の動作検証に 10 日間を要することが分かった。一方，WAF による対策は，脆弱性 X を悪用した攻撃を防ぐ効果があり，動作検証を含めて 2 日間で実施可能と分かった。

そこで，WAF による対策について，更に検討することにした。次は，WAF のルールについてのＳ主任とＴさんの会話である。

Ｓ主任：WAF では，どのようにルールを記述するのかな。

Ｔさん：表 3 のように記述します。表 3 の[パターン]列には，正規表現で示された文字列を指定します。当初，①“^class¥..*”という[パターン]がセキュリティ専門家によって公表されましたが，これでは遮断されない攻撃が見つかりました。その後，表 3 に示す正しい[パターン]が別のセキュリティ専門家によって公表されました。

表 3　WAF のルール例

項番	[検証対象]	[パターン]	[動作]
1	b	(^ |¥W)[cC]lass¥W	c
2	d	(^ |¥W)[cC]lass¥W	e
3	f	(^ |¥W)[cC]lass¥W	g

Ｓ主任：では，表 3 どおりに記述することにしよう。他に注意することはあるかな。

Ｔさん：攻撃ではない HTTP リクエストを遮断してしまう h に注意する必要があります。例えば，表 3 のルールでは，“class.abc”を含む HTTP リクエストが遮断されてしまいます。さらに，WAF による対策に加えて，攻撃時のリスク軽減対策として，②現在の WAS の動作権限設定を見直します。

Ｓ主任は，修正モジュールが提供されている場合は，一般的には修正モジュール適用による対策が望ましいが，本ケースでは WAF による対策を選択すべきと判断し，経営陣に説明して了承を得た。開発検証用のシステムで③動作検証を実施し，問題ないことを確認後，本番環境のシステムで設定を行い，Ｅシステムを再稼働させた。

本来ならば，追加した WAF のルールで攻撃を遮断する前に，④本番環境のシステムに追加したルールの[動作]に“検知”を指定し，一定期間運用するのが望ましい。

しかし，今回は緊急対応のため，そのような運用はしなかった。

その後，Q 社では，脆弱性 X の修正モジュール適用による悪影響がないことを確認し，それを適用した。

設問1　E システム及び F システムそれぞれについて，Q 社のビジネスを踏まえて，情報セキュリティの 3 要素のうち重視すべき要素とその理由を，重視すべき要素は 5 字以内，理由は 25 字以内でそれぞれ述べよ。

設問2　本文中の [a] に入れる適切な字句を，表 2 中の字句を用いて 15 字以内で答えよ。

設問3　〔脆弱性への対策〕について，(1)～(4) に答えよ。

(1)　表 3 中の [b] ～ [g] に入れる適切な字句を，図 2 中の字句を用いて答えよ。

(2)　本文中の下線①に示した[パターン]にマッチする文字列を解答群の中から全て選び，記号で答えよ。

解答群

ア　anObject.class.classLoader　　イ　class.ClassLoader

ウ　class.classLoader　　エ　class['classLoader']

(3)　本文中の [h] 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　　エ　フォールスポジティブ

(4)　本文中の下線②について，設定をどのように見直すべきか。25 字以内で述べよ。

設問4　本文中の下線③について，WAF に関して具体的に何を検証すべきか。二つ挙げ，それぞれ 30 字以内で述べよ。

設問5　本文中の下線④について，WAF のルールの[動作]に“検知”を指定し，一定期間運用することにはどのような利点があるか。45 字以内で述べよ。