次の問1は必須問題です。必ず解答してください。

問1　Web サイトを用いた書籍販売システムのセキュリティに関する次の記述を読んで，設問1～4に答えよ。

K 社は技術書籍の大手出版社である。従来は全ての書籍を書店で販売していたが，顧客からの要望によって，高額書籍を自社の Web サイトでも販売することになった。K 社システム部の L 部長は，Web サイトを用いた書籍販売システム（以下，Web システムという）の開発のためのプロジェクトチームを立ち上げ，開発課の M 課長をリーダに任命した。L 部長は，情報セキュリティ確保のための対策として，サイバー攻撃による Web システムへの侵入を想定したテスト（以下，侵入テストという）を実施するように M 課長に指示した。M 課長は，開発作業が結合テストまで完了した段階で，Web システムのテスト環境を利用して侵入テストを実施することにした。

〔Web システムのテスト環境〕

Web システムは，高額書籍を購入する顧客の氏名，住所，購入履歴などの個人情報（以下，顧客情報という）を内部ネットワーク上のデータベースサーバ（以下，DB サーバという）に保存し，Web サーバが DB サーバ，業務サーバにアクセスして販売処理を行う。Web システムのテスト環境の構成を図1に示す。

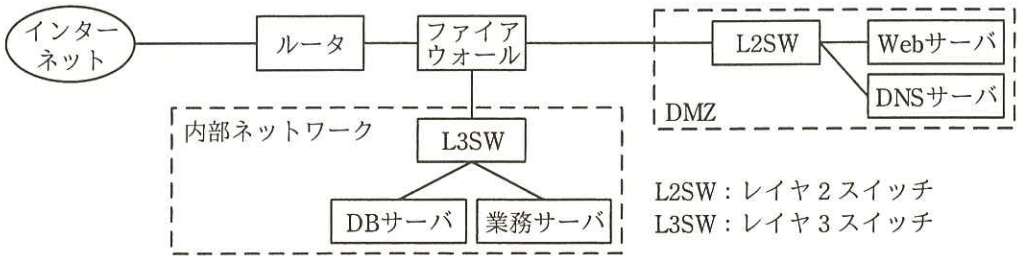

図1　Web システムのテスト環境の構成

〔Web システムの認証と通信〕

顧客が Web システムを利用する際，利用者 ID とパスワードで認証する。また，顧客との通信には，インターネット標準として利用されている［　a　］による暗号化通信を用いる。

サーバ管理者は，各サーバやファイアウォールのログを定期的にチェックすることによって，Web システムにおける不正なアプリケーションの稼働を監視する。

〔侵入テストの実施〕

M 課長は，社外のセキュリティコンサルタントの N 氏に侵入テストの実施を依頼した。N 氏は，表 1 に示す侵入テストのテスト項目を作成し，M 課長に提出した。

表 1　テスト項目（抜粋）

項番	内容
1	攻撃者が，Web サーバの構成情報の調査結果から Web システムの脆弱性を確認することが可能か。
2	Web システムへの攻撃によって，Web システム内に侵入した後，Web サーバの管理者権限の奪取が可能か。
3	Web アプリケーションの脆弱性を意図的に利用した攻撃が可能か。

〔結果〕

N 氏は，テスト項目に沿って侵入テストを実施し，その結果と改善項目を M 課長に報告した。テスト結果と改善項目を表 2 に示す。

表 2　テスト結果と改善項目（抜粋）

項番	テスト結果	改善項目
1	Web システムのサービスに必要がないポートが，インターネットに公開されていた。インターネットから Web サーバの構成情報を調査できた。	Web システムのサービスに必要なポートだけをインターネットに公開する。Web サーバが必要のない問合せに応答しないようにする。
2	Web サーバの脆弱性を利用して，Web サーバを［ b ］にし，そこを中継点として内部ネットワークに侵入できた。	セキュリティ機器を導入して，Web サーバへの不正アクセスを防御し，脆弱性の存在自体が広く公表される前にそれを悪用する［ c ］攻撃のリスクを軽減する。ファイアウォールとサーバのログ管理を強化する。
3	Web アプリケーションを対象とした次の攻撃について，対処されていないので，Web アプリケーションを誤作動させることが可能であった。 ・バッファオーバフロー ・SQL インジェクション さらに，DB サーバに不正アクセスし，顧客情報の奪取や改ざんが可能であった。	開発課で開発した Web アプリケーションの脆弱性の原因となっているセキュリティホールを修正する。

〔改善項目とその対策〕

M 課長と N 氏は，Web システムの侵入テストの結果と，セキュリティ上の改善項目について，表 1 と表 2 を基にして L 部長に報告した。

N 氏　：現在の Web システムには，サイバー攻撃に対して多くの脆弱性が存在します。

L 部長：項番 1 について説明してください。

N 氏　：攻撃者は①Web サーバの構成情報の調査によって，攻撃するために有用な情報を得ることで，Web サーバの脆弱性を探ってきます。

L 部長：どのような対策が有効ですか。

N 氏　：②ポートスキャンについては，Web サーバやファイアウォールの設定で防止する必要があります。Web サーバの構成情報の調査については，Web サーバの設定情報を変更して，必要のない問合せに応答しないようにすることで対処します。

L 部長：項番 2 で，Web サーバについて改善項目がありますが，どのような対策が必要ですか。

N 氏　：③Web サーバへの攻撃の疑いがあるアクセスを遮断するセキュリティ機器の導入が効果的です。保護する対象を Web アプリケーションに特化しており，Web サーバ上で使用するアプリケーションに潜む未知の脆弱性を突く攻撃を，プロトコルの異常などによって検知し，遮断できるようになります。

L 部長：項番 3 のバッファオーバフローと SQL インジェクションについては，どのような対策が必要ですか。

N 氏　：ソースコードをチェックするツールを使用して，Web アプリケーションの脆弱性を調査し，その結果に基づいたソースコードの修正が必要です。バッファオーバフローは，バッファにデータを保存する際に［　d　］を常にチェックすることで防ぐことができます。SQL インジェクションは，データを SQL に埋め込むところで，データの特殊文字を適切に［　e　］することで防ぐことができます。

M課長：改善項目に対応するよう Web アプリケーションのソースコードを修正しま

す。

N氏　：Web システムの構成にも問題点があります。攻撃者が，攻撃の発見を遅らせるために，Web システム内でログを消去するおそれがあります。

L部長：対策方法はありますか。

N氏　：各サーバやファイアウォールのログを集中して保存する専用のサーバを設置し，ログが消去されることを防ぎます。また，④ログをリアルタイムにチェックするツールを導入します。

N氏の指摘に基づいて，開発課がWebシステムを改善し，L部長はWebシステムの総合テストの実施を承認した。

設問1　本文中の［　a　］及び表2中の［　b　］，［　c　］に入れる適切な字句をそれぞれ4字以内で答えよ。

設問2　本文中の［　d　］，［　e　］に入れる適切な字句をそれぞれ解答群の中から選び，記号で答えよ。

解答群

ア　エスケープ　　イ　データサイズ

ウ　マイグレーション　　エ　リダイレクト

オ　ルートクラック

設問3　〔改善項目とその対策〕について，(1)～(3)に答えよ。

(1)　本文中の下線①について，Web サーバの構成情報の調査によって得られる，Web サーバを攻撃するために有用な，アプリケーションに関する情報を二つ挙げ，それぞれ7字以内で答えよ。

(2)　本文中の下線②について，Web サーバへのポートスキャンの対策として効果的な方策は何か。15字以内で答えよ。

(3)　本文中の下線③で，N氏が導入を推奨するセキュリティ機器とは何か。アルファベット3字で答えよ。

設問4　本文中の下線④について，ログのリアルタイムでのチェックで，サイバー攻撃の可能性があると判断される痕跡を解答群の中から全て選び，記号で答えよ。

解答群

ア　DNS を使用せず URL の中に IP アドレスを直接書き込んで通信している。

イ　URL フィルタのホワイトリストに一致した通信が発生している。

ウ　送られてくるファイルの拡張子が偽装されている。

エ　業務時間外に内部ネットワークから業務サーバへのアクセスが減少している。

オ　通信元の IP アドレスが，想定した範囲から外れている。