次の問1は必須問題です。必ず解答してください。

問1　通信販売サイトのセキュリティインシデント対応に関する次の記述を読んで，設問1～4に答えよ。

R社は，文房具やオフィス家具を製造し，店舗及び通信販売サイトで販売している。通信販売サイトでの購入には会員登録が必要である。通信販売サイトはECサイト用CMS（Content Management System）を利用して構築している。通信販売サイトの管理及び運用は，R社システム部門の運用担当者が実施していて，通信販売サイトに関する会員からの問合せは，システム部門のサポート担当者が対応している。

〔通信販売サイトの不正アクセス対策〕

通信販売サイトはR社のデータセンタに設置されたルータ，レイヤ2スイッチ，ファイアウォール（以下，FWという），IPS（Intrusion Prevention System）などのネットワーク機器とCMSサーバ，データベースサーバ，NTPサーバ，ログサーバなどのサーバ機器と各種ソフトウェアとで構成されている。通信販売サイトは，会員情報などの個人情報を扱うので，様々なセキュリティ対策を実施している。R社が通信販売サイトで実施している不正アクセス対策（抜粋）を表1に示す。

表1　通信販売サイトの不正アクセス対策（抜粋）

項番	項目	対策
1	ネットワーク	IPSによる，ネットワーク機器及びサーバ機器への不正侵入の防御
2		ルータ及びFWでの不要な通信の遮断
3	ログサーバ	各ネットワーク機器，サーバ機器及び各種ソフトウェアのログを収集
4	CMSサーバ データベースサーバ	不要なアカウントの削除，不要な［　a　］の停止
5		OS，ミドルウェア及びCMSについて修正プログラムを毎日確認し，最新版の修正プログラムを適用
6		CMSサーバ上のWebアプリケーションへの攻撃を，［　b　］を利用して検知し防御

IPSは不正パターンをシグネチャに登録するシグネチャ型であり，シグネチャは毎日自動的に更新される。

項番4の対策をCMSサーバ及びデータベースサーバ上で行うことで不正アクセスを受けにくくしている。R社では，①項番5の対策を実施するために，OS，ミドルウ

エア及び CMS で利用している製品について必要な管理を実施して，脆弱性情報及び修正プログラムの有無を確認している。また，項番 6 の対策で利用している［ b ］は，ソフトウェア型を導入していて，シグネチャは R 社の運用担当者が，システムへの影響がないことを確認した上で更新している。

〔セキュリティインシデントの発生〕

ある日，通信販売サイトが改ざんされ，会員が不適切なサイトに誘導されるというセキュリティインシデントが発生した。通信販売サイトを閉鎖し，ログサーバが収集したログを解析して原因を調査したところ，特定のリクエストを送信すると，コンテンツの改ざんが可能となる CMS の脆弱性を利用した不正アクセスであることが判明した。

R 社の公式ホームページでセキュリティインシデントを公表し，通信販売サイトの復旧と CMS の脆弱性に対する暫定対策を実施した上で，通信販売サイトを再開した。

今回の事態を重く見たシステム部門の S 部長は，セキュリティ担当の T 主任に今回のセキュリティインシデント対応で確認した事象と課題の整理を指示した。

〔セキュリティインシデント対応で確認した事象と課題〕

T 主任は関係者から，今回のセキュリティインシデント対応について聞き取り調査を行い，確認した事象と課題を表 2 にまとめて，S 部長に報告した。

表 2　セキュリティインシデント対応で確認した事象と課題（抜粋）

項番	確認した事象	課題
1	CMS の脆弱性を利用して不正アクセスされた。	CMS への修正プログラム適用は手順どおり実施されていたが，今回の不正アクセスに有効な対策がとられていなかった。
2	［ b ］のシグネチャが更新されていなかった。	［ b ］は稼働していたが，運用担当者がシグネチャを更新していなかった。
3	通信販売サイトが改ざんされてからサイト閉鎖まで時間を要した。	サイト閉鎖を判断し指示するルールが明確になっていなかった。
4		改ざんが行われたことを短時間で検知できなかった。
5	原因調査に時間が掛かり，R社の公式ホームページなどでの公表が遅れた。	ログサーバ上の各機器やソフトウェアのログを用いた相関分析に時間が掛かった。

S部長はT主任からの報告を受け，セキュリティインシデントを専門に扱い，インシデント発生時の情報収集と各担当へのインシデント対応の指示を行うインシデント対応チームを設置するとともに，今回確認した課題に対する再発防止策の立案をT主任に指示した。

〔再発防止策〕

T主任は，再発防止のために，表2の各項目への対策を実施することにした。

項番1については，CMSサーバを構成するOS，ミドルウェア及びCMSの脆弱性情報の収集や修正プログラムの適用は実施していたが，②今回の不正アクセスのきっかけとなった脆弱性に対応する修正プログラムはまだリリースされていなかった。このような場合，OS，ミドルウェア及びCMSに対する③暫定対策が実施可能であるときは，暫定対策を実施することにした。

項番2については，［ b ］の運用において，新しいシグネチャに更新した際に，デフォルト設定のセキュリティレベルが厳し過ぎて正常な通信まで遮断してしまう［ c ］を起こすことがあり，運用担当者はしばらくシグネチャを更新していなかったことが判明した。運用担当者のスキルを考慮して，運用担当者によるシグネチャ更新が不要なクラウド型［ b ］サービスを利用することにした。

項番3については，［ d ］がセキュリティインシデントの影響度を判断し，サイト閉鎖を指示するルールを作成して，サイト閉鎖までの時間を短縮するようにした。

項番4については，サイトの改ざんが行われたことを検知する対策として，様々な検知方式の中から未知の改ざんパターンによるサイト改ざんも検知可能であること，誤って検知することが少ないことから，ハッシュリスト比較型を利用することにした。

項番5については，④各ネットワーク機器，サーバ機器及び各種ソフトウェアからログを収集し時系列などで相関分析を行い，セキュリティインシデントの予兆や痕跡を検出して管理者へ通知するシステムの導入を検討することにした。

T主任は対策を取りまとめてS部長に報告し，了承された。

設問1　表1中の［　a　］に入れる適切な字句を5字以内で答えよ。

設問2　本文及び表1，2中の［　b　］に入れる適切な字句をアルファベット3字で答えよ。

設問3　本文中の下線①で管理するべき内容を解答群の中から全て選び，記号で答えよ。

解答群

ア　販売価格　　イ　バージョン

ウ　名称　　エ　ライセンス

設問4　〔再発防止策〕について，(1)～(5)に答えよ。

(1)　本文中の下線②の状況を利用した攻撃の名称を8字以内で答えよ。

(2)　本文中の下線③について，暫定対策を実施可能と判断するために必要な対応を解答群の中から選び，記号で答えよ。

解答群

ア　過去の修正プログラムの内容を確認

イ　修正プログラムの提供予定日を確認

ウ　脆弱性の回避策を調査

エ　同様の脆弱性が存在するソフトウェアを確認

(3)　本文中の［　c　］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　過検知　　イ　機器故障　　ウ　未検知　　エ　予兆検知

(4)　本文中の［　d　］に入れる適切な組織名称を本文中の字句を用いて15字以内で答えよ。

(5)　本文中の下線④のシステム名称をアルファベット4字で答えよ。