平成 27 年度 秋期 情報セキュリティスペシャリスト

＜午後 I　解答・解説＞

＜問1＞ ソフトウェアの脆弱性への対応

■設問 1

〔試験センターによる解答例〕

E システム

要素：可用性（3 字）

理由：販売チャネルの大部分を担い，常時稼動が必要なため（24 字）

F システム

要素：完全性（3 字）

理由：投資家に正確な財務情報，会社情報を提供するため（23 字）

E システム

本文の冒頭に「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，**常時稼動している**」とあるように，一見して高い**可用性**が求められるシステムであることがわかる。

F システム

F システムについての説明はわずかであるが，「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**」とあることから，情報が正確であること（**完全性**）が最重要であり，機密性や不要であること，そして F システムほどの可用性は求められていないことがわかる。

■設問 2

〔試験センターによる解答例〕

a：公開ディレクトリ（8 字）

表 2 の項番 1 に「WAS ログの出力先を公開ディレクトリ上に変更する」とある。したが

って［ a ］には「**公開ディレクトリ**」が入る。

■設問 3

〔試験センターによる解答例〕

(1) b：ANY

c：遮断

d：COOKIE

e：遮断

f：Multipart

g：遮断

※b，d，f は順不同

(2) イ，ウ

(3) h：エ

(4) WAS を必要最小限の権限で動作させる。(19 字)

(1)［ b ］，［ d ］，［ f ］には，脆弱性 X を悪用した攻撃への対策として，WAF の［検証対象］に指定する文字列が入る。図 2 より，［検証対象］には，GET，POST，ANY，COOKIE，Multipart のいずれかを指定できることがわかる。問題文の〔脆弱性の確認〕の T さんの説明によれば，「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」とのことである。これらの中から三つを指定するのであるから，GET と POST をまとめて **ANY** を指定し，残る二つを **COOKIE**，**Multipart** とすればよい。

［ c ］，［ e ］，［ g ］は，WAF の［動作］に指定するルールであり，図 2 より，“遮断”，“検知”，“許可”のいずれかが指定できることがわかる。攻撃を防ぐには“遮断”を指定する必要があるが，問題文の下線④にあるように，本来は WAF のルールで攻撃を遮断する前に“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」とあることから，“**遮断**”が該当する。

(2)図 2 より，下線①の“^class¥..*”という［パターン］は，次のような意味になることがわかる。

^：文字列の先頭にマッチする。
class：“class”にマッチする。
¥.：“.”とマッチする。
.：任意の文字とマッチする。
*：直前の要素（任意の文字）と 0 回以上マッチする。

つまり，“class”で始まり，続いて任意の文字が続く文字列ということになる。解答群の中でこれに該当するのは，“**class.ClassLoader**”と“**class.classLoader**”である。

(3) [h]には，「攻撃ではない HTTP リクエストを遮断してしまう」ことに該当する用語が入る。解答群の各用語の意味は次のようになる。

ア　“**フェールセーフ**”とは，システムに障害等が発生した場合に，安全な方向に向かうように制御することである。
イ　“**フェールソフト**”とは，システムに障害等が発生した場合に，機能を縮退させて運用を継続することである。
ウ　“**フォールスネガティブ**”とは，対処すべき攻撃等を見逃してしまうことである。
エ　“**フォールスポジティブ**”とは，正常な事象を攻撃等と誤認識してしまうことである。

したがって[h]に該当するのは，**エ**の“フォールスポジティブ”である。

(4)WAS の動作権限に関する記述を確認すると，表 1 に，現在の WAS の動作権限設定は“管理者権限”となっていることがわかる。そして，〔脆弱性の確認〕に，脆弱性 X が悪用されると，攻撃者は「WAS の動作権限で任意の攻撃コードを実行できる」とあることから，そのままにしておけば攻撃により非常に大きな被害を受ける可能性がある。このリスクを軽減するには，**WAS を必要最小限の権限で動作させる**よう設定変更する必要がある。

■設問 4

〔試験センターによる解答例〕

・脆弱性 X を突く攻撃を防げること（15 字）

・E システム利用のための正常な通信が許可されること（24 字）

WAF による対策を実施する目的は，**脆弱性 X を悪用した攻撃を防ぐこと**であるから，まずはそれが想定通りに行われることを検証する必要がある。ただし，問題文で T さんが述

べているように，フォールスポジティブが発生しないことが前提となる。具体的には，WAF による対策を実施しても，**E システムを利用するための正常な通信が攻撃として誤認識されることなく，許可されること**を検証する必要がある。

■設問 5

〔試験センターによる解答例〕

販売機会損失など，ビジネスへの影響を与えずに誤検知の検証ができる。(33 字)

問題文から，E システムは Q 社の販売チャネルの大部分を担っている重要なシステムであり，ビジネス上の理由から，5 日以内に再稼動させる必要があることがわかる。WAF による対策を実施した結果，フォールスポジティブで正常な通信が遮断されたとすれば，販売機会損失など，Q 社のビジネスに多大な影響が出ることが懸念される。

一方，WAF のルールの動作に“検知”を指定した場合には，フォールスポジティブが発生しても通信が遮断されることはないため，ビジネスへの影響を与えずに WAF の動作検証を行うことができる。ただし，その間に WAF が実際の攻撃を検知したとしても遮断されないため，検知結果を常時監視し，迅速かつ適切な対応がとれるようにしておく必要がある。

＜問2＞ 特権 ID の管理

■設問 1

〔試験センターによる解答例〕

a：Y 社の管理者（6 字）

表 2 にあるように，［ a ］は，「委託用特権 ID をあらかじめ登録する」「委託用特権 ID の使用許可操作を行う」「委託用特権 ID の使用解除操作を行う」「レポートを確認する」といったことを行っている。内容からして，これは管理者の役割であり，問題文冒頭にある Y システムの保守作業手順に登場する「**Y 社の管理者**」が該当する。

■設問 2

〔試験センターによる解答例〕

(1)委託用特権 ID：DBMS 操作 ID（8 字）

理由：業務アプリが DB サーバにアクセスする ID と同じ ID であるから（30 字）

(2)b：S 社 PC

c：管理用サーバ

(3)不正操作の記録が管理用サーバの操作履歴に残るから（24 字）

(1)DB サーバ上のアクセスログから特定するという記述から，対象となる委託用特権 ID は DBMS 上のデータに対する操作権限をもつ「**DBMS 操作 ID**」である。表 2 より，製品 Q では，プログラム K が作業者の個人 ID による委託用特権 ID の使用が許可されていることを確認後，委託用特権 ID とパスワードを用いて作業対象サーバに自動ログインする仕組みとなっている。また，問題文冒頭の説明に「各業務アプリは，DBMS 操作 ID を用いて，DB サーバから顧客情報を取得して Y 社の従業員にサービスを提供している」とあることから，各業務アプリも DBMS 操作 ID を共用して DB サーバ上にアクセスしていることがわかる。そのため，**DB サーバへアクセスした者を DB サーバ上のアクセスログから特定することができない**。

(2)案 2 の説明にあるように，製品 Q では，作業者は **S 社 PC** から，サーバ LAN 上に設置した管理用サーバのプログラム K にログインし，作業を行う。作業者がログインすると，プログラム K は作業対象サーバへ自動ログインする。したがって，S 社 PC からは，**管理用サーバ**へのアクセスだけを許可するように FW3 の設定を変更することによって，作業対象サーバだけにアクセス可能とすることが可能となる。

(3)表 2 の「操作履歴の取得」に「作業対象サーバでの操作履歴は管理用サーバに保存される。保存された操作履歴へのアクセスには管理用サーバのシステム管理権限が必要であり，Y 社内の限られた者だけがアクセスできる」とある。これにより，作業者が作業対象サーバ上のアクセスログを書き換えたとしても，**管理用サーバに操作履歴が残るため，不正操作を検知することが可能となる**。

■設問 3

〔試験センターによる解答例〕

(1)個人 ID が本人以外に使われるおそれがないように管理していること（31 字）

(2)抑止効果（4 字）

(3)委託先 PC にインストールするプログラムの資産管理をせずに済むから（32 字）

(1)表 1 の調査結果にあるように，対策実施前は委託用特権 ID が共用されていたり，作業者

以外が委託用特権 ID を使用するおそれがあったりして，実際の使用者が特定できないことが問題となっていた。対策実施後は個人 ID が付与されたため，このような問題は発生しにくくなったが，管理不備により，付与された本人以外の者が個人 ID を使用したとすれば，要件 2 を満たすことができなくなる。そのため，Y 社は，S 社におけるプログラム K の個人 ID の管理状況を確認する必要がある。

(2)委託用特権 ID を使った者が特定されることをプログラム K のログイン画面に表示し，作業者に周知させることにより期待されるのは，作業者に不正な顧客情報の持出しなどを思いとどまらせることである。これを**抑止効果**という。

(3)案 1 の製品 P は，管理用サーバにインストールするプログラム H と，PC にインストールするプログラム J で構成されている。問題文中に「S 社 PC と FW1 は，S 社の資産である」とあるように，製品 P を採用すると，委託先の S 社の資産である PC にもプログラム J をインストールする必要があり，資産管理が煩雑になることが問題点として挙げられる。これに対し，案 2 の製品 Q は，管理用サーバにインストールするプログラム K だけで構成されるため，製品 P のように，**委託先 PC にインストールするプログラムの資産管理をせずに済む**。

＜問3＞ Web サイトにおけるインシデント対応

■設問 1

〔試験センターによる解答例〕

a：WebAP サーバ 2

b：WebAP サーバ 1

c：Web サーバ

表 2 より，WebAP サーバ 1 から Web サーバに administrator でログインしていることがわかる。また表 3 より，上記よりも前に WebAP サーバ 2 から WebAP サーバ 1 に administrator でログインしていることがわかる。WebAP サーバ 2 には administrator のログイン履歴がないが，これは下線①にあるように，OS へのログインではなく，サーブレットコンテナの管理画面からログインが成功したためであることがわかる。したがって，ログインされたのは **WebAP サーバ 2→WebAP サーバ 1→Web サーバ**の順である。

■設問 2

〔試験センターによる解答例〕

(1) d：2

e：404

f：14

g：200

(2) No. 3 から 10 までのステータスコードが 401 で失敗を繰り返しており，No. 11 は 200 でログインに成功しているから（58 字）

(1)表 5 で demo ディレクトリに対してリクエストを送っているのは，No.2 と No.14 以降である。**No.2** のステータスコードは **404**（要求されたページが存在しない）であるため，この時点では demo ディレクトリは存在しなかったと判断できる。一方，**No.14** のステータスコードは **200**（リクエストが正常終了）であることから，攻撃者が No.14 の直前で demo ディレクトリを作成したと判断できる。

(2)表 5 を見ると，No.3 から No.10 まで，manager ディレクトリの同じ URL に対するリクエストでステータスコードが 401（認証に失敗）となっており，No.11 では同 URL に対するリクエストのステータスコードが 200（リクエストが正常終了）となっている。また，これらのリクエストは短時間で機械的に繰り返されていることから，よく使われる利用者 ID とパスワードでログインが試行され，その結果ログインが成功したものと推察される。

■設問 3

〔試験センターによる解答例〕

(1) 3，4

(2) 項番：5

サービス：・ファイル共有

・リモートデスクトップ

(1)図 1 より，内部 LAN のネットワークアドレスは 192.168.50.0/24 であり，DB サーバとファイルサーバが稼動していることがわかる。内部 LAN への影響を特定するために，侵入

されたサーバからのアクセスにおいて取得されるログを確認するのであるから，表 6 で該当するのは，送信元が侵入されたサーバ（WebAP サーバ 1，WebAP サーバ 2），宛先が内部ネットワークのサーバ（DB サーバ，ファイルサーバ）となっている**項番 3** と**項番 4** である。

(2)図 1，図 2 と表 6 のフィルタリングルールを一つずつ確認してみると，項番 5 で，運用端末（192.168.90.20）から，DMZ（192.168.0.0/24）と内部 LAN（192.168.50.0/24）に対し「全て」のサービスが許可されている。図 2 を見ると，「運用端末では，ファイル共有とリモートデスクトップのサービスを使用して各サーバを操作できる」とあり，項番 5 の設定は「業務上必要なサービスだけを FW で許可する」というポリシを満たしていないことがわかる。ポリシを満たすには，**項番 5** で許可するサービスを，**ファイル共有**と**リモートデスクトップ**の二つにする必要がある。

■設問 4

〔試験センターによる解答例〕

(a) サーブレットコンテナの管理画面に対するインターネットからの不正アクセス（35 字）

(b) 自動的にログインを行う OS の仕様を利用した，他のサーバへの侵入（31 字）

(a)〔侵入された原因の特定〕にあるように，今回 WebAP サーバに侵入された原因は，設定に誤りがあり，インターネットからサーブレットコンテナの管理画面にアクセスできるようになっていたためである。(a)は，これを防ぐための対策であり，送信元の IP アドレスがループバックアドレス（各サーバ自身を示すアドレス）の場合だけ**サーブレットコンテナの管理画面へのアクセスを許可する**。

(b)A 氏の説明にあるように，攻撃者が失敗することなく短時間で他のサーバへのログインに成功した原因は，全サーバで利用者 ID “unyou”，“administrator” に同じパスワードが設定されていたことで，OS の仕様により自動的にログインが行われていたためである。(b)は，これを防ぐための対策である。