平成28年秋 情報セキュリティ 販売支援システムの情報セキュリティ

問1　販売支援システムの情報セキュリティ（情報セキュリティ）　(H28秋-FE 午後問1)

【解答】

［設問1］　イ
［設問2］　ウ
［設問3］　a－オ，b－エ，c－ウ

【解説】

インターネットを介したWebアプリケーションの利用に向けたセキュリティ設計に関する問題である。具体的に問われたのは出題趣旨にもあるように「サーバの適切な配置及びファイアウォールにおけるフィルタリングの設定を理解する能力や，情報セキュリティの3要素の理解」である。昨今のWebサーバに対する攻撃が増えている実情を踏まえた出題となっている。

ファイアウォールの基本的な設計と，情報セキュリティの3要素を理解していれば，問題文を深く読まずにセキュリティの知識だけで正解できた受験者もいるかもしれない。全問正解も可能であったと思われる。

しかし，セキュリティの基礎知識を使いながら，問題文のヒントを基に正解を導くという解き方を，忘れずに実践していきたい。

［設問1］

Webサーバと DBサーバの配置場所を答える。図1「A社のネットワーク構成」を見ると，DMZに「サーバ群X」，LANに「サーバ群Y」があり，それぞれをどちらに配置するかという組合せを答える形式になっている。

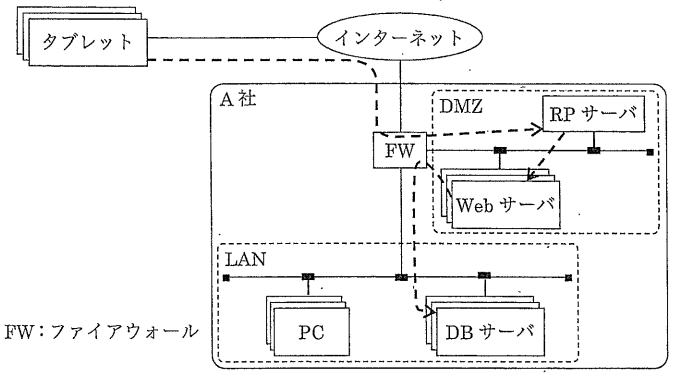
まず，タブレットから販売支援システムにアクセスする通信の流れを確認しよう。流れは，表1「通信経路で利用するプロトコル及び宛先ポート番号」の「通信経路」2行目～4行目を見れば分かる。「タブレット　→　RPサーバ　→　Webサーバ　→　DBサーバ」という流れである。

これを踏まえて，表2「FWにおけるフィルタリングの設定」から，解答を導く。まず，RPサーバからWebサーバの通信を考える。この通信に関して，表2でフィルタリングの設定はない。つまり，この通信はFWを経由しないので，RPサーバとWebサーバは，同一セグメントに設置すべきであるということが分かる。このため，「Webサーバはサーバ群X」に配置される。

次に，WebサーバからDBサーバの通信を考える。この通信に関して，表2では項番2にフィルタリングを許可する設定がある（ただし，この設定は最適ではないので，設問2で改善される）。つまり，この通信はFWを経由するので，WebサーバとDBサーバは別セグメント設置すべきであるということが分かる。このため，「DBサーバはLANのサーバ群Y」に配置される。

これらのことから，（イ）が正解である。

参考までに，配置されたサーバと通信の流れは次のようになる。この内容は，設問2にも関連する



図A　サーバと通信の流れ

［設問2］

設問文にあるように，「表2に示したFWにおけるフィルタリングの設定では，インターネットからDBサーバに直接アクセスされるおそれがある」。その理由は，表2項番2を見ると，「任意」の「送信元」からDBサーバへの通信が「許可」されているからである。そこで，FWで必要最小限の通信に絞る。

それでは，必要最小限の通信とは何か。設問1で解説したように，DBサーバへの通信というのは，「タブレット　→　RPサーバ　→　Webサーバ　→　DBサーバ」という流れである（図A参照）。ここから，DBサーバへの通信は，「Webサーバだけから」ということが分かる。

したがって，（ウ）にあるように「項番2の送信元を“Webサーバ”に変更する」ことがふさわしい。

他の選択肢を見てみよう。

ア：項番2が残ったままなので，この設定を追加しても，悪意のある人によってDBサーバに直接アクセスされることを防ぐことはできない。

イ：（ア）と同じく，項番2が残ったままである。また，この設定を追加すると，Webサーバまでインターネットから直接アクセスされてしまう。

エ：項番2の動作を”拒否”に変更すれば，DBサーバに直接アクセスされることを防ぐことができる。しかし，本来通信すべきWebサーバまでがDBサーバと通信できなくなってしまう。

［設問3］

情報セキュリティの3要素として，「機密性」，「完全性」，「可用性」がある。この内容に関して，総務省は次のように説明している。

> 情報セキュリティという言葉は，一般的には，情報の機密性，完全性，可用性を確保することと定義されています。
> 機密性とは，ある情報へのアクセスを認められた人だけが，その情報にアクセスできる状態を確保すること。完全性とは，情報が破壊，改ざん又は消去されていない状態を確保すること。可用性とは，情報へのアクセスを認められた人が，必要時に中断することなく，情報にアクセスできる状態を確保することをいいます。
> (http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/intro/security/index.html から)

3要素の用語に関する知識があれば，難しくなかったと思われる。

（i）～（vi）を見ていく。

（i）：「DBサーバ中のデータの正規化」……正規化をする主目的は「データの一貫性を保つ」ことである。例えば，「24型テレビ」の料金が，テーブルAとテーブルBで異なるといった不整合をなくすことである。セキュリティとは関係がない。

（ii）：「RPサーバとWebサーバとの間でのHTTPの利用」……セキュリティには関係がない。仮に，HTTPSによる暗号化通信をしているのであれば，機密性に関する内容になる。

（iii）：「Webサーバのクラスタリング」……クラスタリングとは，冗長化技術と考えればよい。例えば，Webサーバの1台が故障しても，もう1台でサービスを提供するということである。これによって，可用性が高まる。空欄cには（ウ）が入る。

（iv）：「コンテンツが改ざんされていないことの定期的な確認」……完全性に関する内容である。空欄bには（エ）が入る。

（v）：「社員IDとパスワードによるログイン」……認証されていない人にアクセスをさせない仕組みである。つまり，不正な第三者に情報を見られないための内容なので，機密性を高める。空欄aには（オ）が入る。

（vi）：「タブレットの利用」……利便性が高まるとは思うが，セキュリティを高める効果はない。むしろ，紛失などのリスクが増えることも考えられる。

まとめると，空欄aには（オ）が，空欄bには（エ）が，空欄cには（ウ）が入る。