●平成26年度秋期

午後問題 解答・解説

問1　ネットワークセキュリティ（情報セキュリティ）　(H26秋-FE 午後問1)

【解答】

［設問1］　ア
［設問2］　a－エ，b－ウ
［設問3］　c－ア
［設問4］　d－イ

【解説】

公開サーバでの会員登録とメールマガジン発行を題材にした，ネットワークセキュリティに関する問題である。設問では，ファイアウォールの設定に関する問題を軸に，会員登録における2段階手順の目的と，SSH（Secure SHell）による安全な通信の仕組みが問われている。

設問だけを読んで正解にたどり着くのは難しく，問題文をきちんと理解する必要がある。特にファイアウォールの設定に関しては，会員登録の流れと照らし合わせて，理解する必要がある。

問題文を読み込む必要はあるが，ネットワークとセキュリティに関する基礎知識があれば，正解が導き出せるように工夫されている。例えば，ファイアウォールのルールの書き方は問題文に解説されているし，プロトコルとそのポート番号も提示されている。セキュリティに関する知識を問われているよりは，実務に合わせて読み解く力，考える力が求められている。

［設問1］

会員登録において，2段階の手順を踏む目的が問われている。正解選択肢を理解するだけでなく，不正解選択肢がなぜ間違いなのかも理解しておこう。

では，選択肢を順に見ていく。

ア：「他人のメールアドレスや間違ったメールアドレスが登録されないようにする」とある。会員登録処理の流れは，(1)の手順で登録希望者がメールアドレスを入力した後，(2)の手順で入力されたメールアドレス宛てにメールを送信している。

このとき，メールが正しく届けば，メールアドレスが間違っていないことの確認ができる。また，他人のメールアドレスを登録した場合，(2)の手順でのメールを受け取れない。よって，他人のメールを登録しても処理ができない。つまり，（ア）の目的が達成できる。

そして，この確認をした上で，(3)の手順にて登録希望者が会員情報を入力する（2段階の手順）。

イ：通信を暗号化するのは，HTTPSによる処理であって，2段階の手順とは関係がない。

ウ：「登録希望者が会員情報DBにアクセスできないようにする」には，DMZとLANを分け，ファイアウォールでアクセス制限をするなどの要件が求められる。2段階の手順とは関係ない。

エ：会員情報は，登録希望者が自ら入力する。残念ながら，その間違いをチェックする処理が問題文に記載されていない。（エ）の要件を実現するのは不可能である。

以上から，（ア）が正解である。

［設問2］

ルータにおけるファイアウォールの設定が問われている。まずは，設定の書き方を問題文から確認しよう。

設問文には「設定は，送信元，送信先，通信ポートの順に“,”で区切って記述する。これは，送信元から送信先の通信ポート宛てのパケットの通過を許可することを意味する」とある。これをきちんと理解した上で，図2を確認する。

空欄a，bだけを考えるのではなく，上から順に確認しておくと，より確実な答えにたどり着ける。順に見ていく。

・1行目 `if0,203.0.113.2,80`
　外部（インターネット）からWebサーバへのWeb閲覧（HTTP通信）を許可する。
・2行目　`if0,203.0.113.3,25`
　外部（インターネット）からメールサーバへのメール送信（SMTP通信）を許可する。
・3行目　`203.0.113.3,if0,25`
　メールサーバから外部（インターネット）へのメール送信（SMTP通信）を許可する。
・4行目　`if2,203.0.113.2,80`
　内部（LAN）からWebサーバへのWeb閲覧（HTTP通信）を許可する。
・5行目　`if2,203.0.113.2,443`
　内部（LAN）からWebサーバへの暗号化されたWeb閲覧（HTTPS通信）を許可する。
・6行目　`if2,203.0.113.3,25`
　内部（LAN）からのメールサーバへのメール送信（SMTP通信）を許可する。
・7行目　`if2,203.0.113.3,110`
　内部（LAN）からのメールサーバに対するメール受信（POP3通信）を許可する。
・8行目　`if0,` [a]
・9行目　`203.0.113.2,` [b]

ここで，問題文の会員登録処理の流れと照らし合わせてみよう。流れの(2)と(5)は，外部へのメール送信なので，3行目のルールが該当する。

しかし，(1)と(3)の外部からWebサーバへのHTTPSの通信と，(4)のWebサーバから会員管理サーバへの通信ルールの記載がない。これが，それぞれ8行目と9行目に該当する。

ここで，空欄aとbに入れる答えを考えよう。

・空欄a：8行目は，(1)と(3)の外部（`if0`）からWebサーバ（`203.0.113.2`）へのHTTPS（443）の通信であるから，次のルールになる。

`if0,203.0.113.2,443`

したがって，空欄aには（エ）が入る。

・空欄b：9行目は(4)のWebサーバ(`203.0.113.2`)から会員管理サーバ(`192.168.0.3`)への通信である。会員情報DBへのアクセスは，表1から独自プロトコルで4194番が待受けポート番号であるから，次のルールになる。

`203.0.113.2,192.168.0.3,4194`

したがって，空欄bには（ウ）が入る。

［設問3］

インターネット経由で，外部のPCからWebサーバにSSHでアクセスするための設定を答える。考え方は設問2と同じであり，ファイアウォールの設定の方法を，問題文の指示どおりにすれば，難しくない。

おさらいであるが，「設定は，送信元，送信先，通信ポートの順に“,”で区切って記述する」とある。送信元は，PCであるから`198.51.100.2`，送信先はWebサーバであるから`203.0.113.2`，通信ポートはSSHであるから22である。よって，（ア）が正解になる。

また，（イ）であっても，メンテナンスは可能であり，要件を満たすことができる。なぜなら，（ア）の設定よりも緩い設定で，送信先を`if0`上のある端末全てに設定しているからである。しかし，これはセキュリティ上よくない。必要最低限のルールにしておかないと，不正に侵入される可能性が出てしまう。よって，（イ）は不正解である。（ウ），（エ）は送信元がPCでないので除外。

なお補足すると，設問文に「SSHサービス」とあるが，これはサーバがSSHの機能をクライアントに提供することである。Linuxなどではsshの機能を提供するソフトであるsshdデーモンのことをサービスといい，設問文のように「SSHサービスを稼働させる」という表現になる。

［設問4］

SSHによる暗号化通信の流れが記載されている。この問題は，単に答えを解くだけに留めるのはもったいない。問題文の内容を理解することで，SSHの仕組みが詳しく分かる。時間があれば，セキュリティの本質を理解するために，丁寧に読んでほしい。現在では，パブリッククラウドサービスなどを利用する場合でもSSHの理解は必須である。なお，問題ではSSHはデフォールトのポート番号22としているが，セキュリティ上攻撃を受けやすいので，知られていない別のポート番号にするのが一般的である。

さて，この問題は，空欄dに入る言葉を解答群の中から選ぶ。設問文には「公開鍵認証方式では，クライアントがサーバのSSHサービスを利用する際に，パスワードや [d] をネットワーク上に流す必要がない」とある。ネットワーク上に流す必要がないということは，機密に管理したいということが分かる。よって，（イ）の「秘密鍵」が答えと想像がついた人もいるだろう。公開鍵は公開するものであるから，わざわざ機密にする必要がない。

しかし，答えにアタリを付けるのは悪くないが，設問文から丁寧に確認して答えを導き出すことも大切である。

設問文をよく読んで解答を導き出そう。(1)～(3)のやり取りの中で，ネットワークに情報を流しているのは(1)だけである。しかも，その情報は「公開鍵をサーバに送る」とあることから，「公開鍵」だけである。このことから，「公開鍵」が含まれている選択肢（ア）と（ウ）は不正解になる。そして，「秘密鍵」をネットワーク上に流すという記述がないことから，（イ）の「秘密鍵」が正解であることが分かる。