問1　テレワークの導入（情報セキュリティ）　(R1秋-FE 午後問1)

【解答】

［設問1］　a－エ，b－オ
［設問2］　オ
［設問3］　イ

【解説】

テレワークの導入をテーマに，リモートアクセスを安全に行うための技術であるVPN及びVDIについての出題である。問題文が長く，図や表も多いため，読むだけで予想以上に時間を使ってしまった受験者もいたことであろう。また，基本的な用語やIPアドレス，ファイアウォールに関する知識も必要になる。

設問1で登場する192.168.64.0/23は，192.168.64.0/24（事務VM）と192.168.65.0/24（開発VM）の二つのネットワーク空間を一つの表現としてまとめたものを意味する。これは基本情報技術者試験の受験者には馴染みがなく，ネットワーク技術者が実践の場で多用する表現方法であり，ファイアウォール装置の設定における書式でもある。

［設問1］

表1「A社FWに設定するパケットフィルタリングのルール表」の次の記述に「表1のルール案ではルール番号7の条件に誤りがあり」とある。そこで，ルール番号7を確認する。

表A　ルール番号7

ルール番号	送信元	宛先	サービス	動作
7	192.168.64.0/23	192.168.128.0/20	HTTPS，SSH	許可

送信元は，192.168.64.0/23である。これは192.168.64.0/24（事務VM）と192.168.65.0/24（開発VM）の二つのネットワークを意味する。

この点は，IPアドレス，及びサブネットの知識があれば理解できるが，念のため確認しておこう。

〔192.168.64.0/24のネットワーク〕

IPアドレスの範囲は，192.168.64.0～192.168.64.255である。これを2進数で表してみよう。

10進数		2進数	
192.168.64. 0	→	11000000 10101000 00100000	00000000
～			
192.168.64.255	→	11000000 10101000 00100000	11111111

サブネットは/24なので，24ビット目までが共通である。

ネットワーク部は，24ビット目より後ろ全てを0にした192.168.64.0である。

〔192.168.65.0/24のネットワーク〕

IPアドレスの範囲は，192.168.65.0～192.168.65.255である。こちらも2進数で表してみよう。

10進数		2進数	
192.168.65. 0	→	11000000 10101000 00100001	00000000
～			
192.168.65.255	→	11000000 10101000 00100001	11111111

ネットワーク部は，24ビット目より後ろ全てを0にした192.168.65.0である。

ここで，192.168.64.0/24（事務VM）と192.168.65.0/24（開発VM）の二つのネットワークを合わせた場合，IPアドレスの範囲は，192.168.64.0～192.168.65.255になる。2進数で表すと，次のようになる。

10進数		2進数	
192.168.64. 0	→	11000000 10101000 0010000	0 00000000
～			
192.168.65.255	→	11000000 10101000 0010000	1 11111111

23ビット目までが共通なので，サブネットは/23である。

ネットワーク部は，23ビット目より後ろ全てを0にした192.168.64.0である。

このことから，192.168.64.0/24（事務VM）と192.168.65.0/24（開発VM）の二つのネットワークを合わせると，192.168.64.0/23になる。

宛先の192.168.128.0/20は，開発サーバのネットワークである。また，サービスはHTTPSとSSHを許可している。

では，このルールのどこが誤っているのか。問題文から誤っている部分を探せば，それが空欄aの答えである。また，その部分を正しく変更すれば，空欄bの答えを導くことができる。

・空欄a：問題文には，「A社FWでは，開発室のネットワークだけから開発サーバにHTTP over TLS（以下，HTTPSという）又はSSHでアクセスできるように通信を制限している」とある。しかし，ルール番号7では，「開発VM（192.168.65.0/24）」だけでなく，「事務VM（192.168.64.0/24）」からも通信が許可されてしまう。この点が問題である。

したがって，（エ）の「事務VMから開発サーバにアクセスできる」が正解である。

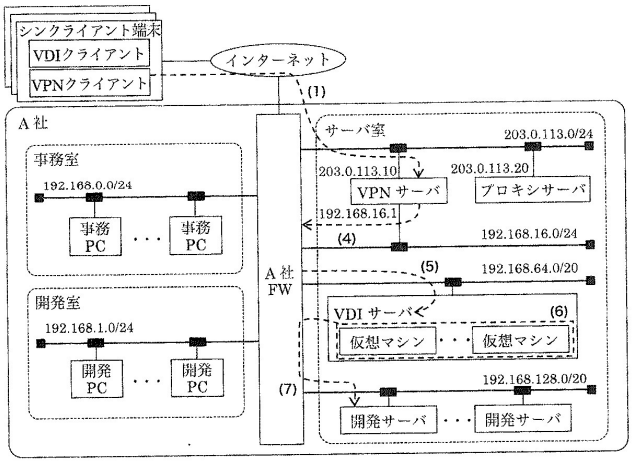
・空欄b：この誤りを修正する方法か，「開発サーバに対するアクセスを正しく制限するために，ルール番号7の条件について，送信元を［ b ］に変更した」である。送信元を開発VM（192.168.65.0/24）だけに限定すればよい。したがって，正解は（オ）である。

［設問2］

シンクライアント端末から開発サーバにアクセスするときの接続経路を答える。問題文と図2「テレワーク導入後のA社のネットワーク構成案」を照らし合わせて読んでいく。

〔A社が検討したテレワークによる業務の開始までの流れ〕に関して，接続経路に関する内容を抜粋したものが，次の(1)，(4)～(7)である。図2に(1)，(4)～(7)を対応させたものが図Aである。

(1)　シンクライアント端末のVPNクライアントを起動して，VPNサーバに接続する。
(4)　VPNクライアントは，VPNサーバ経由でA社のネットワークに接続する。
(5)　VDIクライアントを起動して，VDIサーバに接続する。
(6)　VDIサーバは，仮想マシンを割り当てる。
(7)　利用者は，仮想マシンにログインして業務を開始する。→つまり，開発サーバにアクセスできる。



図A　接続経路

このように，図に接続経路を書き込むことで正解を導くことができる。シンクライアント端末から開発サーバへの接続経路は図Aのようになり，シンクライアント端末 → VPNサーバ → VDIサーバ → 仮想マシン（開発VM）→ 開発サーバ という経路を通る。したがって，（オ）が正解である。

［設問3］

設問文が長いが，「事務PC及び開発PCからも仮想マシンを使用したい」という要望を実現するためのルールを考える。

事務室のセグメントは192.168.0.0/24，開発室のセグメントは192.168.1.0/24であり，両者を併せて192.168.0.0/23になる。設問1の解説と同様に，これが送信元のセグメントになる。また，仮想マシンのセグメントは，192.168.64.0/20であり，これが宛先のセグメントである。利用用途は「仮想マシンを使用」であるから，サービスを「VDI」にする。もちろん，動作は「許可」とする。

したがって，（イ）の「ルール番号3と4の間に，送信元を192.168.0.0/23，宛先を192.168.64.0/20，サービスをVDI，及び動作を許可とするルールを新たに挿入する必要がある」が正解である。

「ルール番号3と4の間」と記述されているが，ここに限定される必要はない。つまり，別のルール番号に追加してもよい。ルール番号3にVDIを許可するルールがあるので，分かりやすいようにここに配置していると考えられる。

他の選択肢も見ておこう。

ア：変更する必要があるので適切ではない。

ウ：このルールは，仮想マシンから事務PCや開発PCへの通信を許可するものである。通信の流れが逆である。注記2に，「許可された通信に対する戻りのパケットは，無条件に許可される」とある。（イ）のルールを追記すれば，このルールを追記する必要はない。

エ：このルールはインターネットからの接続のルールである。今回は，A社内の「事務PC及び開発PCからも仮想マシンを使用したい」という要望であるため，適切ではない。