問4　ネットワークの障害分析と対策（ネットワーク）　（H30 秋-FE 午後問 4）

【解答】

［設問］　a－イ，b－オ（順不同）
　　c－ウ
　　d－ア，e－カ（順不同）

【解説】

本問は，最初にネットワーク構成図とネットワーク構成の問題文があり，〔障害の発生〕，〔セグメントの追加〕，〔障害発生の予防〕と続き，空欄が設けられている。

〔障害の発生〕では，障害発生のシチュエーションが示され，障害箇所を特定するために試行した結果から原因を特定する。〔セグメントの追加〕では，セグメントの追加の内容とそれに伴って設定したファイアウォールについて，その設定誤りから発生する事象を解答する。〔障害発生の予防〕では，ルータの増設の二つの構成案から構成案1を採用した理由を解答する。

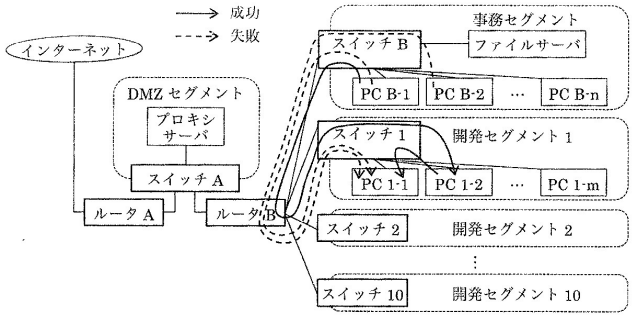
［設問］

最初の〔障害の発生〕に，「ある日，“事務セグメント内の PC B-1 から，リモートデスクトップ機能を用いて，開発セグメント 1 内の PC 1-1 を遠隔操作しようとしたが，接続できなかった”と報告があった」という記述があり，この障害の報告から二つの試行をしている。

① 事務セグメント内の PC B-2 から，PC 1-1 にリモートデスクトップ機能を用いて接続を試みたが，失敗した。
② 事務セグメント内の PC B-1 から SSH を用いてログインした開発セグメント 1 内の PC 1-2 で ping コマンドを実行し，PC 1-1 から応答が返ってくることを確認した。

障害内容と①と②の結果をネットワーク構成図上に表現すると図 A になる。

②の成功から，PC B-1 から PC 1-2 までの経路上の機器と PC 1-2 から PC 1-1 までの経路上の機器は OSI 参照モデルのネットワーク層レベルの問題がないことが分かる。障害の発生内容と①の失敗から，リモートデスクトップ接続で利用しているプロトコルが，経路上もしくは PC 1-1 で受け付けられなくなっていると推測できる。具体的には，ネットワーク構成の(6)に「ルータ B は，内蔵のパケットフィルタ型のファイアウォール機能によってセグメント間の通信の可否を制御しており」とあるように，ファイアウォール設定ができるルータ B，もしくは PC 1-1 上で動作しているリモートデスクトップ接続サービスのいずれかとなる。空欄 a，b の解答群では（イ）の「PC 1-1 のソフトウェア」，（オ）の「設定を含むルータ B のソフトウェア」が該当するので，（イ）と（オ）が障害の原因と考えられる不具合であり，解答となる。



図A　G社のネットワーク構成と障害

次の〔セグメントの追加〕では，開発セグメント 11 を追加し，ルータ B に対してファイアウォールの設定を追加したが誤りがあり，それに関することを空欄 c で解答する。このファイアウォール設定に必要な事項については，ネットワーク構成の(3)，(4)に記述されている。

(3) 事務セグメント内の PC は，リモートデスクトップのクライアント機能又は SSH を用いて，開発セグメント内の PC を遠隔操作できる。
(4) 開発セグメント内の PC は，事務セグメント内のファイルサーバにアクセスできる。

(3)，(4)からルータ B に設定すべきファイアウォールの設定は表 A のようになる。網掛け部分は，開発セグメント 11 内の PC から事務セグメント内のファイルサーバにアクセスできるようにする，送信元ネットワークと宛先ネットワークの設定である。この部分が表 1 では逆に設定されているため，アクセスできない。したがって，（ウ）の「当該 PC から事務セグメント内のファイルサーバにアクセスできない」が解答になる。

表A　ルータ B に追加すべきファイアウォールの設定

送信元ネットワーク	宛先ネットワーク	ポート番号（サービス）	可否
10.1.11.0/24	10.0.0.0/16	445（ファイル）	可
10.0.0.0/16	10.1.11.0/24	22（SSH）	可
10.0.0.0/16	10.1.11.0/24	3389（リモートデスクトップ）	可

最後の〔障害発生の予防〕では，ルータ C を増設することでルータ B の負荷を分散させることを目的に構成案 1 と構成案 2 が検討され，最終的に構成案 1 を採用することになった。ここで構成案 1 を採用するときに重視した点を，空欄 d，e として解答する。（ア）～（カ）について，構成案 1 と構成案 2 を比較してみる。

ア：「可用性を高められる」……構成案 1 ではルータ B，ルータ C のどちらかが故障しても，もう一方が動作していれば通信は継続できるので可用性を高められる。構成案 2 ではルータ B が故障した場合は事務セグメントとインターネット間の通信ができなくなり，ルータ C が故障した場合は事務セグメントと開発セグメント間の通信ができなくなる。このため，構成案 1 の方が可用性を高められる。

イ：「機密性を高められる」……どちらの構成案でも機密性を高めることはできない。

ウ：「障害発生時に原因を特定しやすい」……構成案 2 では何らかの障害が発生した場合にルータ B，ルータ C のどちらの経路で障害が発生したのか，原因を特定しやすいが，構成案 1 では構成案 2 に比べてルータ B，ルータ C のどちらの経路で障害が発生したのか，原因を特定しにくい。

エ：「セグメント間で通信する際に経由する機器が少なくなる」……セグメント間の通信で許可されているものは，事務セグメントと DMZ セグメント，事務セグメントと開発セグメント 1～11 であり，どちらの構成案でも経由する機器の数は同じである。

オ：「ルータ B，C とスイッチ間をつなぐ LAN ケーブルの本数が少なくて済む」……図 2 から，スイッチ 1～11 の接続について考えみる。構成案 1 ではスイッチ 1～11 がルータ B にもルータ C にも接続されている。構成案 2 ではルータ C だけに接続されている。このことから考えても，LAN ケーブルの本数が少なくて済むのは構成案 2 である。

カ：「ルータ B とルータ C の負荷に大きな差が生じないように調整できる」……構成案 1 はルータ B とルータ C の役割が同じであるため，負荷の調整はできる。構成案 2 はインターネットとの通信と開発セグメントとの通信で負荷の差があれば，そのままルータ B とルータ C の負荷の差が生じる。

これらの比較結果から，構成案 1 を採用するときに重視したのは，（ア）と（カ）の二つである。