平29　高等学校情報（6枚のうち1）

（解答はすべて、解答用紙に記入すること）

Ⅰ　次の各問いに答えなさい。

1　HDMIの説明として，適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　映像，音声及び制御信号を1本のケーブルで伝送するインタフェースである。

イ　携帯電話間での情報交換などで使用される赤外線を用いたインタフェースである。

ウ　外付けハードディスクなどをケーブルで接続するシリアルインタフェースである。

エ　多少の遮へい物があっても通信可能な，電波を利用した無線インタフェースである。

2　音響データのサンプリング（標本化）に関する記述について，適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　音量を上げてサンプリングすると，データの量は増加する。

イ　サンプリング周波数とサンプリングのビット数を同一にしたまま，符号化方式をステレオからモノラルに変更すると，データ量は1／4になる。

ウ　サンプリング周波数を11kHzから22kHzにすると，データ量は2倍になる。

エ　サンプリング周波数を低くすると，得られるデータの音程は原音よりも低くなる。

3　10進数0.625を2進法に変換した値を次のア～エの中で適切なものを1つ選び，その符号を書きなさい。

ア　0.110　　イ　0.111　　ウ　0.101　　エ　0.1011

4　フィルタリングで閲覧を不可とするWebサイトやカテゴリを指定して，閲覧を制限する方法を何というか。適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　ブラックリスト方式　　イ　パターンマッチング方式　　ウ　ホワイトリスト方式　　エ　水平負荷分散方式

5　ランサムウェアの説明として，適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　ワープロソフトや表計算ソフトの文書ファイルに感染する。

イ　PCやファイルを使用不能にするなどして，回復のための金銭を要求する。

ウ　利用者がキーボードから入力した情報を記録し，外部に送信する。

エ　ウイルスなどを検知して，コンピュータを脅威から守り，安全性を高めるソフトウェアの総称。

6　物品の形状，模様，色彩など，ものの外観としてのデザインを保護するための権利として，最も適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　特許権　　イ　意匠権　　ウ　実用新案権　　エ　商標権

7　IPv6で扱えるアドレスの個数を次のア～エから1つ選び，その符号を書きなさい。

ア　2^{32}個　　イ　2^{64}個　　ウ　2^{100}個　　エ　2^{128}個

8　ネットワークを介して商品やサービスを取引することを電子商取引というが，顧客と顧客がネットオークションを利用した個人間のやりとりなどをする形態として適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　B to B　　イ　P to P　　ウ　B to C　　エ　C to C

9　ある携帯電話会社のパケット通信料は，1パケットが128バイトであり，税込みで0.05円，また1パケットの中に入っているヘッダが28バイトである。この条件で，携帯電話によりWebページから500Kバイトの画像データをダウンロードしたとき，理論上パケット通信料はいくらになるか。次のア～エの中から1つ選び，その符号を書きなさい。ただし，1Kバイト＝1,024バイトとする。

ア　128円　　イ　256円　　ウ　512円　　エ　1,024円

10　データベースの論理的構造を規定した論理データモデルのうち，関係データモデルの説明として適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　データとデータの処理方法を，ひとまとめにしたオブジェクトとして表現する。

イ　データ同士の関係を網の目のようにつながった状態で表現する。

ウ　データ同士の関係を木構造で表現する。

エ　データの集まりを表形式で表現する。

平29　高等学校情報（6枚のうち2）

（解答はすべて、解答用紙に記入すること）

Ⅱ　文字列を圧縮するアルゴリズムに関する次の文章と図1，図2をもとに，あとの問いに答えなさい。

文字列を圧縮するアルゴリズムとして，同じ文字データが連続して現れる箇所を，その文字データと連続している回数との組に変換して表す方法がある。以下に，文字列を圧縮する方法として，圧縮の表現形式の異なる2つの方法を比較する。

［圧縮方法1］

圧縮の表現形式として，［圧縮対象文字］［連続回数］を用いる方法である。例えば，文字列「ABBBBCCCCCDD」を圧縮すると「A1B4C5D2」と表す。これは，Aが1回，次にBが4回，Cが5回，さらにDが2回続いていることを表している。

例えば，［圧縮方法1］で文字列「ABBBBBCCDEFFFF」を圧縮した場合の結果は，「（　a　）」となり，圧縮前のデータより圧縮後のデータの方が小さくなることがわかる。しかし，文字列「ABCDDDDEF」を圧縮した場合の結果は，「（　b　）」となり，圧縮前のデータより圧縮後のデータの方が逆に大きくなってしまう。このことから，［圧縮方法1］を用いた場合，①文字列によっては，圧縮後のデータが圧縮前のデータより最大で（　c　）倍になってしまうことがある。

そこで，これを防ぐ方法の一つとして，ある一定の数だけ同じ文字データが繰り返した場合にのみ圧縮を行う以下の方法を考える。

［圧縮方法2］

圧縮の表現形式として，同じ文字データが4回以上連続する場合に［圧縮表現文字］［圧縮対象文字］［連続回数］を用いる方法であり，同じ文字データの連続が3回以下の場合は，変換せずそのままとする方法である。例えば，文字列「ABBBBCCCCCDD」を圧縮すると「A*B4*C5DD」と表す。なお，圧縮表現文字は「*」で表すものとする。

例えば，［圧縮方法2］で文字列「ABCDDDDEF」を圧縮した場合の結果は，「（　d　）」となり，圧縮前のデータより圧縮後のデータが小さくなることがわかる。

次に，［圧縮方法2］によって文字列を圧縮するアルゴリズムを＜アルゴリズムA＞，［圧縮方法2］によって圧縮された文字列を圧縮前の文字列に戻すためのアルゴリズムを＜アルゴリズムB＞とし，以下に示す手順で行うものとする。ただし，圧縮前と圧縮後のデータは，配列を用いて管理する。圧縮前のデータを配列Tに，圧縮後のデータを配列Pに，圧縮前に戻したデータを配列Lに格納する。各配列はデータを格納する十分な領域が確保されているものとし，配列の各要素には，文字データの場合は8ビット表現の文字コードが，数値データの場合は0～255の整数が格納されるものとする。ただし，配列T，配列P，配列Lの添字は0から始まり，配列内の文字列の最後には「@」が格納されることとする。

＜アルゴリズムA＞

(i)　図1のように配列Tに格納されている文字列を先頭からコピーして配列Pを作成する。このとき，配列Tに格納された文字列中に，同じ文字が連続して4個以上出現したときだけ，「*」と文字と文字数の3要素に置き換え，配列Pにコピーする。

(ii)　(i)の操作を，配列Tの要素に「@」が現れるまで繰り返し，配列Pを作成する。

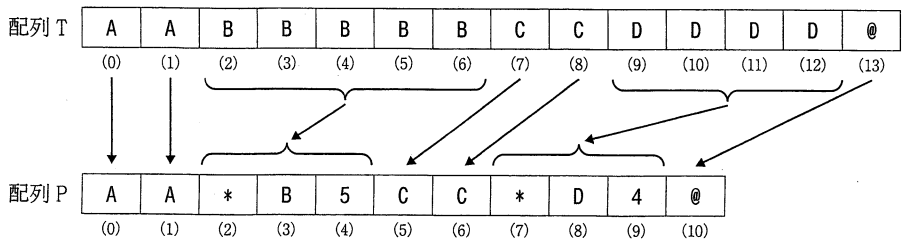


図1

＜アルゴリズムB＞

(i)　図2のように＜アルゴリズムA＞によって圧縮された配列Pに格納されている各要素を先頭からコピーして配列Lを作成する。このとき，配列Pに格納された文字列中に「*」を発見したとき，＜アルゴリズムA＞の(i)の手順の逆を行い，配列Lにコピーする。

(ii)　(i)の操作を，配列Pの要素に「@」が現れるまで繰り返し，配列Lを作成する。

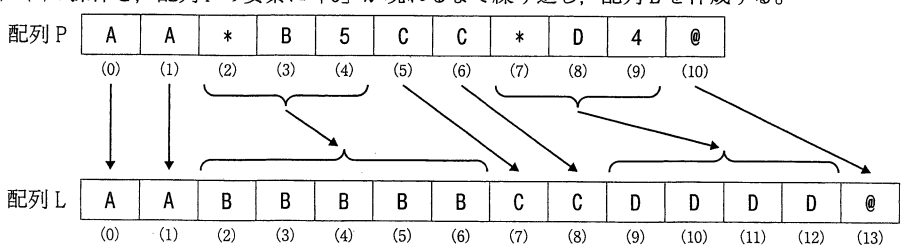


図2

平29　高等学校情報（6枚のうち3）

（解答はすべて、解答用紙に記入すること）

以下は，＜アルゴリズムA＞と＜アルゴリズムB＞を記述形式に従い表したプログラムである。

＜アルゴリズムA＞

```
・配列Tに文字列を読み込む
・i ← 0
・k ← 0
■ T[i] ≠ "@"
  ・hozon ← T[i]
  ・n ← 0
  ■
    ・i ← i + 1
    ・n ← n + 1
  ■ T[i] = hozon
    e
    ■ n ≠ 0
      ・P[k] ← hozon
      ・k ← k + 1
      ・n ← f
    ■
  ・P[k] ← "*"
  ・P[k + 1] ← hozon
  ・P[k + 2] ← n
  ・k ← g                ⇦ α
■
・P[k] ← "@"
```

＜アルゴリズムB＞

```
・i ← 0
・k ← 0
■ P[i] ≠ "@"
  ▲ P[i] = "*"
    ・hozon ← P[i + 1]
    ・n ← 1
    ■ n ≦ P[i + 2]
      ・L[k] ← hozon
      ・k ← k + 1
      ・n ← h
    ■
    ・i ← i + 3
  ・L[k] ← P[i]
  ・k ← i
  ・i ← i + 1
■
・L[k] ← "@"
```

［記述形式の説明］

記述形式		説明
処理	・変数←式	変数に式の値を代入する。
	▲条件式 ・処理 ▼	単岐選択処理を示す。 条件式が真のときは処理を実行する。
	▲条件式 ・処理1 ・処理2 ▼	双岐選択処理を示す。 条件式が真のときは処理1を実行し，偽のときは処理2を実行する。
	■条件式 ・処理 ■	前判定繰り返し処理を示す。 条件式が真の間，処理を繰り返し実行する。
	■ ・処理 ■条件式	後判定繰り返し処理を示す。 処理を実行し，条件式が真の間，処理を繰り返し実行する。

1　文中の空欄（　a　）～（　d　）に入る適切な語句を書きなさい。

2　［圧縮方法1］の説明文の下線部①とはどのような文字列の場合であるか，次のア～エから1つ選び，その符号を書きなさい。

ア　ABCABC　　イ　AABBCC　　ウ　AAABBB　　エ　AAAAAA

3　＜アルゴリズムA＞と＜アルゴリズムB＞の空欄 e ～ i に入る適切なものを，それぞれ次のア～コから1つ選び，その符号を書きなさい。

ア　n＜3　　イ　n＜4　　ウ　n＋1　　エ　n－1　　オ　k＋1

カ　k－1　　キ　k＋2　　ク　k－2　　ケ　k＋3　　コ　k－3

4　次の配列Tを＜アルゴリズムA＞により圧縮した場合，点線囲み部分 α を何回処理するか書きなさい。

配列T	A	A	A	A	B	B	C	C	C	D	D	D	D	D	@
	(0)	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)

Ⅲ　次の事例をもとに情報セキュリティに関する教材を作成した。あとの問いに答えなさい。

日ごろ忙しいAさんは，ネットショッピングをよく使っています。ある日Aさんは，野球観戦のチケットを購入しようとオンラインショップで検索しましたが，多くのショップが売り切れとなっていました。さらにAさんは，ネットを検索し続け，そのチケットについて「在庫あり」と表示しているショップをやっと見つけました。

Aさんは，そのチケットをすぐに購入カートに入れ，(x) URLの最初の部分が「https://」となっているクレジットカードの情報を入力する決済のページに進みました。すると，「(y)このWebサイトのセキュリティ証明書には問題があります」という警告画面が出てきました。Aさんは，この警告画面を見て，どうしようか迷いましたが，せっかく見つけたチケットが売り切れてしまっては困ると思い，警告を無視して，クレジットカードの情報を入力し，決済を完了させてしまいました。

しかし，それから何日経ってもチケットは届きません。しかも，身に覚えのない購入履歴が記載されたクレジットカードの請求書が届くようになりました。Aさんは，野球観戦チケットを買ったオンラインショップが怪しいと思い，そのチケットを買ったサイト運営者の連絡先を探しましたが，どこにも記載されていませんでした。

1　下線部(x)に関する通信について，適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　HTTPによる通信を二重化して可用性を高めるためのプロトコルである。

イ　HTTPよりも通信手順を簡略化するためのプロトコルである。

ウ　Webを使った商取引の成立を保証するためのプロトコルである。

エ　通信内容を暗号化するためのプロトコルである。

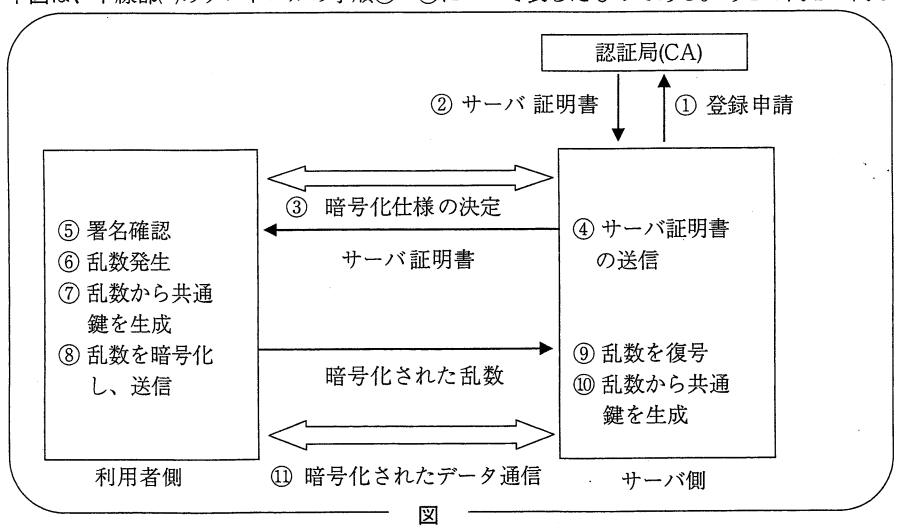
平29　高等学校情報（6枚のうち4）

（解答はすべて、解答用紙に記入すること）

2　下線部(x)に関する通信のプロトコルを何といいますか。適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　SMTP　　イ　POODLE　　ウ　SSL/TLS　　エ　SSH

3　下図は、下線部(x)のプロトコルの手順①～⑪について表したものである。あとの問1～問6に答えなさい。



図

①　サーバを運用している会社は，認証局にサーバ証明書の交付を申請する。
②　認証局は申請された会社の実在性を確認し，サーバ証明書を発行する。サーバ証明書には（　1　）などが含まれている。
③　利用者側が利用できる暗号化の仕様リストから暗号化仕様を決定する。
④　認証局から送られてきたサーバ証明書を利用者に送る。
⑤　利用者は送られてきたサーバ証明書の署名を（　2　）で復号し，署名の検証を行い，サーバ証明書が正しいことを確認する。
⑥　利用者側で乱数を発生させる。
⑦　⑥の乱数から共通鍵を生成する。
⑧　⑥の乱数を（　3　）で暗号化し，送信する。
⑨　暗号化された乱数を（　4　）で復号する。
⑩　サーバ側で乱数から共通鍵を生成する。
⑪　通信文を（　5　）で暗号化し，送受信する。

問1　空欄（　1　）にあてはまる言葉を次のア～エから1つ選び，その符号を書きなさい。

ア　サーバの公開鍵，認証局の公開鍵で暗号化した署名
イ　サーバの公開鍵，認証局の秘密鍵で暗号化した署名
ウ　サーバの秘密鍵，認証局の公開鍵で暗号化した署名
エ　サーバの秘密鍵，認証局の秘密鍵で暗号化した署名

問2　空欄（　2　）～（　5　）にあてはまる言葉を次のア～コからそれぞれ1つ選び，その符号を書きなさい。

ア　サーバ　　イ　サーバの公開鍵　　ウ　サーバの秘密鍵　　エ　認証局　　オ　認証局の公開鍵
カ　認証局の秘密鍵　　キ　利用者　　ク　利用者の公開鍵　　ケ　利用者の秘密鍵　　コ　共通鍵

問3　公開鍵を使って暗号化して，N人が相互に通信する場合，全体で必要となる異なる鍵の数を次のア～エから1つ選び，その符号を書きなさい。ここで，ひと組の鍵は2個と数える。

ア　N+1　　イ　$N(N-1)/2$　　ウ　$\log_2 N$　　エ　2N

問4　公開鍵暗号方式の暗号アルゴリズムを次のア～エから1つ選び，その符号を書きなさい。

ア　ＡＥＳ　　イ　ＤＥＳ　　ウ　KCipher-2　　エ　ＲＳＡ

問5　⑤では，ハッシュ関数SHA-256を使用してサーバ証明書からメッセージダイジェスト作成し，署名を復号した値との検証を行っている。このハッシュ関数SHA-256を用いて，64ビット，256ビット，1,024ビットの三つの長さのメッセージからハッシュ値を求めたとき，それぞれのメッセージのハッシュ値の長さはどれか。次のア～エから1つ選び，その符号を書きなさい。

メッセージ長さ		64	256	1,024
ハッシュ値	ア	64	256	256
	イ	64	256	1,024
	ウ	256	256	256
	エ	256	256	1,024

問6　⑤の検証で発見できないものを，次のア～ウから1つ選び，その符号を書きなさい。

ア　盗聴　　イ　改ざん　　ウ　なりすまし

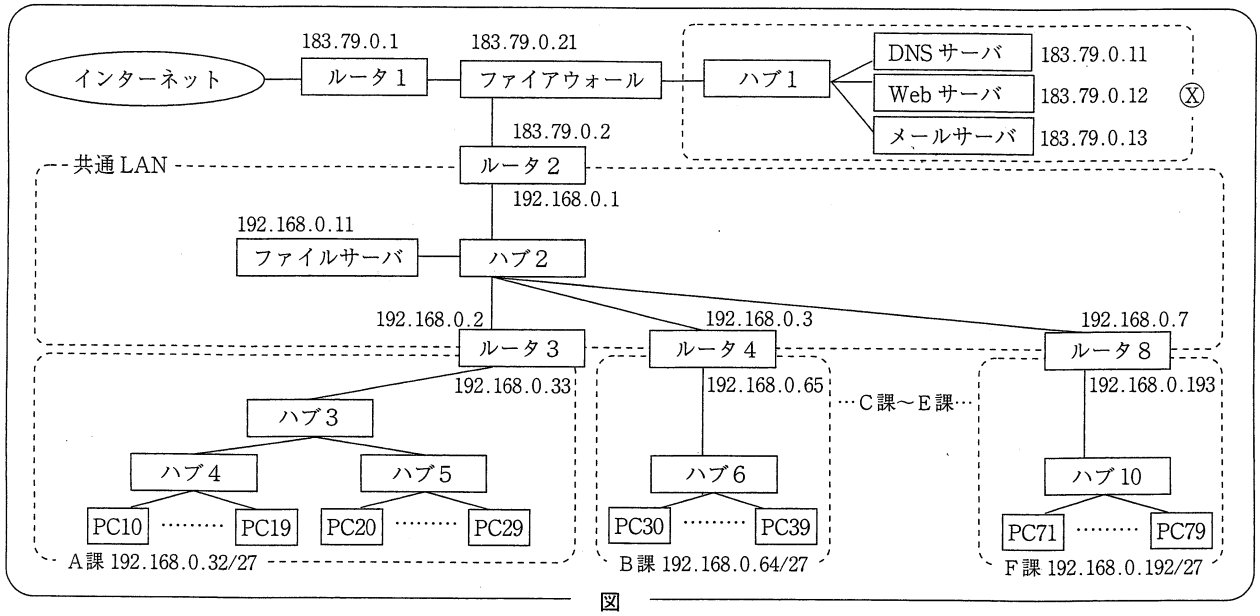
4　下線部(y)の警告が表示された証明書は，特定の認証局が発行したCRLに登録されたものであった。CRLについて，適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　CRLには，有効期限内のディジタル証明書のうち破棄されているディジタル証明書と破棄された日時の対応が提示されている。
イ　CRLには，失効されたディジタル証明書に対応する秘密鍵が登録されている。
ウ　CRLは，鍵の漏えい，破棄申請の状況をリアルタイムに反映するプロトコルである。
エ　CRLには，所有者が新たなディジタル証明書を取得するまでの間，有効期限切れで失効したディジタル証明書が登録される。

平29　高等学校情報（6枚のうち5）

（解答はすべて、解答用紙に記入すること）

Ⅳ　下図は，ある企業のネットワーク構成図である。このネットワークは，外部から直接アクセスできる機器と，アクセスできない機器に分割されている。また，サブネットを利用して，共通LANとA課～F課の各課のネットワークは、それぞれ別のネットワークに細分化されている。あとの問いに答えなさい。



図

1　図中Ⓧの領域の名称をアルファベット3文字で書きなさい。

2　DNSサーバの役割として適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　異なるプロトコルどうしの通信を可能にする。
イ　ドメイン名とIPアドレスを対応付ける。
ウ　ネットワーク内で重複しないIPアドレスをクライアントに割り振る。
エ　プライベートアドレスをグローバルアドレスへ変換する。

3　文字，画像，レイアウト情報などを一元的に保存・管理し，HTML言語などの専門知識がない利用者でもWebによる情報発信が容易にできるようにしたシステムの略称を次のア～エから1つ選び，その符号を書きなさい。

ア　CMS　　イ　CSS　　ウ　CSV　　エ　CVS

4　図の設定の場合，A課においてPCに設定できるホストアドレスの最大数を求めなさい。

5　A課のPCに設定するサブネットマスクの値として適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　255.255.255.0　　イ　255.255.255.192　　ウ　255.255.255.224　　エ　255.255.255.248

6　B課のPCに設定するゲートウェイの値として適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　183.79.0.1　　イ　183.79.0.11　　ウ　192.168.0.33　　エ　192.168.0.65

7　B課のPCに設定できるIPアドレスの値として適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　192.168.0.64　　イ　192.168.0.80　　ウ　192.168.0.95　　エ　192.168.0.100

8　業務に関係のないメールが多く届くようになったため，メールサーバを調査したところ，**表1**の調査結果が得られた。ファイアウォールのフィルタリング制御で，送信元IPアドレス「220.110.64.0/18」から届くメールを遮断する設定を行った場合，**表1**で遮断されるメールの総数を求めなさい。

表1　調査結果

送信元IPアドレス	メール数	送信元IPアドレス	メール数
220.110.81.10	90	220.110.65.20	50
220.110.97.30	60	220.110.145.1	20
220.110.225.2	50	220.110.113.3	80

9　各課のPC5台ずつ計30台に，新規のソフトウェアを一括して購入したい。**表2**の購入方法がある場合，最も安く購入できる合計金額として適切なものを次のア～エから1つ選び，その符号を書きなさい。ここで，各課には1冊のマニュアルを必要とする。なお，購入にあたって，ライセンスやマニュアルに余りが生じてもよい。

表2　購入方法

	ライセンス	マニュアル	金額（円）
製品パッケージ版	1	1	15,000
ダウンロード版A	2	0	24,000
ダウンロード版B	5	0	45,000

ア　270,000　　イ　315,000　　ウ　318,000　　エ　330,000

10　F課では，無線LANを構築することになり，無線アクセスポイントの存在を他者に見られないように設定を行った。この機能について適切なものを次のア～エから1つ選び，その符号を書きなさい。

ア　ビームフォーミング　　イ　暗号化　　ウ　ステルスSSID　　エ　MACアドレスフィルタリング

11　A課のPC10からファイルサーバへ，突然接続できなくなった。同課のPC20からファイルサーバへは正常に接続できている。このとき，通信経路の観点から障害箇所の疑いとして考えられるものを次のア～シからすべて選び，その符号を書きなさい。ただし，PC10本体は正常に稼働している。

ア　ハブ2　　イ　ハブ3　　ウ　ハブ4　　エ　ハブ5　　オ　ファイルサーバとハブ2の間のケーブル
カ　ルータ3　　キ　ハブ2とルータ3の間のケーブル　　ク　ルータ3とハブ3の間のケーブル
ケ　ハブ3とハブ4の間のケーブル　　コ　ハブ3とハブ5の間のケーブル　　サ　ハブ4とPC10の間のケーブル
シ　ハブ5とPC20の間のケーブル