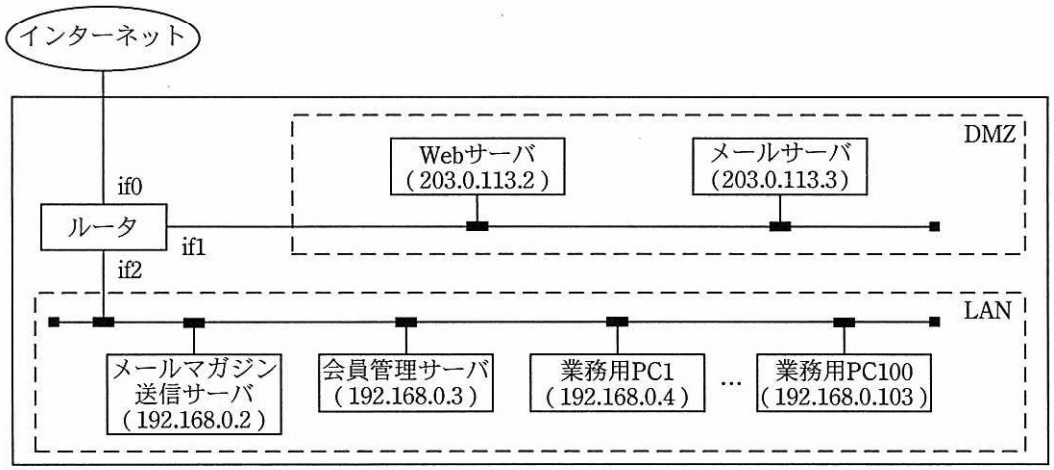
次の問1は必須問題です。必ず解答してください。

問1　ネットワークセキュリティに関する次の記述を読んで，設問1～4に答えよ。

A社は，社内に設置したWebサーバ上に，自社の製品を紹介するWebサイトを構築し，運営している。A社は，このWebサイトで会員登録を受け付け，登録された会員に対してメールマガジンを発行している。

A社のネットワーク構成を，図1に示す。



注記1　カッコ内は各機器のIPアドレスを表す。
注記2　if0，if1及びif2はルータのネットワークインタフェースを表す。

図1　A社のネットワーク構成

会員登録処理の流れは次のとおりである。

(1)　登録希望者は，インターネットを介し，Webサーバが管理する入会申込用Webページに HTTP over SSL/TLS（以下，HTTPSという）でアクセスし，メールアドレスを入力する。

(2)　Webサーバは，登録希望者ごとに，登録希望者専用の会員情報入力用Webページを生成し，そのURLを記載した電子メール（以下，メールという）を，入力されたメールアドレス宛てに送信する。

(3)　登録希望者は，(2)で送信されたメールに記載されたURLが示すWebページ

に HTTPS でアクセスして，氏名や職業などの会員情報（メールアドレスは含まない）を入力する。

(4) Web サーバは，(1)のメールアドレスと(3)の会員情報を，会員管理サーバ上で稼働しているデータベース（以下，会員情報 DB という）に登録する。

(5) Web サーバは，会員登録完了を知らせるメールを，(1)のメールアドレス宛てに送信する。

メールマガジン発行の流れは次のとおりである。

(1) メールマガジン担当者は，業務用 PC の Web ブラウザから，メールマガジン送信サーバのメールマガジン入力用 Web ページに HTTP でアクセスし，メールマガジンの本文を入力する。

(2) メールマガジン送信サーバは，会員情報 DB から全ての会員のメールアドレスを取得し，取得したメールアドレス宛てにメールでメールマガジンを送信する。

なお，メールは，メールサーバで稼働しているメール転送サービスを介して送信する。また，本問では，URL やメールアドレスなどの名前解決については，考慮しなくてよいこととする。

設問 1 会員登録の際，登録希望者が最初にアクセスする入会申込用 Web ページでは，登録希望者のメールアドレスだけを入力させ，会員情報の入力は別途行わせる方式を採っている。このように 2 段階の手順を踏む主な目的として適切な答えを，解答群の中から選べ。

解答群

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。

イ 通信を暗号化し，登録希望者の会員情報が第三者に漏れないようにする。

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。

エ 間違った会員情報（メールアドレスは含まない）が登録されないようにする。

設問2　次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

ルータは，動的なパケットフィルタ型のファイアウォール機能を搭載していて，設定で許可したパケットだけを通過させる。

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。許可されたパケットに対する応答パケットの通過も許可される。

送信元及び送信先には，IP アドレス又はネットワークインタフェースを指定する。IP アドレスを指定したときに許可の対象となるパケットは，送信元又は送信先の IP アドレスが，指定された IP アドレスであるパケットである。ネットワークインタフェースを指定したときに許可の対象となるパケットは，そのネットワークインタフェースから入ってくるパケット（送信元として指定したとき），又は出ていくパケット（送信先として指定したとき）である。

通信ポートには，各サービスがパケットを待ち受けるポート番号を指定する。A 社の各サーバ上で稼働している各サービスが使用するプロトコルと待受けポート番号を，表1に示す。

表1　サービスごとのプロトコルと待受けポート番号

サービス	プロトコル	待受けポート番号
Web	HTTP	80
	HTTPS	443
会員情報 DB	独自プロトコル	4194
メール取得	POP3	110
メール転送	SMTP	25

現在のルータの設定を，図2に示す。

1 行目の設定で，インターネットから Web サーバに HTTP でアクセスすることを許可し，2 行目の設定で，インターネットから入ってくるメールを，メールサーバに転送することを許可している。

```
if0,203.0.113.2,80
if0,203.0.113.3,25
203.0.113.3,if0,25
if2,203.0.113.2,80
if2,203.0.113.2,443
if2,203.0.113.3,25
if2,203.0.113.3,110
if0,[ a ]
203.0.113.2,[ b ]
```

図２　現在のルータの設定

解答群

ア	192.168.0.2,443	イ	192.168.0.2,4194
ウ	192.168.0.3,4194	エ	203.0.113.2,443
オ	203.0.113.2,4194	カ	if0,443

設問３　次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

A 社は，Web サーバのメンテナンスを外部委託し，委託先内の特定の PC から，インターネットを介して，Web サーバを操作できるようにした。そのために，Web サーバ上に待受けポート番号 22 で SSH サービスを稼働させ，ルータの設定に“［　c　］”の行を追加した。

なお，この PC から送信されたパケットがルータに到着したとき，このパケットの送信元 IP アドレスは，198.51.100.2 となっている。

解答群

ア	198.51.100.2,203.0.113.2,22	イ	198.51.100.2,if0,22
ウ	203.0.113.2,198.51.100.2,22	エ	if0,198.51.100.2,22

設問4　次の記述中の［　　］に入れる正しい答えを，解答群の中から選べ。

SSH サービスがクライアントを認証する方式には，パスワード認証方式と公開鍵認証方式がある。A 社は公開鍵認証方式を採用した。

公開鍵認証方式では，秘密鍵で作成した署名が，対応する公開鍵で検証できることを利用して，次のようにクライアントを認証する。

(1)　クライアントは，秘密鍵を使って作成した署名と，その秘密鍵に対応する公開鍵をサーバに送る。

(2)　サーバは，(1)の公開鍵がサーバに登録されていることを確認し，公開鍵で(1)の署名を検証する。

(3)　検証に成功すれば，クライアントがサーバに登録されている公開鍵に対応する秘密鍵をもっていることが証明されるので，サーバは，クライアントを認証する。

このように，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。

解答群

ア　公開鍵

イ　秘密鍵

ウ　秘密鍵及び公開鍵