問１　リモートアクセスにおけるセキュリティの確保に関する次の記述を読んで,設問 1～3 に答えよ。

X社では,これまで社内ネットワーク上でクライアント／サーバの処理形態で行っていた業務を，外出先や自宅からインターネット経由で行えるようにすることになった。セキュリティの確保のため，インターネットと社内ネットワークの間はファイアウオールによって適切に接続するほか，本業務のクライアントとサーバの間で相互の認証及び電文の暗号化を行い，なりすましや盗聴を防ぐことにする。

クライアントがサーバと接続するときに，まずクライアントとサーバの間で相互に認証を行う。ID とパスワードを平文（暗号化していない電文）で送る認証方式では，盗聴される危険性があるので，パスワードを直接には送らずに認証するチヤレンジ･レスポンス方式と呼ばれる手順が考え出されている。その手順は，まず認証する側が適当な長さの乱数の電文を生成して相手に送る（チャレンジ)。認証される側は，自分のパスワードをかぎとしてその電文を暗号化し，送り返す（レスポンス）。認証する側はそのレスポンスを [a] して [b] と一致することを確認して，相手を認証する。

ここでは，クライアントとサーバの間の相互の認証に，このチャレンジ･レスポンス方式を採用する。使用する暗号の方式は，かぎの設定や保管などの運用面を考慮して公開かぎ暗号方式とし，次のように名付けた四つのかぎを使用する。

KI：クライアントがもつ秘密かぎ
K2：KI とペアの公開かぎ
K3：サーバがもつ秘密かぎ
K4：K3 とペアの公開かぎ

相互の認証の完了後，暗号化した電文の送受信を行う。ここでは，処理速度を考慮し，電文の暗号化には共通（秘密）かぎ暗号方式を使用する。ただし，そこで使う共通かぎはクライアントとサーバの接続の都度生成することにし，それを相手に送る際には公開かぎ暗号方式を使用する。そのときのかぎは，認証で使用するのと同じものを利用する。

設問１　クライアントとサーバの間の認証に関する記述中の [a] , [b] に入れる適切な字句を答えよ。また，図 1 に示すクライアントによるサーバ認証の手順中の [c] , [d] に入れる適切なかぎを，K1 ～ K4 の中から選べ。

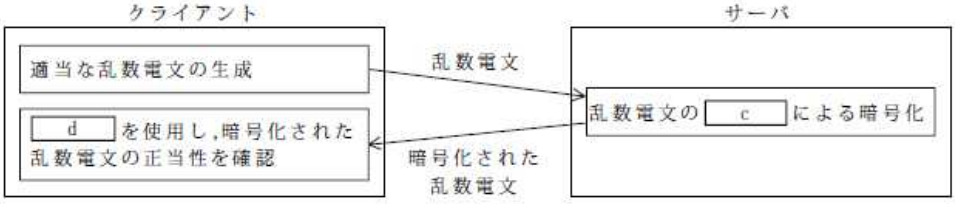


図１　クライアントによるサーバ認証の手順

設問２　暗号化した電文の送受信を行うために，クライアント側で共通かぎを生成してサーバに送り，クライアントとサーバの間で暗号化通信を始める手順を図 2 に示す。この手

順中の［ e ］，［ f ］に入れる適切なかぎを，K1 ～ K4 の中から選べ。

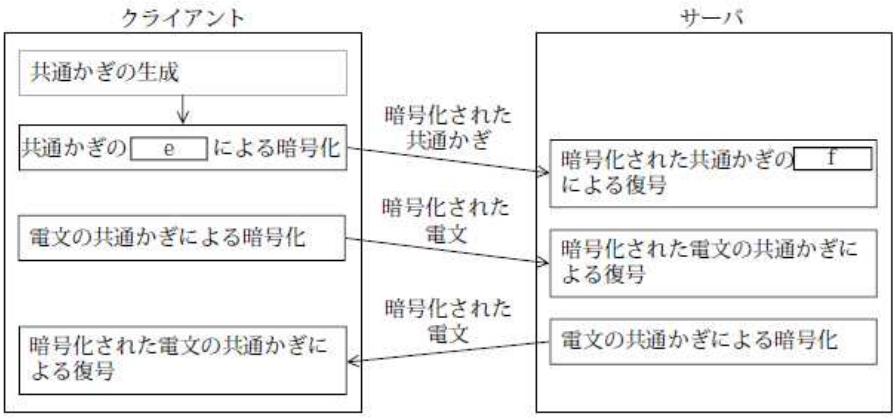


図２　クライアントとサーバの間で暗号化通信を始める手順

設問３　クライアントやサーバの台数が多い場合の対応に関する次の記述中の［ g ］～［ k ］に入れる適切な字句又は式を答えよ。

多数のクライアントやサーバのそれぞれに認証のために別個のかぎをもたせると，かぎの設定などの運用が煩雑になる。これを公開かぎ暗号方式の特長を活かして簡素化することを考える。

クライアントやサーバの設置にあたり，それらがもつ秘密かぎについては，その機器で注意深く保管する必要がある。しかし，そのペアの公開かぎについては，あらかじめ通信の相手となる各機器に保持させておかずに，接続の都度送ってもよい。ただし，なりすましの防止のために，送られた公開かぎの正当性は確認できるようにしておく必要がある。

そこで，認証局を設置し，認証局がもつ秘密かぎについては，認証局内で厳重に保管する。そのペアの公開かぎは,正当性確認の問題がないように，あらかじめ［ g ］に設定しておく。各クライアントやサーバは，自分の ID と公開かぎを認証局に送って，認証局の［ h ］で暗号化したもの(公開かぎ証明書と呼ぶ)を発行してもらい,用意しておく。認証局は，正当なクライアントやサーバからの要求に対してだけ，公開かぎ証明書を発行する。各クライアントやサーバは，接続の都度，その公開かぎ証明書も通信相手に送る。相手は，送られてきた公開かぎ証明書を認証局の［ i ］で復号することによって，送信元の公開かぎの正当性を確認できる。

なお，クライアントやサーバの廃止などに伴って公開かぎとその証明書を無効にするには，そのための仕組みが別途必要である。

M台のクライアントとN台のサーバが既に稼働しているときに,1台のクライアントが増設されて，かぎのペアを追加生成する場合を考える。公開かぎを必要なクライアントやサーバ機器にあらかじめ保持させておく方式では，追加の秘密かぎや公開かぎの設定作業が［ j ］台の機器で必要となる。一方，認証局を設置し，接続の都度，公開かぎ証明書を送る方式では，追加の秘密かぎや公開かぎ証明書の設定作業が必要な機器は，公開かぎ証明書を発行する認証局の１台を含めて［ k ］台である。ここで，各クライアント

から接続する相手はすべてのサーバとする。また，台数には増設されるクライアント自体も含める。

問２　オブジェクト指向分析に関する次の記述を読んで，設問１～３に答えよ。

A君は缶飲料自動販売機のシステムを開発することになった。最初に，簡単なシナリオを記述し，そのシナリオを基にしてUML（Umfied Modeling Language）のクラス図とシーケンス図を使って，システムのモデリングを行うことにした。

シナリオ：

缶飲料を購入する顧客は，自動販売機に対して入金口から入金する。入金されたお金は，自動販売機内のレジスタに入れられる。レジスタには,今までの売上も含めたお金が蓄えられている。自動販売機は，入金されるたびに，入金総額をインジケータに表示する。入金総額が缶飲料の価格に達すると，自動販売機は価格に達した缶飲料に対応する購入可能ランプを点灯する。顧客は自分が購入したい缶飲料のランプが点灯するまで，自動販売機に入金する。購入したい缶飲料のランプが点灯し，顧客がその缶飲料を購入するためのボタンを押すと，自動販売機は選択された缶飲料を商品口に置き，購入可能ランプを消灯し，インジケータの表示を0にする。つり銭がある場合には，レジスタから必要な金額のつり銭を出し，返却金口に戻す。

A君はこのシナリオを基に，初期モデルのクラス図（図 1）とシーケンス図（図２）を作成した。

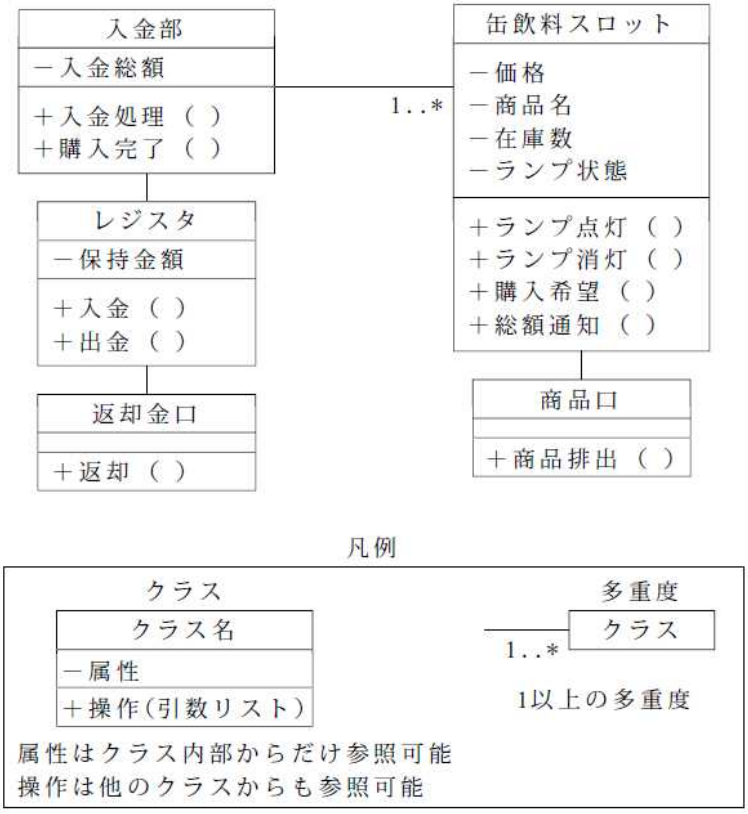


図１　最初のクラス図

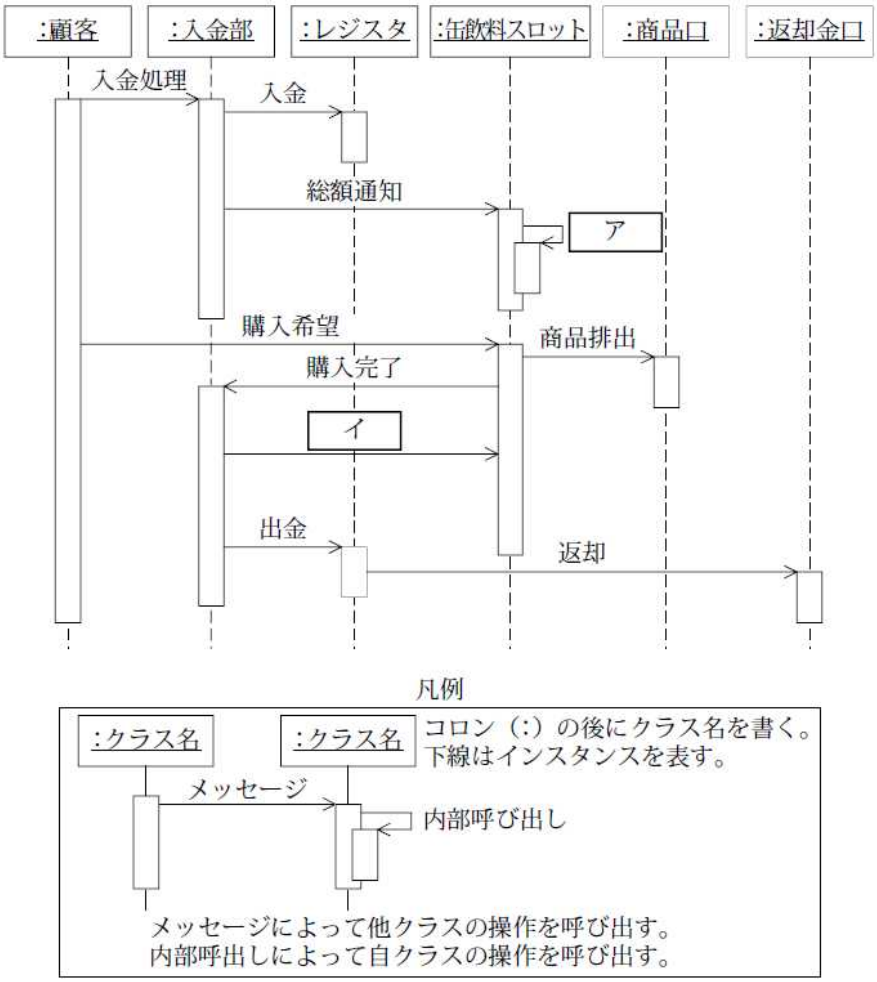


図２　最初のシーケンス図

設問１　図１のクラス図に入金総額をインジケータに表示する操作を加えたい。どのクラスに加えるのが適切か。クラス名を答えよ。

設問２　図２中の［　ア　］，［　イ　］に入れる適切な操作名を答えよ。

設問３　A 君が図１のクラス図を見直したところ，入金部が複数の機能をもっていると考え，各機能ごとにクラスを割り当てることにして図 1，2 を修正した。修正したクラス図とシーケンス図がそれぞれ図 3，4 である。また，図 4 のシーケンス図では，操作に必要な引数を記入することにした。ここで図 4 では，既に自動販売機に 100 円投入されている状態で，更に 100 円投入して 120 円の缶飲料を購入する場合を表しており，必要に応じて，オブジェクト間のメッセージとともに渡される引数も示している。

図 3，4 中の［　ウ　］～［　サ　］に入れる適切な字句を答えよ。

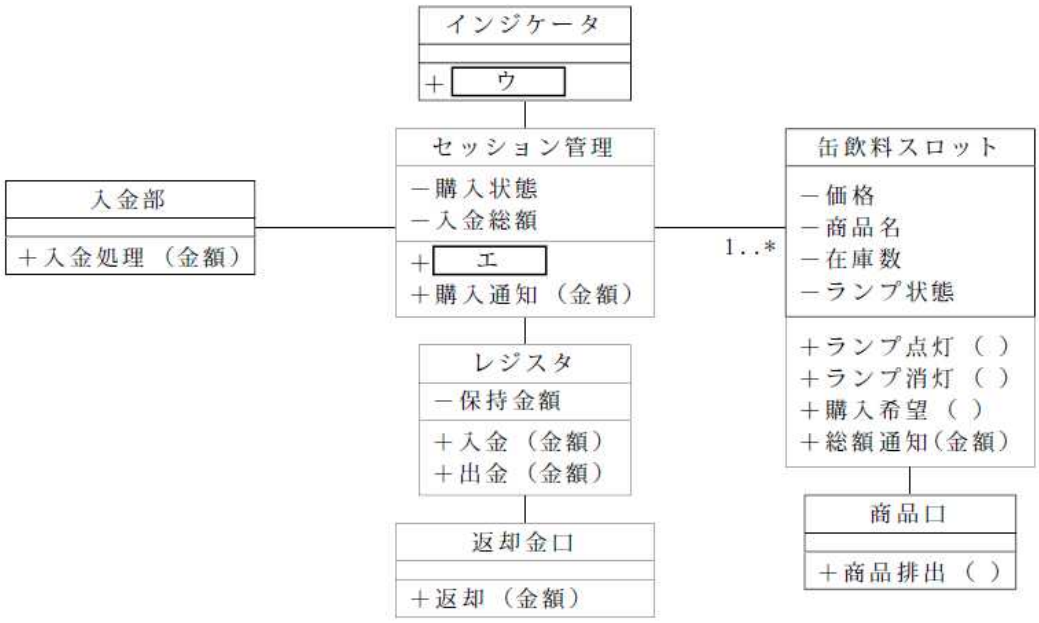


図３　修正したクラス図

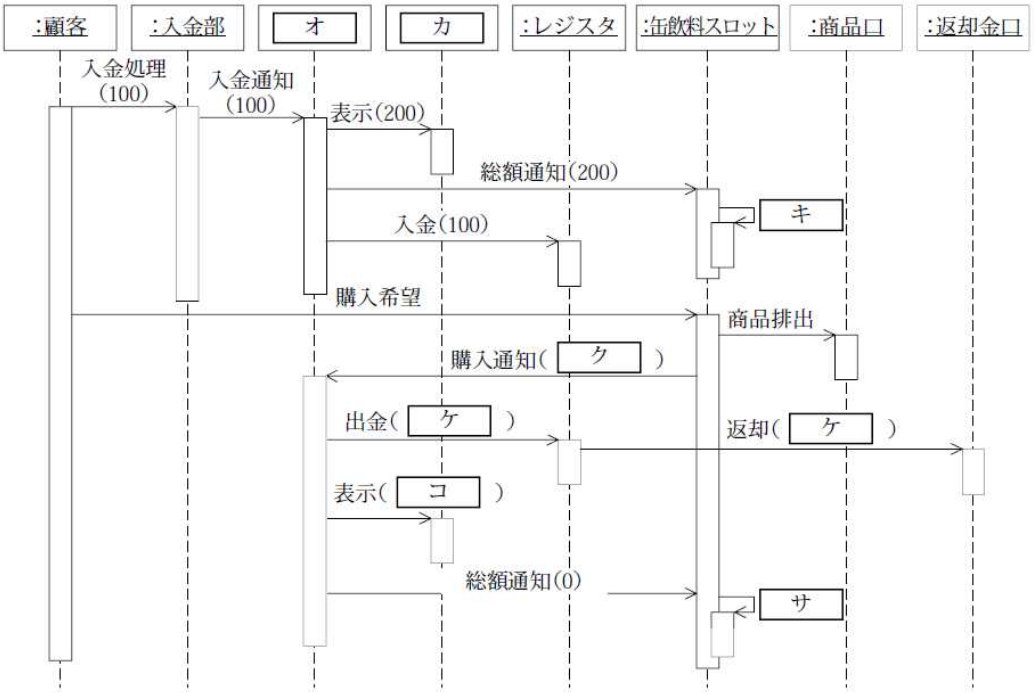


図４　修正したシーケンス図

5　問３　Web ベースの検索システムに関する次の記述を読んで，設問 1 ～ 3 に答えよ。

図 1，2 に示すような，Web ベースの検索システムがある。

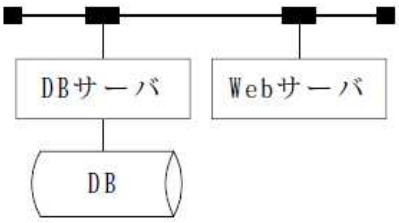


図１　検索システム１

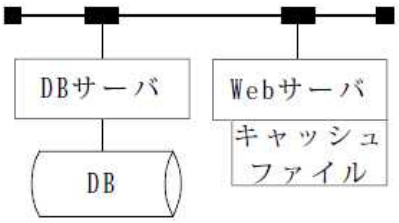


図２　検索システム２

図１と図 2 は，Web サーバのキャッシュファイルの有無以外は同構成のシステムで，各処理の所要時間は表 1 のようになっている。データベース（ＤＢ）に格納されているレコードは，画像が含まれた 2M バイトの固定長レコードである。

図１の検索システムでは，利用者から Web サーバに検索要求があるたびにＤＢサーバに問合せを行う。

図 2 の検索システムでは，利用者から検索要求があると，Web サーバはキャッシュファイルに該当するレコードがある場合は,そのレコードを読み込んで検索結果を利用者に通知する。このとき，レコードの参照時刻フィールドに現在のシステム時刻を設定して，キャッシュファイル中のレコードを更新する。キャッシュファイルに該当するレコードがない場合は，Web サーバからＤＢサーバに問合せを行う。 Web サーバは，キャッシュファイルに空きがある場合は，ＤＢサーバから受け取ったレコードを，キャッシュファイルへ書き出し，キャッシュファイルに空きがない場合は，最も古い参照時刻をもつレコードをキャッシュファイルから削除し，ＤＢサーバから受け取ったレコードをキャッシュファイルへ書き出す。 Web サーバは，ＤＢサーバから受け取ったレコードをキャッシュファイルへ書き出した後，検索結果を利用者に通知する。

表１　検索システムにおける各処理の所要時間

項番	処　理	所要時間
1	Web サーバ上の各処理に要する時間	
1.1	利用者からの検索要求を受け付ける処理	無視できる
1.2	検索要求のあったキー値をもつレコードがキャッシュファイルに存在するかしないかを確認する処理	0.1 秒
1.3	キャッシュファイルから１レコードを読み込む処理	0.1 秒
1.4	キャッシュファイルへ１レコードを書き出す処理	0.1 秒
1.5	キャッシュファイルに存在するレコードを更新する処理	0.1 秒
1.6	キャッシュファイル中の最も古い参照時刻をもつレコードを削除する処理	0.1 秒
1.7	DB サーバにレコードの検索を要求するための依頼電文を編集する処理	無視できる
1.8	検索結果画面を編集し，利用者へ検索結果を通知する処理	0.1 秒
2	Web サーバと DB サーバの間の通信と，DB サーバ上でのデータベースアクセスに要する時間	2.5 秒

設問 1　図２の検索システムで，キャッシュファイルの容量を 10M バイトとし，キャッシュファイルは空に初期化されているものとする。表２のキー値をもつレコードを検索番号の順に検索する場合，キャッシュファイルからレコードが読み込まれるのは，どの検索番号のときか。複数ある場合は，すべて答えよ。

表２　レコードの検索順序

検索番号	1	2	3	4	5	6	7	8	9	10
キー値	701	702	703	800	778	702	714	703	701	712

設問２　図１の検索システムと図２の検索システムで，それぞれ，１レコードを取り出し利用者に検索結果を通知するのに要する時間を整理する。

次の記述中の [a] ，[b] に入れる適切な数値を答えよ。

図１の検索システムの場合は，レコードを検索する際に必ずDBサーバに問合せを行う。したがって，１レコードを取り出し利用者に検索結果を通知するためには2.6秒必要である。

次に図２の検索システムについて，キャッシュファイルが満杯になっていることを前提として考える。

Webサーバがキャッシュファイルを調べ,キャッシュファイル中に検索したいレコードが存在する場合は，キャッシュファイルから該当レコードを読み出し，レコードの参照時刻フィールドに現在のシステム時刻を設定してキャッシュファイル中のレコードを更新する。したがって，１レコードを読み出し，利用者に検索結果を通知するのに，[a] 秒必要である。

キャッシュファイル中に検索したいレコードが存在しない場合は,DBサーバに問合せを行う。DBサーバは，データベースにアクセスしWebサーバに結果を返す。 Webサーバは，幾も古い参照時刻をもつレコードをキャッシュファイルから削除し，DBサーバから受け取ったレコードの参照時刻フィールドに現在のシステム時刻を設定して，キャッシュファイルに書き出す。したがって，利用者に検索結果を通知するのに [b] 秒必要である。

設問３　検索回数が十分多い場合に図１の検索システムに比べ，図２の検索システムの平均応答時間が1/2倍となるようにキャッシュファイルを準備したい。前提条件として，データベース中にレコードが10,000件格納されており，かつ，参照頻度の高い上位100件のレコードが80 %の確率で参照される場合について考える。説明文中の [c] ～[f] に入れる適切な字句を答えよ。

なお，[a] ，[b] には，設問２と同じ数値が入る。

参照頻度の低い下位9,900件のレコードについては，キャッシュファイル上にレコードが存在しない可能性が高い。したがって，見積りを簡単にするため，下位9,900件のレコードは，利用者からの参照要求が発生する都度，必ずDBサーバにアクセスするものとして考えると，[b] 秒を要するアクセスが20 %の確率で発生する。

次に上位100件のレコードは80 %の確率で参照されるので，キャッシュファイル中にレコードが存在する可能性が高い。上位100件の任意の一つのレコードがキャッシュファイル中に存在する確率をxとし，上位100件のレコードはどれも同じ確率で出現すると仮定すると，次式が成立する。

2.6/2 ＝ 0.8 ×([c] × [a] + [d] × [b]) +0.2 × [b]

したがって，xは，［ e ］となる。

下位 9,900 件のレコードはキヤッシュされないという前提で，必要なキャッシュファイルの容量を算出すると，［ f ］Mバイトとなる。

問4　Webを用いた情報提供システムに関する次の記述を読んで，設問に答えよ。

［現在のシステム構成］

A社では，Web を用いた情報提供サービスを行っている。そのシステム構成を図 1 に示す。現在の構成では，提供すべき情報コンテンツの種類ごとに3台の Web サーバにファイルを分散配置している。社内 LAN には，コンテンツの作成やシステムの運用･保守などに用いるテスト用 Web サーバやパソコン（PC）が接続されている。最近，利用者の増加によって，利用者から，A社の Web ページにアクセスできない，情報のダウンロードに以前より時間がかかるなどの苦情が寄せられるようになった。そこで，A社では，現在のアクセス状況を調査した上で，Webサーバの構成を再検討することにした。

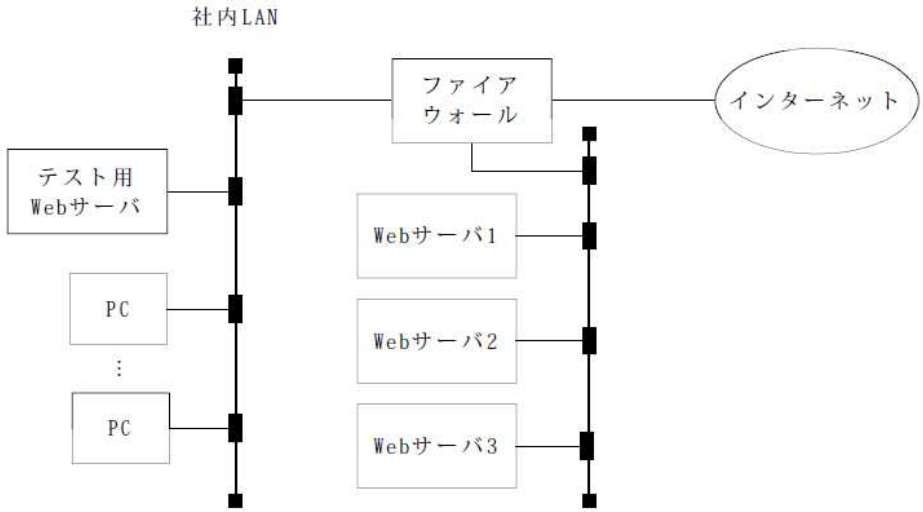


図1　A社の情報提供システムの構成

［システム構成の見直し案］

アクセス状況を調査したところ，Web サーバ 1 ～ 3 の間に負荷のアンバランスがあることが判明した。A社では，負荷が均等になるようにファイルを再配置することも検討したが，将来的に各ファイルへのアクセス状況が変わると，再び負荷のアンバランスが発生するであろうことを考慮し，次の方策をとることにした。

・磁気ディスク装置を増設して，各 Web サーバで同一のファイルを重複して保持するようにする。

・各 Web サーバの負荷の状況を1分ごとに監視しておき，アクセス要求があったときには，直前の監視結果において最も負荷が少ない Web サーバにアクセスを振り分ける"振分けサーバ"を導入する。

設問　A社では,当初,見直し案によるシステムの性能は,M/M/3 モデルを用いて解析できると考えた。しかし，その後の検討によって,見直し案における Web サーバ上での処理時間は,実際には,M/M/3 モデルを用いて解析した結果とは一致しないと想定されることが判明した。

（1）M/M/1 モデルの模式図を次の図２に示す。この図にならって，M/M/3 モデルの模式図を描け。

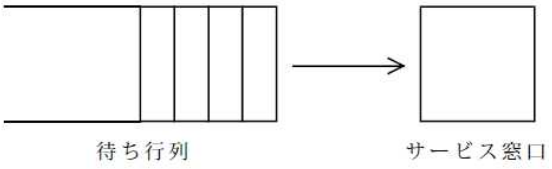


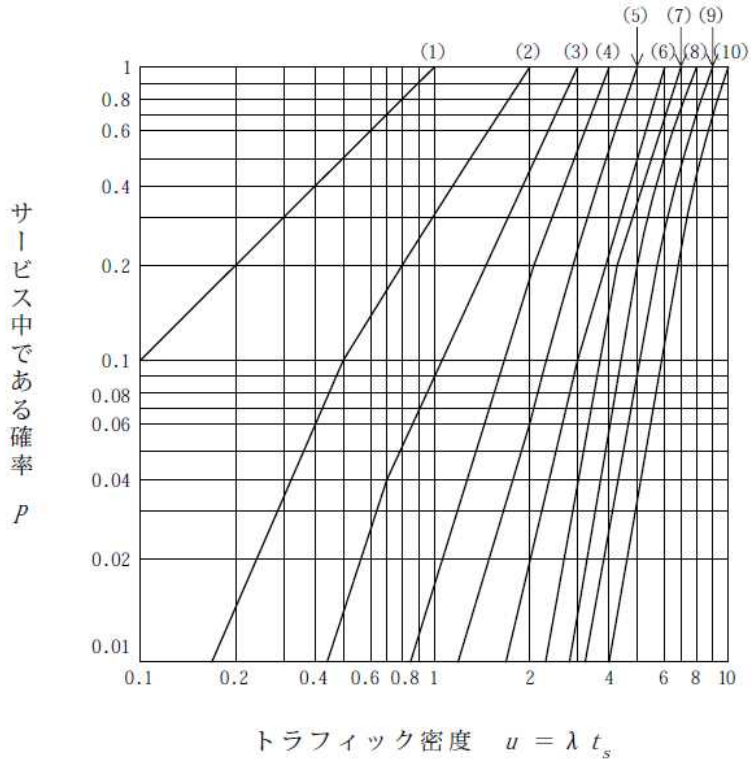
図２　M/M/1 モデルの模式図

（2）A 社のシステムのアクセス件数は１秒当たり平均 10 件，アクセス１件の平均処理時間は 70 ミリ秒である。見直し案が M/M/3 モデルに従うと仮定した場合の，待ち時間を含めた Web サーバ上での平均処理時間を求める手順に関する次の記述中の [a] ～ [f] に入れる適切な数値を答えよ。答えは小数第３位を四捨五入して，小数第２位まで求めよ。なお，M/M/m モデルにおける平均待ち時間は，次の式で算出される。

$$\text{平均待ち時間} = \frac{P t_s}{m - \lambda t_s}$$

ここで，λは平均到着率，t_s は平均サービス時間である。P は，すべての窓口がサービス中である確率で，図３のグラフで表される。

なお，図３の横軸はトラフィック密度 $u = \lambda t_s$ である。



注　(1)～(10) は窓口数である。

図３　m 個の窓口がすべてサービス中である確率

$\lambda =$ [a] (/秒)，$t_s =$ [b] (秒)であるから，$u =$ [c] となる。グラフから，$m = 3$，$u =$ [c] のときの P は [d] となる。

したがって，平均待ち時間は，[e] ミリ秒となり，待ち時間を含めた平均処理時間は，[f] ミリ秒となる。

(3) 見直し案における待ち時間を含めた Web サーバ上での平均処理時間は，M/M/3 モデルを用いて解析した結果とは一致しないと想定される理由に関する，次の記述中の [g]，[h] に入れる適切な字句を答えよ。

見直し案では，アクセス要求が到着した時点でそれを処理する Web サーバを決定している。したがって，このシステムでは，アクセス要求は [g] に処理されるとは限らない。この点が M/M/3 モデルとの相違となる。実際には，待ち時間を含めた平均処理時間は，M/M/3 モデルに基づいて計算した時間よりも [h] なることが想定される。

問 5　Base64 の変換プログラムに関する次の記述を読んで，設問 1 ～ 4 に答えよ。

Base64 は，電子メールなどでバイナリデータをテキストにして送るための規格で，バイナリデータを 6 ビットごとに区切り，64 進数で表記したものである。数値と文字の対

応は，次の表のとおりである。

表　64進数の対応表

0 A	16 Q	32 g	48 w
1 B	17 R	33 h	49 x
2 C	18 S	34 I	50 y
3 D	19 T	35 j	51 z
4 E	20 U	36 k	52 0
5 F	21 V	37 l	53 1
6 G	22 W	38 m	54 2
7 H	23 X	39 n	55 3
8 I	24 Y	40 o	56 4
9 J	25 Z	41 p	57 5
10 K	26 a	42 q	58 6
11 L	27 b	43 r	59 7
12 M	28 c	44 s	60 8
13 N	29 d	45 t	61 9
14 O	30 e	46 u	62 +
15 P	31 f	47 v	63 /

３バイトをまとめると24ビットとなり，これを６ビットで分割すると64進数４けたで表記できるので，変換は３バイト単位で行う。各バイトを６ビットに切り分けるときには，各バイトの上位ビットから順に切り出すものとする。切り出した64進数は，対応する文字コードに変換され，１けたが１バイトを占める。最後の変換データが１バイトの場合は，後に２バイトの0を補って変換し，４文字の最後の２文字を"="で置き換える。同様に２バイトの場合は，１バイトの0を補って変換し，最後の１文字を"="で置き換える。

デコードのときは，受け取ったデータ中の"="の個数を調べることで，実際に送られたデータのバイト数を知ることができる。エンコードの出力は，76文字ごとに改行し，最後の行は76文字未満でも改行することにする。ここでは，改行,"="及び表中の文字以外は一切出現しないものとする。

設問１　次の問いに答えよ。ただし，ここでは改行を無視して考える。

（1）4バイトのデータ（10進数）10，20，30，40をエンコードした結果の文字列を示せ。

（2）2バイトのデータをエンコードした結果"ghg="をデコードして，元の２バイトの値を復元し，バイトごとに10進数で示せ。

設問２　1,000バイトのデータをエンコードした結果は何バイトになるか。ここでは，改行は１バイトと数える。

設問３　大きさ３の配列bに変換前の３バイトのデータがあるとき，大きさ４の配列b6に６ビットずつ切り出す処理は次のとおりである。次の［ア］，［イ］に入れる適切な式を答えよ。ここで，配列の添字は0から始まる。また，x shl yはxをyビット左にシフトする演算，x shr yはxをyビット右にシフトする演算である。右シフトは論理

シフトを行うものとする。 and と or はビット演算の論理積と論理和である。シフト演算は論理演算より優先順位が高いものとする。

```
b6[0]←［ ア ］
b6[1]←［ イ ］
b6[2]←(b[1] and 15) shl 2 or b[2] shr 6
b6[3]← b[2] and 63
```

設問 4　Base64 でエンコードされたデータファイルのデコード処理の大まかな流れは，次のようになる。次の ［ ウ ］ ～ ［ キ ］ に入れる適切な字句を答えよ。

```
i ← 0
while(ファイルの終わりでない) {
        ch ←次のエ 1 字を読む
        if(ch が改行でない) {
                c[i]← ch
                i ← i + 1
                if( ［ ウ ］ ) {
                        c をデコードした結果を b に入れる
                        n ← 3
                        if(c[3]が'=') ［ エ ］
                        if(c[2]が'=') ［ オ ］
                        b の n バイトを書き出す
                        ［ カ ］
                }
        }
}
if( ［ キ ］ )エラーメッセージ（入力データの形式が正しくない）
```

問 6　オークションシステムに関する次の記述を読んで，設問 1 ～ 4 に答えよ。

T社では，登録された会員相互間のオークションのサービスを提供するシステムを構築することになった。本システムでは，会員はクライアントからネットワークを経由してT社のオークション情報を管理するサーバにログインし，出品や入札などの操作を行うことによって，オークションに参加することができる。

会員が商品をオークションに出品するためには，商品の分類，名称，説明，最低上乗せ額，オークション終丁日時などのデータを入力して出品操作を行う。

商品を購入したい会員は，出品された商品を検索して現在価格（それまでに入札された最高の入札価格，初期値は 0）を含む出品商品の情報を取得し，欲しいものがあれば，入

札価格を指定して入札操作を行う。

入札操作の処理において，入札価格が"現在価格＋最低上乗せ額"以上の場合に入札が成立し，その入札価格が新たな現在価格になる。入札処理は入札操作の要求がシステムに到着して受け付けられた順に実行される。同一出品商品に対して同じ価格の複数の入札操作があった場合は，システムの受付け順の最も早い入札操作以外の入札は成立しない。入札操作に対する回答として，入札が成立したか否かを画面に表示する。現在価格を入札している会員を，その出品商品の落札候補会員と呼ぶ。新たな入札が成立したときには落札候補会員が変わり，それまでの落札候補会員にその旨がシステムから電子メールで通知される。

なお，会員は同一出品商品に対し，何度でも入札できるが，入札価格の減額や入札の取消しはできない。出品商品のオークション終了日時になると入札は締め切られ，その時点の落札候補会員が落札することになる。出品会員及び落札した会員には，その旨がシステムから電子メールで通知される。本システムの操作の一覧（一部）を表に示す。

表　操作の一覧（一部）

操作	実行者	概要
出品	会員	出品処理を行う。
商品検索・入札	会員	出品商品の検索・表示を行い，入札処理を行う。
出品状態表示	出品会員	当該会員による出品の状態を表示する。
入札状態表示	入札会員	当該会員による入札の状態を表示する。

商品検索･入札操作において，出品商品の検索結果を表示して入札操作を行う画面の例を図１に示す。

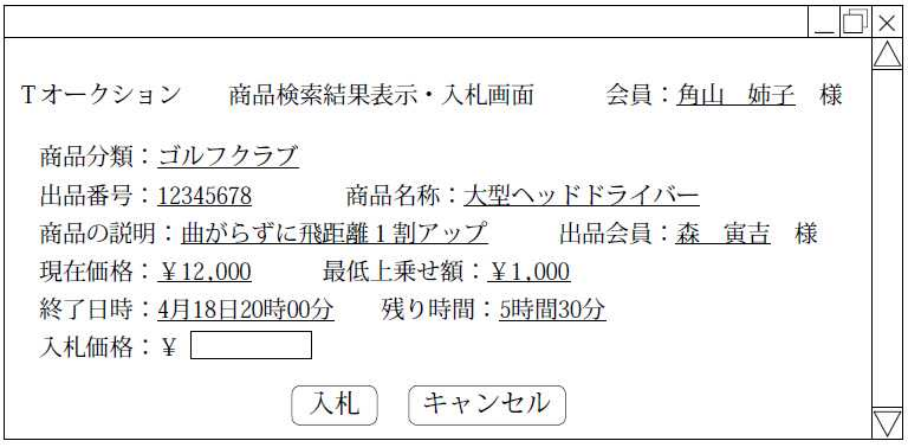
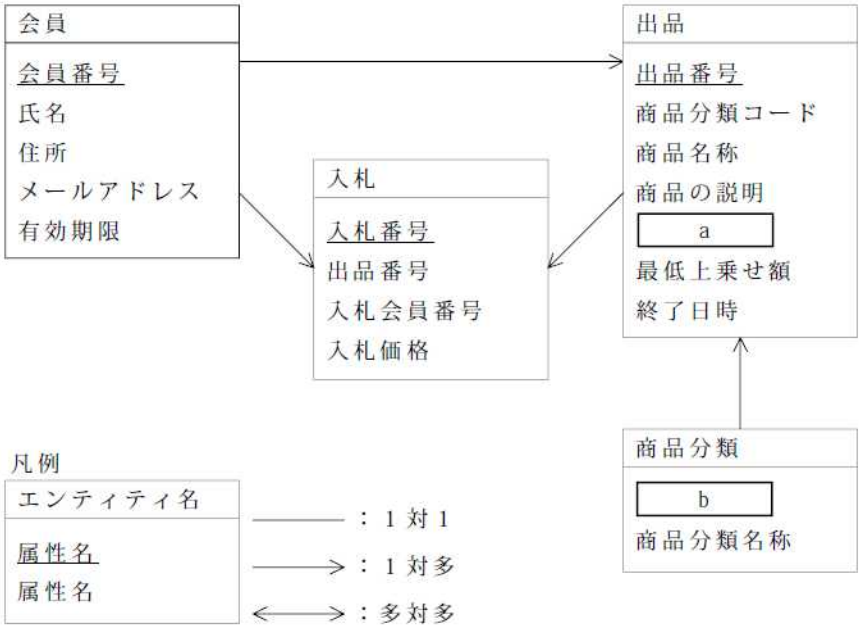


図１　入札操作の画面例

本システムのＥ･Ｒ図を図２に示す。



注　属性名の下線は主キーを示す。

図2　E-R図

ここでは，E・R図に合わせてエンティティ名を表名，属性名を列名にして適切なデータ型で表定義した関係データベースによってテータを管理することにする。また，使用されるホスト変数は，適切なデータ型で定義されているものとする。エンティティ"入札"に対応する表には，成立した入札のデータだけが挿入され，その後に新たな入札が成立しても，それまでの入札のデータは削除しないものとする。

設問1　図2中の［a］，［b］に入れる適切な属性名を答えよ。主キーの場合は，下線を引いて示せ。

設問2　入札を成立させた会員（会員番号がホスト変数":会員番号"に格納されている）が，入札状態表示操作を行った場合の表示データ（出品番号，商品名称，当該会員の入札価格，現在価格，終了日時）を求めるSQL文を次に示す。

なお，当該会員が複数の出品商品に入札している場合は，それぞれの出品商品について表示する。ある出品商品に対し複数回入札している場合は,"当該会員の入札価格"として当該会員が成立させた入札の最高の入札価格を表示する。SQL文中の［c］～［h］に入れる適切な宇句又は式を答えよ。

```
SELECT 出品.出品番号，商品名称，
  MAX（入札 1.入札価格）As 当該会員の入札価格，［c］，終了日時
    FROM 出品，入札入札 1，［d］
    WHERE［e］
```

AND 出品.出品番号＝入札１.出品番号
AND [f]
[g] 出品.出品番号，商品名称，[h]

設問３　入札操作の処理におけるデータの整合性確保に関する次の記述中の [i]，[j] に入れる適切な字句を答えよ。また，[k]，[l] に入れる適切な記号を，図３中のア～オの中から選べ。

商品検索･入札操作における商品検索結果表示･入札画面に入札価格を入力し，入札ボタンをクリックすると，図３に示す一連の流れによって，会員についての有効期限のチェック，出品の終了日時のチェック及び現在価格の取得を再度行い，入札が成立する場合に"入札"表への挿入を行う。ただし，このままでは，複数の入札要求を同時に処理したときには，不適正な処理が行われ [i] のデータが [j] されてデータの不整合が起きるおそれがある。

そこで，DBMS のトランザクション処理機能を利用して排他制御を行い，複数要求の同時並行処理時における不適正な処理を防止することにする。図３に示す処理の流れにおいて設定すべき最短なトランザクション範囲は，[k] ～ [l] になる。

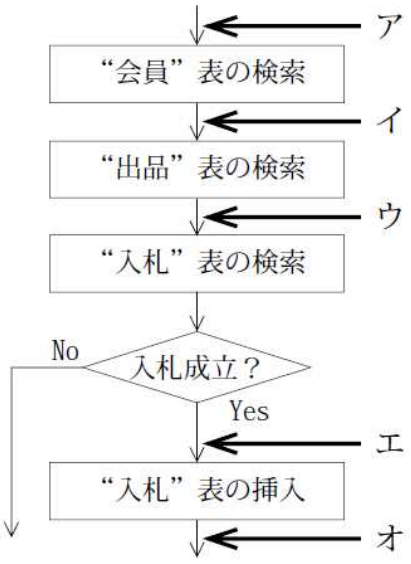


図３　入札操作の処理

設問４　本システムの運用を開始したところ，人気商品のオークション終了日時直前に入札が殺到してシステムの処理性能が不十分となる事態が発生した。その対策の一つとして，入札操作の処理の負荷軽減について検討した。次の記述中の [m]，[n] に入れる適切な字句を答え，[o]，[p] に入れる適切な記号を，図４中のカ～コの中から選べ。さらに，図４中の [q]，[r] に入れる適切な字句を答えよ。

データベース検索処理の負荷軽減をねらい,"[m]" 表に [n] のデータを追加すれ

ば，更新処理を一つ追加する必要があるが，検索処理を一つ省略することができる。処理の流れの改良案を図4に示す。この場合，不適正な処理を防止するために設定すべき最短なトランザクション範囲は，［　o　］～［　p　］になる。

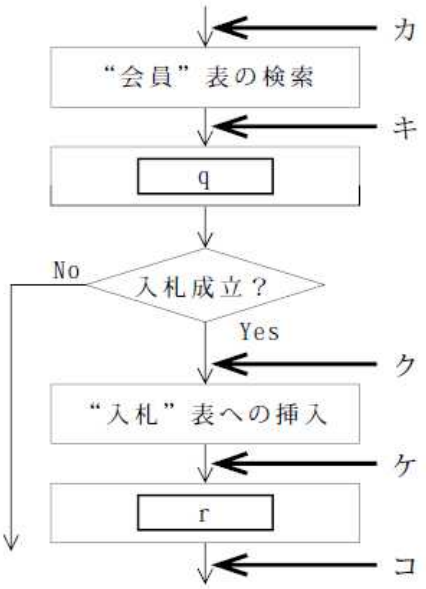


図４　入札操作の処理の改良案

5

【解答】

この解答例は、独立行政法人情報処理推進機構　情報処理技術者試験センターが公表しているものである。

問１

設問１　a　復号　b　チヤレンジ　又は　元の乱数電文　c　K3　d　K4

設問２　e　K4　f　K3

設問３　g　全クライアント及びサーバ　h　秘密かぎ　i　公開かぎ

j　N＋１　k　２

問２

設問１　入金部

設問２　ア　ランプ点灯　イ　ランプ消灯

設問３　ウ　表示（金額）　エ　入金通知（金額）　オ　：セッション管理

カ　：インジケータ　キ　ランプ点灯　ク　120

ケ　80　コ　0　サ　ランプ消灯

問３

設問１　６と８

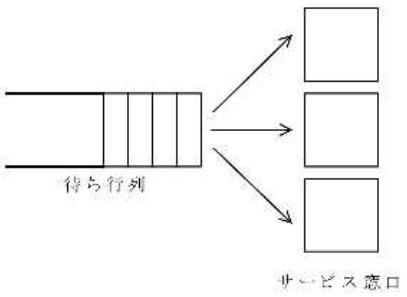
設問２　a －0.4　b －2.9

設問３　c －x　d －(1 －x)　e －0.8　f －160

問４

設問１

（1）



（2）a －10　b －0.07　c －0.7　d －0.04　e －1.22

f －71.22

（3）g 一到着順　h 一長く

問５

設問１（1）a　ChQeKA==　（2）b　130,　24

設問２　1354

設問３　ア　b［0］shr 2　　イ　（b［0］and 3）sh1 4 or b［1］shr 4
設問４　ウ　iが４に等しい　　エ　n←2　又は　n←n-1
オ　n←1　又は　n←n-1　　カ　i←O　　キ　i＞0

問６
設問１　a　出品会員番号　　b　商品分類コード
設問２　c　MAX（入札 2. 人札価格）　AS 現在価格
d　入札　入札２
e　入札 1.入札会員番号＝：会員番号
f　入札 2.出品番号＝入札 1.出品番号　又は　入札 2.出品番号＝出品.出品番号
（注）ｅとｆは順不同
g　GROUP BY
h　終了日時
設問３　i　成立しない入札　　j　挿入　　k　ウ　　1　オ

設問４　m　出品　　n　現在価格　　o　キ　　p　コ
q　" 出品"表の検索　　r　" 出品"表の更新