

平成 17 年度 春期 ソフトウェア開発技術者 午後 問題

問 1 トランザクション処理に関する次の記述を読んで、設問 1～4 に答えよ。

X 社は、オンラインショッピングのサイト運営の事業を始めるに当たって、それを実現するシステム（以下、本システムという）を構築することになった。

本システムは、ログインした顧客に対し、商品を検索して、商品を買物かごに入れる操作、買物かごに入れた商品を取り消す操作、買物かごに入れた商品を一括して購入する操作などの機能を提供する。そのうち、商品を買物かごに入れる操作に関する機能の概要は、次のとおりである。

- ・本システムは、取り扱う各商品の在庫量を含む商品データを保持している。
- ・本システムでは、顧客のログインごとに新しい買物かごを用意する。
- ・本システムでは、ログインした顧客が商品を買物かごに入れる操作を行うと、その商品の在庫量を減らしてから、買物かごに商品のデータを書き込む。

連携した複数のデータ更新処理では、システム障害が発生した場合や複数要求の同時並行処理を行う場合に、データの整合性を保てるようにするためのトランザクション処理が必要になる。本システムでは、商品を買物かごに入れるときに発生する商品データと買物かごデータに対する更新要求に関するトランザクション処理を、アプリケーションプログラムで実現することにし、それを 1 台のシステムで処理する場合と、複数台のシステムで処理する場合を検討する。

なお、本システムでは、次の事柄を前提とする。

- ・システムに障害が発生すると主メモリの内容は失われるが、ディスクに書き込まれているデータは正常に残る。
- ・商品データ及び買物かごデータはディスク上にある。それぞれのレコード構成を図 1、2 に示す。データの読み書きは、レコード単位に行う。買物かごデータのキーであるログイン通番は、顧客がログインするたびに 1 ずつ増える番号である。

キー（商品番号）	更新通番	データ内容（含在庫量）
----------	------	-------------

図 1 商品データのレコード構成

キー（ログイン通番）	更新通番	データ内容（0 個以上の商品のデータ）
------------	------	---------------------

図 2 買物かごデータのレコード構成

- ・図 1、2 における更新通番は、各レコードごとに、初期値を 0 として更新するたびに 1 ずつ増える番号である。
- ・ディスクへのデータの書込みは、バッファリングせずに即時に行う。書込み時にシステム障害が発生しても、レコード全体が正常に書き込まれるか、又は全く書き込まれないかのどちらかである。また、

書込み処理が完了してから次の処理が実行されるので、書込み処理の順番と、データがディスクに書き込まれる順番が入れ替わることはない。

- ・システム障害が発生した後のシステム再起動時にデータの整合性を回復可能とするため、処理途中の適切な時点で、処理状況や更新内容などのデータをログとしてディスクに書き込む。

〔1 台のシステムで処理する場合〕

商品を買物かごに入れる処理を、1 台のシステムにおける一つのプログラムで行う場合の処理方式を検討する。

商品データと買物かごデータの両方を同時に更新することはできないので、システム障害が発生するタイミングによっては、一方のデータが更新後、他方のデータが更新前となり、整合性が損なわれる可能性がある。これを回復可能にするためには、冗長なデータをディスク上にもち、データの更新中においても、常に両方の更新前のデータ又は両方の更新後のデータを、何らかの形でディスク上に存在させることが必要である。これによって、システム障害が発生した後の回復処理時に、データの更新がどこまで進んでいるかを調べ、両方のデータを更新前又は更新後にそろえることができる。

更新処理時のディスクでの冗長なデータのもち方として、商品データ又は買物かごデータのいずれか一方のレコードの内容と、もう一方のデータのキー及び更新通番（内容を書く方の更新状態に対応した更新通番）を、あらかじめログに書き込んでおくことにする。商品データ又は買物かごデータの内容を含むログのレコード構成を、それぞれ図 3、4 に示す。

ヘッダ	商品データ			買物かごデータ	
	キー	更新通番	データ内容（含在庫量）	キー	更新通番

図 3 商品データの内容を含むログのレコード構成

ヘッダ	商品データ		買物かごデータ		
	キー	更新通番	キー	更新通番	データ内容

図 4 買物かごデータの内容を含むログのレコード構成

ログに更新前のデータを書き込むか、又は更新後のデータを書き込むかで、次の二つの方法を考える。

方法 1：商品データ又は買物かごデータのいずれか一方の更新前のレコードの内容を、ログに書き込む（他方のデータの更新通番も更新前のものとする）。

方法 2：商品データ又は買物かごデータのいずれか一方の更新後のレコードの内容を、ログに書き込む（他方のデータの更新通番も更新後のものとする）。

システム障害が発生したときには、回復処理として、前回受付開始時（データの整合性が确实であった時点）からのログ及びその中のキーで示されている商品データや買物かごデータを読み込み、不整合がある場合はログの内容をいずれかのデータに書き込んで不整合を解消する。方法 1 の場合には、両方のデータを更新前に、方法 2 の場合には、両方のデータを更新後にそろえる。この回復処理の完了後、顧客からの操作の受付を再開する。

商品データ及び買物かごデータの更新の順序と、ログに書き込むデータが更新前(方法1)又は更新後(方法2)のいずれであるかによって、ログにどちらのデータを書き込むかが決まる。方法1と方法2のデータの更新に関する処理の流れを図5に、それに対応する回復処理の流れを図6に示す。

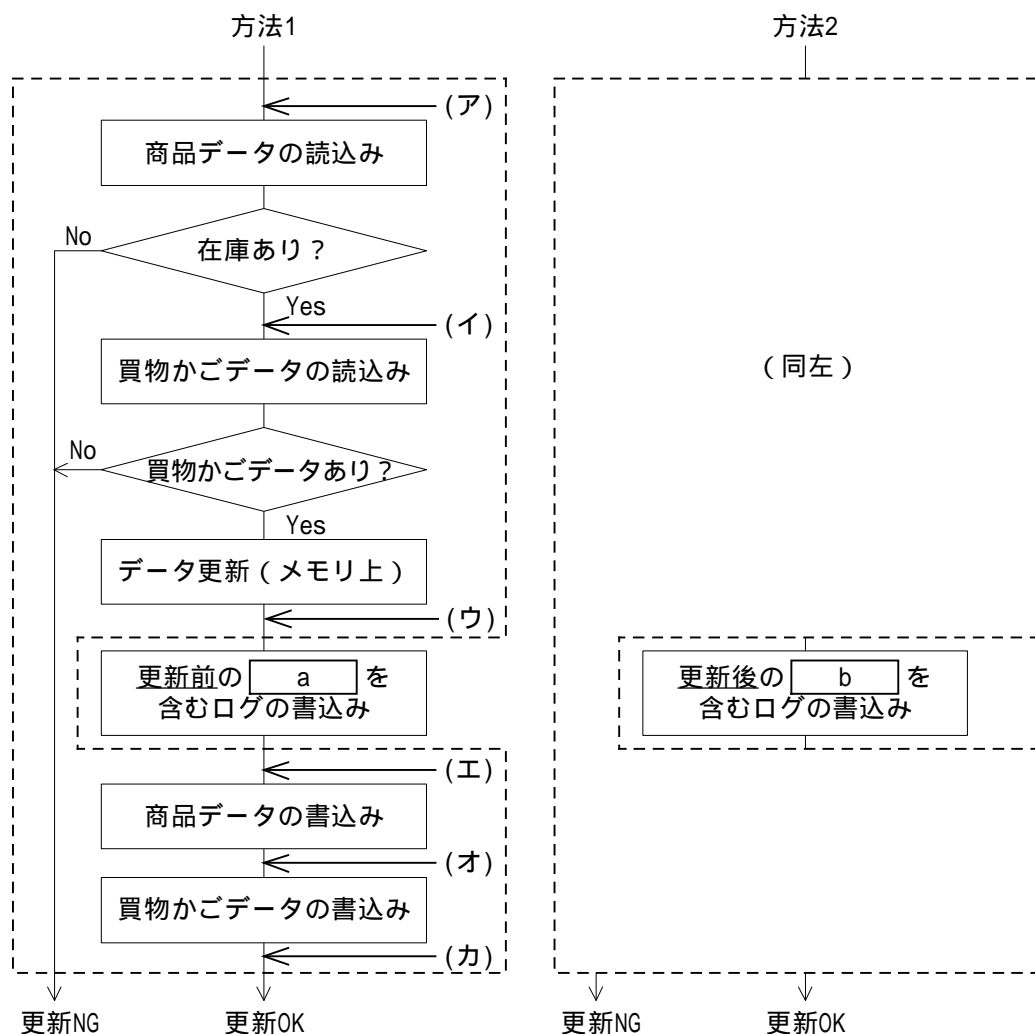


図5 1台のシステムで行う場合のデータ更新に関する処理の流れ

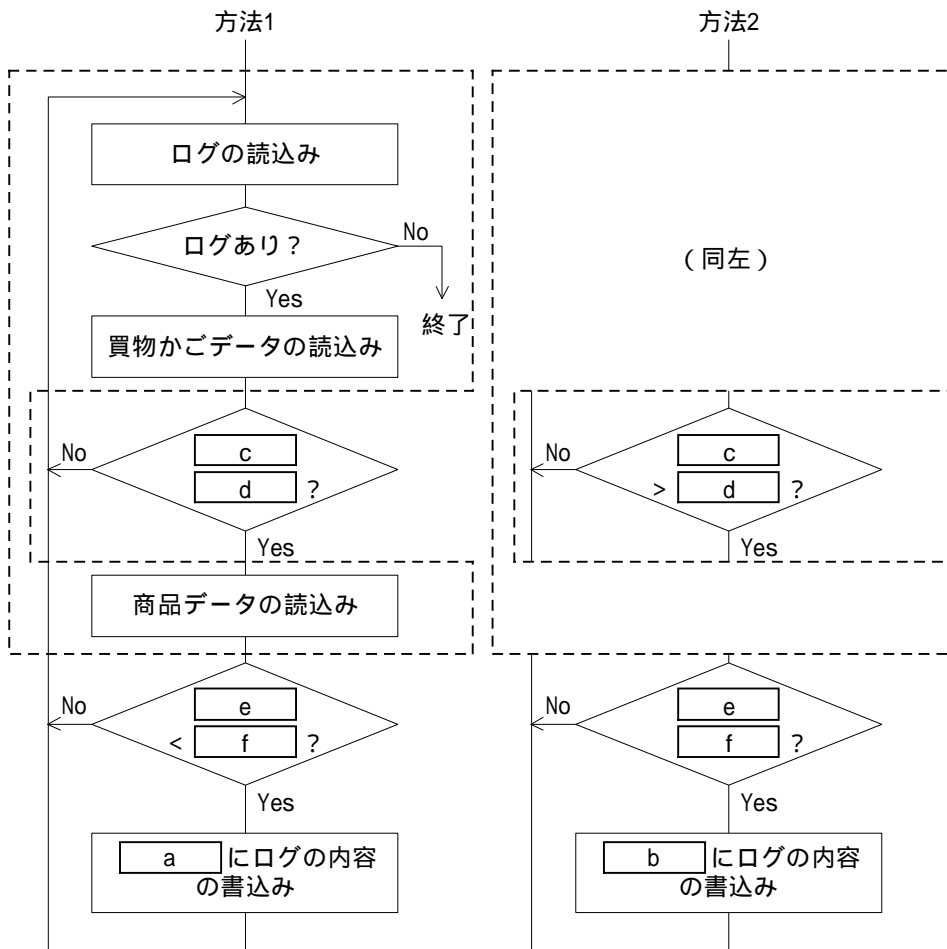


図6 1台のシステムで行う場合の回復処理の流れ

〔複数台のシステムで処理する場合〕

システムの分散化による拡張性及び保守性の向上のため、商品データを管理するシステム（以下、商品管理システムという）と買物かごデータを管理するシステム（以下、買物かご管理システムという）を分離し、それぞれをメインシステムから呼び出して処理する方法を検討する。システムの全体構成を図7に示す。

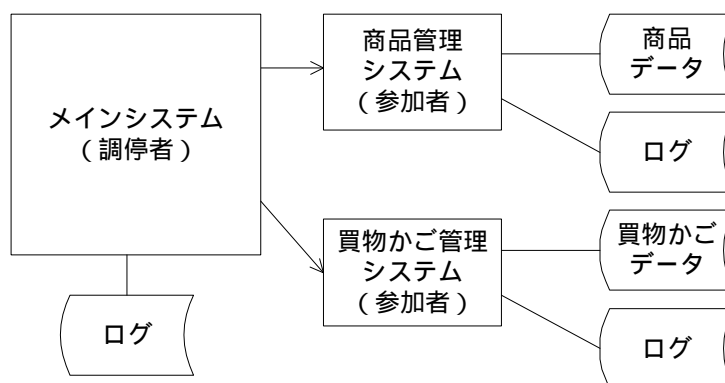


図7 複数台のシステムからなるシステムの全体構成

ここでは、トランザクション処理の方式として、分散構成における標準的な手順である 2 相コミットを使用する。2 相コミットでは、調停者及び複数の参加者からなるシステム構成において、調停者が参加者を、更新準備、コミット、ロールバックの 3 種類のインタフェースで呼び出す。ここでは、メインシステムが調停者に相当し、商品管理システム及び買物かご管理システムが参加者に相当する。

2 相コミットの手順は、次のとおりである。

調停者がすべての参加者に更新準備要求を送る。

参加者は、更新準備要求を受け取ると、更新が可能な場合には、更新後のデータをディスクに一時的に保存した後、OK 回答を返す。それ以外の場合には、NG 回答を返す。

調停者は、すべての参加者から更新準備の OK 回答を受け取ると、更新を実行することを決定し、すべての参加者にコミット要求を送る（たとえ、途中で何らかのエラーが発生しても、コミット要求による更新処理を貫く）。それ以外の場合は、更新を実行しないことを決定し、NG 回答を返した参加者以外のすべての参加者にロールバック要求を送る。

参加者は、更新準備要求に対して OK 回答を返した後は、コミット要求又はロールバック要求を受け取るまで（この間の状態を“更新準備中”と呼ぶ）、コミットが可能であることを保証するため、ほかのトランザクションからの当該データ更新の要求は受け付けない。

参加者は、更新準備中にコミット要求を受け取ると、更新後のデータをディスクに書き込んで更新を確定し、OK 回答を返す。更新準備中にロールバック要求を受け取ると、一時的に保存してあった更新後のデータを破棄し、OK 回答を返す。

途中でエラーが発生した後など、参加者がコミット要求を受け取ったとき更新準備中になっていない場合（既に更新済の場合）は、何もせずに OK 回答を返す。また、参加者がロールバック要求を受け取ったとき更新準備中になっていない場合（既にロールバック済の場合を含む）も、何もせずに OK 回答を返す。

調停者は、コミット要求又はロールバック要求に対して OK 回答を受け取らなかった場合には、システムで自動的に回復できないデータの不整合が発生した可能性があるため、アラームを発してその対処を人間系に促す。

本システムで 2 相コミットの手順に沿った処理を行うための、メインシステムから商品管理システムをデータ更新のために呼び出すインタフェースを表に示す。買物かご管理システムも同様のインタフェースをもつ。

表 商品管理システムをデータ更新のために呼び出すインタフェース

インタフェース	機能
商品データの更新準備	商品データの更新準備を行う。
商品データのコミット	商品データの更新準備で行った更新を確定する。
商品データのロールバック	商品データの更新準備で行った更新をとりやめる。

メインシステムでは、回復処理時に処理がどこまで進んでいたかを分かるようにするため、トランザクションごとにそれを特定するためのトランザクション番号を付与し、3 段階の処理時点（処理の順に処理時点 1～3 という）において、その処理時点を表す値などとともにログに書き込む。メインシステムのログのレコード構成を図 8 に示す。

ヘッダ	トランザクション 番号	処理時点	商品データ		買物かごデータ	
			キー	（省略）	キー	（省略）

図 8 メインシステムのログのレコード構成

商品管理システム及び買物かご管理システムは、データの更新準備の一部として、更新後のデータ内容（キー及び更新通番を含む）を、メインシステムから通知されたトランザクション番号とともにログに書き込む。

2 相コミットの手順に沿ったメインシステム及び商品管理システムの処理の流れを、それぞれ図 9、10 に示す（図 10 では商品データのロールバック処理は省略）。

商品管理システム及び買物かご管理システムでシステム障害が発生したときは、回復処理として、前回受付開始時（データの整合性が確実であった時点）からのログ及びその中のキーで示されているデータを読み込み、更新準備中のデータを把握して必要な状態に回復する。その後、メインシステムからのインタフェースの呼出しの受付を再開する。

メインシステムでシステム障害が発生したときは、回復処理として、商品管理システム及び買物かご管理システムとの接続を再確立した後、前回受付開始時からのログを読み込んでトランザクションの処理状態を調べる。処理途中のトランザクションがあれば、データ更新のためのインタフェースを使用して、商品管理システム及び買物かご管理システムに対しコミット又はロールバックの適切な要求を行い、データの不整合と更新準備中の状態を解消する。この回復処理の完了後、顧客からの操作の受付を再開する。

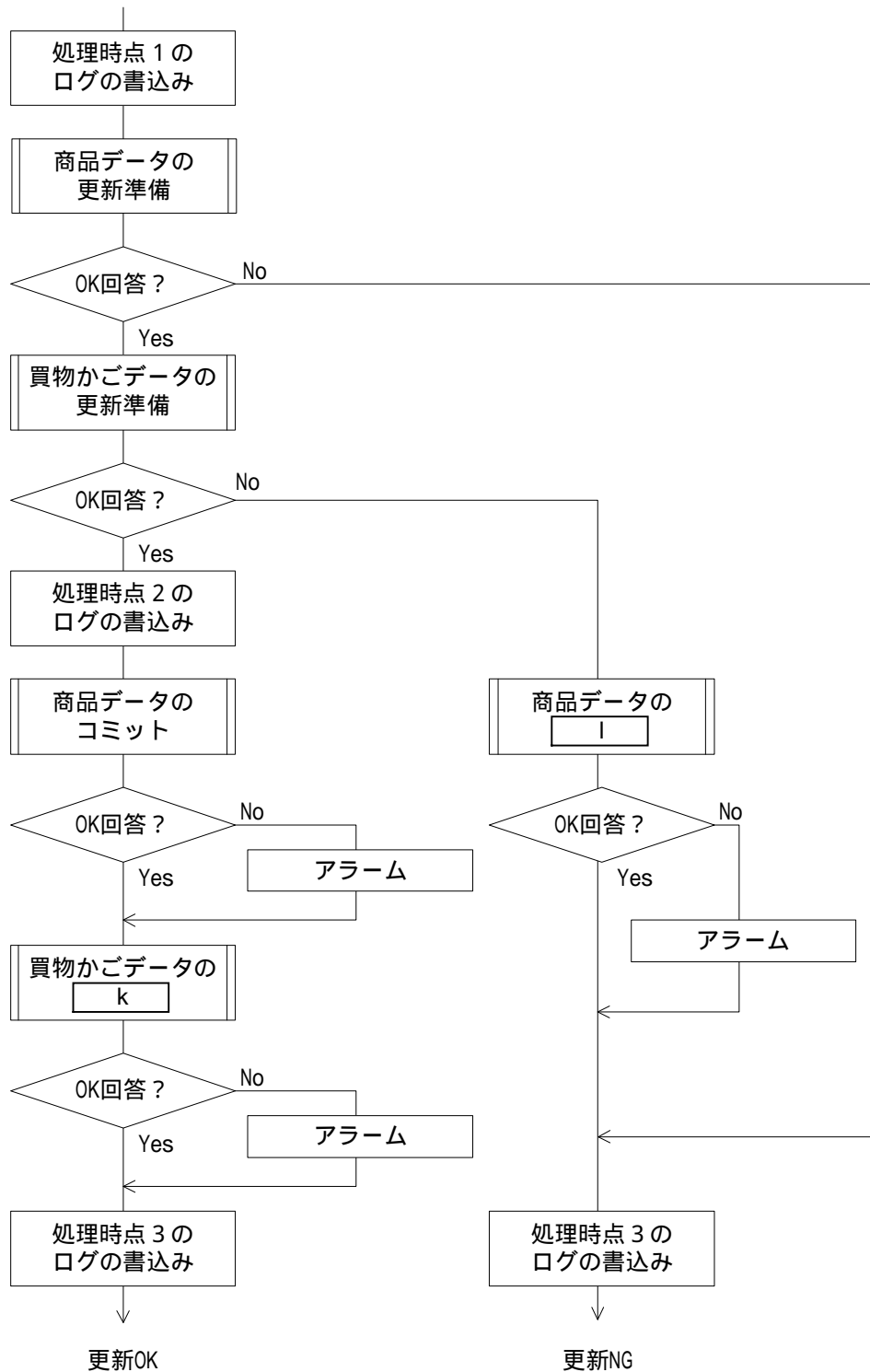
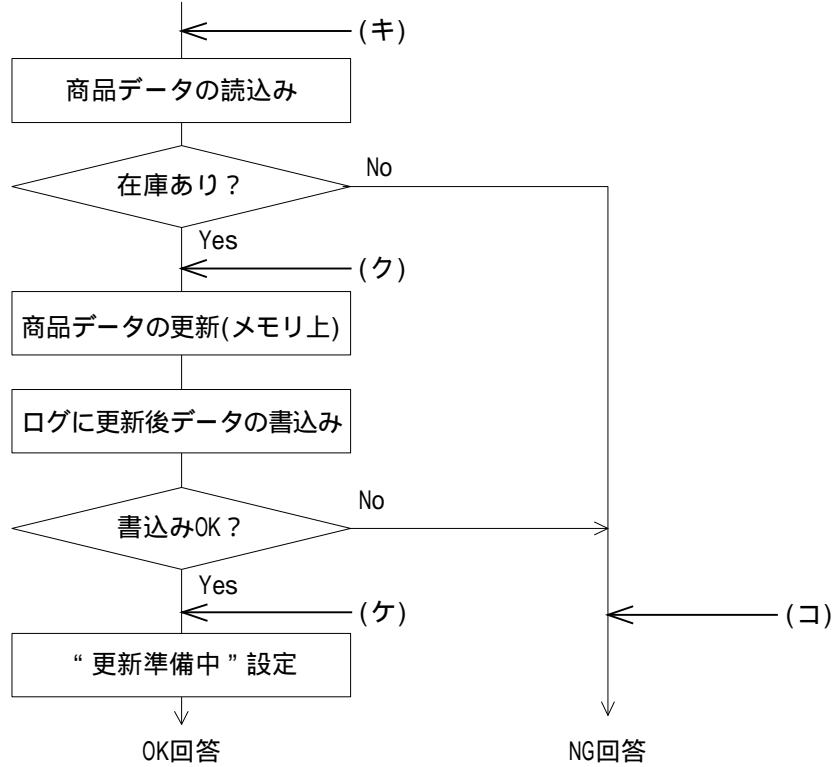


図9 メインシステムの処理の流れ

商品データの更新準備



商品データのコミット

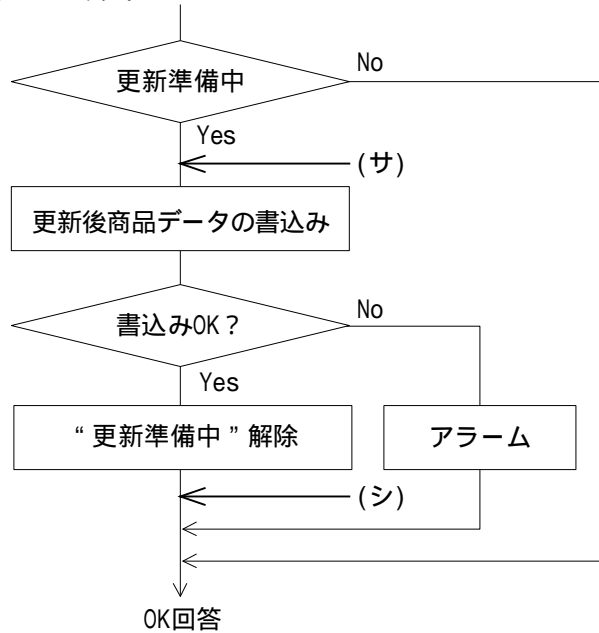


図 10 商品管理システムの処理の流れ

設問1 図5及び図6中の ~ に入れる適切な字句を解答群の中から選び、記号で答えよ。

解答群

- | | |
|--------------------|------------------|
| ア 買物かごデータ | イ 買物かごデータの更新通番 |
| ウ 商品データ | エ 商品データの更新通番 |
| オ ログ上の買物かごデータの更新通番 | カ ログ上の商品データの更新通番 |

設問2 〔1台のシステムで処理する場合〕において、複数要求の同時並行処理の実施を検討した次の記述中の , に入れる適切な字句又は数値を答えよ。また、 に入れる適切な記号を、図5中の（ア）～（カ）の中から選べ。 に入れる適切な字句を“前”、“後”から選べ。

同時並行処理においてデータ更新の整合性を保つために、各データのレコードに読み書きの排他制御のためのロックをかけて処理を直列化する。ただし、性能への影響を考慮して、ロックは必要最小限の範囲にとどめる。商品データには、その読み込みから書き込みまで、すなわち図5において方法1、方法2ともに（ア）から（オ）まで、ロックをかけておくことにした。買物かごデータについては、本システムでは1ログインから 要求を受け付けないようにし、ロックは不要とした。

しかし、この方法では商品データの更新に問題が起こるおそれがあることが分かった。その問題が起こるのは方法 において、 の時点で別のトランザクションによる商品データの更新 にシステム障害が発生した場合である。対策として、商品データのロックの範囲を（ア）から（カ）までに変更すればよい。

設問3 図9中の , に入れる適切な字句を答えよ。また、同時並行処理を行う場合において、データの整合性を確保するために各データのレコードにロックをかけて処理を直列化する場合、図10中の（キ）～（シ）の中から、ロックをかける適切な位置を1か所、ロックを解除する適切な位置を2か所選び、それぞれ記号で答えよ。

設問4 〔複数台のシステムで処理する場合〕のメインシステムにおいて、各トランザクションについて書かれているログは、“処理時点1だけ”、“処理時点2まで”、“処理時点3まですべて”の3通りに分かれる。メインシステムの回復処理において、読み込んだトランザクションごとのログがこれら3通りのそれぞれの場合に、データの不整合と更新準備中の状態を解消するために、商品管理システム及び買物かご管理システムに対して同じ処理を要求する。それぞれの場合に要求すべき適切な処理内容を答えよ。ここで、処理要求が不要の場合は“不要”と答えよ。