

問2 業務委託におけるアクセス制御に関する次の記述を読んで、設問1, 2に答えよ。

A社は従業員数200名の通信販売業者である。一般消費者向けに生活雑貨、ギフト商品などの販売を手掛けており、商品の種類ごとに販売課が編成されている。

[Z販売課の業務]

現在、Z販売課は、商品Zについて顧客から電子メール又はファックスによる注文及び問合せを受け、その対応を行っている。商品Zの販売に関わる要員（以下、商品Z関連要員という）は、販売責任者であるZ販売課N課長、及びその管理下に5名の担当者、並びに業務委託先の管理者であるB社運用課L課長、及びその管理下に8名の担当者の、計15名で構成されている。商品Z関連要員の業務を図1に示す。

1. 受注管理業務

顧客から届く注文を確認し、受注手続を行う。受注管理システム（以下、Jシステムという）を利用する。本業務は、A社のZ販売課の要員が担当する。

(1) 入力

担当者は、届いた注文（変更、キャンセルを含む）の内容を確認し、不備があれば顧客に問い合わせる。不備がなければその情報をJシステムに入力し、販売責任者に承認を依頼する。

(2) 承認

販売責任者は、注文の内容とJシステムへの入力結果を突き合わせて確認し、問題がなければ承認する。問題があれば差し戻す。

2. 問合せ対応業務

顧客からの問合せに対応する。問合せ管理システム（以下、Tシステムという）を利用する。本業務は、業務委託先であるB社の運用課の要員が担当する。

(1) 入力

担当者は、顧客から届いた問合せの内容を確認し、回答案をTシステムに入力して、管理者に承認を依頼する。

(2) 承認

管理者は、回答案を確認し、問題がなければ承認する。これによってTシステムから顧客に回答が返信される。問題があればコメントを付記して差し戻す。

補足：Jシステム及びTシステムはA社の情報システム部が運用している。

図1 商品Z関連要員の業務（概要）

B社は、自社内にA社からの受託業務専用のオペレーションルームをもち、そこからA社のTシステムにアクセスしている。B社は、A社からの受託業務に必要な

設備及び管理体制を整えており、A 社が定める情報セキュリティ要件を満たしている。

[J システム及び T システムの操作権限]

Z 販売課では、J システム及び T システムについて、次の利用方針を定めている。

- [方針 1] 1 人の利用者に、一つの利用者 ID を登録する。
- [方針 2] 一つの利用者 ID は、1 人の利用者だけが利用する。
- [方針 3] ある利用者が入力した情報は、別の利用者が承認する。
- [方針 4] 販売責任者は、Z 販売課の全業務の情報を閲覧できる。

J システム及び T システムでは、業務上必要な操作権限を利用者に与えるためにシステム上の役割（以下、ロールという）を定義する機能が実装されている。ロールには、業務上必要な操作権限の組合せが付与される。利用者 ID にロールを設定することによって、利用者の操作権限が決まる。一つの利用者 ID にはロールを一つだけ設定する。システム利用部署の長は、所属する利用者の利用者 ID に対するロール設定を情報システム部に依頼する。情報システム部が受けた依頼はシステムに登録され、翌営業日の朝 5 時に自動的にシステムに反映される。

J システム及び T システムにおいて、商品 Z 関連要員の利用者 ID に設定されているロールの種類とその操作権限を表 1 に示す。

表 1 ロールの種類とその操作権限

ロール	J システム			T システム		
	閲覧	入力	承認	閲覧	入力	承認
A 社販売責任者	○		○	○		
A 社販売担当者	○	○		○		
B 社管理者				○		○
B 社 T システム担当者				○	○	

注記 ○は、操作権限が付与されていることを示す。

例えば、N 課長の利用者 ID には“A 社販売責任者”というロールを設定して、J システムの閲覧及び承認並びに T システムの閲覧の権限をもたせている。

〔受注管理業務の委託〕

Z 販売課では、受注管理業務を担当する A 社の従業員の作業量が受注増によって増えていることから、この業務の入力作業を B 社に対して追加で委託することにした。追加の業務委託で必要となる J システムの操作権限の見直しを、A 社の販売課全体の情報セキュリティリーダーを務める販売管理課の M 主任が支援することになった。

M 主任は、受注管理業務における A 社と B 社の役割分担について、Z 販売課の N 課長からヒアリングした内容を次のとおり整理した。

〔要求 1〕 B 社が入力した場合は、A 社が承認する。

〔要求 2〕 A 社の担当者が入力した場合は、現状どおりに A 社の販売責任者が承認する。

これに基づき M 主任が作成した新しい操作権限案を表 2 に示す。

表 2 新しい操作権限案

ロール ロール	J システム			T システム		
	閲覧	入力	承認	閲覧	入力	承認
A 社販売責任者	○		○	○		
A 社販売担当者	○	○		○		
B 社管理者	◎	◎		○		○
B 社 T システム担当者				○	○	
B 社 J システム担当者	◎	◎				

注記 1 ○は、付与される操作権限のうち、表 1 と同じものを示す。

注記 2 ◎は、付与される操作権限のうち、表 1 に比べて新しく追加したものを示す。

次は、この操作権限案についての M 主任と N 課長との会話である。

M 主任 : N 課長の要求に従ってロールとその操作権限を見直してみました。

N 課長 : 確かに、要求どおりだ。ただ、販売責任者は私だけなので業務が停滞することが心配だ。B 社で入力した情報は A 社の担当者が承認すればよいので、“A 社販売担当者” ロールに承認権限を追加できないだろうか。

M 主任 : 承認権限を追加すると、① J システムで利用方針に違反してしまいます。

N 課長 : “A 社販売担当者” ロールに承認権限を追加し、その上で、利用方針にも合

うようにしたい。例えば a ことはできるだろうか。

M 主任：それならば、利用方針は順守できそうです。ただ、システムの改修が必要ですね。また、② [要求 2] を満たせません。別の案ですが、b ようにシステム改修するのはどうでしょう。

N 課長：確かに、それなら [要求 2] も満たせる。早速、その方針で情報システム部にシステム改修の相談をしてくれないか。

M 主任：承知しました。確認ですが、N 課長は、出張などで承認手続きができなくなるようなケースはありませんか。

N 課長：今のところ問題ない。ただ、③ 来年度から毎年 2, 3 回, 2 週間ほどの海外出張に出る予定なので、誰かに代行してもらう必要が出てくる。この対応も検討したい。それと、B 社の L 課長からの話だが、一日の中でも問合せ数が少ない時間に、問合せ対応業務の担当者の一部が受注管理業務を応援できる運用を希望していたよ。あらかじめ担当者を任命して教育もしておくそうだ。

M 主任：承知しました。すぐに B 社に詳細を確認して④ 必要な操作権限を与える方法を検討します。

M 主任は、B 社の管理者及び A 社の情報システム部と調整して、N 課長とともに J システムの改修案、運用案を取りまとめた。

#### [B 社担当者の追加及び変更]

A 社情報システム部では、社内データベースに格納された情報を閲覧するための情報閲覧システム（以下、D システムという）を提供している。D システムで商品 Z 関連要員に付与されている閲覧権限を表 3 に示す。

なお、利用者 ID は、J システム及び T システムと共通である。

表3 商品Z関連要員に付与されている閲覧権限（抜粋）

情報の オーナー部署	情報	...	A社Z販売課の 要員	B社運用課の 要員
販売管理課	在庫情報	...	○	○
販売管理課	販売計画・実績情報	...	○	
サービス企画課	お客様情報	...	○	○
商品企画課	商品カタログ情報	...	○	○
商品企画課	問合せ履歴情報	...	○	○

注記 ○は、閲覧権限が付与されていることを示す。

A社では、Dシステムの閲覧権限の付与について、次の手続を定めている。

- (1) 各情報のオーナー部署の長が、閲覧権限を付与する対象者を決める。
- (2) 情報システム部は、情報のオーナー部署の長の決定に従ってDシステムの閲覧権限を設定する。
- (3) 利用部署の希望によって閲覧権限を付与する場合は、利用部署の長が、その情報のオーナー部署の長に申請して承認を得る。申請を承認した情報のオーナー部署の長は、情報システム部に対して閲覧権限の付与を依頼する。
- (4) 利用部署が、業務委託先要員への閲覧権限付与を希望する場合は、c。

次は、B社の担当者の追加及び変更に関する、M主任とN課長の会話である。

M主任：新しく追加されるB社Jシステム担当者に付与する閲覧権限について相談があります。dのリスクを低減するために、表3に示すDシステムの閲覧権限を見直して、必要最小限にした方がよいと思います。

N課長：Jシステム担当者の作業は、届いた注文の確認と入力だ。商品カタログ情報とお客様情報の閲覧だけだな。

M主任：では、N課長からeに対して、閲覧権限の付与を申請していただけますか。

N課長：新しいB社担当者の名簿はできているかな。

M主任：はい。B社から情報を受領しました。Jシステム担当者は3名です。

N課長：Tシステム担当者に変更はないかな。

M主任：あります。⑤来月中に1人が退任し1人が新規に着任すると聞きました。

引継ぎを兼ねて、おおよそ1週間は2人とも在籍してTシステムとDシステムを利用して業務を行う予定です。必要な権限を正しくシステムに登録するために、B社に担当者変更がある場合、原則2週間前に f から情報提供してもらうよう業務委託契約で定めています。後ほど、⑥正式に情報を受領します。

N課長：分かった。今回、業務委託の対象システムも人員も増えるので、改めて情報漏えい対策に力を入れていきたい。頼りにしているよ。

こうしてN課長とM主任は必要な準備を進め、新しい体制で業務を開始することができた。

設問1 〔受注管理業務の委託〕について、(1)～(6)に答えよ。

(1) 本文中の下線①について、どの利用方針に違反するか。違反が考えられる利用方針だけを全て挙げた組合せを、解答群の中から選べ。

解答群

- |         |                 |
|---------|-----------------|
| ア [方針1] | イ [方針1] , [方針2] |
| ウ [方針2] | エ [方針2] , [方針3] |
| オ [方針3] | カ [方針3] , [方針4] |

(2) 本文中の下線①について、この利用方針違反はどのリスクを高めると考えられるか。解答群のうち、最も適切なものを選べ。

解答群

- ア 正しく入力された注文が承認されず滞留してしまう。
- イ 正しく入力された注文の情報が窃取されてしまう。
- ウ 不正に入力された注文が差し戻されて滞留してしまう。
- エ 不正に入力された注文が承認されてしまう。

(3) 本文中の  ,  に入れる適切な字句を、解答群の中から選べ。

a, b に関する解答群

- ア “A 社販売責任者” ロールを設定した利用者 ID を二つに増やす
- イ “B 社 J システム担当者” ロール又は “B 社管理者” ロールを使って入力された注文だけを承認できる権限を追加する
- ウ 自分が承認したい注文だけを検索できる機能を追加する
- エ 承認できる利用者 ID を、入力者が指定する権限を追加する
- オ 他の利用者 ID によって入力された注文だけを承認できる権限を追加する

(4) 本文中の下線 ② について、なぜ  では [要求 2] を満たせないのか。その理由を、解答群の中から選べ。ここで、 には正しい答えが入っているものとする。

解答群

- ア “A 社販売責任者” ロールの利用者が、B 社で入力された情報を承認できなくなるから。
- イ “A 社販売責任者” ロールの利用者が、自分宛での承認依頼に気づくとは限らないから。
- ウ “A 社販売担当者” ロールの利用者が複数人いるとき、1 人が入力し、別の 1 人が承認することができるから。
- エ “B 社管理者” ロールの利用者が承認権限をもっているから。

- (5) 本文中の下線③について、N 課長が出張中に他の者が代行するための措置のうち、利用方針に合致するものを、解答群の中から選べ。

解答群

- ア “A 社販売責任者” ロールを設定した利用者 ID を一つ追加発行し、A 社の担当者の 1 人が、代行者として利用する。
- イ A 社の担当者の 1 人を代行者に任命し、“A 社販売責任者” ロールの権限を追加で付与した新しいロールを作成して、代行者の利用者 ID に設定する。
- ウ N 課長が、出張の期間に限り、自分の利用者 ID、パスワードを別の販売課の課長に貸す。
- エ N 課長の上長に代行を依頼し、代行者の利用者 ID を J システム及び T システムに登録して“A 社販売責任者” ロールを設定する。
- (6) 本文中の下線④について、情報システム部に依頼して必要な操作権限を与える方法はどれか。解答群のうち、最も適切なものを選べ。ここで、応援に回す B 社担当者を B 社応援担当者という。

解答群

- ア “B 社 J システム担当者” ロールを設定した貸出し用の利用者 ID を準備し、応援の都度、B 社応援担当者はこの利用者 ID を利用させる。
- イ “B 社 T システム担当者” ロールの権限と “B 社 J システム担当者” ロールの権限を併せ持つ新しいロールを定義し、B 社応援担当者の利用者 ID に設定しておく。
- ウ B 社応援担当者の利用者 ID に対して “B 社管理者” のロールを設定しておく。
- エ 応援の都度、B 社応援担当者の利用者 ID に設定されたロールを “B 社 J システム担当者” に切り替えてもらう。



設問2 [B社担当者の追加及び変更]について、(1)～(4)に答えよ。

- (1) 本文中の  に入れる字句はどれか。解答群のうち、最も適切なものを選べ。

cに関する解答群

- ア 業務委託先の管理者が、利用部署の長に名簿を提出するとともに、情報のオーナー部署の長に申請する
- イ 業務委託先の従業員が、利用部署の長に申請し、利用部署の長が、情報のオーナー部署の長に申請する
- ウ 利用部署の長が、業務委託先から提出された申請書を情報のオーナー部署の長に転送する
- エ 利用部署の長が、業務委託先の管理者から提出された利用者の情報に基づき、情報のオーナー部署の長に申請する

- (2) 本文中の  ～  に入れる適切な字句を、解答群の中から選べ。

dに関する解答群

- ア 内部不正
- イ 入力時のタイプミス
- ウ 病欠

e, fに関する解答群

- ア B社の管理者
- イ 情報システム部
- ウ 情報のオーナー部署の長

- (3) 本文中の下線⑤について、対応するために必要な利用者 ID 管理の手続はどれか。解答群のうち、最も適切なものを選べ。

解答群

- ア 新任者がすぐに業務を開始できるよう、あらかじめ新任者用の利用者 ID の登録を情報システム部に依頼しておく。退任者の利用者 ID は削除しなくても支障はないのでそのままにしておく。
- イ 退任者が本当に業務を離れたことを確認してから、退任者の利用者 ID を新任者用に割り当てるよう、情報システム部に依頼する。
- ウ 引継ぎ開始に当たり、新任者の利用者 ID を発行し、引継ぎ期間後、直ちに退任者の利用者 ID を無効化するよう、情報システム部に依頼する。
- エ 引継ぎ開始に当たり、直ちに退任予定者の利用者 ID を無効化すると同時に、新任者の利用者 ID を発行するよう、情報システム部に依頼する。

- (4) 本文中の下線⑥について、今回の担当者変更のために受領する情報としては**不要なもの**を、解答群の中から選べ。

解答群

- ア 新任者の閲覧希望情報
- イ 新任者の着任予定日
- ウ 退任者の退任予定日
- エ 退任者の利用者 ID