

演習

サービス継続及び可用性管理

平成25年度 問2

問 サービス継続及び可用性管理に関する次の記述を読んで、設問1～3に答えよ。

X社は、自社ブランドの陶磁器の製造・販売会社である。本社と工場は北陸にあり、営業所と倉庫は関東にある。販売は、主に関東近辺のデパートで行っている。

工場の生産管理部では生産の計画・管理、工場に隣接する本社では一般管理業務、営業所の販売部では商品の販売業務・売上分析、営業所の近郊にある倉庫ではデパートへの商品発送業務を行っている。また、情報システム部は、北陸のデータセンタA（以下、DC-Aという）と関東のデータセンタB（以下、DC-Bという）で主要システムの運用を行っており、生産管理部及び販売部の業務支援サービスを提供している。

〔主要システムの構成〕

X社の主要システムの構成を図1に示す。情報システム部は、DC-Aで販売管理システムと生産管理システムを運用し、DC-Bで売上分析システムと在庫管理システムを運用している。また、DC-Bでは、販売管理システムの待機系システムが稼働可能である。ただし、DC-Bは仮想サーバで構築されている関係から、待機系システムが稼働する際は売上分析システムの停止が必要になる。本番系システムに障害が発生した場合は、売上分析システムを停止してから待機系システムを起動し、システムの切替えに必要な作業を行って、販売管理システムのサービスを再開する。

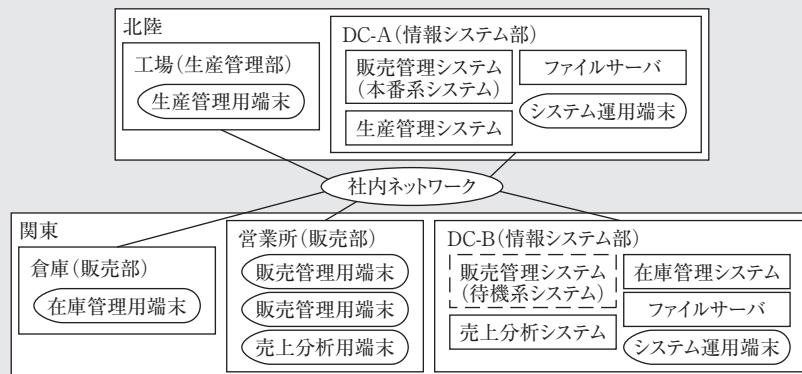


図1 X社の主要システムの構成

〔販売管理システムの機能概要〕

販売部は、顧客から商品の注文を受けると、手書きで注文伝票を作成する。注文伝票の注文情報は、オンラインで販売管理用端末から販売管理システムに入力される。注文情報は、販売管理システムから在庫管理システムに連携されて、商品の在庫引当処理と出荷指示処理が行われる。注文情報は日次バッチ処理で受注情報として確定し、顧客ごとに受注実績が集計される。受注実績は、翌日にはオンラインで参照可能となり、顧客との商談に利用される。

販売管理システムは、毎日9時から20時までをオンライン処理時間帯、20時から翌日5時までをバッチ処理実施可能時間帯としている。バッチ処理では、販売管理システムの一部であるジョブ管理ツールによって、ジョブが順番に起動される。販売管理システムにおけるバッチ処理の区分と内容を、表1に示す。

表1 販売管理システムにおけるバッチ処理の区分と内容

区分	ジョブ番号	処理内容	所要時間
日次バッチ処理	1-1	注文情報のバックアップを取得する。	1時間
	1-2	業務日付 ¹⁾ を更新する。	5分
	1-3	注文情報を加工して受注情報として確定し、顧客ごとに集計し、受注実績とする。	5時間
週次バッチ処理 ²⁾	2-1	業務日付 ¹⁾ 、受注情報及び受注実績のバックアップを取得して、取得情報をDC-Bのファイルサーバに転送する。	1時間

注¹⁾ OSなどが使用するシステム日付とは別に、業務アプリケーションが参照する日付として“業務日付”が定義されている。

²⁾ 週次バッチ処理は、毎週金曜日の日次バッチ処理終了後に実行される。

〔販売管理用端末の増設〕

X社では現在、営業所に2台の販売管理用端末があるが、販売業務の拡大に備えて、端末を2台増設することになった。販売管理システムには許可された端末からしか接続できないので、ITサービスマネージャのU氏は、増設される端末からの接続を許可するように本番系システムの設定変更を計画した。情報システム部の担当者は変更計画に従って変更を行い、増設された端末の本番運用を開始した。本番系システムの設定変更を待機系システムへ反映する作業については、変更をできるだけ早く展開する必要があるが、売上分析システムの稼働スケジュールとの関係から、3か月に1回設けられている売上分析システムの次回定期保守日に行うことにしている。また、規定に従い、本番系システムの変更に合わせて、“待

機系システムの変更に必要なリリース”及び“リリースの展開に必要な関連文書”を、DC-Bに設置されているファイルサーバに格納し、DC-Bの情報システム部に通知した。

〔事業継続計画の検討〕

営業所に販売管理用端末を増設してから1か月後、X社は、事業継続計画（以下、BCPという）を策定することになり、BCP策定プロジェクト（以下、プロジェクトという）を発足させた。プロジェクトは、生産管理部、販売部などの責任者から成る全社横断チームで構成され、意思決定には経営陣が関与した。情報システム部からはT部長が参画した。プロジェクトでは、BCPを策定する際の災害発生から全面復旧に至るまでの想定フェーズを図2のように整理した。

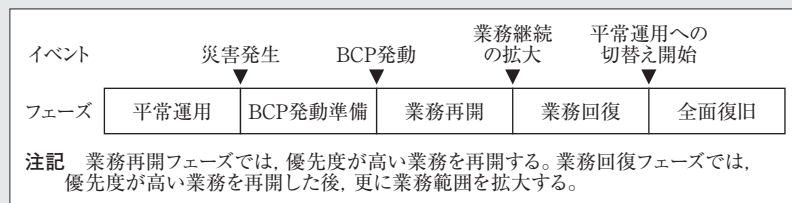


図2 災害発生から全面復旧に至るまでの想定フェーズ

プロジェクトでは、北陸に地震が発生し、交通の混乱、通信障害及び大規模停電によって、本社、工場及びDC-Aが1週間稼働できない事態を想定した。

なお、本社、工場及びDC-Aの建物・設備に直接の被害はないものとする。また、関東では、地震による被害は発生しないものとし、X社の主要顧客やデパートは関東地区に集中しているので、被災による顧客やデパートへの影響は少ないものとする。

プロジェクトでは、これらの想定の下で、BCPの方針を表2のように整理した。

表2 BCPの方針

項番	方針
1	地震の発生によって、事業が受ける影響度を分析した。その結果、事業を継続する上で優先度が最も高いのは、販売業務であることが分かった。そこで、生産が1週間滞った場合でも販売を継続できるように、必要な在庫調整を行う。販売業務については、災害発生直後は販売管理用端末からのオンラインによる注文情報の入力を諦め、手書きによる注文伝票の作成だけで業務を継続させる。また、生産業務については、業務回復フェーズに北陸で再開する。

（次ページに続く）

項番	方針
2	災害発生時には、社長を対策本部長とする対策本部を設置し、意思決定機関としてBCPの実施を指揮する。対策本部長の下に生産、販売といった機能別のチーム体制を編成し、情報システム部からはT部長が対策本部に加わる。

プロジェクトでは、商品を販売する際は、販売部が顧客などと商談を行う必要がある点を踏まえ、災害発生から3時間以内に待機系システムで販売管理システムのオンライン機能を正常に使用できるようにすることを、事業継続の要件として取り決めた。また、当日のオンライン開始から災害発生までに登録された注文情報については、販売部が注文伝票を基に再入力することとした。

T部長はこれらのBCPの検討を受け、販売管理システムがオンライン処理時間帯に被災することを想定し、図2のBCP発動準備フェーズから全面復旧フェーズまでを対象範囲としたサービス継続計画を作成するよう、U氏に指示した。

〔サービス継続計画の作成〕

U氏は、災害発生後の販売管理システムの業務再開に向けての目標値について、販売部と確認した。その結果、目標復旧時間(以下、RTOという)及び目標復旧時点(以下、RPOという)については、プロジェクトの検討結果を踏まえ、RTOを a 以内、RPOを b 時点に設定した。また、平常運用フェーズではオンラインの応答時間の目標値を3秒以内としているが、業務再開フェーズと業務回復フェーズでは待機系システムでのサービス提供になるので、応答時間の目標値は5秒まで許容することにした。

U氏は、T部長からの指示を踏まえ、BCPと連携したサービス継続計画を作成し、BCP発動を受け、サービス継続計画が発動されることを規定した。サービス継続計画が発動された場合は、待機系システムを起動し、転送済みのバックアップから必要なデータをリストアした上で、待機系システムに切り替える予定である。しかし、現在のバッチ処理の構成ではRPOの目標値を達成できないと考えたU氏は、(ア)バッチ処理の内容を見直した。

T部長はサービス継続計画の内容を確認し、U氏に試験の実施を指示した。

〔サービス継続計画の試験〕

U氏は、BCP発動準備フェーズから全面復旧フェーズまでを対象として、サービス継続計画の試験計画書を作成した。この試験によって、情報システム部員の訓練だけでなく、サービス継続計画全体が正しく機能するかどうかを確認する。試験計画書の内容を、表3に示す。

表3 サービス継続計画の試験計画書の内容

項番	フェーズ	実施項目	確認すべき内容	試験方法
1	BCP発動準備	復旧作業要員の配置	復旧作業に関わる情報システム部員への連絡	机上チェック
2	業務再開	待機系システムを使ったサービス運用の開始	売上分析システムの正常停止、待機系システムの起動、データリストアの実施、切替えの実施確認、及び提供サービスの正常稼働確認	実機訓練
3	業務回復	サービス運用の拡大	生産管理システムの起動及び提供サービスの正常稼働確認	実機訓練
4	全面復旧	全面復旧手順の確認	<div style="border: 1px solid black; padding: 2px; display: inline-block;">c</div>	実機訓練

U氏は、関係者の協力を得て試験を行った。試験では、増設された2台の販売管理用端末から待機系システムに接続できないという事態が発生し、混乱した。原因は、売上分析システムの定期保守日に実施予定であった変更リリースが展開される前に試験を実施したからであり、必要な対応を行い、試験は無事終了した。

試験終了後、T部長は、(イ)サービス継続計画の発動後に今回のような混乱が発生しないように、業務再開フェーズに必要な作業内容の追加をU氏に指示した。

設問1 [事業継続計画の検討]において対策本部を設置するとしているが、災害発生当初に関係者全員を招集できるとは限らない。このような状況を考慮した上で考えられる、対策本部の要員配置に必要な検討内容を、35字以内で述べよ。

設問2 [サービス継続計画の作成]について、(1)、(2)に答えよ。

- (1) 本文中の

a

 に入れる適切な字句を5字以内で、

b

 に入れる適切な字句を15字以内で、それぞれ答えよ。
- (2) 本文中の下線(ア)について、見直し後のバッチ処理の内容を、50字以内で具体的に述べよ。

設問3 [サービス継続計画の試験]について、(1)～(3)に答えよ。

- (1) 表3中の項番2の業務再開フェーズにおいて、提供サービスの正常稼働に関して、機能面に加えて、確認すべき内容を、35字以内で具体的に述べよ。
- (2) 表3中の

c

 に入れる確認すべき内容を、55字以内で述べよ。
- (3) 本文中の下線(イ)について、業務再開フェーズに追加すべき作業内容を、55字以内で具体的に述べよ。

解答例

設問1 35字以内

対策本部に招集できた者によってチーム編成等を決め、最適な要員配置をする

〔試験センターによる解答例〕

- 予定された要員を招集できない場合に備えて代替要員を定める。
- 要員が不足する場合は、招集できた要員で役割分担を決める。

設問2 (1) a：5字以内, b：15字以内 (2) 50字以内

(1)

空欄a

3 時間

空欄b

当日のオンライン開始

〔試験センターによる解答例〕

- 空欄a：3時間
- 空欄b：当日のオンライン開始

(2)

週次バッチ処理のジョブ番号2-1をジョブ番号1-3の後に移動し、日次バッチ処理の一部として実行する

〔試験センターによる解答例〕

ジョブ番号2-1を週次バッチ処理から日次バッチ処理に変更し、ジョブ番号1-3の後に実行する。

設問3 (1) 35字以内 (2) 55字以内 (3) 55字以内

(1)

待	機	系	シ	ス	テ	ム	で	の	オ	ン	ラ	イ	ン	の	応	答	時	間	が	5	秒	以	内	に	収	ま	っ	て	い
る	こ	と																											

5 10 15 20 25 30

〔試験センターによる解答例〕

販売管理システムのオンラインの応答時間が5秒以内であること

(2)

待	機	系	シ	ス	テ	ム	の	停	止	,	本	番	系	シ	ス	テ	ム	の	起	動	,	売	上	分	析	シ	ス	テ	ム
の	起	動	,	提	供	サ	ー	ビ	ス	の	正	常	稼	働	確	認													

5 10 15 20 25 30

〔試験センターによる解答例〕

販売管理システム(本番系システム)への切り戻し、売上分析システムの起動及び提供サービスの正常稼働確認

(3)

本	番	系	シ	ス	テ	ム	の	設	定	変	更	を	待	機	系	シ	ス	テ	ム	に	反	映	す	る	作	業	が	あ	れ
ば	試	験	前	に	実	施	す	る	か	,	未	実	施	で	も	試	験	可	能	か	判	定	す	る					

5 10 15 20 25 30

〔試験センターによる解答例〕

待機系システムに未実施の変更がある場合は、切替え前までに当該リリースの展開実施判断を行い、必要ならば展開する。

設問別解説

設問のパターンと難易度

設問1	C 記憶＋記述型	中
設問2 (1)	A 解答探索型	易
(2)	B ヒント＋記述型	中
設問3 (1)	A 解答探索型	易
(2)	B ヒント＋記述型	中
(3)	B ヒント＋記述型	難

設問1

“表2 BCPの方針”の項番2は、下記のとおりである。

災害発生時には、社長を対策本部長とする対策本部を設置し、意思決定機関としてBCPの実施を指揮する。対策本部長の下に生産、販売といった機能別のチーム体制を編成し、情報システム部からはT部長が対策本部に加わる。

本設問は、災害発生当初に関係者全員を対策本部に招集できるとは限らない状況を想定して、対策本部の要員配置に必要な検討内容を問うている。例えば、社長が対策本部に来られない状況になった場合に、対策本部の要員配置はどうなるのだろうか。社長がいないのであるから、災害発生時に本社などの指定された場所に駆けつけてきた副社長や専務などの中から対策本部長を選任するしかない。他の者についても同様であり、生産チームや販売チームのメンバーも、対策本部にいる者の中から配員されることになる。

したがって、解答は“対策本部に招集できた者によってチーム編成等を決め、最適な要員配置をする”のようにまとめられる。

設問2

(1) 空欄a、bを含む文は、下記のとおりである。

その結果、目標復旧時間（以下、RTOという）及び目標復旧時点（以下、RPOという）については、プロジェクトの検討結果を踏まえ、RTOを 以内、RPOを 時点に設定した。

目標復旧時間 (RTO : Recovery Time Objective) は災害が発生してから復旧するまでに必要な時間であり、目標復旧時点 (RPO : Recovery Point Objective) は災害が発生した場合に復旧できる最新のデータの時点である。

RTOとRPOを図で示せば、下記になる。



表2から下へ1, 2文目は、下記のとおりである。

プロジェクトでは、商品を販売する際は、販売部が顧客などと商談を行う必要がある点を踏まえ、災害発生から3時間以内に待機系システムで販売管理システムのオンライン機能を正常に使用できるようにすることを、事業継続の要件として取り決めた。また、当日のオンライン開始から災害発生までに登録された注文情報については、販売部が注文伝票を基に再入力することとした。

上記の実線の下線部はRTOを示しているので、空欄aは“3時間”である。上記の点線の下線部より、当日のオンライン開始から災害時までに登録された注文情報は再入力しなければならない(=失われる)ので、RPO (=空欄b)は“当日のオンライン開始”になる。

(2) 本文中の下線(ア)を含む文とその1文前は、以下のとおりである。

サービス継続計画が発動された場合は、★待機系システムを起動し、転送済みのバックアップから必要なデータをリストアした上で、待機系システムに切り替える予定である。しかし、●現在のバッチ処理の構成ではRPOの目標値を達成できないと考えたU氏は、(ア)バッチ処理の内容を見直した。

上記●の下線部より、第1のヒントは“現在のバッチ処理の構成”であり、それは次の“表1 販売管理システムにおけるバッチ処理の区分と内容”に示されている。

区分	ジョブ番号	処理内容	所要時間
日次バッチ処理	1-1	注文情報のバックアップを取得する。	1時間
	1-2	業務日付を更新する。	5分
	1-3	注文情報を加工して受注情報として確定し、顧客ごとに集計し、受注実績とする。	5時間
週次バッチ処理	2-1	業務日付、受注情報及び受注実績のバックアップを取得して、取得情報をDC-Bのファイルサーバに転送する。	1時間

上記★の下線部より、第2のヒントは①：待機系システムの起動、②：転送済みのバックアップからの必要なデータのリストア、③：待機系システムへの切り替えの時間がRTOに関連していることである。さらに、“図1 X社の主要システムの構成”より、待機系システムはDC-B内にあり、②は“転送済みのバックアップからのDC-B内の待機系システムへの必要データのリストア”と書き換えられる。

①～③の観点で表1を検討すると、ジョブ番号2-1と②が関連している。週次バッチ処理前の時点で災害が発生すると、受注情報及び受注実績等はDC-Bにはないので、DC-A内の本番系システムからバックアップを取得し、DC-Bに送付する時間が必要になる。この時間がRTOの目標値(3時間以内)を達成できない原因になっている。RPOは当日のオンライン開始時点なので、ジョブ番号2-1を週次バッチ処理から、日次バッチ処理に移動させればこの問題は解決する。ジョブ番号2-1でバックアップされる受注実績はジョブ番号1-3で集計(更新)されているので、ジョブ番号2-1はジョブ番号1-3の前には実行できない。したがって、解答は“週次バッチ処理のジョブ番号2-1をジョブ番号1-3の後に移動し、日次バッチ処理の一部として実行する”のようにまとめられる。

設問3

- (1) 本設問のヒントは、下記の空欄a、bの次の文である。

また、平常運用フェーズではオンラインの応答時間の目標値を3秒以内としているが、業務再開フェーズと業務回復フェーズでは待機系システムでのサービス提供になるので、応答時間の目標値は5秒まで許容することにした。

上記の下線部より、業務再開フェーズにおいて、提供サービスの正常稼働に関して確認すべき内容(=解答)は、“待機系システムでのオンラインの応答時間が5秒以内に収まっていること”のようにまとめられる。

(2) “表3 サービス継続計画の試験計画書の内容”は、下記のとおりである。

項番	フェーズ	実施項目	確認すべき内容	試験方法
1	BCP発動準備	復旧作業要員の配置	復旧作業に関わる情報システム部員への連絡	机上チェック
2	業務再開	待機系システムを使ったサービス運用の開始	★売上分析システムの正常停止, ●待機系システムの起動, ▲データリストアの実施, 切替えの実施確認, 及び▼提供サービスの正常稼働確認	実機訓練
3	業務回復	サービス運用の拡大	生産管理システムの起動及び提供サービスの正常稼働確認	実機訓練
4	全面復旧	全面復旧手順の確認	c	実機訓練

空欄cは全面復旧フェーズで確認すべき事項であるから、業務再開フェーズで縮小されたITサービスの復旧を確認する事項になる。

上記★の下線部の逆は、“売上分析システムの起動”である。図1から上へ1文目は、下記のとおりである。

本番系システムに障害が発生した場合は、売上分析システムを停止してから待機系システムを起動し、システムの切替えに必要な作業を行って、販売管理システムのサービスを再開する。

上記から類推すると、売上分析システムは本番系システム起動後に起動しなければならない。したがって、解答の一部は“本番系システムの起動、売上分析システムの起動”になる。

上記●の下線部の逆は、“待機系システムの停止”である。これは最初にしなければならないので空欄cの先頭にもってくる。

上記▲の下線部は復旧には関係ないので、解答を構成しない。

上記▼の下線部は復旧にも妥当するので、そのまま解答の最後に付ける。

今までの検討をまとめると、解答は“待機系システムの停止、本番系システムの起動、売上分析システムの起動、提供サービスの正常稼働確認”のようになる。

- (3) 本文中の下線(イ)を含む文とその1, 2文前は, 下記のとおりである。

U氏は、関係者の協力を得て試験を行った。試験では、●増設された2台の販売管理用端末から待機系システムに接続できないという事態が発生し、混乱した。★原因は、売上分析システムの定期保守日に実施予定であった変更リリースが展開される前に試験を実施したからであり、必要な対応を行い、試験は無事終了した。

試験終了後、T部長は、(イ)サービス継続計画の発動後に今回のような混乱が発生しないように、業務再開フェーズに必要な作業内容の追加をU氏に指示した。

下線(イ)に記述されている混乱の原因は、上記★の下線部に記述されている。

上記●の下線部にある“増設された2台の販売管理用端末”のもう少し詳しい説明は、下記の問題文〔販売管理用端末の増設〕に記述されている。

X社では現在、営業所に2台の販売管理用端末があるが、販売業務の拡大に備えて、端末を2台増設することになった。販売管理システムには許可された端末からしか接続できないので、ITサービスマネージャのU氏は、増設される端末からの接続を許可するように本番系システムの設定変更を計画した。情報システム部の担当者は変更計画に従って変更を行い、増設された端末の本番運用を開始した。◆本番系システムの設定変更を待機系システムへ反映する作業については、変更をできるだけ早く展開する必要があるが、売上分析システムの稼働スケジュールとの関係から、3か月に1回設けられている売上分析システムの次回定期保守日に行うことにしている。(後略)

上記◆の下線部に違反して、上記★の下線部は“売上分析システムの定期保守日に実施予定であった変更リリースが展開される前に試験を実施した”としている。

解答は上記◆の下線部をヒントにして、“本番系システムの設定変更を待機系システムに反映する作業があれば試験前に実施するか、未実施でも試験可能か判定する”のようにまとめる。