SM

平成28年度　秋期
ITサービスマネージャ試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1～問3
選択方法	2問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。3問とも○印で囲んだ場合は，はじめの2問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問1，問3を選択した場合の例〕

選択欄	
2問選択	○問1
	問2
	○問3

M
炎Ⅰ

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　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。

R 社は，中堅の製薬会社である。R 社の本社は関東地方の C 市にあり，工場，関東支店及びサーバ室（全て同じ建物内にある）は C 市に隣接する D 市に，近畿支店は近畿地方の E 市にある。両支店には倉庫が併設されており，関東支店は東日本地域の注文受付と入出庫，近畿支店は西日本地域の注文受付と入出庫を担当している。

R 社の製造部の部員は，工場に勤務して製品の製造記録及び倉庫への輸送記録を端末から生産管理システムに入力している。R 社の販売部の部員は，関東支店又は近畿支店に勤務して注文の入力を行っている。顧客からの注文は，両支店で毎日 8 時から 19 時までの間，電話又はファックスで受け付け，端末から販売管理システムに入力している。また，端末から製品の入出庫を販売管理システムに入力している。

〔システム全体の構成〕

R 社のシステム全体の構成を図1に，システム全体の概要を表1に示す。

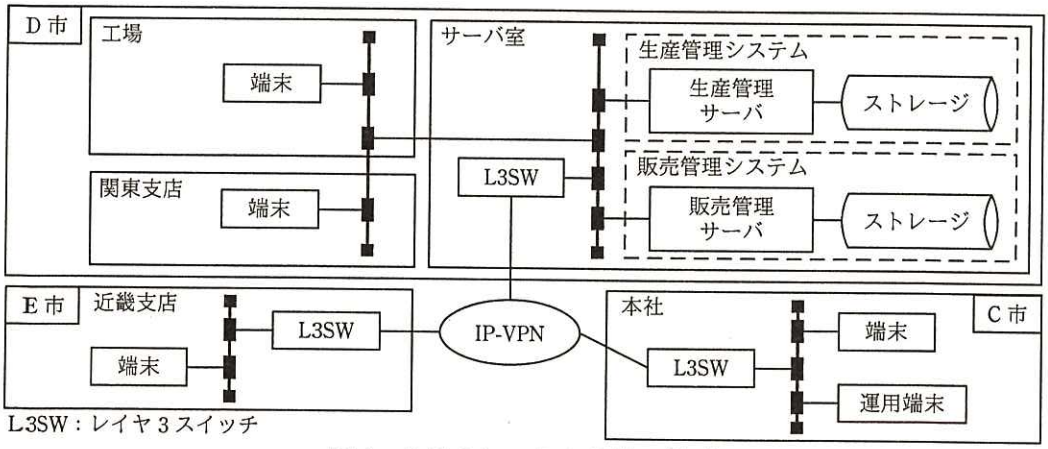


図1　R 社のシステム全体の構成

表1　R 社のシステム全体の概要

項番	内容
1	工場と同じ建物内のサーバ室には，製品の製造から倉庫への輸送までを管理する生産管理システム，及び顧客との取引と製品の入出庫を管理する販売管理システムが設置されている。
2	工場，両支店及び本社には，両システム共用のデータ入力用の端末が設置されている。
3	本社には，運用端末が設置されており，IP-VPN 経由で両システムの運用に使われている。
4	生産管理システムのストレージには製品の製造及び倉庫への輸送の記録ファイルが格納され，販売管理システムのストレージには受注ファイル及び在庫ファイルが格納されている。

〔両システムの運用〕

R 社の情報システム部員は，本社に勤務して両システムを運用している。両システムとも，毎日 4 時から 23 時までオンライン処理を行う。23 時から 24 時までは，テープ媒体にファイルのフルバックアップを取得し，サーバ室に保管している。

システムのオペレーションは，販売管理システム専任の A チームと，生産管理システム専任の B チームの 2 チームに分かれている。部員は自身が担当するシステムについて教育を受け，オペレーションを実施している。

なお，部員は自身が担当するシステム以外のオペレーションは実施していない。両チームともシフト体制を組み，それぞれ 1 シフト 1 名でオペレーションを実施している。

〔事業継続計画の策定〕

関東地方に震度 6 弱レベルの地震が発生した場合の，R 社の建物が損傷を受けるリスクについて調査した。その結果は次のとおりである。

(1) C 市にある本社の建物は耐震性能が高く，震度 6 弱レベルの地震で損傷を受ける確率が低い。

(2) D 市にある R 社の敷地の地盤は軟弱であって，R 社の建物（工場，関東支店，倉庫及びサーバ室）は，震度 6 弱レベルの地震で損傷を受ける確率が高い。

(3) E 市にある近畿支店の建物及び倉庫は，損傷を受ける確率が低い。

この調査結果を受け，R 社では情報システム部も参加する検討チームを設置して，事業継続計画（以下，BCP という）の策定に着手した。BCP の概要を表 2 に示す。

表 2　BCP の概要（抜粋）

項番	業務	計画内容
1	販売活動	・関東支店は注文受付と入出庫を停止する。 ・近畿支店は在庫を活用して，注文受付と出庫を通常どおり継続する。
2	製造活動	・3 年後を目途に，地盤が強固な地域に工場を移転する。 ・移転までの間に被災した場合は，一時的に工場の操業及び近畿支店への輸送を停止する。

〔災害対策用システムの検討〕

工場，関東支店及びサーバ室の建物の被災によって両システムが停止することが想定された。一方で，近畿支店の販売活動は可能なので，販売管理システムの RTO

（目標復旧時間）は被災時点から 120 分，生産管理システムの RTO は被災時点から 5 日と設定した。ただし，RPO（目標復旧時点）は関係部署との調整が必要なので，継続して検討することになった。

RTO の設定を受け，IT サービスマネージャである G 氏は，被災時の技術的対策の検討を始めた。検討した結果，現在稼働中の販売管理システムと同一機能で，被災時だけ使用する災害対策用システム（以下，災対システムという）を構築することになった。概要は次のとおりである。

・災対システムと本社との間に専用線を新規に敷設し，本社の運用端末から遠隔操作を行う。

・クラウドサービスの活用も検討する。現在稼働中の販売管理システムとの互換性を考慮し，クラウド事業者が提供する PaaS を利用する。PaaS は，サービスの利用量に応じた料金体系であり，システム環境の構築だけであれば少額の費用で利用できる。

G 氏はこれらの検討結果を踏まえ，災対システムの方式案を表 3 のようにまとめた。

表 3　災対システムの方式案

方式案	概要	費用 [1]	復旧時間 [2]	RPO
案 1	・災対システムを近畿支店に構築し，被災時はフルバックアップからデータを復元する。 ・フルバックアップの取得先を，現在のテープ媒体から，近畿支店に新設するストレージに変更する。取得対象データと取得時期は現在のままとする。	1.3	a	被災当日のオンライン開始時点
案 2	・災対システムはクラウドサービスを使用して構築し，現在稼働中の販売管理システムとホットスタンバイ構成とする。	1.0	60 分	被災時点
案 3	・災対システムはクラウドサービスを使用して構築し，被災時はフルバックアップからデータを復元する。 ・フルバックアップの取得方式を，データ保管サービス [3] の利用に変更する。取得対象データと取得時期は現在のままとする。	0.7	120 分	b 時点

注 [1]　総所有費用（TCO）のことである。数値は，案 2 を 1.0 とした場合の相対的な倍率である。

[2]　インシデントの発生（被災時点）からサービスが再開されるまでの所要時間である。被災時点から災対システムの起動開始までには，被災状況の確認作業などが必要であり，所要時間は 30 分である。また，その後の作業内容は案ごとに異なるが，必要となる場合には，災対システムの起動作業に 30 分，フルバックアップからのデータ復元に 30 分，システムの正常稼働の確認に 30 分掛かる。

[3]　クラウドサービスの利用者が指定するデータを，利用者が指定する時期に複写し，クラウド事業者のデータセンタに保管するクラウドサービスのことである。

案 1 で，RPO を被災当日のオンライン開始時点と設定した場合，（ア）情報システ

ム部が販売部とあらかじめ合意すべき内容がある。

G氏は，案1～3について検討した結果，案3を推奨案として検討チームに提案し，案3に決定した。

〔復旧手順の検討及びクラウドサービスの選定〕

案3の決定を受けて，G氏は，販売管理システムの復旧手順の検討と，使用するクラウドサービスの選定に着手した。

(1) 復旧手順の検討

① 災対システムは，平常時は停止状態としておき，被災時に運用端末から起動する。被災状況の確認作業などに30分，その後，災対システムの起動作業に30分，さらに，フルバックアップからのデータ復元に30分掛かる。データ復元の完了後，システムの正常稼働の確認に30分掛かるが，RTO内に復旧できる。

② ストレージは，平常時は最低限の容量だけを確保しておき，被災時点のデータ量に応じて，災対システムの起動作業と並行して容量の追加を行う。

(2) 災対システム稼働中にインシデントが発生した場合の対応

災対システム稼働中にインシデントが発生し，災対システムが停止した場合，クラウド事業者がインシデントの解決及び災対システムの起動を実施する。その後，R社でフルバックアップからのデータ復元及びシステムの正常稼働の確認を実施し，サービスを再開する。

(3) クラウドサービスの選定

G氏は，災対システムの候補として，表4の4社のクラウドサービスを選んだ。

表4 G氏が検討したクラウドサービス

項番	クラウド事業者	データセンタの所在地 1)	ストレージ容量追加の所要時間 2)	インシデントが発生した場合，クラウド事業者が行う作業所要時間 3)
1	Q社	九州地方	20分以内	40分
2	S社	北陸地方	30分以内	20分
3	U社	関東地方	30分以内	60分
4	W社	中部地方	40分以内	60分

注 1) サービスを提供しているクラウド事業者のデータセンタの所在地

2) 利用者がクラウド事業者に申込みを行ってから，利用可能となるまでの時間

3) 災対システム稼働中にPaaSでインシデントが発生し，災対システムが停止した場合，クラウド事業者はインシデントの解決を行い，災対システムを起動する。作業所要時間とは，インシデントの発生から解決までの時間であり，災対システムを起動する時間は含まない。

G氏は，各社のサービスを比較し，次の条件に合致するクラウドサービスを提供する1社を選定した。

・事業継続に関する要求事項として，サービスを提供するデータセンタが，R社のサーバ室と同じ地方にないこと

・災対システム稼働中にインシデントが発生し，災対システムが停止した場合，インシデントの発生から120分以内にサービスが再開可能なこと

・［　　c　　］

〔災対システムの構築〕

G氏は変更計画として，災対システムの構築計画，災対システムに関連する既存システムの稼働環境の修正計画，及び既存システムのオペレーションマニュアルの修正計画をまとめた。変更計画はR社で規定する変更管理プロセスに従って承認され，災対システムが構築された。災対システムの構築が完了した後，G氏は災害対策用マニュアル（以下，災対マニュアルという）も作成した。

当初，災対システムと本社との間は，1本の専用線で接続する予定であった。しかし，災対システムの構築完了後，G氏は予備の専用線を追加して，可用性を向上させることにした。この場合，災対システムの正常稼働の確認で予備の専用線の切替え作業と疎通確認作業が増えるが，想定している30分の範囲内で作業可能と判断した。予備の専用線の追加は，変更管理プロセスに従って承認された後，予備の専用線の敷設作業が実施された。

〔災害復旧訓練の準備・実施〕

災対システムの構築完了後，G氏は災害復旧訓練（以下，訓練という）の実施を計画した。訓練には，実施日時に勤務中の販売管理システム専任のAチームのオペレータと運用責任者が参加し，実機を使用して災対システムへの切替えなどを行う。

G氏は訓練の計画書を作成し，参加者向け会議で訓練計画及び災対マニュアルについて説明を行った。会議において，“被災時には，勤務中のAチームのオペレータが何らかの理由で作業を行えなくなり，非番のオペレータも招集できないという不測の事態も考えられる。RTO内に復旧するために，こうしたリスクへの備えも必要である。”という指摘を受け，G氏は（イ）対策を検討した。

訓練は予定した日時に実施された。訓練終了後，訓練実施者の会議において，“（ウ）災対マニュアルの復旧手順では，予備の専用線の疎通確認が漏れていたので，作業に手間取ってしまった。”という報告があった。

設問1　〔災害対策用システムの検討〕について，(1)，(2)に答えよ。

(1) 表3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，合意すべき内容を40字以内で述べよ。

設問2　〔復旧手順の検討及びクラウドサービスの選定〕について，(1)，(2)に答えよ。

(1) 本文中の［　c　］には，ストレージに関する条件が入る。適切な条件を，40字以内で具体的に述べよ。

(2) 表4のクラウド事業者のうち，G氏が選定した1社を答えよ。

設問3　〔災害復旧訓練の準備・実施〕について，(1)，(2)に答えよ。

(1) 本文中の下線（イ）について，有効な対策を50字以内で述べよ。

(2) 本文中の下線（ウ）について，サービスマネジメントの観点から，改善すべき内容を40字以内で述べよ。

問2　キャパシティ管理に関する次の記述を読んで，設問1～3に答えよ。

F社は，通信事業者である。F社の情報システム部門では，F社の顧客が利用するインターネット受付サービス，代理店が利用する代理店サービス，及び社員が利用する顧客管理サービスを運用している。これらのサービスはF社の営業部門が統括している。

〔サービスの概要〕

インターネット受付サービス及び代理店サービスは，オンライン処理形態で提供されている。インターネット受付サービスはインターネット受付システムで，代理店サービスは代理店システムで処理されている。インターネット受付サービスのサービス提供時間帯は24時間365日で，代理店サービスは平日の8～21時である。

顧客管理サービスは，契約管理，課金管理，問合せ管理，請求・入金，受注分析の五つのサービスで構成され，顧客管理システムで処理されている。

・契約管理サービス，課金管理サービス及び問合せ管理サービスは，オンラインでサービスを行っている。サービス提供時間帯は，平日の8～21時である。
・請求・入金サービスは毎週1回提供されるサービスである。毎週日曜日の22時に起動する顧客管理システムのバッチ処理として運用されている。
・受注分析サービスは毎日1回提供されるサービスである。請求・入金サービスのバッチ処理との競合を避けるために9時以降に処理を開始する必要があり，毎日9時に起動する顧客管理システムのバッチ処理として運用されている。

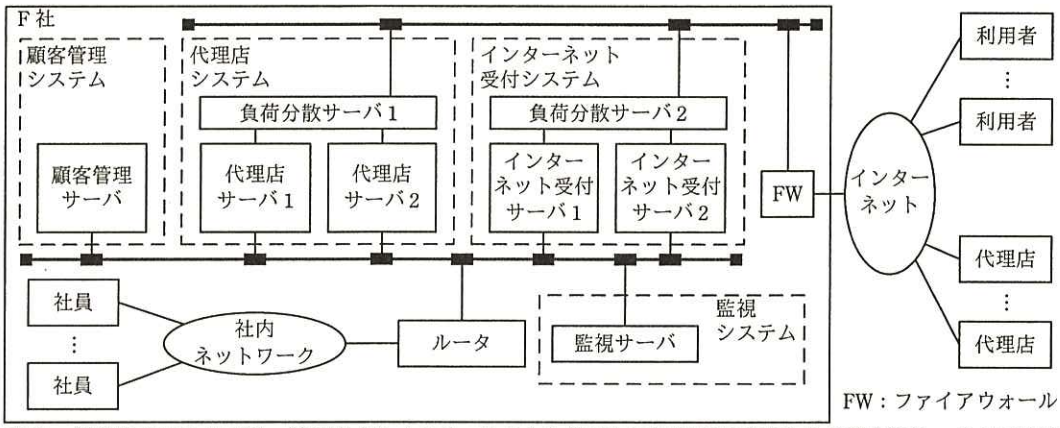
各サービスのSLA項目（抜粋）を，表1に示す。

表1　各サービスのSLA項目（抜粋）

サービス名		SLA項目	目標値
インターネット受付サービス		オンライン応答時間[1)]	3秒以内
代理店サービス		同上	2秒以内
顧客管理サービス	契約管理サービス	同上	5秒以内
	課金管理サービス	同上	同上
	問合せ管理サービス	同上	同上
	請求・入金サービス	バッチ処理完了時刻	月曜日の8時まで
	受注分析サービス	同上	毎日13時まで

注[1)]　オンライン応答時間とは，サービスを提供するシステムのコンポーネントである業務サーバが要求を受け付けてから応答するまでの時間のことである。

F社のシステム構成を図1に示す。



注記　代理店システムでは，代理店からインターネットを経由して処理要求があると負荷分散サーバ1で振り分け処理をしている。負荷分散サーバ1は，同じ処理能力をもった代理店サーバ1又は代理店サーバ2のどちらかの業務サーバに，負荷が均等になるように処理要求を振り分ける。負荷分散サーバ1では，ソフトウェアで負荷分散機能を実行している。インターネット受付システムも，負荷分散サーバ2を用いて同様に負荷分散を行っている。

図1　F社のシステム構成

なお，受注分析サービスは，F社でサービス提供を開始した当初は，1時間で処理を完了していたが，処理対象データの増加に伴って処理時間が長くなり，現在では処理完了までに1時間30分掛かっている。

〔キャパシティ計画の策定〕

情報システム部門のL氏は，ITサービスマネージャとしてキャパシティ管理を担当している。L氏は，F社の規程に従ってキャパシティ計画を次のとおり策定した。

・営業部門から入手した，現在及び将来のサービスに対する需要とサービス利用者の見通しから，データ処理量の増加を見積もる。

・営業部門と合意したオンライン応答時間などの要求事項，データ処理量を基に，ハードウェア，ソフトウェアなどのコンポーネントのキャパシティ及び構成を計画する。

・コンポーネントのキャパシティを増強するための方式及び構成を計画する。

なお，F社の規程では，サービス開始後は，実際のオンライン応答時間，キャパシティのニーズなどに基づいて，“毎年，キャパシティ計画を変更する”としている。

〔サービス運用段階のキャパシティ管理〕

L氏は，サービス運用段階のキャパシティ管理として次の活動を実施している。

(1) キャパシティ監視

① サービスがオンライン処理形態の場合は，サーバの CPU 使用率，サーバの処理件数及びオンライン応答時間を監視項目とする。これらの監視項目は，監視システムによって 1 分間隔で測定し，監視データとして収集される。一方，サービスがバッチ処理形態の場合は，サーバの CPU 使用率及びバッチ処理完了時刻を監視項目とする。

なお，LAN 及び社内ネットワークには十分なキャパシティがあり，サービス提供に支障がないので，監視項目を設定していない。

② オンライン応答時間の測定値が，あらかじめ決められたしきい値を超えた場合は，監視システムがインシデントとして検知する。しきい値には，各サービスの SLA 項目の目標値を設定しており，キャパシティに関わるインシデントが発生した場合は，直ちに監視システムからL氏に通知される。

(2) 分析及び対策

① 監視システムによって収集した監視データについて，各サービスの SLA 項目の目標値の達成に影響を与える可能性がないか，キャパシティ計画どおりにコンポーネントのキャパシティが使われているかなどの視点で分析する。

② キャパシティ不足が懸念される場合には，キャパシティの増強計画を作成する。キャパシティの増強は，サービス提供時間以外の計画停止時間帯に実施する。

〔顧客管理サービスのインシデントとその対策〕

ある月曜日の 10 時に，顧客管理サービスにおいてオンライン応答時間がしきい値を超えるというインシデントが発生し，監視システムから L 氏に通知があった。その後，11 時までの間に同一インシデントが数回発生した。また，営業部門からサービスデスクに，“サービスの応答が遅くなっている”とのクレームが寄せられた。L氏が監視データを調査したところ，10～11 時の時間帯で顧客管理サーバの CPU 使用率が 90～100％で推移していたことが判明した。その調査結果を表 2 に示す。

表 2　顧客管理サーバの CPU 使用率の調査結果

顧客管理サービス名	CPU 使用率[1]（%）			
	9～10 時	10～11 時	11～12 時	12～13 時
契約管理サービス	10	20	5	2
課金管理サービス	10	20	5	2
問合せ管理サービス	5	10	5	1
請求・入金サービス	0	0	0	0
受注分析サービス	60	45	0	0
顧客管理サービス全体	85	95	15	5

注[1]　1 分間隔で測定された結果に基づく，1 時間の平均値

顧客管理サーバの利用状況を調査したところ，1 日のオンライン処理件数のうち約 2 割が 10～11 時のピーク時間帯に集中していた。L 氏は，根本対策として，顧客管理サーバのキャパシティの増強が必要と判断した。しかし，増強には時間が掛かるので，暫定対策を策定し，営業部門と協議することにした。

〔代理店サービスのオンライン応答時間の悪化〕

ある日の 22 時に，負荷分散サーバ 1 の機器障害が発生した。機器障害の発生時刻はサービス提供時間帯ではなかったので，サービス利用者に影響しなかったが，翌日のサービス提供開始までには回復する必要があった。情報システム部門でサーバ運用を担当している T 氏は，負荷分散サーバ 1 の交換作業が必要と判断し，次の手順で対応した。

・変更管理プロセスに従って，緊急変更の作業計画を策定し，実施の許可を得た。
・翌日の 6 時から，負荷分散サーバのメーカ作業員とともに変更作業を実施した。
・変更作業の最後の作業項目として，代理店システムの機能の確認作業を行った。この作業で代理店サービスが利用できることを確認して，8 時までに作業を終了した。

代理店サービスは，予定どおり 8 時に開始されたが，9～10 時のピーク時間帯に代理店からサービスデスクに“サービスの応答が遅くなっている”というクレームが多数寄せられた。サービスデスクから調査を依頼された L 氏は，今回の緊急変更作業が影響したと判断し，T 氏に調査を依頼した。

しばらくして，T 氏から，“緊急変更作業で，負荷分散機能を実行するソフトウェアの負荷分散先サーバの登録を誤り，代理店サーバ 1 に処理が集中してボトルネッ

クとなってしまった。直ちに，設定を修正する。”という回答があった。

〔キャパシティ計画の変更〕

インターネット受付サービスは，サービスを開始してから1年が経過し，F社では，キャパシティ計画を変更することになった。そこで，L氏はインターネット受付サービスの現状を次のとおり整理した。

・オンライン応答時間は，SLA項目の目標値は達成しているが，サービス開始時に比べて悪化している。

・インターネット受付システムはWeb型のシステムであって，主にサーバの処理能力がパフォーマンスに影響を与える。

・オンライン応答時間のSLA項目の目標値を達成するために，将来の需要の予測が必要である。

そこで，L氏は，まず，（ア）サービスの需要と達成されているパフォーマンスの状況を調査することにした。

設問1　〔顧客管理サービスのインシデントとその対策〕について，(1)～(3)に答えよ。

(1) キャパシティ監視でインシデントと認識するためのしきい値には問題があり，変更が必要である。しきい値の変更内容を，SLAとの関連性を含めて40字以内で述べよ。

(2) サービスの応答が遅くなっていることへの対策として，営業部門と協議して実施する暫定対策を35字以内で述べよ。

(3) (2)の暫定対策が有効であると考えた理由を，40字以内で述べよ。

設問2　〔代理店サービスのオンライン応答時間の悪化〕について，L氏は，緊急変更作業の終了後に，サービス提供開始から数分間の監視データを分析しておくべきであった。キャパシティ管理担当として，監視データを分析し，確認すべきであった内容を60字以内で述べよ。

設問3　〔キャパシティ計画の変更〕について，(1)，(2)に答えよ。

(1) 本文中の下線（ア）として実施すべき内容を，30字以内で述べよ。

(2) キャパシティ計画を変更するに当たって監視データ以外にL氏が入手すべき情報を，入手先を含めて40字以内で述べよ。

問3　インシデント管理に関する次の記述を読んで，設問1～4に答えよ。

M 社は，中堅の通信販売会社である。M 社では，数年前からインターネット経由で注文を受け付ける販売サービスを開始した。サービス提供時間は 24 時間 365 日である。最近では，インターネット経由の注文が増えており，更なる売上拡大のために販売サービスの充実が課題となっている。また，受注した商品を顧客に配送する業務を支援する配送管理サービスが M 社の社員向けに提供されている。サービス提供時間は毎日 6 時から 23 時までである。

〔システムの概要〕

システム部では，販売サービスを提供する販売システム，及び配送管理サービスを提供する配送管理システムを開発し，運用している。システムの開発は開発チームが担当し，運用は運用チームが担当している。

① 販売システムは，外部の顧客が利用する M 社の重要システムであり，5 台の Web サーバで冗長システムを構成している。M 社では，Web 管理端末から Web サーバにコンテンツを登録している。また，外部の顧客との連絡手段として電子メールを使っていることから，社員間でも利用するメールサーバを販売システムのコンポーネントとして管理している。

② 販売システム及び配送管理システムは，運用チームが監視システムを利用して常時監視し，インシデントが発生した場合は 1 次対応を行っている。インシデントはインシデント管理システムで管理している。

③ 監視システムに表示されるメッセージ（以下，表示メッセージという）は，M 社の統一基準に従って分類されている。表示メッセージの種類を表 1 に示す。

表 1　表示メッセージの種類

種類	内容	インシデントとしての扱い
通知	運用状態の通知 1)	インシデントとして扱わない
警告	調査が必要なことを示す事象 2)	インシデントとして扱う
異常	正常に運用されていない状態を表す事象 3)	インシデントとして扱う

例 1)　バッチ処理の正常終了
2)　システム資源使用状況のしきい値超過
3)　システムの異常終了

〔システム部のインシデント管理〕

システム部では，表示メッセージの種類が“警告”又は“異常”の場合，インシデントとして扱い，インシデント管理システムに記録する。また，サービスを早期に回復させるために，既知の誤りのデータベース（以下，KEDB という）を利用している。KEDB には，過去のインシデントの発生原因と，サービスの回復方法又はサービスへの影響を低減する有効な回避策が登録されている。運用チームはインシデントの対応手順の中で，KEDB を参照する。

運用チームが実施するインシデントの対応手順を表 2 に示す。

表 2　インシデントの対応手順

手順	概要
記録	・監視システムの表示メッセージの種類からインシデントの発生を認識する。インシデントを受け付け，インシデント管理システムに記録する。
優先度の割当て	・全てのインシデントに優先度 1) として，“高”，“中”，“低”のいずれかを割り当て，目標復旧時間 2) を設定する。
分類	・インシデントをサービスごとに決められたカテゴリに分類する。
記録の更新	・割り当てた優先度及び分類したカテゴリの内容で，インシデント管理システムの記録を更新する。
段階的取扱い	・優先度が“高”及び“中”の場合は，開発チームに直ちに緊急連絡を行う。優先度が“低”の場合も開発チームに連絡する。 ・目標復旧時間内に回復できないおそれがある場合は，開発チームに回復処理を依頼する。
解決	・サービスを早期に回復させるために，回復を試みる。 ・KEDB を参照して，サービスを早期に回復させる回避策を探し，必要な回復処理を行う。
終了	・インシデントが解決したことを確認する。 ・開発チームに回復処理を依頼した場合は，開発チームからの回復処理完了の連絡を受けた後，回復状況を確認する。 ・回復内容などの記録を更新し，終了する。

注 1)　サービスごとに表 3，表 4 で定める優先度判定ルールに従って優先度を割り当てる。
2)　インシデントの記録の開始から解決までの最長時間。優先度に基づく目標復旧時間を表 5 に示す。

表 3　販売サービスの優先度判定ルール

項番	表示メッセージの種類	優先度
1	異常	高
2	警告	中

表 4　配送管理サービスの優先度判定ルール

項番	表示メッセージの種類	優先度
1	異常	中
2	警告	低

表5　優先度に基づく目標復旧時間

項番	優先度	目標復旧時間
1	高	30分
2	中	2時間
3	低	12時間

発生したインシデントが情報セキュリティインシデントに該当するおそれがある場合，運用チームの担当者は，システム部の情報セキュリティ担当要員に連絡して，指示に従って対応する。情報セキュリティ担当要員は，インシデントが情報セキュリティインシデントに該当するかどうかを判断する。該当する場合は，M 社の情報セキュリティ管理プロセスの規程に従って対応を指示し，自ら迅速に対応策を実施して被害を最小限に抑える。

〔販売サービスのインシデント〕

ある日，販売システムの5台の Web サーバのうち，1台の CPU 使用率がしきい値を超え，監視システムで“警告”のメッセージが表示された。監視していた運用チームの Y 氏は，インシデントの対応手順に従って対応した。対応状況は次のとおりである。

① インシデントをインシデント管理システムに記録した。

② 表3及び表5を参照し，優先度を“中”と割り当て，目標復旧時間を2時間に設定した。その後，分類したカテゴリの内容で記録の更新を行った。

③ インシデントの解決を図るために，解決策を立案し実施することにした。そこで，必要な回復処理を行うために KEDB を参照したところ，特定の条件の下で販売システムのバッチ処理プログラムの負荷が高くなって，CPU 使用率が上昇した事例を見つけた。回避策として，バッチ処理プログラムを強制終了させる方法，又は Web サーバの再起動を行う方法が記載されていた。そこで，Web サーバを確認したが，バッチ処理プログラムは稼働していなかった。

④ CPU 使用率のしきい値超過は，販売システムの Web サーバ1台だけで発生しており，他の4台の Web サーバでは発生していない。Y 氏は，サービス継続の観点から，利用者への影響は小さいと判断し，インシデントの原因を調査する

ことにした。Y 氏は，CPU 使用率のしきい値超過が発生している Web サーバを調査し，CPU 使用率が高いプログラムを特定した。

⑤ CMDB に登録されている販売システムのプログラム一覧を確認したところ，特定したプログラムは CMDB には登録されていなかった。そこで，Y 氏は開発チームの Z 氏に調査を依頼した。

Z 氏は，稼働環境で販売サービスを利用したところ，応答遅延が発生する場合があることを確認した。次に，Z 氏は，CMDB を確認し，当該プログラムは CMDB に登録されておらず，M 社が開発したプログラムではないことが分かった。更に調査したところ，不正プログラムであることが判明した。Z 氏は Y 氏に調査結果を回答し，強制終了する手順を伝えた。Y 氏は Z 氏の指示に従って，不正プログラムを強制終了した。その結果，Web サーバの CPU 使用率の低下を確認できたことから，Y 氏はインシデントが解決したと判断した。

なお，Z 氏は，CMDB に登録されていないプログラムが稼働していた場合に強制終了する手順を回避策として整備し，後日 KEDB に登録することにした。

〔標的型攻撃メールの検出〕

Z 氏は，インシデントの根本原因を特定するために調査し，次の事実が判明した。

① Web 管理端末にも不正プログラムがあった。

② 不正プログラムは，販売システムの 5 台の Web サーバのうち，1 台の Web サーバだけに存在していた。

③ メールサーバのログには，不審なファイルが添付された Web 管理者宛ての電子メールの受信記録があった。また，同じファイルが添付された電子メールが社内の他部署の社員にも送信されている記録があった。

そこで，Z 氏は，“外部から送付された標的型攻撃メールに添付されたファイルを Web 管理端末で開封した。その際，不正プログラムが起動され，Web 管理端末と，メンテナンス作業のために接続していた該当の 1 台の Web サーバに不正プログラムがコピーされ，動作するよう設定された。”と推定した。Z 氏は，今回のインシデントが情報セキュリティインシデントに該当するおそれがあるとして，情報セキュリティ担当要員の K 氏に連絡した。K 氏は，情報セキュリティインシデントに該当すると判断し，Z 氏に，1 台の Web サーバと Web 管理端末を LAN から切り離すように

指示した。そこで，Z氏はY氏に，該当機器をLANから切り離すよう依頼した。

次に，K氏は，類似の標的型攻撃メールが送付された宛先を，［ a ］から調査し，標的型攻撃メールが届いた全ての社員に対して，次の内容を直ちに指示した。

・社員が添付ファイルを開封していた場合，開封操作を行った機器をLANから切り離す。その後，指示に従って不正プログラムの確認をすること。

・社員が添付ファイルを開封していない場合，［ b ］をすること。

そして，K氏は，社内に今回の標的型攻撃メールに対する注意喚起を行った。

〔標的型攻撃メールの対策〕

システム部の部長は，K氏から，“今回の標的型攻撃メールには，情報窃取を目的として，マルウェアを仕掛けたファイルが添付されていた。幸い外部への情報漏えいは確認されなかった。また，社内への注意喚起も完了した。”という報告を受けた。システム部では，標的型攻撃メールへの対策として，マルウェアが仕掛けられた標的型攻撃メールを検出した場合，電子メールから添付ファイルを削除したり，不正な通信を検出したりすることができるシステム（以下，防御システムという）を検討し，導入することにした。システム部は，防御システムを販売システムのコンポーネントとして管理する。また，システム部は，標的型攻撃メールを検出した場合の対応として，次のとおり決定した。

① 検出された電子メールの添付ファイルは，調査用に防御システムのストレージに保存される。情報セキュリティ担当要員は，保存されたファイルの内容を定期的に調査し，対策が必要と判断した場合は，適切な対策を立案し実施する。

② 防御システムで，特定の基準以上の危険性がある不正な通信を検出した場合は監視システムに通知する。（ア）通知された監視システムでは，“警告”のメッセージを表示する。

③ 運用チームは，インシデントを記録し，管理する。

〔配送管理サービスの変更〕

M社では，顧客へのサービス充実を目的に，インターネット経由の注文について，配送時間を短縮することを決定した。そのためには，M社の物流拠点間で深夜に商品を配送する必要がある。営業部とシステム部は，配送管理サービスのサービス要

求事項について，次のとおり合意した。

① 物流拠点からいつでも配送管理サービスを利用できるように，配送管理システムを 24 時間稼働に変更する。

② システム障害による配送業務の停止は，サービスの低下につながるので，システム停止を伴うインシデントが発生した場合には，インシデントの対応手順に従って，30 分以内に回復させる。

システム部では，サービス要求事項を基に，サービス変更の活動を開始した。

設問 1 〔販売サービスのインシデント〕について，(1)，(2)に答えよ。

(1) Y 氏が実施したインシデント対応の問題点を二つ挙げ，それぞれ 30 字以内で述べよ。ただし，情報セキュリティに関する内容は除くこと。

(2) Z 氏が，KEDB に回避策を登録した目的を，40 字以内で述べよ。

設問 2 〔標的型攻撃メールの検出〕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 15 字以内で答えよ。

(2) 本文中の［ b ］で指示すべき事項を，20 字以内で答えよ。

設問 3 〔標的型攻撃メールの対策〕について，本文中の下線（ア）で，監視システムに“警告”のメッセージを表示させる理由を，40 字以内で述べよ。

設問 4 〔配送管理サービスの変更〕について，サービス要求を満たすためにインシデントの対応手順を変更する必要がある。変更内容を 40 字以内で述べよ。

6. 退室可能時間に途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
13. 午後Ⅱの試験開始は **14:30** ですので，**14:10** までに着席してください。