演習　インシデント管理

平成28年度 問3

問　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。

解答例

設問1　（1）30字以内　（2）40字以内

（1）

①

優先度は“中”なのに，開発チームに直ちに緊急連絡をしていない

②

サービスの早期回復を試みず，インシデントの原因調査をした

〔試験センターによる解答例〕

①：優先度に従って開発チームに緊急連絡を行っていない。

②：サービスの早期回復を優先せずに原因の調査を続けた。

（2）

今回のようなインシデントが発生した場合に，サービスを早期に回復させるため

〔試験センターによる解答例〕

同類のインシデントが再発した場合に，サービスを早期に回復させるため

設問2　（1）15字以内　（2）20字以内

（1）

空欄a

メールサーバのログ

〔試験センターによる解答例〕

空欄a：メールサーバのログ

（2）

空欄b

添付ファイルと標的型攻撃メールの削除

〔試験センターによる解答例〕

空欄b：標的型攻撃メールの削除

設問3　40字以内

運用チームの担当者が，情報セキュリティ担当要員に連絡しなければならないから

〔試験センターによる解答例〕

情報セキュリティ担当要員に連絡して，早期に対応する必要があるから

設問4　(1) 30字以内 (2) 40字以内

配送管理サービスの優先度判定ルールにおける“異常”の優先度を，“高”に変更する

〔試験センターによる解答例〕

配送管理サービスの優先度判定ルールで“異常”の優先度を“高”に変更する。

設問別解説

設問のパターンと難易度

設問1	(1)	B ヒント＋記述型　難
	(2)	B ヒント＋記述型　中
設問2	(1)	A 解答探索　易
	(2)	C 記憶＋記述型　易
設問3		B ヒント＋記述型　難
設問4		B ヒント＋記述型　易

設問1

(1) 問題文〔販売サービスのインシデント〕に記述されているY氏のインシデント対応状況を，“表2　インシデントの対応手順”と照合すると，下表のようにまとめられる。

表2の手順	〔販売サービスのインシデント〕の対応状況	問題点
記録	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。	なし
優先度の割当て	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。(後略)	なし
分類	②(前略)その後，分類したカテゴリの内容で記録の更新を行った。	なし
記録の更新	②(前略)その後，分類したカテゴリの内容で記録の更新を行った。	なし
段階的取扱い	▼記述なし	あり
解決	▲記述なし	あり
終了	〔販売サービスのインシデント〕の最後から1，2文目 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。	なし

上表▼の“段階的取扱い”が1つ目の問題点に該当する。表2の“段階的取扱い”の概要は＜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＞となっており，問題文〔販売サービスのインシデント〕②は，“表3及び表5を参照し，優先度を“中”と割り当て”としているので，1つ目の解答は＜優先度は“中”なのに，

開発チームに直ちに緊急連絡をしていない＞(30字)のようにまとめられる。
上表▲の“解決”が2つ目の問題点に該当する。表2の“解決”の概要は＜サービスを早期に回復させるために，回復を試みる＞となっており，問題文〔販売サービスのインシデント〕④の最終文から2文目は，“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”としているので，2つ目の解答は＜サービスの早期回復を試みず，インシデントの原因調査をした＞(28字)のようにまとめられる。

(2) 問題文〔販売サービスのインシデント〕の最終文は，下記のとおりである。

> 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。

本設問は，上記を使って作られており，Z氏がKEDBに登録した回避策とは，“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”である。しかし，これは，KEDBに回避策を登録した目的ではない。問題文〔システム部のインシデント管理〕の2，3文目は，下記のとおりである。

> 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。

上記が本設問のヒントになっており，上記★の下線部を使って，解答(KEDBに回避策を登録した)は，“今回のようなインシデントが発生した場合に，サービスを早期に回復させるため”(36字)のようにまとめられる。

設問2

(1) 空欄aを含む文は，下記のとおりである。

> 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。

問題文〔標的型攻撃メールの検出〕③は，下記のとおりである。

> 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。（後略）

上記より，メールサーバのログには，電子メールの宛先が記録されている。したがって，空欄aには“メールサーバのログ”（9字）が入る。

（2）空欄bを含む文は，下記のとおりである。

> 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。

問題文〔標的型攻撃メールの検出〕③から下へ1文目は，下記のとおりである。

> 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。

上記より，標的型攻撃メールに添付されたファイルを開封すると，不正プログラムが起動される。したがって，空欄bには“添付ファイルと標的型攻撃メールの削除”（18字）が入る。

設問3

問題文〔標的型攻撃メールの対策〕②は，下記のとおりである。

> 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。

上記より，下線（ア）は，“●特定の基準以上の危険性がある，標的型攻撃メールのような不正な通信を検出した場合，監視システムは，“警告”のメッセージを表示する”と解釈できる。表5から下へ1文目は，下記のとおりである。

> ★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。

前述●の下線部は，前述★の下線部が想定するケースの1つに該当するので，標的型攻撃メールのような不正な通信を検出した場合，前述◆の下線部のように，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なければならない。したがって，本設問（監視システムに“警告”のメッセージを表示させる理由）の解答は，“運用チームの担当者が，情報セキュリティ担当要員に連絡しなければならないから”（37字）のようにまとめられる。

なお，問題文〔標的型攻撃メールの対策〕③は，下記のとおりである。

> 運用チームは，インシデントを記録し，管理する。

試験センターの採点講評は，本設問に関して，＜“記録を残すためにインシデントとして管理する”などの誤った解答が多かった＞としている。この誤答は，上記を引用して作られたものと推測される。また，当然ではあるが，別解には該当しない。

設問4

問題文〔配送管理サービスの変更〕②は，下記のとおりである。

> 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。

上記が，本設問が問う“インシデントの対応手順を変更する必要があるサービス要求事項”である。表1は，下表のとおりである。

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

上記★の下線部は，▼上表では“異常”に該当する。表5は，下表のとおりである。

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

前述●の下線部は，▲上表では“優先度：高”に該当する。表4は次のとおりである。

項番	表示メッセージの種類	優先度
1	異常	中
2	警告	低

上表では，“異常の優先度”は“中”になっているが，上記★・●の下線部より，“高”に変更しなければならない。したがって，本設問（変更内容）の解答は，＜配送管理サービスの優先度判定ルールにおける“異常”の優先度を，“高”に変更する＞（39字）のようにまとめられる。