問 1　社内システムの再構築に関する次の記述を読んで，設問 1～5 に答えよ。

A 社は，社員数 500 名の医薬品卸売業者であり，全国の 7 か所の営業所で販売業務を行っている。

本社には，各営業所の営業部門を統括する営業本部，A 社のシステムの開発・運用を担当する情報システム部，及び取扱商品の購買を一括して担当する購買部がある。購買部では，購買管理システムを用いて，商品の発注，検収などの業務を行っている。購買管理システムを含む，A 社のすべてのシステム（以下，現システムという）は，10 年ほど前に構築され，その後，自社で改修を重ねてきた。現システムは，小型汎用機と端末で運用されているが，構築してから年数が経過しており，機能改良や性能維持が困難になりつつあった。

〔購買管理システムの概要〕

購買管理システムには，取引先マスタや商品マスタなどが格納されており，取引先マスタには，取引先コード，取引先名，配送方法，支払条件などがあらかじめ登録されている。

各営業所の営業担当者は，適切な在庫量を維持するために，取扱商品の売行きや在庫量を見計らいながら，発注品目や発注数量などを記入した紙の発注依頼票を起票して営業本部に送付する。

購買部の発注担当者は，各営業所の営業担当者から営業本部あてに送付された紙の発注依頼票を営業本部から受け取ると，取引先マスタや商品マスタと照合し，取引状況や支払条件などを確認した上で，取引先に見積りを依頼し，取引先と条件交渉を行う。最終の見積内容で合意できなければ，営業担当者に差し戻すが，合意できれば，発注依頼票に記入された発注数量どおりに，発注担当者が購買管理システムで発注入力を行って発注を確定し，印刷出力した注文書と納品書を取引先に郵送する。納品書は，納品時に商品とともに配送してもらうための A 社専用の伝票であり，購買管理システムが自動採番して管理する発注番号に対応したバーコードが印刷されている。

納品日に商品が入荷すると，購買部の検収担当者は，商品とともに送られてきた納品書を参照しながら商品を検収し，問題がなければ，納品書に印刷されたバーコードを購買管理システムで読み取り，入荷・検収処理を行う。

〔購買管理システムの利用状況〕

購買管理システムは，本社の購買部の正社員のはかに，購買部が契約している派遣社員や臨時雇用社員が利用している。正社員には，個別の利用者 ID が振り出されているが，派遣社員や臨時雇用社員は，共用の利用者 ID を使用している。

情報システム部の正社員は，一つの共用の特権 ID で購買管理システムにログインし

て運用管理を行っている。情報システム部の正社員は，この特権 ID を使用して，取引先マスタや商品マスタの更新などを含む，一般の利用者 ID で実施できない操作をすべて行っている。

〔トラブルの発生〕

ある日，営業担当者が，一部の商品の在庫量が異常に多いことに気付き，購買部に問い合わせて確認したところ，営業本部から発注を依頼された数量と，購買部が実際に発注入力した数量が食い違っていた。購買部では，原因を特定して対策を検討するために，購買管理システムの利用状況の確認を情報システム部に依頼した。

連絡を受けた情報システム部が，購買管理システムのログを確認したところ，3 週間ほど前のログの中から，通常の取引数量よりもかなり多い発注入力の記録を発見した。しかし，その発注入力を行った発注担当者を①特定することができなかった。

購買部では，数量が食い違っていた原因を特定するために，保管している大量の発注依頼票と納品書を突合して確認した。その結果，発注入力時にけた数を誤った可能性のある書類を複数選び出すことはできたが，発注担当者の特定には至らなかった。

そこで，上記のトラブルを受けて，購買部では，発注担当者が発注番号を記入する欄と，なつ印する欄を，発注依頼票に新たに設け，購買管理システムで発注入力を行った際に，発注番号を記入の上，なつ印することにした。そうすることで，発注担当者が発注依頼票に誤りなく記入，なつ印さえすれば，トラブルの際にも発注担当者を特定できるようになった。しかし，②発注の誤り自体を防ぐ仕組みにはなっていなかったので，その後の発注入力でもトラブルが再発してしまった。

〔新システムの検討〕

A 社では，構築してから年数が経過して，機能改良や性能維持が困難になりつつある現システムを更改する計画があった。そこで，一連のトラブルが，更に再発することを防ぐために，その更改に併せて一部の発注手順を変更することにした。

新システムの構築に先立って，情報システム部の B 部長を責任者，営業本部の C 部長を副責任者，情報システム部の D 主任などをメンバとする検討チームを設置して，企画・検討することになった。

検討チームによる検討の結果，新システムでは，従来の小型汎用機と端末の組合せを廃し，PC 上のブラウザから，社内 Web サーバ上の業務ポータル画面を介して各種の業務用サーバにアクセスする構成を採用することにした。また，本社と各営業所間は，IP-VPN を利用して常時接続し，電子的に情報をやり取りできる環境を整えることにした。

さらに，社内の IT インフラを全面的に再構成し，社内外との電子メール（以下，メールという）送受信，社外 Web の閲覧などの機能を実現することにした。

図 1 は，検討段階の新システムの概要である。

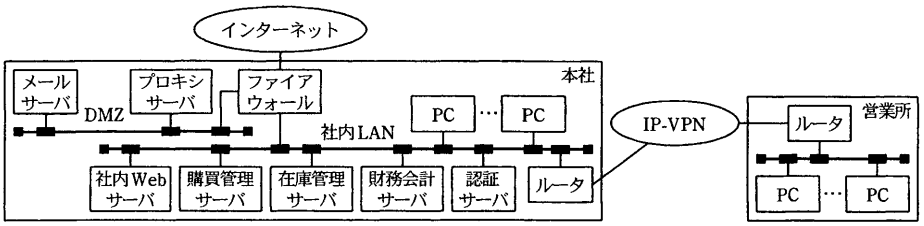

図 1　新システムの概要

新システムでは，正社員には 1 人 1 台ずつ，派遣社員と臨時雇用社員には，2，3 人に 1 台ずつ PC を用意する。PC 上のブラウザからは，購買部の全社員が，社内 Web サーバ上の業務ポータル画面を介して，購買管理サーバや在庫管理サーバにアクセスすることができる。さらに，DMZ 上のプロキシサーバを介して，インターネット上の外部 Web を閲覧することもできる。

また，PC 上のメールクライアントからは，DMZ 上のメールサーバを介して，社内外とメール送受信を行うことができる。

新システムを導入することで，営業担当者が，取引先の Web を閲覧して商品情報を確認したり，顧客との間で情報をメールで交換したりできること，また，発注担当者が，営業担当者との間で，発注依頼票を紙ではなくメールの添付ファイルとして電子的にやり取りしたり，取引先との間で見積情報をメールで交換したりできるようになることから，業務の大幅な効率向上と迅速化が期待された。

次に，検討チームは，新システムのセキュリティ要件の検討を開始した。現システムでのトラブルを踏まえ，利用者 ID とパスワードの管理に関するセキュリティ要件，ログ管理に関する要件，新システムの機能で重要なメールに関するセキュリティ要件から検討を開始することにした。

〔利用者 ID とパスワードの管理に関するセキュリティ要件の検討〕

新システムでは，業務ポータル画面を利用する際に利用者 ID とパスワードを一度入力すると，その後は，各種の業務用サーバ上にある業務アプリケーション（以下，業務アプリという）を利用する際に利用者 ID とパスワードを入力せずに済む，シングルサインオンの機能を導入することにした。この機能を導入することで，利用者の利便性は向上するが，万が一，利用者 ID とパスワードが流出したり破られたりしてしまうと，シングルサインオンできるすべての業務アプリを簡単に不正利用されてしまうというリスクが伴う。そこで B 部長は，パスワードの厳重な管理を義務付けることにした。D 主任は，B 部長の指示を受けて，パスワードの管理に関するセキュリティ要件を，図 2 のようにまとめた。

・パスワードを保存する場合には，その内容を暗号化すること
・パスワードを送信する場合には，その内容を暗号化すること
・利用者に対し，定期的にパスワードを変更するように促すこと
・利用者が自らパスワードを変更できること
・利用者が定期的にパスワードを変更していることを，管理者が確認できること
・利用者が定期的にパスワードを変更しないと，その利用者はシステムを利用できなくなること
・破られやすいパスワードは設定できないこと
・それまでに利用していたパスワードは再設定できないこと

図2　パスワードの管理に関するセキュリティ要件

次は，図2に関する，B部長とC部長の会話である。

C部長：パスワードを守るために保存や送信の際に暗号化することや，パスワードを定期的に変更する必要があることは理解できる。しかし，利用者が自分でパスワードを変更できることが，なぜ要件として必要なのかが分からない。

B部長：利用者のパスワードを変更する方式には2案ある。一つは，利用者が自分で変更する方式であり，もう一つは，情報システム部が一括して変更し，それを利用者に通知する方式である。しかし，情報システム部が一括して変更し，それを利用者に通知する方式は，③情報セキュリティ対策上，望ましくないので，利用者が自分でパスワードを変更できることを要件として設定した。

C部長：なるほど，情報セキュリティ対策として必要なら，仕方ないな。承知した。

〔ログ管理に関する要件の検討〕

次の日，B部長は，ログ管理に関する要件を，D主任と一緒に検討した。次は，B部長とD主任の会話である。

D主任：ログの取得は，利用者認証のような［ a ］のための対策にはなりませんが，いつ，どのような事象が発生したかを記録しておくことは，［ b ］のための対策として重要だと思います。

B部長：確かに君の言うとおり，ログの取得はとても重要なので，しっかりと検討しなくてはならない。例えば，サーバへのログイン状況を確認するために取得するログには，日時，ログインを試みた利用者ID，ログインを試みたサーバ，ログインの成否などの項目を記録することが考えられるな。まずは，④新システムの各サーバ上で取得するログに記録すべき項目を検討してほしい。

D主任：分かりました。検討の際に注意すべき点はありますか。

B部長：そうだな。ログ管理では，ログの取得だけではなく，ログを保護するためのセキュリティ対策も必要だ。ログを収めるファイルは，サイズが大きくなりがちなので，⑤ログを収めるサーバのハードディスク容量を使い切らないようにするための機能を考えておかなければならないだろう。さもないと，肝心なときに，ハードディスクが満杯になってしまい，ログが残っていなかっ

たという失敗も考えられるからな。ほかにも，⑥ログを収めたファイルがリモートから不正アクセスされて改ざん又は消去されるというリスクを低減するための機能も必要だろうし，取得した⑦ログの点検・分析を支援するための機能などもあるとよいだろう。

D 主任：分かりました。取得するログに記録すべき項目と，ログ管理に関するセキュリティ要件を検討します。

D 主任は，B 部長との検討結果を基に，ログ管理に関するセキュリティ要件を図 3 のようにまとめた。また，新システムの利用者に対して，システム上でログを取得し，点検・分析することを⑧周知することにした。

・ログを収めるサーバのハードディスク容量を使い切ってしまい，ログが書き出せなくなることを防ぐための機能を設ける。
・ログを収めたファイルの改ざんや消去を防ぐための機能を設ける。
・取得したログの点検・分析を支援するための機能を設ける。

図 3　ログ管理に関するセキュリティ要件

〔メールに関するセキュリティ要件の検討〕

次に B 部長は，今回，新たに導入することにしたメールに関するセキュリティ要件を，D 主任と一緒に検討することにした。次は，B 部長と D 主任の会話である。

B 部長：メールに関するセキュリティ要件としては，スパムメールの排除，添付ファイルのウイルス対策などの検討が必要かと思う。それらをどのように実現するのがよいか，具体的に案を検討してくれないか。

D 主任：はい。まず，スパムメールの排除ですが，市販のスパムフィルタを導入するのがよいと思います。次に，添付ファイルのウイルス対策ですが，PC にウイルス対策ソフトを導入するだけでなく，メールの転送時に，当社のメールサーバと連携してウイルス検査を行うゲートウェイ型のウイルス対策ソフトを追加で導入するのがよいと思います。ただし，ゲートウェイ型のウイルス対策ソフトを導入するには，そのウイルス対策ソフトを動作させるための専用サーバを新システムに追加する必要がありそうです。

B 部長：ゲートウェイ型のウイルス対策ソフトを導入するのならば，PC にはウイルス対策ソフトを導入しなくてもよいのではないか。

D 主任：ゲートウェイ型のウイルス対策ソフトだけを導入し，PC にウイルス対策ソフトを導入しない場合には，［ c ］といったセキュリティ上のリスクが残ります。PC のウイルス対策ソフトと，ゲートウェイ型のウイルス対策ソフトの両方を導入しておけば，そうしたリスクを低減することができます。さらに，PC のウイルス対策ソフトとゲートウェイ型のウイルス対策ソフトの製造

元を別にしておけば，［ d ］に起因するセキュリティ上のリスクも低減できます。

B 部長：確かにそうだな。それでは両方とも導入することにして，メールに関するセキュリティ要件をまとめておくように。

D 主任は，B 部長との検討結果を基にし，さらに，幾つかの要件を加えて，メールに関するセキュリティ要件を図 4 のようにまとめた。

・スパムと判断されたメールは，できるだけ管理負荷の少ない方式で削除する。
・社外から社内，又は社内から社外へのメールでは，特定の拡張子が付いた添付ファイルを削除する。
・添付ファイルのウイルス検査を行う。
・添付ファイルがパスワード付きファイル又は暗号化ファイルの場合は，内容を確認できないので，そのまま転送する。
・PC のウイルス対策ソフトとゲートウェイ型のウイルス対策ソフトを導入する。二つの製造元は別にする。

図 4　メールに関するセキュリティ要件

〔セキュリティ要件の見直し〕

B 部長と D 主任は，新聞やテレビなどで報道されているセキュリティ上の事件や事故を踏まえると，図 2～4 のセキュリティ要件だけでは不十分であると考えていた。

そこで B 部長は，新システムの構築を依頼する予定のシステムインテグレータ E 社とは別に，情報セキュリティコンサルティング会社の F 社に情報セキュリティ対策の検討支援を依頼した。B 部長は，F 社の情報セキュリティコンサルタントである G 氏の助言に基づいて，新システムの業務アプリに想定されるリスクを洗い出し，その上で追加の情報セキュリティ対策を検討することにした。

G 氏からは様々な指摘と助言があったが，その一つに，⑨購買管理システムにおける特権 ID の運用に関する問題点の指摘と，それを踏まえた対策の助言があった。

B 部長は，図 2～4 及び G 氏の助言を基に，情報セキュリティ対策を要件定義書として取りまとめ，E 社に提示するとともに，必要な対策の実装を依頼した。さらに，F 社と協力して E 社によるシステム構築の進捗状況を適宜確認し，無事に新システムを稼働させることができた。

設問 1　本文中の［ a ］～［ d ］について，(1)，(2) に答えよ。

(1)　［ a ］，［ b ］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　検収　　イ　検知　　ウ　修正　　エ　集約　　オ　予防

(2)　［ c ］，［ d ］に入れる適切な字句を，それぞれ 25 字以内で述べよ。

設問 2　〔トラブルの発生〕について，(1)，(2) に答えよ。

(1) 本文中の下線①で，取得したログから発注担当者を特定できるようにするためには，運用上どのような対策が必要か。40 字以内で述べよ。

(2) 本文中の下線②で，発注の誤りを防ぐために購買管理システムを改修するとした場合における，改修後のシステムでの入力内容の確認と発注の承認に関する業務の流れを，60 字以内で述べよ。

設問 3　本文中の下線③で，望ましくないとしている理由を，40 字以内で述べよ。

設問 4　〔ログ管理に関する要件の検討〕について，(1) ～ (5) に答えよ。

(1) 本文中の下線④について，本文中で述べたようなトラブルの原因を特定するために，購買管理サーバにおける発注入力処理時に取得するログに記録すべき項目を，“日時”以外に五つ，本文中の字句を用いて，それぞれ 12 字以内で答えよ。

(2) 本文中の下線⑤について，考えられる機能を，35 字以内で述べよ。

(3) 本文中の下線⑥について，考えられる機能を，30 字以内で述べよ。

(4) 本文中の下線⑦について，このような機能を利用することによって，情報セキュリティ対策の面で得られる利点を，25 字以内で述べよ。

(5) 本文中の下線⑧を実施することで期待できる効果を，25 字以内で述べよ。

設問 5　本文中の下線⑨について，(1)，(2) に答えよ。

(1) 特権 ID に関する問題点を，15 字以内で述べよ。

(2) 実施すべき対策を，40 字以内で述べよ。

問 2　情報セキュリティインシデントへの対応に関する次の記述を読んで，設問 1～5 に答えよ。

Y 社は大手の総合小売業者で，全国に店舗を展開している。5 年前にインターネットでの通信販売を開始し，通販会員登録をしている購入者に対してポイントサービスを実施するなど，拡販に力を入れている。3 年前には，通信販売サイトをポータルサイトとしてリニューアルし，通販会員に対して Web メールやブログのサービスを開始した。

〔情報セキュリティ推進委員会の設置及び位置付け〕

Y 社では，通信販売の開始とともに，全社横断的な組織として情報セキュリティ推進委員会を設置し，情報セキュリティポリシを策定した。情報セキュリティ推進委員会は社長直属の組織であり，情報セキュリティポリシ策定後も，Y 社の情報セキュリティに関する意思決定組織として存続している。しかし，ここ 2 年ほどは会議が開かれることもなく，実質的な活動は行っていない。

Y 社の組織を，図 1 に示す。

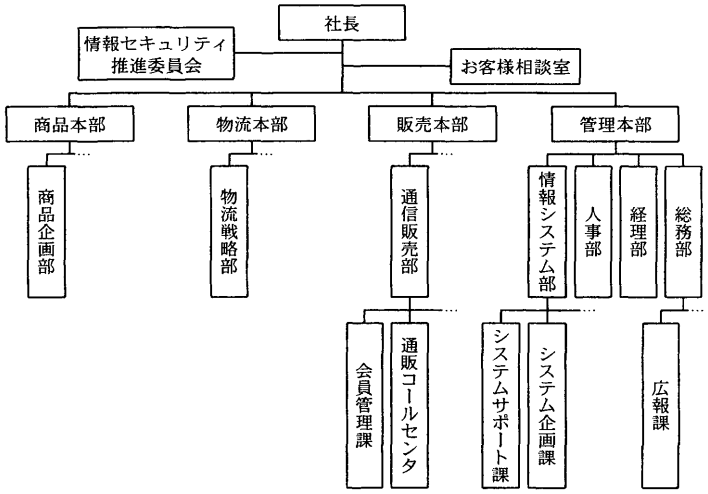

図 1　Y 社の組織（抜粋）

〔ポータルサイトの運用〕

ポータルサイトを含めた全社の情報システムのインフラは，情報システム部が管理している。ポータルサイトについては，サーバ機器及び主要プロセスの稼働を 24 時間 365 日遠隔で監視する業務を，Z 社に委託している。ポータルサイトの障害対応手順として，Z 社は，機器又はプロセスのダウンを検知した場合，平日の 9 時～17 時であればシステムサポート課へ連絡し，夜間や休日であれば一次対応を行う。Z 社による一次対応は，機器又はプロセスの再起動の試行と，再起動しても復旧しない場合の“メンテナンスのためサービス停止中”の画面表示への切替えまでである。本格的な復旧作業は，情報システム部が翌営業日に実施することになっている。

ポータルサイトで提供するサービスの企画や運営は，販売本部の通信販売部が担当している。会員管理課は通販会員情報管理を，通販コールセンタはポータルサイトに関する社外からの問合せ対応を，それぞれ担当している。社外からの一般的な問合せは，お客様相談室に寄せられることもある。

〔情報セキュリティインシデントの発生と対応〕

あるとき，Y 社のポータルサイトを模したフィッシングサイト（以下，偽ポータルサイトという）が構築され，通販会員の情報が危険にさらされるという，情報セキュリティインシデント（以下，インシデントという）が発生した。経過は次のとおりである。

(1) ある通販会員（以下，会員 X という）から，Y 社から送信された“会員情報再確認のお願い”という電子メール（以下，お願いメールという）に記述されたリンク先の“会員情報の照会／更新”画面の操作方法について，通販コールセンタに電話

で問合せがあった。

(2) 通販コールセンタの担当者は，お願いメールの存在について知らなかったことと，会員 X の説明する画面表示が Y 社ポータルサイトの“会員情報の照会／更新”画面と異なっていることから，調べて折返し回答する旨を会員 X に伝えて，いったん電話を切った。

(3) 通販コールセンタの担当者が会員管理課に確認したところ，お願いメールを送信した事実はないことが判明した。通販コールセンタの担当者は，会員に再度連絡し，第三者の悪質ないたずらである可能性が高いとして，当該メールを無視するよう伝えた。また，当該メールを通販コールセンタまで転送してもらうことにした。

(4) 会員 X から転送された当該メールの内容を確認した会員管理課は，次の点から，当該メールは偽ポータルサイトへ誘導するために第三者が送信した電子メールであると判断した。

1. 通信販売部は，当該メールを送信していない。
2. 当該メールの差出しメールアドレスは，通信販売部が通常，通販会員向け電子メールで利用しているものとは異なっている。
3. 当該メールの本文中に記載されている URL のドメイン名は，Y 社のものと異なっている。
4. 当該メール本文中のリンクを実際にたどってみたところ，リンク先が，Y 社のポータルサイトとよく似たデザインの偽ポータルサイトであることを確認した。

(5) 会員 X から通販コールセンタに問合せがあった日の翌日，Y 社の通販会員ではない人物から，お客様相談室にお願いメールについての問合せがあった。

(6) お客様相談室は会員管理課に確認した結果，偽メールであると認識したので，問合せをしてきた人物に対して，お願いメールを無視するよう回答した。

(7) お客様相談室には，その後も，通販会員以外から同様の問合せが多数寄せられたが，いずれの問合せにも，お願いメールを無視するように回答することで対応した。

通信販売部は，通販会員以外にもお願いメールが多数送信されていることから，お願いメールが無差別に送信されていると考え，通販会員のメールアドレスが漏えいした可能性は低いと判断した。偽ポータルサイトが Y 社とは異なるドメイン名のサイト上に構築されていることからも，通信販売部として積極的な対応は不要と判断し，通販コールセンタ及びお客様相談室への問合せに対しては，お願いメールを無視するように回答することにした。

〔インシデント対応の見直し〕

その後，インターネットの掲示板やブログで偽ポータルサイトの出現が話題になり始め，問合せをしてきた通販会員にお願いメールを無視するように回答しているだけ

のY社の対応について，疑問の声が上がるようになった。また，時を同じくして，Y社のポータルサイトにクロスサイトスクリプディングの脆弱性が存在することを指摘した書込みも，幾つかの掲示板に現れた。

これらの動きに注目した，IT関係のニュースを発信しているWebサイトの記者から，Y社の広報課に取材の申込みがあった。広報課では，偽ポータルサイトについて何も把握していなかったので，情報システム部に問い合わせた。しかし，情報システム部でも把握しておらず，ポータルサイトに関する内容ということで，通信販売部に確認して，ようやく事態を把握できた。

このような状況を憂慮した情報システム部のQ部長は，通信販売部の対応に問題があると考え，通信販売部のP部長に改善策の検討を打診した。P部長とQ部長は，通信販売部及び情報システム部の課長を加えた打合せの場を設けて改善策を検討した。その結果，次の対応を取ることにした。

（A）Y社のポータルサイトに，お願いメールの存在とお願いメールを受け取った場合の対応について掲示する。また，掲示と同様の内容を記述した電子メール（以下，対応メールという）を全通販会員に送信する。

（B）図2に示す，偽ポータルサイトの見分け方を，ポータルサイトに載せる。

（C）通販コールセンタ及びお客様相談室の担当者に（A）及び（B）の内容を周知し，問合せに対して適切なアドバイスができるようにする。

（D）Y社従業員がお客様から今回のインシデントについて問合せを受けた場合，個別に回答せず，問合せ内容を会員管理課へ連絡するよう指示する。

（E）偽ポータルサイトの閉鎖に向けた働きかけを，社外の調整機関へ依頼する。

次の事項のいずれかに該当する場合，当社ポータルサイトを模したフィッシングサイトへの接続が疑われますので，通販コールセンタへご連絡ください。
・ブラウザのアドレスバーに表示されるURLのドメイン名の部分が，当社ポータルサイトのドメイン名になっていない。
・会員情報の照会／更新画面において，ブラウザに鍵マークが表示されていない。
・会員情報の照会／更新画面において，ブラウザに鍵マークが表示されているが，次の方法で表示される値が，当社ポータルサイトのドメイン名になっていない。
① 鍵マークをクリックする。
② 表示された証明書ダイアログの詳細タブをクリックする。
③ “サブジェクト”を選択する。

図2 偽ポータルサイトの見分け方

実際にこれらの対応を取った結果，全通販会員に送信した対応メールが一部の通販会員の混乱を招き，通販コールセンタが対応に追われることになったが，偽ポータルサイトの閉鎖も確認され，事態は収束に向かった。

〔情報セキュリティ推進委員会の活動再開〕

今回のインシデント対応については，発生当初の対応が不適切であったこと，さらに，批判を受けてから対応を検討し始めたことなど，多くの反省点を残すこととなっ

た。

そこで，P 部長と Q 部長は，活動停止状態にあった情報セキュリティ推進委員会の活動を再開させ，情報セキュリティポリシの改訂も含めた今後の対策を協議することにした。また，Z 社のコンサルタントである S 氏にも，外部の専門家として対策の協議への参画を要請した。

〔クロスサイトスクリプテイングへの対応〕

S 氏は，ポータルサイトのクロスサイトスクリプテイングの脆弱性がインターネット上の掲示板などで指摘されている点を問題視し，一刻も早くこの脆弱性の有無を確認し，もし存在するならば，早急に対処すべきであると指摘した。S 氏によれば，この脆弱性が存在する場合，攻撃者によってポータルサイトのページに［　ア　］が埋め込まれてしまう可能性があり，仮に［　イ　］といった動作を行う［　ア　］が埋め込まれると，偽ポータルサイトが図 2 の方法では見分けられなくなってしまうとのことであった。

Q 部長は，S 氏の指摘に従い，情報システム部の担当者に対応を指示した。

〔インシデント対応の問題点〕

情報セキュリティ推進委員会では，今回のインシデントの経緯を改めて調査し，対応における問題点を次のように整理した。

(1) 今回のインシデントに対しては，当初，通信販売部とお客様相談室だけが対応を進めており，はかの部署への連絡や協力の依頼がなされなかった。その結果，情報システム部や広報課が事態を把握できず，技術的な対策やマスコミへの対応が遅れてしまった。最終的には，必要な部署すべてに連絡することができたものの，もっと早い段階で関係部署に連絡すべきであった。また，今回のインシデントに関連した問合せが複数の部署にあったが，それらの情報を取りまとめる部署がなかった。

(2) Y 社の情報セキュリティポリシでは，インシデントが発生した場合，情報システム部と情報セキュリティ推進委員会に連絡することが規定されているが，周知徹底が不十分であった。また，情報システム部と情報セキュリティ推進委員会に連絡するにしても，インシデントの発見者が連絡するのか，それとも発見者の上司などが連絡するのかなどは規定されていなかった。情報セキュリティ推進委員会が実質的に活動停止状態にあったので，連絡先が不明であることと併せて，連絡及び報告の経路が明確になっていなかった。

(3) Y 社には，クロスサイトスクリプテイングとフィッシングサイトの関係について理解している者がいないことから，〔インシデント対応の見直し〕の時点でクロスサイトスクリプテイングへの対応が行われなかった。また，インシデントに対して適切な技術的対策を取るためには，公開されている技術的脆弱性や攻撃手法などの

情報を把握する仕組みが必要だが，これもY社にはなかった。

(4) お願いメールと対応メールのどちらを信用すべきか迷った通販会員がいて，混乱を招いた。

〔今後の対策〕

情報セキュリティ推進委員会では，〔インシデント対応の問題点〕で挙げられた問題点を更に検討し，今後，次の対策を実施することを決定した。

(a) インシデントの定義やインシデント発生時の連絡及び報告の経路，インシデントに対応する際の各部署の役割や部署間の連絡体制などの対応方針を明確にした規程を整備する。

(b) (a) で整備した規程の周知徹底を図り，インシデント発生時に速やかに対応できる体制を作る。詳細は，(i) ～ (iii) のとおりとする。

(i) 今回のインシデントのように，複数の部署が協調して対応する必要がある場合に備え，全社横断的なインシデント対応チーム（以下，IRTという）を設置する。IRTは，情報セキュリティ推進委員会の下部組織として位置付けられる。

(ii) IRTの事務局をシステム企画課に設置する。インシデント発生時には，事務局が必要なメンバをIRTメンバの中から選んで招集する。

(iii) インシデント発生時の連絡及び報告の経路は，図3のとおりとする。

(c) 情報システムの脆弱性や情報システムに対する攻撃手法の情報を収集・評価し，関係者に周知する体制を作る。あわせて，<u>①ポータルサイトを構成するハードウェア及びソフトウェアの構成情報を管理する</u>。

(d) インシデント対応において，通販会員に電子メールで通知する場合は，なりすましメール対策として，同じ内容をポータルサイト上に掲載した上で，ポータルサイトも併せて参照するよう電子メール本文に記載する。

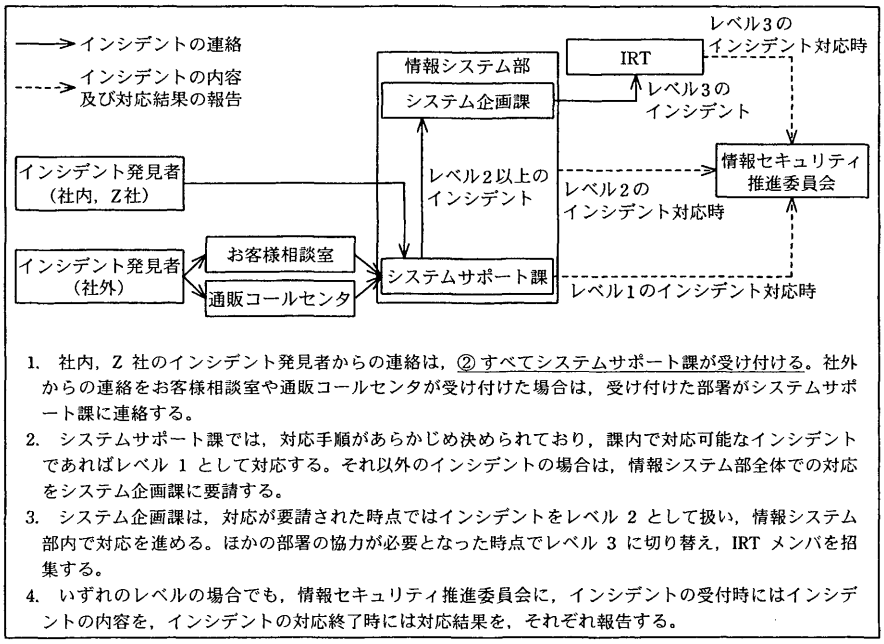

図3　インシデント発生時の連絡及び報告の経路

〔今後の対策についての S 氏のコメント〕

(d) の対策について，S 氏からは，③Y 社からの電子メールであることを確実に判別できる PKI 技術を利用した方法があるとアドバイスを受けた。しかし，この方法は，通販会員への事前説明が必要なこと，通販会員が利用するメールソフトによっては対応できないことなどから，Y 社では今後導入を検討していくが，今回は見送ることになった。

そのはか，S 氏からは，④ポータルサイトに関するインシデントについては，ポータルサイトの利用者を考慮すると即時対応が必要となる可能性が高いが，⑤現状のポータルサイトの障害対応手順と同じ手順でのインシデント対応では，即時性に欠けるとの指摘がなされた。あわせて，⑥レベル 1 のインシデントのうちポータルサイトに関するものについては，Z 社にも対応させるという方法があるという提案も受けた。

情報セキュリティ推進委員会では，〔今後の対策についての S 氏のコメント〕の S 氏のコメントへの対応を検討した上で，必要な対策を実施していくことにした。

設問 1　本文中の［　ア　］に入れる適切な字句を，5 字以内で答えよ。また，本文中の［　イ　］に入れる記述を 50 字以内で述べよ。

設問 2　図 4 は，〔情報セキュリティインシデントの発生と対応〕中のインシデントを，会員からの問合せを受けて，仮に図 3 に従って各部署へ連絡した場合の経路を示している。図 4 中の［　a　］～［　d　］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。

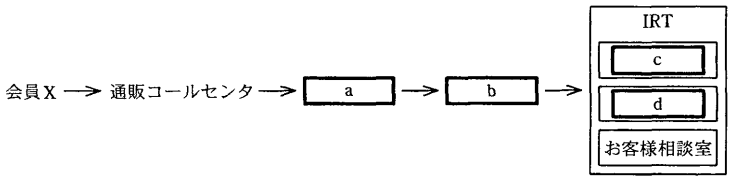

図4　各部署へ連絡した場合の経路

解答群

ア　会員管理課　　イ　経理部　　ウ　広報課　　エ　システム企画課

オ　システムサポート課　カ　商品企画部　　キ　人事部　　ク　物流戦略部

設問3　〔今後の対策〕について，(1)，(2) に答えよ。

(1) 本文中の下線①の構成管理をインシデント対応のために実施する理由を，40字以内で述べよ。

(2) 図3中の下線②のように，インシデントの連絡を特定の部署が一括して受け付ける体制の利点を，インシデントの対応側にとっての利点と，社内のインシデント発見者にとっての利点とに分けて，それぞれ45字以内で述べよ。

設問4　本文中の下線③の方法でY社から送信された電子メールを，通販会員が受信した際に，Y社からの電子メールであることを確実に判別するために通販会員が実施すべき作業を，40字以内で述べよ。

設問5　インシデントの即時対応について，(1) ～ (4) に答えよ。

(1) 本文中の下線④の理由を，25字以内で述べよ。

(2) 本文中の下線⑤で，即時性に欠けると指摘された点を，35字以内で述べよ。

(3) 本文中の下線⑥について，レベル1のインシデントに確実に対応してもらうために，Z社に提示する必要のある事項を，25字以内で述べよ。

(4) 本文中の下線⑥の対応を実施した上で，レベル2以上のインシデントについても即時対応できるようにするために検討すべき点を，45字以内で述べよ。