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

X社は，従業員数300名のソフトウェア開発会社である。X社の主要な事業内容は，ソフトウェア製品の自社開発，Webアプリケーションの受託開発及びオープンソースソフトウェア（OSS）を利用したサーバとネットワークの構築サービスである。また，契約した顧客に対しては，ハードウェア及びソフトウェアの保守サポートも有償で提供しているが，顧客のシステムの運用は行っていない。

X社の組織を図1に示す。

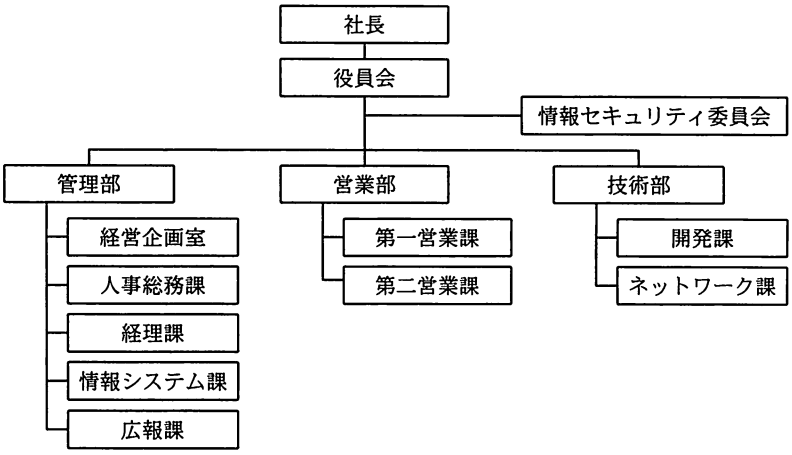

図1　X社の組織

X社では，各部署の部長及び課長から構成される情報セキュリティ委員会と，その委員会の事務局を担当している情報システム課が連携して，情報セキュリティポリシ（以下，ポリシという）の策定やセキュリティ対策の実施を行っている。

X社では，社内の情報システム，ネットワークなどは自社で企画し，開発や構築を行っている。社内の情報システムは業務系システムと開発系システムの二つに分かれており，セキュリティ確保の観点からこの二つのシステムはネットワークを分け，それぞれ別の回線を通じてインターネットに接続されている。業務系システムの運用は情報システム課が行い，開発系システムの運用は開発課とネットワーク課が共同で行っている。

業務系ネットワークには各部署のLANが接続され，全社共通のグループウェアサーバや営業管理サーバ，経理事務サーバなどの業務系サーバ群と接続できるようになっ

ている。また，DMZ 上にメールサーバ，Web サーバ及び DNS サーバが設置され，インターネットに公開されている。

開発系システムは技術部のプロジェクト単位で開発環境が構築されており，その上でソフトウェアの開発や機器のテストなどを行っている。それぞれの開発環境からは OSS の技術情報収集やセキュリティパッチ取得のために，インターネットに対して HTTP や FTP でのアクセスが可能になっている。ただし，インターネットに対して公開しているサーバは開発系ネットワークにはない。

X 社のシステム構成を図 2 に示す。

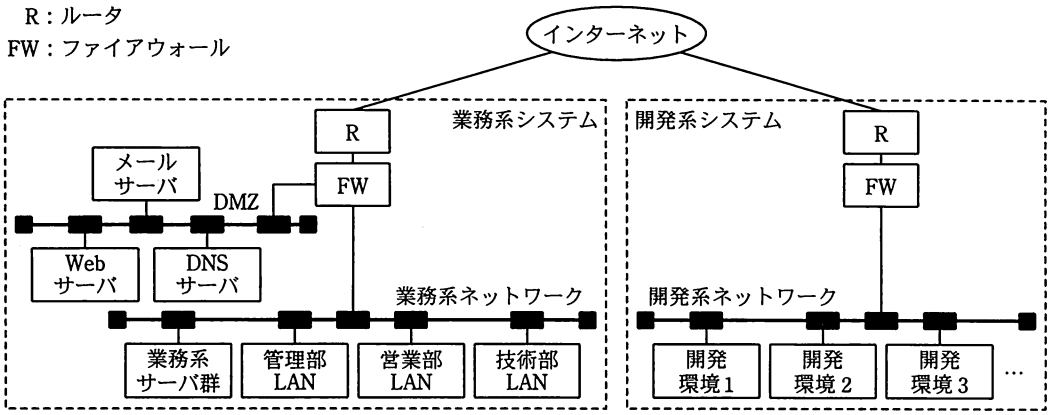

図 2　X 社のシステム構成

年度末を控えたある日，X 社の営業部員が外出した際に，顧客のシステムに関する重要な情報が保管されている業務用のノート PC を紛失するという情報セキュリティインシデント（以下，情報セキュリティインシデントをインシデントという）が発生した。

このインシデントへの X 社の対応は迅速とは言い難かった。ノート PC には指紋認証機能が備わっていたので，正当な利用者以外の者がハードディスクや OS にアクセスする可能性は低かったものの，連絡体制の不備から事実関係の把握に手間取り，顧客への連絡も遅れてしまった。数日後にノート PC は発見され，情報流出の可能性は極めて低いものと判断されたが，このインシデントによって X 社はインシデント対応の重要性を改めて認識した。このため，情報セキュリティ委員会は今回の反省を踏まえてインシデント対応についての取組みを強化することとし，事務局である情報システム課にインシデント対応計画を策定させることとした。

〔インシデント対応計画の策定〕

次は，情報システム課のSさんとT課長の会話である。

Sさん：当社ではこれまで，予防策を中心としたセキュリティ対策を進めてきましたが，今回のインシデントでそれだけでは不十分なことがよく分かりました。

T課長：一つは，社内の連絡体制に問題があった。紛失者から直属の上司である第一営業課の課長にはすぐ連絡があったが，第一営業課ではその先の連絡先が分からなかったことに加えて，発生が金曜日の夕方だったこともあり，本来ならすぐに通知すべき情報システム課や情報セキュリティ委員会への連絡が遅れてしまった。連絡することはポリシに記載されているのだが，インシデント発生時の具体的な連絡先についての周知，教育が不足していたことは否めないね。

Sさん：社内だけでなく，社外への連絡が遅れたことも反省しなければいけませんね。

T課長：インシデントが発生したときの，関係者へ連絡を行う担当や手順が明確になっていなかったことも反省点だね。また，当社では個人情報を扱う業務はそれほど多くないので付与を受けていないが，JIPDEC などの機関から［ a ］の付与を受けた企業では，個人情報の漏えいが発生したときだけでなく，本人以外の個人情報を含むノート PC の紛失などの際にも，その機関に対して事故報告書を提出する必要があるようだ。

Sさん：今回はノート PC の紛失でしたので警察にも遺失物届を出しましたが，Web サーバのコンテンツが改ざんされるなど，被害が発生した場合には，警察への連絡が必要になりますね。

T課長：場合によっては発生したインシデントの内容を［ b ］/CC（コーディネーションセンター）のような外部機関に報告する必要もありそうだ。そのような場合の手順も整備しないといけないね。

Sさん：どれだけ予防策をとってもインシデントの発生をゼロにすることはできないので，<u>①インシデント対応の体制を事前に作っておくこと</u>が必要ではないでしょうか。

T課長：そうだね。これまでは情報システム課が業務系システムのインシデント発生に対応してきたが，情報システム課だけでは対応しきれないことも多い。全社横断的なインシデント対応チーム（以下，IRT という）を設置して，PC 紛

失のような事例も含めて，インシデント対応に関する社内の体制と役割を明確にするのがよいだろうね。

Sさん：システムに関するインシデントでは技術的なセキュリティ対策に関する知識やシステムの実装に関する情報が必要になります。技術的なセキュリティ対策については技術部の方が詳しいですし，こちらでは開発系システムについて詳しく把握できていないこともありますから，技術部と互いに協力して会社全体でのインシデント対応を進められるとよいですね。

このように情報システム課で議論した結果，社内に IRT を設置し，インシデントに対応していく計画を情報セキュリティ委員会へ提案することにした。情報システム課がまとめたインシデント対応計画の骨子を図3に示す。

(1) 本計画は，当社におけるインシデントへの対応を定めるものである。
(2) 当社は全社横断的に IRT を組織し，選任された従業員が IRT メンバを兼務する。
(3) IRT が対応を行うインシデントは，次のとおりとする。
  (a) 当社の所有する情報資産の紛失，改ざん，漏えいなどが疑われる場合
  (b) 当社の業務系システムに異常，不具合などが発生した場合
  (c) 当社の開発系システムに異常，不具合などが発生した場合
(4) IRT は，インシデント対応のために，社内の各部署及び社外の各機関との連携を図る。
(5) IRT は，インシデント対応マニュアルを整備する。
(6) IRT は，社内で発生したインシデントについての報告先となる。
(7) IRT は，インシデント検知のために，社内の情報システム及びネットワークのログなどにおける異常事象を分析する。
(8) IRT は，インシデント対応に必要な脆弱(ぜいじゃく)性情報やセキュリティパッチに関する情報（以下，セキュリティ情報という）を収集し，関連する社内の部署に情報提供を行う。
(9) IRT は，インシデントを検知した際の初期対応を実施する。
(10) IRT は，インシデント対応に必要な証拠の収集と保全，分析を行う。
(11) IRT は，従業員に対してインシデント対応に関する周知，教育を行う。

図3　X社におけるインシデント対応計画の骨子

この対応計画を情報セキュリティ委員会に提案したところ，<u>②X 社の事業内容を踏まえると，図 3 で対象としたインシデント以外にも，IRT が対応すべきインシデントがあるのではないかとの意見があり</u>，情報システム課は対応計画を修正した。その後，情報セキュリティ委員会での審議と役員会の承認を経て，社内のポリシが改定され，IRT が発足することとなった。これに伴って X 社は情報セキュリティに関して表1のように各組織で役割を分担することとした。

表１　情報セキュリティに関するＸ社の組織と役割分担

組織	役割
情報セキュリティ委員会	情報セキュリティ全体の継続的改善
IRT	発生したインシデントの報告の受付 業務系システムと開発系システムのログなどにおける異常事象の分析 インシデント発生時の初期対応と原因究明 セキュリティ情報の収集と提供
情報システム課	業務系システムの運用と監視，セキュリティ対策の実施
広報課	Web コンテンツの作成，更新 重大なインシデントが発生した際の対外広報
開発課	開発系システムの運用と監視，セキュリティ対策の実施 セキュリティを保ったソフトウェア開発 ソフトウェア製品の保守サポート ソフトウェア製品のセキュリティパッチ作成
ネットワーク課	開発系システムの運用と監視，セキュリティ対策の実施 セキュリティを保ったネットワーク構築 ハードウェア機器の保守サポート

〔IRT メンバ向けのインシデント対応マニュアルの整備〕

新たに発足した IRT には，情報システム課の T 課長と S さんのほか，社内の各部署からメンバが選出され，T 課長がチームリーダを務めることとなった。IRT では，インシデント対応を円滑に行うために IRT メンバ向けのインシデント対応マニュアルを作成することとし，その具体的な内容として図 4 に示す各項目を検討した。

(1)　インシデント対応に必要なリソース（機器や情報など）の整備
(2)　ログ管理
(3)　ログなどにおける異常事象の分析
(4)　インシデント発生時の初期対応と作業の記録
(5)　インシデントの証拠収集
(6)　収集した証拠の分析と原因の究明，システムの復旧方法
(7)　社内外の連絡方法と最新のセキュリティ情報の収集

図４　IRT メンバ向けのインシデント対応マニュアルに記載する内容

図 4 中の (1) に関し，必要な機器については，予算面の問題もあることから，優先度の高いものから順に整備を進めていくことになった。また，業務系システムと開発系システムの構成情報は情報システム課と開発課，ネットワーク課が個別に管理していたが，既存のグループウェアを利用して IRT メンバが双方のシステムの構成情報を閲覧できるようにした。

図 4 中の (2) については，まず，現状を把握するために，現在の業務系と開発系のシステムで取得しているログの情報を収集し，リストアップすることにした。その結果，取得しているログの管理が機器ごとにそれぞれ異なることが判明した。このままでは，インシデントの原因究明に必要な情報を安全に確保及び保全することが困難なことから，IRT では今年度中に③ログ管理のポリシを策定することとした。来年度以降には各機器のログのバックアップと統合管理を行うシステムの導入を検討する予定である。

図 4 中の (3) については，情報システム課と共同でシグネチャベースの IPS（侵入防止システム）を DMZ に導入し，攻撃を受ける可能性が高い DMZ 上のサーバへの脅威を分析することとした。開発系システムにも IPS の導入を検討したが，予算が厳しいことと，インターネットに対して公開しているサーバがないことから今年度の導入は見送った。ただし，開発系システムの FW のログについては定期的な分析を行うことにした。

図 4 中の (4) については，インシデント発生の報告を受けた後の対応について検討した。PC の紛失やサーバへの攻撃など，インシデントのタイプを何種類か想定し，そのタイプごとにインシデント原因の究明，被害の拡大防止及び仮復旧の方法をマニュアル化することにした。また，作業記録のフォーマットを整備し，個々のインシデント対応に当たってどのような作業を実施したかを記録することにした。

図 4 中の (5) は，いわゆるコンピュータフォレンジクスの技法についての検討である。インシデント発生時の被害の内容及び範囲の確認並びに発生原因の調査のために必要な情報を確実に保全し，発生した事象を様々な要素から解明することが目的である。IRT では，ネットワークのインシデントに関する情報は IPS 及び FW での監視並びにログの取得を行うことで保全することとした。また，コンピュータに接続された記憶媒体上の情報は専用の機器を導入して保全できるようにした。保全された情報は，IRT が分析を行うことにした。

図 4 中の (6) については，コンピュータフォレンジクスで利用する機器やソフトウェアのベンダや，セキュリティ団体が主催するセミナに IRT メンバが出席するなどして，具体的な技法の習得と (6) の手順化に努めることにした。

図 4 中の (7) については，インシデント発生時の社内の連絡網及び外部の連絡先を整理し，関連部署への周知を図った。また，外部からのセキュリティ情報の収集の際

に IRT では，インシデント対応のコミュニティにおいて広く利用されている実績がある④PGP を利用した電子署名を採用することにした。

このような検討を経て，IRT メンバ向けのインシデント対応マニュアルが完成し，X 社のインシデント対応が本格的に始動することになった。

〔IPS の運用〕

情報システム課はネットワーク課の協力を得て DMZ に IPS を導入した。この IPS ではネットワークの脅威を検知して不正な通信を遮断することができる。また，脅威の検知時刻，通信パケットの送信元及びあて先それぞれの IP アドレス及びポート番号，検知した脅威の種類を示すシグネチャの識別番号（ID），脅威の名称，詳細な通信の内容などの情報をログに記録できる。IPS の管理端末からはこのログを閲覧できるほか，脅威についての解説も閲覧できる。さらに，脅威の検知状況を日次，週次及び月次でレポート化することができる。

なお，IPS のシグネチャは，定期的に最新の状態に更新することとした。

シグネチャによって検知される個々の脅威の危険度はベンダによって 4 段階のレベルに分類されており，レベル 4 が最も危険度が高く，レベル 1 が最も危険度が低い。ただし，利用者側で個々のシグネチャの設定を変更して危険度のレベルを変えることが可能であり，利用者側で設定した脅威の危険度はシグネチャが更新されても維持される。

シグネチャの設定は既定値のままとし，レベル 4 又はレベル 3 の脅威が検知されたときには IRT メンバに対して警告メールが送信される設定を行った上で試験運用を開始したところ，最初の 1 時間のうちに大量の警告メールが IRT メンバに送信された。このため，T 課長はネットワーク課の IRT メンバである U 君に協力を求め，一緒に対応に当たることにした。T 課長が IPS の管理端末から 1 時間の脅威の検知件数を確認したところ，表 2 のような結果が得られた。

表 2　IPS で検知した脅威の集計

ID(1)	危険度のレベル	脅威の名称	件数
1040	4	TCP SYN/FIN Packet	135
1042	4	TCP NULL Packet	123
5021	4	Password File Access Attempt	14
5829	3	HTTP Tunneling	2

注(1)　脅威の種類を示す IPS のシグネチャの識別番号

次は，T 課長と U 君の会話である。

T 課長：とりあえずこの集計を見てくれるかな。どう思うかね。

U 君　：警告が出た脅威は IPS で遮断しているので，特に問題はないと思いますが，警告メールが多すぎるのは困りますね。調べてみましょう。

U 君は IPS の管理端末でログを確認し，検知した脅威に関する解説を表示させた。

U 君　：ID が 1040 番と 1042 番の脅威は，Web サーバとメールサーバの IP アドレスに対する特殊なポートスキャンのようですね。1040 番の脅威は，TCP のコネクションを開始する際に SYN/FIN フラグが付加されていたものです。1042 番の方は，どのフラグも付加されていなかったものです。

T 課長：通常のポートスキャンとはどう違うのかな。

U 君　：この方法では TCP のコネクションが正常に確立しないので，対象となったホスト上で［　c　］されにくいという特徴があります。こうした特徴から，ステルススキャンなどと呼ばれることもあるようです。しかし，この脅威も IPS で遮断されていますし，DoS 攻撃が成立するほど大量に発生しているわけでもありませんので，システムへの影響はないと思います。

T 課長：次に進もうか。5021 番の脅威では，図 5 のようなアクセスがたくさんあるようだが，これは当社の Web サーバには影響はないと考えていいね。

```
GET /cgi-bin/enquete.cgi
view=../../../../../../../../../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
```

図 5　5021 番の脅威と判定したパケットに含まれていた文字列

U 君　：はい。これは，広く使われている CGI プログラムに対する無差別攻撃のようですね。この CGI プログラムは当社では利用していないはずですが，念のため，後で Web サーバの設定とアクセスログを確認してみます。パケットに含まれる文字列からすると，CGI プログラムに含まれる［　d　］の脆弱性を利用して，パスワードファイルを取得することをねらったもののようです。

T 課長：5829 番の脅威では図 6 のようなアクセスが発生しているが，これはどうだろう。Web サーバを悪用する攻撃のようだが。

e	mail.example.com:25 HTTP/1.1

図6　5829番の脅威と判定したパケットに含まれていた文字列

U君　：設定に問題のあるWebサーバを悪用して，外部のメールサーバとSMTPで通信させようとしたようですね。

T課長：Webサーバなのに SMTPで通信しようとしているというのはちょっと変じゃないかな。

U君　：図6を見ると，HTTP/1.1で定義されている［　e　］というメソッドが利用されています。これはWebサーバがいわゆるプロキシサーバとして動作しているときに，TCPの通信を透過的に中継させる目的で利用されるものです。主にSSLを中継させるのに使うことが多いのですが，SMTPのようなプロトコルも中継させることができます。

T課長：なるほど。この脅威についてはどのように対処しているのかな。

U君　：IPSで遮断していますが，当社ではWebサーバをプロキシサーバとして利用しないので，⑤Webサーバではこのメソッドを受け付けない設定になっていますから，仮にIPSで遮断しなくても問題は発生しません。

T課長：今日の警告メールについては，システムへの問題はないということだね。それにしても，警告メールが大量に来るのはちょっと困るな。⑥一定の条件を満たす場合には警告メールを送らないよう，シグネチャの設定を調整して危険度のレベルを変えるのがよいだろうね。

U君　：そうですね。シグネチャの設定を調整し，対応マニュアルも書き換えます。

U君がシグネチャの設定を調整したところ，IRTメンバに大量の警告メールが来ることはなくなった。

〔インシデントの発生と対応〕

その後，大きな問題もなく数か月が経過したある日，U君が開発系システムのFWのログを分析したところ，開発系システムの特定のIPアドレスからインターネット上の幾つかのIPアドレスに対して，通常見られない大量の通信が行われていることに気が付いた。

開発系システムの構成情報で送信元の IP アドレスを確認したところ，送信元の IP アドレスに該当する機器が記載されていなかったので，U 君は開発課に問い合わせた。担当者の話によると，この機器は，近々顧客に納入する Web コンテンツの動作検証を行うため，開発課が一時的に開発環境に接続したサーバ機であるとのことだった。

U 君が更にログを確認したところ，通信の内容に不審なところが見られたことから，U 君は T 課長に連絡し，インシデント対応マニュアルに従って初期対応に取り掛かった。

U 君が証拠収集に必要な機材を持参して開発課に駆けつけたところ，当該サーバ機は U 君が電話で問い合わせた直後に担当者がシャットダウンし，電源が切断された後だった。このため，⑦U 君はこのサーバ機の電源を再投入せず，サーバ機からハードディスクを取り出した。取り出したハードディスクの内容は，専用の複製装置を用いて別のハードディスクに全セクタを複製し，⑧この複製に対してフォレンジックツールを実行して解析を行った。

解析の結果，サーバ機が最近流行しているボットに感染し，インターネットと通信を行っていた形跡が認められた。開発課によると，サーバ機を開発系ネットワークに接続する前に行うべき OS のパッチ適用を怠っていたとのことであった。情報を最終的に総合すると，パッチ未適用で OS の脆弱性が放置されたまま，フリーのソフトウェアの配布先にアクセスし，その際に脆弱性を悪用するボットに感染したため，インターネットと通信を行っていたものと推測された。

IRT はこうした解析結果を開発課に伝え，ボットに感染したサーバ機を再感染しないように再構築するよう指示した。開発課は IRT の指示に従ってハードディスクを初期化した上で OS を再インストールし，最新のパッチをすべて適用した上でサーバ機を再構築した。納期が迫る中ではあったが，再構築したサーバの動作検証は順調に進み，開発課は無事に顧客への納品を済ませることができた。

〔インシデントからの反省〕

今回のボット感染のインシデント対応が一段落した後で，IRT はメンバ全員を集めて反省会を行った。その席で，IRT での対応に関する反省に加え，⑨従業員に対する周知，教育が不足していたために対応に問題が生じたのではないかとの意見があった。そこで，IRT は，全従業員向けのインシデント対応マニュアルを作成してインシデン

ト対応に関する周知，教育を図るという改善計画を，情報セキュリティ委員会に提出した。

IRT は改善計画に従ってインシデント対応マニュアルを作成するとともに，全従業員への周知，教育を行い，社内でのインシデント対応への取組みを強化することができた。

設問 1　〔インシデント対応計画の策定〕について，(1)～(3) に答えよ。

(1) 本文中の［ a ］，［ b ］に入れる適切な字句を，それぞれ 10 字以内で答えよ。

(2) 本文中の下線①について，“事前に作っておくこと”のメリットを，インシデントの原因究明の観点から，35 字以内で述べよ。

(3) 本文中の下線②について，X 社では更にどのようなインシデントを対象として追加すべきか。35 字以内で述べよ。

設問 2　〔IRT メンバ向けのインシデント対応マニュアルの整備〕について，(1)，(2) に答えよ。

(1) 本文中の下線③について，ログ管理のポリシに盛り込むべき具体的な内容を，25 字以内で述べよ。

(2) 本文中の下線④について，IRT では PGP を利用した電子署名を主にどのようなことを確認する目的で採用したと考えられるか。IRT の業務に即して 35 字以内で述べよ。

設問 3　〔IPS の運用〕について，(1)～(3) に答えよ。

(1) 本文中の［ c ］～［ e ］に入れる適切な字句を，それぞれ 15 字以内で答えよ。

(2) 本文中の下線⑤について，IPS が設置されておらず，かつ Web サーバでこのメソッドが受け付けられる設定になっている状態で図 6 の脅威が発生した場合には，Web サーバでどのような問題が発生する可能性が高いと考えられるか。30 字以内で述べよ。

(3) 本文中の下線⑥について，T 課長がシグネチャの設定を調整するように求めたセキュリティ上の理由を 40 字以内で述べよ。また，ある特定の脅威について危険度のレベルを既定値から下げることを許容する場合の条件を 35 字以内で述べよ。

設問4　〔インシデントの発生と対応〕について，(1)，(2)に答えよ。

(1) 本文中の下線⑦について，U君が電源を再投入しなかった理由を40字以内で述べよ。

(2) 本文中の下線⑧について，U君が取り出したハードディスクを直接用いて解析を行わなかった理由を35字以内で述べよ。

設問5　〔インシデントからの反省〕について，本文中の下線⑨の，周知，教育が不足していたために，ボット感染のインシデント対応において露呈したと考えられる問題を二つ挙げ，それぞれ35字以内で述べよ。また，それらの問題への対応として，全従業員向けインシデント対応マニュアルに記載すべき具体的な内容をそれぞれ35字以内で述べよ。