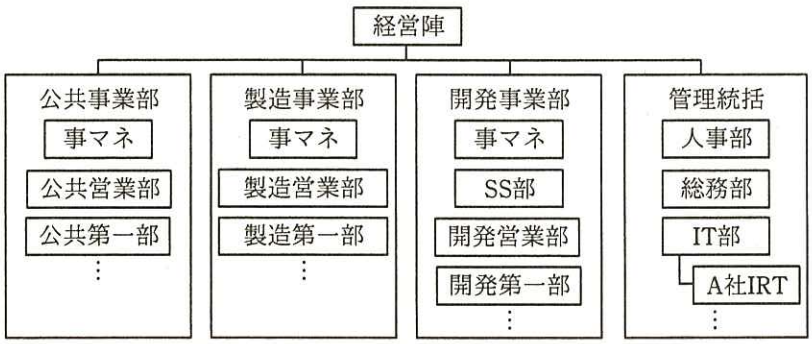
問1　CSIRT 構築とセキュリティ設計に関する次の記述を読んで，設問 1～6 に答えよ。

A 社は，従業員数 3,000 名の独立系ソフトウェア開発会社である。受託開発業務が中心であるが，一部の部署で展開しているサービス事業が拡大傾向にある。

〔A 社の組織〕

A 社には，公共事業部，製造事業部，開発事業部，管理統括の四つの組織がある。公共事業部と製造事業部は，それぞれの業種の顧客システムの開発が事業の中心である。開発事業部には，公共及び製造以外の業種の顧客システムの開発を行う部署と，A 社独自のサービス事業を行う部署とがある。後者のうち，ソリューションサービス部（以下，SS 部という）は，国内の人材をデータベース化し，顧客企業に紹介する Web サービス（以下，高度人材サービスという）を提供している。管理統括は，人事部，総務部，情報システム部（以下，IT 部という）などで構成される。

A 社では，各事業部に事業部マネジメント（以下，事マネという）という組織があり，事業部の実務的な意思決定を行っている。A 社の組織図を図 1 に示す。



注記　“A 社 IRT”は，A 社における CSIRT の呼称である。

図 1　A 社の組織図

〔A 社のセキュリティポリシ〕

A 社のセキュリティポリシでは，セキュリティインシデント（以下，インシデントという）発生時の対応を図 2 のように定めているが，どのような事象がインシデントに該当するかは定義されていない。インシデントの報告を受け付けた際の，A 社 IRT の運用手順の概要を表 1 に示す。

インシデントハンドリング
・A社で発生したインシデントは，A社IRTが対応を主導する。
・インシデント発生時の報告受付窓口を，A社IRTに設置する。
・従業員がインシデントを発見した場合には，必ずA社IRTに報告する。
・A社IRTはインシデント報告を受け付けると，情報セキュリティの専門的な知見を基に，定められた運用手順に従って活動し，該当する部署又は事マネに対して対応の指示を行う。個々の作業の記録を残し，報告の受付から完了までをインシデントごとに管理する。
コーディネーション
・A社IRTは，報告受付後，インシデント対応に関して社内外の組織と次のような連携を行う。
　-インシデントの発見者に情報提供などを依頼し，受け付けた内容の事実確認を行う。
　-インシデントの重要度やインシデント対策の必要性に応じて社外の専門家に調査を依頼する。
（以下，省略）

図2　セキュリティポリシ（抜粋）

表1　A社IRTの運用手順（概要）

番号	手順名	作業内容	次の手順の番号
1	報告の受付	A社IRTは，インシデントの発見者からインシデントの報告を受け付ける。	番号2に進む
2	トリアージ	A社IRTは，受け付けた内容の事実確認を行った上で，あらかじめ定めた基準に従い，重要度や優先度を考慮して，［　a　］を判断する。	［　a　］に応じて，番号3又は番号6に進む
3	調査依頼検討	A社IRTは，インシデントを調査し，あらかじめ定めた基準に従い，重大なインシデントであり，かつ，必要性が認められた場合は，社外の専門家に調査を依頼する。	番号4に進む
4	状況報告検討	A社IRTは，インシデントの対応内容を検討する。あらかじめ定めた基準に従い，重大なインシデントは経営陣に状況を報告し，必要に応じて経営陣に意思決定を依頼する。	番号5に進む
5	対応指示	A社IRTは，あらかじめ定めた基準に従い，インシデントの全社への影響度に基づいて，インシデントの対応内容を決定し，必要な対応指示を行う。また，対応状況を適宜確認する。	番号6に進む
6	完了	A社IRTは，当該インシデントに関する記録を整理し，対応を完了する。	なし

〔A社IRTの現状〕

IT部の部長をA社IRT責任者とし，IT部から選任した2名をA社IRT担当者とする計3名がA社IRTのメンバであるが，3名とも兼務である。A社の従業員に対して，A社IRTの存在を積極的には周知しておらず，A社IRTに報告すべきインシデ

ントの範囲についても明確には定義していない。

多くの従業員は，セキュリティポリシに規定されたA社IRTの機能を知らなかった上に，社内Webサイト上に，“マルウェア感染時の社内の連絡先”の表記があることから，A社IRTをマルウェア感染時の報告先だと認識していた。そのため，マルウェア感染以外のインシデントが事業部で発生した場合は，A社IRTではなく事マネに報告していた。事マネはA社IRTにインシデントを報告せず，事業部内で対応や判断を行っていた。

〔インシデント発生〕

ある日，高度人材サービスの管理者であるSS部のP主任が，見慣れないファイルが高度人材サービス用Webサーバ上にあることを発見した。P主任が，Webサーバのログを確認したところ，インターネットからサイバー攻撃を受け，攻撃者が不正にWebサーバにファイルをアップロードしていたことが分かった。しかし，攻撃者のその後のコマンドは全て失敗しており，実害はないと判断した。P主任は，A社IRTの存在を知っていたので，電子メール（以下，メールという）で状況を報告した。A社IRT担当者からの返事は数日を要した。P主任は，その後もA社IRT担当者と何度かメールでのやり取りを行ったが，他の業務の繁忙期であったので返信が滞り，さらに，A社IRT担当者からのフォローもなかったので，本件はうやむやとなった。

その数か月後，総務部の担当者宛てに，A社が出所と思われる，個人情報が含まれた名簿が出回っているとの問合せがあった。総務部の担当者が人事部に問い合わせたところ，数日後，“人事部が保有する情報ではない。どこかの事業部が作成した名簿ではないか”との回答があった。総務部の担当者は，その後も幾つかの部署に問い合わせてみたが，要領を得た回答が得られなかった。最終的には，IT部に相談した際にA社IRTを紹介され，A社IRTに名簿を確認してもらうことになった。A社IRT担当者は，名簿の内容から高度人材サービスに関するものと推測し，IT部の業務の合間にP主任にメールで問い合わせたところ，確かに高度人材サービス固有の情報を含む名簿であることが分かった。A社IRT担当者が，P主任と協力して調査を進めた結果，数か月前に高度人材サービスにサイバー攻撃があった時に，名簿情報が不正に持ち出された可能性があることが分かった。A社IRT責任者は経営陣に状況を報告した。調査に時間を要したので，総務部の担当者が連絡を受けてから2か

月が経過していた。経営陣は，漏えいした名簿に個人情報が含まれている各人に，おわびと，その時点までに確認された状況の説明を郵送でするよう指示を出した。

この事件はマスコミが大々的に採り上げ，A 社の情報セキュリティの組織的な取組みのまずさや情報公開の遅さが批判された。A 社の顧客や株主からの問合せは，経営陣の想定以上のものがあり，結果的に社長による謝罪会見にまで発展した。本業である受託ソフトウェア開発事業への影響も大きく，経営的にも極めて大きな打撃を受ける結果となった。経営陣は，A 社のインシデント対応には重大な問題があると考えた。

〔A 社 IRT の活動のアセスメントと改善〕

A 社の経営陣は，社外のセキュリティコンサルタント会社の T 社に，A 社のインシデント対応の現状のアセスメントを依頼し，問題点を洗い出してもらうことにした。T 社は，A 社内の様々な関係者へのヒアリングや，過去のインシデント対応の記録の調査，運用手順などのアセスメントを実施し，結果を報告書にまとめた。報告書には，A 社には多くの問題点が存在すること，及びその中で最も重要度が高い問題点は表 2 に示す A 社 IRT に関する問題点であることが明記されていた。

表 2　A 社 IRT に関する問題点（抜粋）

分類	問題点
人員	・A 社 IRT 責任者は，情報セキュリティに関する知識や経験が不足している。 ・A 社 IRT 担当者は，A 社 IRT 以外の業務が恒常的に忙しく，運用手順に従った対応ができていない。
(省略)	b が不明確である。
周知	A 社 IRT の存在と機能が A 社内に十分には周知されていない。
対応指示手順	表 1 の運用手順における“対応指示”手順と異なり，現状はインシデントを発見した事業部が独自に影響度を判断し，事業部の都合を優先させた対応を行っている。A 社 IRT は対応を記録すること，及び対応の完了を確認することしかしていない。

T 社は，現状の A 社 IRT の人員では，A 社 IRT の機能を適切に遂行することに無理があるので，A 社 IRT の人員を見直すよう経営陣に提言した。また，その他の問題点についてもそれぞれ改善策を提言した。

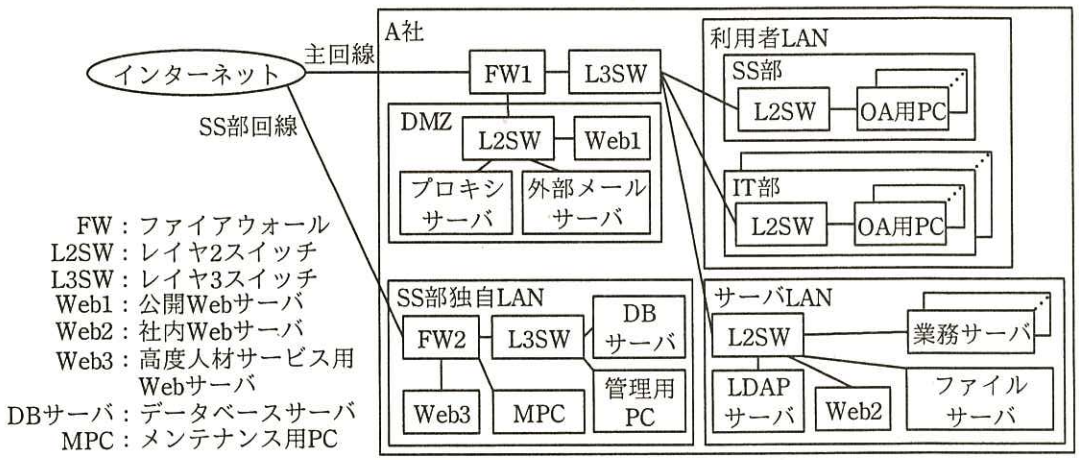
経営陣は，T 社の提言に従い，優先度が高い幾つかの改善策を実行することにした。

最初に，A 社 IRT を IT 部から独立させて経営陣直属の組織とし，A 社 IRT 責任者には，経営陣の中から情報セキュリティに知見がある者を就任させた。また，①表 1 における対応指示は，A 社 IRT が直接行えるようにした。

次に，A 社 IRT 担当者には，情報セキュリティスペシャリスト資格をもつ，ベテランの U 課長と，その部下である Y さんを割り当て，専任とした。U 課長は，［ b ］の明確化や周知の改善などを行い，表 2 の問題点への対策を完了した。さらに，経営陣は，従業員の情報セキュリティの意識改革についても積極的に取り組み，A 社は，インシデント対応を適切に遂行できる組織となった。

〔A 社のネットワーク構成〕

A 社では，OA 用 PC，ネットワーク機器，サーバ，OS，ミドルウェア，アプリケーション（以下，情報機器という）を IT 部が管理している。また，それとは別に各部署が独自に管理する情報機器もある。ネットワークは，全て固定された IP アドレスで運用されている。各部署が独自にインターネット回線や情報機器を調達する際は，IT 部に届け出るルールになっている。その際，IT 部から，A 社に導入実績があるシステム構成を紹介されるケースが多いので，同一ベンダのサーバやミドルウェアが A 社では多く採用されている。A 社のネットワーク構成を図 3 に，情報機器の概要を表 3 に示す。



注記　FW1 と FW2 は同一ベンダのアプライアンスである。

図 3　A 社のネットワーク構成（抜粋）

表3　情報機器の概要（抜粋）

名称	概要
OA用PC	・各従業員に1台ずつ貸与され，資料作成，Web閲覧，メール送受信などに利用される。 ・次の認証情報でログインする。 PC ID：数字6桁で構成された，PCを識別する固有の番号である。 パスワード：OA用PCが従業員に貸与された後，初期パスワードを従業員自らが変更する。
LDAPサーバ	・A社従業員の次の認証情報などを保管し，様々なシステムからのLDAPクエリに応答する。 LDAP ID：8桁の英数字で構成された従業員IDであり，A社の各従業員に付与されている。 パスワード：LDAP IDを従業員に通知後，初期パスワードを従業員自らが変更する。 ・IT部の運用チームが管理を行う。HTTPでアクセスできる管理画面があり，運用チーム4名のLDAP IDでだけログインできる。
FW1	・IT部が管理する。一部の運用保守作業は外部業者に委託している。例えば，ポリシ変更の際は，IT部が外部業者に指示を出し，外部業者の担当者が遠隔地からインターネットを経由し，SSHクライアントソフトを用いて更新作業を行っている。
FW2	・SS部が管理する。ポリシ変更は，FW2のコンソールポートに常時接続されたMPCからだけ許可されている。SS部の担当者がMPCにログインし，SSHクライアントソフトを用いて更新作業を行っている。
MPC	・FW2を管理する専用のPCである。普段はOSの認証機能によってロックされており，SS部の一部の担当者だけがロック解除できる。

〔A社のシステム運用〕

IT部では，外部業者に委託している一部の運用保守を除き，DMZやサーバLANのサーバなどのIT部が管理している情報機器の運用保守は，IT部のOA用PCから実施している。例えば，LDAPサーバの場合は，OA用PCからHTTPで管理画面にアクセスし，運用チームのメンバに付与されたLDAP IDでログインした後，管理者昇格コマンドと管理者パスワードを入力すると，IT部の運用チームだけに与えられている管理者権限が付与され，LDAP IDの追加，削除などを行うことができる。

IT部以外の部署が管理する情報機器は，各部署のルールで管理しており，LDAPサーバとは連携していない。

〔マルウェア感染〕

A社IRTの再発足から半年たったある日，IT部からA社IRTに，LDAPサーバの

ログに大量のサーバログイン失敗が記録されているとの報告が入った。システム障害の原因調査中に，偶然発見したものであった。U課長が，運用手順に従って事実を確認したところ，サイバー攻撃の可能性が高いことが分かり，セキュリティ専門業者のR社に調査を依頼した。

R社が調査した結果，標的型攻撃メールを発端としたサイバー攻撃であることが確認された。この攻撃には，A社で利用しているマルウェア対策ソフトでは検出できないマルウェアが使用されていた。図4は調査によって明らかになった攻撃の概要である。

・攻撃者がマルウェアを添付した攻撃メールをSS部のZ主任に送信した。Z主任が添付ファイルを開いたことによってマルウェアが起動された。
・マルウェアは，Z主任のOA用PC内の認証情報を取得してプロキシサーバを突破し，攻撃者が準備したサーバ（以下，Kサーバという）にアクセスして新たなマルウェアをダウンロードした。このマルウェアによって，Z主任のOA用PCは攻撃者による遠隔操作が可能になった。
・攻撃者は，Z主任のOA用PC上のメールフォルダやネットワークに関する情報を探索し，A社のネットワーク構成情報などを取得した。
・攻撃者は，Z主任のOA用PCから，他の複数のOA用PCをマルウェアに感染させた。
・攻撃者は，Z主任のLDAP ID，及びマルウェアによって不正に取得した複数のLDAP IDの認証情報を用いて，サーバLANの各サーバにアクセスを試み，ファイルサーバの一部のフォルダへのアクセスに成功した。その後，複数のLDAP IDの認証情報を用いて，LDAPサーバの管理画面からのログインを試みたが，いずれも失敗した。
・攻撃者は，IT部の運用チームメンバのLDAP IDを入手し，当該LDAP IDのパスワードを入手するためにLDAPサーバの管理画面でブルートフォース攻撃を行ったが，全て失敗した。
・ブルートフォース攻撃の失敗以降は，攻撃者による遠隔操作は記録されていない。

図4　攻撃の概要

A社IRTは，R社からの報告を受け，Kサーバへの通信の遮断に加え，マルウェアの駆除などの暫定処置を行った。A社IRTは社内外との連携も含め，運用手順どおりにインシデント対応を行った。

〔セキュリティ設計の見直し〕

経営陣は，今回の攻撃に対するA社IRTのインシデント対応には一定の評価を与えたが，A社内のシステムのセキュリティ設計には改善すべき点が多いと考えた。そこで，以前，アセスメントを実施したT社の提言に含まれていたものの，未対応で

あった“マルウェア感染を前提としたシステムのセキュリティ設計の見直し”を U 課長に指示した。U 課長から指示を受けた Y さんは，対策案を表 4 のようにまとめた。

表 4　対策案（抜粋）

分類	対策案
マルウェア感染の拡大や，攻撃者による内部探索，内部侵入を困難にするための対策	対策(1-1) 運用管理セグメントの新設 対策(1-2) パスワードの複雑さに関するポリシの導入 対策(1-3) サーバでのアカウントロック機能の有効化 対策(1-4) 添付ファイル付きメールの送信元が社外であるかどうかの識別性向上施策の導入
マルウェア感染の拡大や，攻撃者による内部探索，内部侵入を早期に検知するための対策	対策(2-1) サーバでのブルートフォース攻撃の検知 対策(2-2) FW1 でのマルウェア通信の検知

Y さんは，各対策案について，IT 部やその他の関係する各部署と調整しながら検討を進めることにした。次は，Y さんが対策(1-1)を IT 部の H さんに説明した時の会話である。

Y さん：運用管理セグメントの新設の検討をお願いします。運用管理セグメントとは，サーバ LAN 上のサーバを管理するために使用する PC（以下，運用管理 PC という）を設置するセグメントであり，SSH などの特定の管理用ポートを用いて，運用管理 PC からサーバ LAN の各サーバにアクセスします。利用者 LAN からサーバ LAN へのアクセスについては，管理用ポートへのアクセスを禁止し，他の PC から運用管理 PC へのアクセスも禁止します。

H さん：現状でもサーバ LAN の各サーバの管理用ポートへのアクセスは，利用者 LAN の IT 部のセグメントからしか許可を与えておらず，実質的には，運用管理セグメントを新設することと同等のセキュリティが既に備わっているので，運用管理セグメントの設置は不要だと思います。

これを Y さんが U 課長に報告したところ，U 課長は，②運用管理セグメントを新設することによって，現状では防ぐことができない攻撃に対処できるようになることを Y さんに説明し，対策(1-1)の趣旨を IT 部に改めて正しく伝えるように指示した。

次は，対策(2-1)に関するYさんとU課長の会話である。

Yさん：対策(2-1)についてですが，LDAPサーバにログインするための，パスワードに対するブルートフォース攻撃を検知するために，同一のLDAP IDによる連続した認証失敗回数をカウントし，その回数が一定値を超過すると，アラートを発生させる仕組みを考えています。

U課長：今回の攻撃はブルートフォース攻撃であったが，次に攻撃を受けるときは，リバースブルートフォース攻撃を受けるかもしれない。リバースブルートフォース攻撃についても検知できる仕組みが必要だな。

Yさん：ご指摘も踏まえ，更に検討を進めます。

Yさんはその後，連続した認証失敗回数をカウントして攻撃を検知する方法に加え，リバースブルートフォース攻撃も検知できるよう，A社のLDAPサーバの運用管理を考慮した③新たな検知方法を考えた。

A社IRTは各部署との調整を進め，対策計画案を作成した。対策計画案は経営陣の承認の上，実行されることになった。

〔脆弱(ぜい)性情報ハンドリング〕

IT部は，IT部が管理する情報機器の脆弱性情報を，インターネット上にあるベンダのWebサイトや，脆弱性情報が記載されたWebサイトなどから収集している。脆弱性修正プログラムは，重要度に応じて適宜適用している。一方，各部署が独自に管理する情報機器の脆弱性情報の収集や脆弱性修正プログラムの適用は，部署ごとに対応が異なっており，多忙なときは，漏れてしまったり，遅くなってしまったりするケースもある。

最近，A社では，各部署が独自に管理する情報機器の脆弱性修正プログラムの適用漏れに起因するインシデントが増加傾向にあった。U課長は，A社IRTが各部署の脆弱性管理を支援すること（以下，脆弱性情報ハンドリングという）によって，この状況を改善できると考えた。具体的には，次のようにする。

・SS 部独自 LAN など，部署独自 LAN の管理を各部署だけに任せるのではなく，A 社 IRT が，各部署の重要な脆弱性修正プログラムの適用状況を把握する。
・A 社が保有する情報機器の脆弱性情報を A 社 IRT が収集し，各部署に発信することによって，各部署が脆弱性情報を収集する負担を低減し，A 社全体で効率化する。

U 課長は，A 社 IRT に“脆弱性情報ハンドリング”機能をもたせるための，現状の課題は図 5 の 3 点であると分析した。

課題 1：情報機器の現状の構成情報を正しく把握していない部署がある。
課題 2：情報機器の脆弱性情報を，ベンダの Web サイトや，脆弱性情報が記載された Web サイトから収集するには多くの工数が必要だが，現状の要員では対応ができない。
課題 3：収集した脆弱性情報に，各部署がどのように重要度や影響度を勘案して対応すべきかについて，A 社としての指針が存在しない。

図 5　現状の課題

課題 1 については，短期的な対応は困難なので，当面はこれまでに各部署が作成した情報資産台帳を入手することにした。長期的には，各部署の構成管理情報を自動的に収集する仕組みを導入し，A 社 IRT が各部署の構成管理情報を把握することを目指す。

課題 2 については，長期的には A 社 IRT を増員することによって対応する。短期的には増員せず，④A 社の各部署の取組みと連携して対応することによって，工数の発生を最小限に抑える。

課題 3 については，汎用的で定量的な評価手法を用いた共通脆弱性評価システムのバージョン 3（以下，CVSS という）を参考にする。CVSS は，三つの基準で脆弱性を評価する手法である。一つ目は“基本評価基準”であり，機密性などのセキュリティの特性や，ネットワークから攻撃が可能かといった攻撃元の特性からスコアを算出する。この基準は，時間の経過や環境の違いによるスコアの変化はない。どこから攻撃可能であるかを評価する攻撃元区分を表 5 に示す。

表5　攻撃元区分

区分名	説明
ネットワーク	対象コンポーネントをネットワーク経由でリモートから攻撃可能である。 例えば，インターネットからの攻撃など
隣接	対象コンポーネントを隣接ネットワークから攻撃する必要がある。 例えば，ローカル IP サブネット，ブルートゥース，IEEE 802.11 など
ローカル	対象コンポーネントをローカル環境から攻撃する必要がある。 例えば，ローカルアクセス権限での攻撃が必要，ワープロのアプリケーションに不正なファイルを読み込ませる攻撃が必要など
物理	対象コンポーネントを物理アクセス環境から攻撃する必要がある。 例えば，IEEE 1394，USB 経由で攻撃が必要など

出典：独立行政法人情報処理推進機構 共通脆弱性評価システム CVSS v3 概説 2.1.1.攻撃元区分（AV: Attack Vector）から引用
（URL：https://www.ipa.go.jp/security/vuln/CVSSv3.html（平成 28 年 3 月 8 日アクセス））

二つ目は“現状評価基準”であり，攻撃コードの出現有無や対策情報が利用可能であるかどうかを基にした評価基準である。ベンダなどの脆弱性への対策状況に応じ，時間の経過によって変化し，脆弱性を公表する組織が，脆弱性の現状を表すために評価する基準である。

三つ目は“環境評価基準”であり，ネットワーク環境やセキュリティ対策状況を含め，攻撃元区分の再評価などによって，組織にとっての最終的な脆弱性の深刻度を評価する基準である。

基本評価基準のスコアは脆弱性ごとに定まるが，環境評価基準は脆弱性が存在する情報機器ごとにスコアが異なる。例えば，図 3 の FW1 と FW2 に関する，ある脆弱性が公表された場合，この脆弱性の基本評価基準のスコアに対して，評価時点の現状評価基準のスコアを算出し，最後に，環境評価基準として，FW1 と FW2 のそれぞれで最終的な深刻度のスコアを算出する。U 課長は実際に，FW1 と FW2 に存在する，ある脆弱性の深刻度を算出してみた。この脆弱性は，FW のポリシ更新のコマンド発行において，特定のパラメタを組み合わせると管理者権限がなくても不正にポリシを更新できるというものである。環境評価基準において，FW1 の攻撃元区分は［ c ］であり，FW2 の攻撃元区分は［ d ］であることから，［ e ］のスコアがより高い値を示した。

A 社 IRT が各部署に発信する脆弱性情報について，該当する情報機器を保有していた場合には，各部署で深刻度を算出してもらい，一定値を超えた場合は，A 社 IRT

に脆弱性の対応計画を提出する仕組みにする。

U 課長の脆弱性情報ハンドリングに関する提案は，A 社 IRT 責任者及び経営陣によって承認され，A 社 IRT は，A 社全体の情報セキュリティを担う，より高度な組織となった。

設問 1　表 1 中の［ a ］に入れる，A 社 IRT が決定すべきことを，10 字以内で答えよ。

設問 2　〔A 社 IRT の活動のアセスメントと改善〕について，(1)，(2)に答えよ。

(1)　表 2 中及び本文中の［ b ］に入れる適切な字句を，〔A 社 IRT の現状〕の内容を踏まえ，20 字以内で答えよ。

(2)　本文中の下線①について，この改善策の目的は何か。40 字以内で述べよ。

設問 3　〔セキュリティ設計の見直し〕について，(1)，(2)に答えよ。

(1)　本文中の下線②について，どのような攻撃に対処できるようになるか。攻撃のシナリオを 70 字以内で具体的に述べよ。

(2)　本文中の下線③について，どのような検知方法か。40 字以内で具体的に述べよ。

設問 4　図 5 中の課題 1 について，(1)，(2)に答えよ。

(1)　A 社 IRT の脆弱性情報ハンドリングにおいて，各部署の情報機器の現状が示された構成管理情報を活用することによる効果を，35 字以内で述べよ。

(2)　A 社 IRT が各部署の構成管理情報を把握しておくと，インシデントハンドリングにおいても有効に活用することができる。どのように活用できるか。45 字以内で具体的に述べよ。

設問 5　図 5 中の課題 2 について，本文中の下線④の各部署の取組みとどのように連携して対応すべきか。連携方法を 30 字以内で述べよ。

設問 6　図 5 中の課題 3 について，(1)，(2)に答えよ。

(1)　CVSS について，ゼロデイ攻撃が可能な脆弱性か否かは，どの評価基準に最も反映されるか。基準名を答えよ。

(2)　本文中の［ c ］～［ e ］に入れる適切な字句を答えよ。［ c ］，［ d ］は表 5 中の区分名から選び，［ e ］は“FW1”又は“FW2”のどちらかで答えよ。