SC

平成28年度　春期
情報セキュリティスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

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2
選択方法	1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。2問とも○印で囲んだ場合は，はじめの1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2を選択した場合の例〕

選択欄	
1問選択	問1
	(問2)

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。

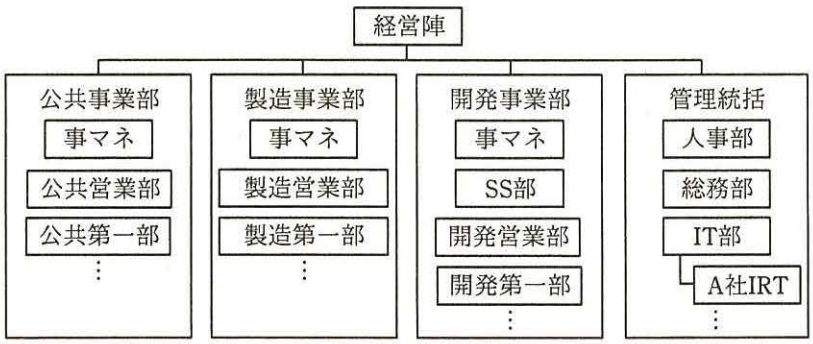
問1　CSIRT 構築とセキュリティ設計に関する次の記述を読んで，設問 1～6 に答えよ。

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。

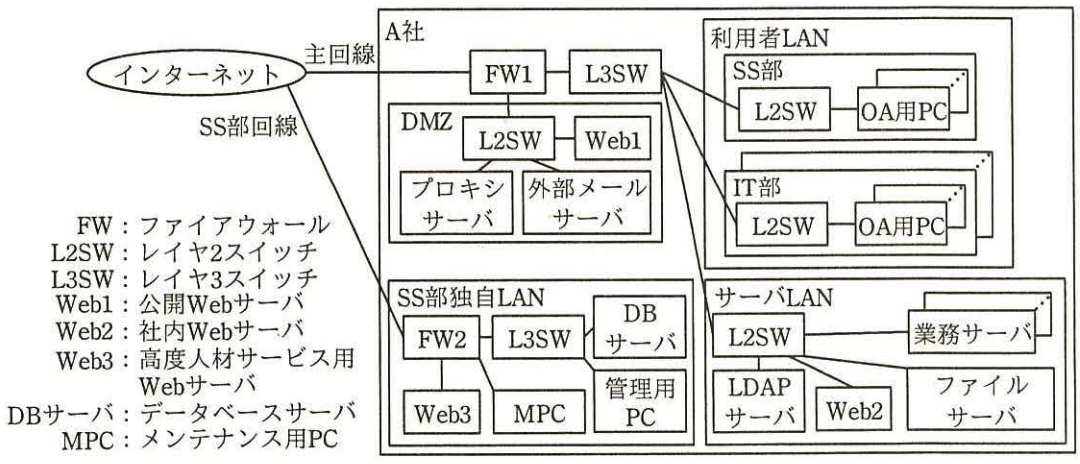
経営陣は，T 社の提言に従い，優先度が高い幾つかの改善策を実行することにした。

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。

問2　テレワークのセキュリティに関する次の記述を読んで，設問1～5に答えよ。

Q社は，従業員数700名のシステムインテグレータである。東京，名古屋及び大阪に事業所がある。各事業所では，固定席をもたないフリーアドレスが採用されている。営業員やシステムエンジニアなど，テレワークを行っている社員はモバイラと呼ばれ，モバイルPCとUSBデータ通信端末が貸与されている。モバイラは，休暇や長期出張などの場合を除き，週1時間以上Q社事業所に出社し，モバイルPCを社内LANに接続することが義務付けられている。

Q社では，モバイルPCを含むIT機器全てを情報システム部（以下，IT部という）が管理している。Q社には，IT全般に関する問合せ窓口としてIT部内にITヘルプデスクが設けられており，電話，電子メール（以下，メールという），チャットでサポートを行っている。ITヘルプデスクは情報セキュリティに関する問合せも受け付けている。

〔モバイラのテレワーク環境〕

Q社では，モバイラの顧客先などでのテレワークを支援するために，表1に示すクラウドコンピューティングで実現されたサービス（以下，クラウドサービスという）を利用させている。クラウドサービス利用に関するQ社のセキュリティガイドラインを図1に示す。

表1　Q社が利用させているクラウドサービス

サービス	機能概要
H社Webメール	メール，SPAMフィルタ及びマルウェア対策の機能を提供する。
J社セキュアプロキシ（以下，Jプロキシという）	利用者認証付きのHTTPプロキシ機能，URLフィルタ機能，及びHTTPリクエストヘッダの文字列検査によるフィルタ（以下，RHフィルタという）機能を提供する。RHフィルタ機能では，正規表現を使用することができる。利用者認証の有効期間は24時間である。
N社コラボレーションツール（以下，Nコラボという）	ファイル共有，掲示板，チャットなどの機能を提供する。各利用者に5Gバイトのファイル保管領域が割り当てられている。利用者がきめ細かなアクセス制御を設定可能である。
P社CRMツール	顧客企業情報管理，案件情報管理などの機能を提供する。

1. ユーザインタフェース上で無操作状態が 5 分以上続いた場合は，自動的にログオフされるよう設定する。
2. 利用者認証が連続して 3 回失敗した場合は，アカウントがロックされるよう設定する。
3. Q 社貸与のモバイル PC 及び社内 LAN からの，HTTP 及び HTTP over TLS（以下，HTTPS という）によるアクセスだけを許可するよう設定する。

図 1　クラウドサービス利用に関する Q 社のセキュリティガイドライン（抜粋）

Q 社のモバイル PC には，マルウェア対策ソフト（以下，AM という）やパーソナルファイアウォール（以下，PFW という），オフィスソフトウェアなどの Q 社が利用を認めたソフトウェア（以下，標準ソフトという）がインストールされている。

Q 社内には，AM 管理サーバがあり，社内 LAN だけからアクセス可能である。モバイル PC は，社内 LAN 接続時に，AM のログを AM 管理サーバにアップロードする。

Q 社のモバイル PC の概要を表 2 に，Q 社のモバイル PC に導入されている PFW の概要を図 2 に示す。

表 2　Q 社のモバイル PC の概要

項目	概要
利用者 ID	利用者は，ローカルユーザの利用者 ID 及び 8 桁以上のパスワードを使用する。各利用者 ID には当該モバイル PC の OS の管理者権限が与えられている。
プロキシ	プロキシ自動設定機能によって，インターネット上の Web サイトへのアクセスは自動的に J プロキシを利用するよう設定されている。
可搬記憶媒体	可搬記憶媒体を利用する場合，媒体上のデータが自動的に暗号化される。
ハードディスク暗号化	ハードディスク全体が暗号化されている。パワーオン時には，OS 起動前にパスワードの入力を求めるプログラムが立ち上がり，認証を行う。認証が成功すると，ハードディスクへの書込み時の暗号化と読出し時の復号を透過的に行うようになり，その後 OS を起動する。OS からは，ハードディスク内にデータが平文で格納されているかのようにアクセスできる。
AM	ファイルの書込み時，読出し時及び実行時にパターンマッチングによるマルウェアスキャンを行う。マルウェアの検知時には，ポップアップを表示し，マルウェア名と対処内容（検知だけ，隔離，駆除済み）を表示するとともに，ログに記録する。マルウェア定義ファイルは，インターネット上の専用サイト（以下，AM サイトという）から自動的にダウンロードされ，更新される。
脆弱(ぜい)性修正プログラム（以下，修正パッチという）	OS の修正パッチは，インターネット上のベンダサイトから自動的にダウンロードされ，適用される。

・次の通信だけを許可する。
　- J プロキシを介した HTTP 通信及び HTTPS 通信
　- PFW 管理サーバ，AM 管理サーバ及び AM サイトへの通信
　- インターネット上のベンダサイトへの OS の修正パッチダウンロード用の通信
　- DHCP 通信，DNS 通信及び NTP 通信
・次のログを記録し，モバイル PC が社内 LAN に接続されたときに，Q 社内に設置されている PFW 管理サーバにアップロードする。
　- モバイル PC 外との許可された通信の場合，通信したプロセスの実行ファイル名，通信先 IP アドレス，通信先ポート番号，自ポート番号及び通信開始時刻
　- モバイル PC 外への許可されていない通信の場合，通信を開始したプロセスの実行ファイル名，通信先 IP アドレス，通信先ポート番号，自ポート番号及び通信開始時刻（アラートを PC 画面上にも表示する。）
　- モバイル PC 外からの許可されていない通信の場合，通信元 IP アドレス，通信元ポート番号，通信先ポート番号及び通信開始時刻
・上記通信許可及びログの記録に関する設定を含むポリシは，PFW 管理サーバ上にあり，それが更新された後，初めてモバイル PC が社内 LAN に接続されたときに，ダウンロードされ，適用される。

図 2　Q 社のモバイル PC に導入されている PFW の概要

Q 社には，モバイル PC のバックアップを自動的に取得する仕組みはない。そのため，必要なファイルは N コラボに保管しておくことが推奨されている。

〔マルウェアの検知〕

Q 社では，マルウェア検知時の対応手順を，図 3 のとおり定めている。

1. マルウェア定義ファイルを最新にした後，PC をネットワークから切り離す。
2. 当該 PC 上で AM のフルスキャンを実行する。
3. フルスキャンでマルウェアが検知された場合，IT ヘルプデスクに報告し，判断を仰ぐ。検知されなかった場合，継続利用してよい。

図 3　マルウェア検知時の対応手順

2 月 1 日，名古屋事業所の B さんから IT ヘルプデスクに“モバイル PC で繰り返しマルウェアが検知される”との連絡が入り，IT 部の情報セキュリティ担当者である C さんが対応した。次は，その時の B さんと C さんの会話である。

B さん：私のモバイル PC で，先週 1 週間に 3 回も同じマルウェア M が検知されました。毎回“駆除済み”と表示されるのですが，駆除できていないのでし

ようか。

C さん：マルウェア検知時の対応手順に従って AM のフルスキャンをしましたか。

B さん：はい。もちろんです。3 回とも実施しましたが，何も検知されませんでした。

C さん：問題ないと思いますが，念のため IT 部で調査します。モバイル PC のホスト名と最後に社内 LAN に接続した日を教えてください。

B さん：ホスト名は PC01 です。今日も，社内 LAN に接続しています。

〔IT 部による調査〕

C さんが AM 管理サーバのマルウェア検知ログを調べたところ，PC01 ではマルウェア M が 3 回検知され，駆除されていた。他のマルウェアは検知されていなかった。

次に，C さんは PFW 管理サーバで，マルウェア検知と同じ時間帯の，PC01 の PFW のログを確認した。PFW のログには，OS 標準の Web ブラウザ（以下，標準ブラウザという）のプロセスからの通信だけが記録されていた。

C さんが，マルウェア検知と同じ時間帯の J プロキシのログを調査したところ，次のことが分かった。

・マルウェア検知の直前に 3 回とも同じ URL にアクセスし，同じ長さのコンテンツがダウンロードされていた。
・当該 URL への HTTP 通信は，HTTP リクエストヘッダの User-Agent（以下，UA という）が標準ブラウザとは異なっていた。
・HTTP リクエストヘッダには，UA と Host だけが設定されていた。

該当するログは表 3 のとおりである。

表3　Jプロキシの該当ログ

Time	CIP	User	RM	URL	SC	CCL	SCL	UA	Ref
2016-01-25 09:13:29 +0900	xx.xx.13.1	user01	GET	http://yy.yy.yy.yy/?v1 =（省略）	200	-	218783	DL2	-
2016-01-27 09:23:34 +0900	10.10.2.101	user01	GET	http://yy.yy.yy.yy/?v1 =（省略）	200	-	218783	DL2	-
2016-01-28 09:12:27 +0900	xx.xx.13.1	user01	GET	http://yy.yy.yy.yy/?v1 =（省略）	200	-	218783	DL2	-

Time：処理終了時刻，CIP：クライアント IP アドレス，User：認証利用者 ID，RM：HTTP リクエストメソッド
SC：HTTP ステータスコード，CCL：クライアントからのリクエストのコンテンツ長
SCL：サーバからのレスポンスのコンテンツ長，Ref：Referer
注記1　“user01”は B さんの認証利用者 ID を示す。
注記2　“xx.xx.13.1”は USB データ通信端末利用時の IP アドレスを，“10.10.2.101”は Q 社の IP アドレスを，“yy.yy.yy.yy”は C&C サーバの IP アドレスを示す。

C さんは，マルウェア M をダウンロードする未知のマルウェアが，UA を DL2 に設定して C&C サーバと通信していると考えた。J プロキシのログから UA が DL2 の通信を検索したところ，次のことが分かった。

・アクセス先 URL は異なるものの，PC01 は，1 月 25 日以降ほぼ毎日 UA が DL2 の通信を行っていた。
・他に PC02～PC04 の 3 台のモバイル PC が，UA が DL2 の通信を行っていた。
・調査日当日も PC01 から UA が DL2 の通信があり，“200 OK”が返っていた。
・①当該アクセス先 URL に，C さんに貸与されている PC の標準ブラウザからアクセスしたところ，“404 Not Found”が返ってきた。

C さんは，これらのログの調査から，B さんのモバイル PC でマルウェアの検知・駆除が繰り返される事象は，未知のマルウェアが原因だと結論付けた。

C さんは，②当該マルウェアによるモバイル PC から C&C サーバへの通信をブロックする必要があることと，PC01 について専門業者による詳細な調査の必要があることを IT 部 D 部長に説明し，調査依頼の承認を得た。

C さんは，C&C サーバへの通信のブロックを担当者に依頼した。次に，C さんは，PC01～PC04 について，利用者に連絡を取り，IT 部への送付を依頼した。B さんを含む各利用者は，当該モバイル PC を IT 部に送付した。

〔専門業者による調査〕

C さんは，PC01 の調査をセキュリティ専門業者の X 社に依頼した。X 社による調査結果は図 4 のとおりであった。

・PC01 の一時ディレクトリに不審なファイル 5 個と削除済みの不審なファイル 13 個があった。
・不審なファイル 5 個のうち，2 個はマルウェア本体，他の 3 個はマルウェアが利用する一時ファイルであった。
・削除済みの不審なファイル 13 個のうち，少なくとも 4 個は実行可能コードを含んでおり，マルウェアの一部であった。また，他の 3 個は先頭部分に圧縮ファイルを示す文字列が含まれていたが，ファイルが不完全であったので展開できなかった。残りの 6 個は詳細が判明しなかった。
・活動している未知のマルウェアのプロセスを解析した結果，その実行ファイルは標準ブラウザであった。標準ブラウザに対し，［ a ］インジェクション攻撃が行われ，不正なコードが呼び出されて実行されていた。この不正なコードを含むファイルは，システムディレクトリにあった。
・当該マルウェアは，改ざんされたバナー広告の表示によって感染が起きるマルウェアの亜種であった。

図 4　X 社による調査結果（抜粋）

〔侵入経路と被害状況の調査〕

X 社の報告を受け，C さんはマルウェアの侵入経路及び外部への情報漏えいの有無を調査した。侵入経路については，Web サイト W からマルウェアをダウンロードしていたことが判明した。Web サイト W で表示していたバナー広告が改ざんされており，当該バナー広告を表示するときに利用するビューア（以下，ビューア V という）の脆弱性を利用して，自動的にダウンローダを導入・実行する攻撃コードが含まれていた。いわゆる［ b ］ダウンロード攻撃であった。ビューア V は以前に業務上必要があったので標準ソフトとして導入されていたが，現在では必要性はなくなっていた。ビューア V の脆弱性は度々報告されていたが，Q 社では標準ソフトの脆弱性を管理しておらず，修正パッチの適用も強制していなかった。

PC02～PC04 も，B さんと同様に利用者が Web サイト W にアクセスしたことによって感染していた。

外部への情報漏えいの有無については，各種ログやハードディスクに残されていたファイルの痕跡からは，判断できなかった。PC01～PC04 のうち，PC01 だけは，お客様プロジェクト関連情報（以下，PJ 情報という）を含むファイルがハードディ

スク上に複数保管されており，いずれも圧縮状態で 200 k バイト以上であった。一方，J プロキシのログは，PC01 から外部に送信された HTTP 通信の CCL が，全て 2 k バイト未満であることを示していた。これらから，C さんは，外部への PJ 情報の漏えいはないと結論付け，調査結果を D 部長に報告した。

次は，調査結果についての C さんと D 部長の会話である。

D 部長：この分析結果から PJ 情報の漏えいがないと判断するのは無理があります。

C さん：なぜですか。

D 部長：まず，PC01 についてですが，マルウェアが PJ 情報の入ったファイルを［ c ］して送信した可能性があります。また，PC01 のハードディスクではなく，［ d ］や［ e ］に格納されていた PJ 情報が窃取された可能性もあります。

C さん：確かにそうですね。再度調査します。

C さんは，再度調査を行ったが，PJ 情報漏えいの痕跡は発見できなかった。C さんはそのことを D 部長に報告した。D 部長は調査結果を了承した。

C さんはこの調査結果を，B さん及び PC02～PC04 の利用者に伝えた。

〔委託元への報告〕

B さんは，名古屋に本社がある流通業 E 社の業務システム開発プロジェクトに参画している。E 社との契約では，情報漏えいなどのセキュリティインシデント発生時には遅滞なく E 社に報告することが定められている。E 社では，業務システムのプログラム開発及びテストには専用の PC を貸与している。B さんは，設計書を含む文書作成は PC01 で行い，プログラム開発及びテストは E 社から貸与された PC で行っていた。

IT 部での調査結果を基に，今回の件では PJ 情報の漏えいはなかったというのが Q 社の見解であるが，営業部，IT 部，法務部及び名古屋事業所の F 部長が協議した結果，IT 部の調査結果を基に E 社に報告することにした。

3 月 28 日，F 部長が E 社に報告したところ，E 社の G 部長から非常に厳しい叱責を受けた。G 部長の見解は図 5 のとおりである。

・マルウェア感染は報告すべきセキュリティインシデントである。
・業務システムの設計書が外部に漏れると，事業上多大な影響がある。
・発生後すぐにセキュリティインシデント報告をすべきであった。
・Q 社内の調査だけで情報漏えいはなかったと結論付けているが信用できない。
・B さんのモバイル PC から E 社に提出又は送信した文書ファイルによって，E 社のシステムがマルウェアに感染した可能性もある。

図 5　E 社 G 部長の見解（抜粋）

F 部長は，営業部，IT 部及び法務部と相談し，図 6 の対応方針をまとめ，早急に対応を進めた。

・次の追加調査を X 社に依頼する。
　- 情報漏えいの痕跡
　- B さんから E 社宛てに送信したメールの添付ファイル
　- B さんが E 社に提出又は送信した文書ファイル
・今回のマルウェア感染に対する再発防止策を策定する。
・上記の調査結果と再発防止策を F 部長から E 社 G 部長に説明する。

図 6　対応方針（抜粋）

X 社の追加調査の結果は，Q 社内での調査と同様，情報漏えいの痕跡は認められないというものであった。また，B さんから E 社宛てに送信したメールの添付ファイル及び E 社に提出又は送信した文書ファイルには，不審なコードは含まれていなかったとの報告であった。

〔再発防止策の策定〕

今回のマルウェア感染に対する再発防止策を，IT 部が中心に策定することとなった。C さんは，調査で判明した事実を基に，他の IT 部のメンバとともに課題を抽出し，対策を検討した。その結果は表 4 のとおりである。

表4　課題と対策

項番	課題	対策
1	（省略）	標準ソフトの脆弱性管理を行い，必要な修正パッチを適用する。
2	ビューア V を含む標準ソフトの［　f　］が行われていなかった。	定期的に標準ソフトの［　f　］を行う。
3	・マルウェアが検知されても，AM で駆除でき，AM のフルスキャンで他のマルウェアが検知されなければ，当該 PC の継続利用を認めていた。 ・AM の検知状況を監視していなかった。	（省略）
4	（省略）	未知のマルウェアに対する対策（以下，未知マルウェア対策という）を行う。

C さんは，課題と対策を D 部長に報告した。D 部長は，表 4 の項番 1～3 の対策を再発防止策とし，可能な対策から順次実施するとともに，項番 4 の対策を具体化するよう指示した。

〔未知マルウェア対策の検討〕

C さんは，D 部長の指示に従い，未知マルウェア対策の検討を始めた。次は，未知マルウェア対策の検討についての C さんと D 部長の会話である。

C さん：未知マルウェア対策として，図 7 の案を考えました。未知のマルウェアを全て検知するのは無理です。そのため，未知のマルウェアへの感染を前提とした対策も必要です。

【未知のマルウェアの検知を目的とした対策】
・入口対策：Web 閲覧やメールで入ってきたファイルをサンドボックスで実行し，振る舞いを調べることによってマルウェアを検知する対策など
・出口対策：レピュテーションやアノマリ検知によって，C&C 通信を発見する対策など
【未知のマルウェアへの感染を前提とした対策】
・マルウェアに感染しても情報が漏えいしない対策（データの暗号化など）
・マルウェアに感染しても感染前の状態に戻せる対策（ブートイメージからの復元など）

図7　未知マルウェア対策案（抜粋）

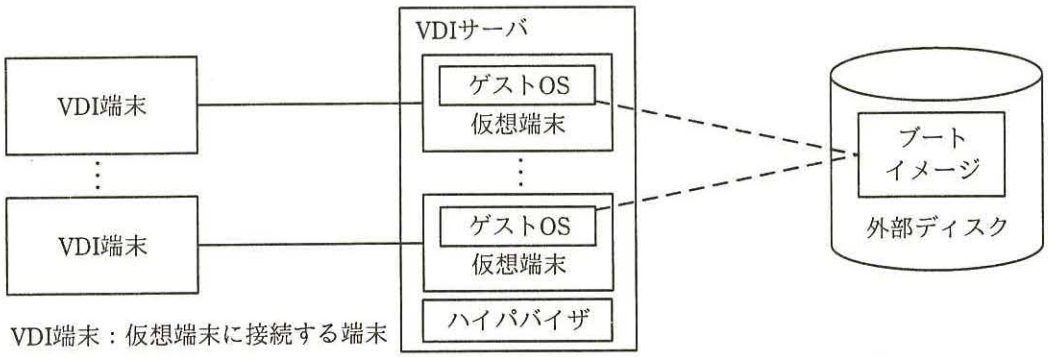
D 部長：我が社のモバイル PC ではハードディスクの暗号化を行っていますが，マル

ウェア感染時の情報漏えいを防げますか。

C さん：残念ながら，③マルウェア感染による情報漏えい対策としては役に立ちません。そうした情報漏えいを防ぐためには DRM のような仕組みが必要になり，取引先にも影響があります。

D 部長：なるほど。ブートイメージからの復元というのはどのようなものですか。

C さん：ブートイメージとは OS の起動に必要なファイルや標準ソフトなどをひとまとめにしたものです。これを読取り専用領域に保存し，起動時に読み込ませることで，動作環境を復元します。実装方法として，モバイル PC 上に読取り専用領域を作成する方法と，図 8 のように，仮想端末上でゲスト OS を動かす，画面転送型の仮想デスクトップ環境（以下，VDI という）の二つがあります。これら二つの対策を我が社が利用した場合，表 5 で示すメリットとデメリットがあります。



VDI端末：仮想端末に接続する端末

注記　破線は，ブートイメージを仮想端末にゲスト OS として読み込むことを示す。

図 8　VDI のシステム構成

表 5　メリットとデメリット（抜粋）

項番	対策	メリット	デメリット
1	モバイル PC 上に読取り専用領域を作成	・実装が容易 ・オフラインでも使える。	・④再起動時に一部のセキュリティ対策が初期化される。 ・利用者ごとの個別の設定が困難 ・運用負荷が高い。
2	VDI	・運用負荷が低い。 ・利用者ごとの個別の設定が容易	・既存の AM 利用時に問題が発生する。 ・設備費用が高い。

D 部長：表 5 によると VDI が良さそうですが，デメリットを解消する方法はありますか。

C さん：AM に関しては，VDI に対応した仮想アプライアンスやゲートウェイ型のものが利用できるクラウドサービスを検討します。

D 部長：VDI 端末としてモバイル PC は使えるのですか。

C さん：はい。モバイル PC を使って USB メモリから VDI 専用 OS を起動する方法があります。

D 部長：VDI 端末には，どのような要件が必要ですか。

C さん：要件は，次の四つです。

要件 1：VDI サーバにログインできる。

要件 2：仮想端末との間では，画面及びキーボード・マウスの操作データだけの送受信を許可する。

要件 3：マルウェア感染を防ぐ仕組みがある。

要件 4：要件 1～要件 3 を満たすのに必要な通信だけを許可する。

D 部長：要件 3 が満たせずに，VDI 端末がマルウェアに感染しても，要件 2 が満たされていれば，仮想端末には影響がないですよね。

C さん：いいえ。⑤要件 2 が満たされても，VDI 端末上のマルウェアによる仮想端末からの情報の窃取は可能です。

D 部長：そうですか。

C さん：そういった情報の窃取を防ぐためには，VDI 端末の徹底的な要塞化が必要です。VDI 端末に汎用 OS を使う場合，VDI 端末の保護のための仕組みが必要になります。一方，VDI 専用 OS を使用する場合，読取り専用の USB メモリに VDI 専用 OS を入れておきます。VDI 端末のハードディスクの中身は全て消去し，USB メモリからだけブートできるようにします。ブートすると VDI に接続するためのソフトウェアが自動的に起動します。

D 部長：なるほど。それでは，その案をベースに，VDI の実装案と移行計画をまとめて提出してください。その際には，既存のガイドラインへの影響なども考慮に入れてください。

C さんは，VDI の実装案，⑥クラウドサービス利用に関する Q 社のセキュリティ

ガイドラインの変更案，及び移行計画を D 部長に提出した。D 部長はこれを承認し，関係各部と調整して年次計画に組み込んだ。

F 部長はこれらの結果を受けて，X 社による追加調査の結果，再発防止策及び未知マルウェア対策の計画を E 社 G 部長に説明し，理解を得た。

設問 1　〔IT 部による調査〕について，(1)，(2)に答えよ。

(1) 本文中の下線①の動作を実現するためには，C&C サーバでどのような仕組みが必要か。表 3 の記載内容を用いて，40 字以内で具体的に述べよ。

(2) 本文中の下線②について，〔モバイラのテレワーク環境〕で述べられている機能を用いて実現する方法が二つある。どの機能でブロックすべきか。それぞれ 20 字以内で答えよ。

設問 2　図 4 中の［ a ］に入れる適切な字句を，5 字以内で答えよ。

設問 3　〔侵入経路と被害状況の調査〕について，(1)，(2)に答えよ。

(1) 本文中の［ b ］，［ c ］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［ d ］，［ e ］に入れる具体的な保管場所を，〔モバイラのテレワーク環境〕を考慮して，それぞれ 10 字以内で答えよ。

設問 4　表 4 中の［ f ］に入れる適切な字句を，5 字以内で答えよ。

設問 5　〔未知マルウェア対策の検討〕について，(1)～(4)に答えよ。

(1) 本文中の下線③について，役に立たない理由を 40 字以内で述べよ。

(2) 表 5 中の下線④について，具体例を二つ，それぞれ 25 字以内で述べよ。

(3) 本文中の下線⑤について，どのような攻撃を想定しているか。20 字以内で述べよ。

(4) 本文中の下線⑥について，VDI 以外のクラウドサービスに関して，セキュリティガイドラインの変更が必要な項目を図 1 中の番号で答えよ。また，変更後の案を 60 字以内で述べよ。

〔 メ モ 用 紙 〕

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	15:10 ～ 16:20

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。
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。

午