全問が必須問題です。必ず解答してください。

問1　サイバー攻撃を想定した演習に関する次の記述を読んで，設問1～4に答えよ。

W 社は，自動車電装部品，ガス計測部品及びソーラシステム部品を製造する従業員数 1,000 名の企業である。経営企画部，人事総務部，情報システム部，調達購買部などのコストセンタ並びに自動車電装部，ガス計測部，及び昨年新規事業として立ち上げられたソーラシステム部の三つのプロフィットセンタから構成されている。ソーラシステム部は現在 30 名の組織であるが，事業を拡大させるために，毎月，3～4 名の従業員を採用しており，組織が拡大している。

W 社では，7 年前に最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会を設置し，情報セキュリティポリシ及び情報セキュリティ関連規程を整備して，ISMS 認証を全社で取得した。経営企画部が，情報セキュリティ委員会の事務局を担当している。また，各部の部長が，情報セキュリティ委員会の委員，及び自部における情報セキュリティ責任者を務めている。各情報セキュリティ責任者は，自部の情報セキュリティに関わる実務を担当する情報セキュリティリーダを選任している。

W 社は年に 1 回，人事総務部が主管となり，大規模な震災などを想定した事業継続計画の演習を実施している。サイバー攻撃を想定した演習は実施したことがないものの，サイバー攻撃などの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）の対応手順はあり，これまで，事業に深刻な影響を与えるようなサイバー攻撃は受けていない。

〔ソーラシステム部の状況〕

ソーラシステム部では，省エネルギーを推進しており，部で使用する全ての PC には，消費電力の少ないノート PC（以下，NPC という）を選定している。省エネルギー対策の一つとして，全ての NPC は，カバーを閉じると自動的にスリープモードに切り替わるように設定されている。また，情報セキュリティ対策の一つとして，全ての NPC では，USB ストレージなどの外部記憶媒体を使用できないように技術的対策を講じている。

ソーラシステム部の情報セキュリティ責任者は E 部長で，情報セキュリティリーダは F さんである。F さんは，最近，競合他社がサイバー攻撃を受け，その対応に手

間取って大きな被害が発生したとのニュースを聞いた。そこで，F さんは，ソーラシステム部内でサイバー攻撃を想定した演習を行うことを提案した。E 部長は提案を承認し，F さんに演習を計画するように指示した。

〔演習の計画〕

サイバー攻撃を想定した演習は，年 1 回行うことにした。演習は，一般的に表 1 に示すような机上演習と機能演習の 2 種類に大別される。機能演習の具体的な形式には，実際のサイバー攻撃に近い形で疑似的なサイバー攻撃を行う［　a　］が含まれる。

表 1　サイバー攻撃を想定した演習の種類

種類	説明	主な目的	具体的な形式
机上演習	議論主体の演習である。参加者の緊急時における役割，及び特定の緊急時の対応策について議論する。	参加者に気付きを与える。	・ワークショップ ・ゲーム
機能演習	作業主体の演習である。参加者の緊急時における役割及び責任を，シミュレーション環境で実践する。	作業手順，社内システム，代替施設などが適切に機能することを検証する。	・サイバーレンジトレーニング ・［　a　］

注記　本表は，NIST SP 800-84 や HSEEP（Homeland Security Exercise and Evaluation Program）などを基に，W 社が独自に作成した。

F さんは，机上演習と機能演習を比較検討した結果，今回は，参加者に気付きを与えられる机上演習として，ワークショップを実施することにした。演習終了後には，参加者からの意見を集めて次回の演習に反映することにした。

F さんは，机上演習のシナリオを検討するに当たり，サイバーキルチェーンを参考にすることにした。サイバーキルチェーンとは，サイバー攻撃の段階を説明した代表的なモデルの一つである。サイバー攻撃を 7 段階に区分して，攻撃者の考え方や行動を理解することを目的としている。サイバーキルチェーンのいずれかの段階でチェーンを断ち切ることができれば，被害の発生を防ぐことができる。サイバー攻撃のシナリオをサイバーキルチェーンに基づいて整理した例を表 2 に示す。

表2　サイバー攻撃のシナリオをサイバーキルチェーンに基づいて整理した例

段階	サイバー攻撃のシナリオ
1　偵察	①インターネット上の情報を用いて組織や人物を調査し，攻撃対象の組織や人物に関する情報を取得する。
2　武器化	攻撃対象の組織や人物に特化したエクスプロイトコード[1]やマルウェアを作成する。
3　配送	マルウェア設置サイトにアクセスさせるためになりすましの電子メール（以下，電子メールをメールという）を送付し，本文中の URL をクリックするように攻撃対象者を誘導する。
4　攻撃実行	攻撃対象者をマルウェア設置サイトにアクセスさせ，エクスプロイトコードを実行させる[2]。
5　インストール	攻撃実行の結果，攻撃対象者の PC がマルウェア感染する。
6　遠隔制御	（省略）
7　目的の実行	探し出した内部情報を圧縮や暗号化などの処理を行った後，もち出す。

注記　本表は，JPCERT コーディネーションセンター“高度サイバー攻撃への対処におけるログの活用と分析方法”などを基に，W 社が独自に作成した。

注[1]　脆弱性を悪用するソフトウェアのコードのことであり，攻撃コードとも呼ばれる。

[2]　この段階では，攻撃対象者の PC はマルウェア感染していない。

F さんは，次の二つの演習のシナリオを取り上げることにした。

シナリオ 1　標的型メール攻撃のシナリオである。W 社の取引先をかたった者から，W 社の公開 Web サイトが停止しておりアクセスできない旨の報告をメールで受信した。メールの本文には，W 社の公開 Web サイトを模した偽サイトの URL が記載されている。この場合の対応を行う。

シナリオ 2　標的型メール攻撃を受けた結果，マルウェア感染したというシナリオである。従業員の NPC のマルウェア対策ソフトからアラートが画面に表示された。アラートは，マルウェア感染らしき異常が認められたというものである。この場合の対応を行う。

シナリオ 1 は，表 2 の“ b1 ”の段階での対応であり，シナリオ 2 は，表 2 の“ b2 ”の段階での対応である。

〔演習の実施〕

演習にはソーラシステム部の全メンバが参加した。F さんは，メンバを会議室に招集し，参加者を三つのグループに分けて，ワークショップを実施した。ワークショ

ップでは，F さんは，ファシリテータとして，参加者に対して二つのシナリオを提示した。参加者はグループごとに，W 社のインシデント対応手順に従って取るべきアクションを議論し，発表した。W 社のインシデント対応手順は，図 1 のとおりである。

1　検知
・インシデント又はインシデントのおそれを発見した場合は，直ちに自部の情報セキュリティリーダに報告する。
2　エスカレーション
・上記 1 の報告を受けた情報セキュリティリーダは，情報セキュリティ責任者，情報システム部及び関連組織に報告する。
・社外の利害関係者に連絡する場合は，次の手順に従う。
（省略）
3　原因の特定
（省略）
4　一次対応
　情報セキュリティリーダは，上記 3 で特定した原因に対して，必要に応じて情報システム部や関連組織の協力を得ながら，次の一次対応を行う。
・マルウェア感染が疑われる場合は，感染が疑われる NPC などをネットワークから切り離すことを最優先に実施する。
・ランサムウェア感染が疑われる場合は，上記の一次対応に加えて，電源の強制切断 1) を実施する。
（省略）
5　証拠保全
　情報セキュリティリーダは，上記 4 を実施後，証拠として，W 社証拠保全ガイドに従って，情報システム部や関連組織の協力を得ながら，インシデントに関係するコンピュータ，デバイスなどの機器を，操作せずに保管する。
　なお，必要に応じて，②証拠保全した機器の調査を情報システム部が外部のセキュリティ専門業者に依頼することがある。
（省略）
6　その他
　情報セキュリティリーダは，上記 2～5 の対応に当たり，インシデントに至る経緯や対応を，適宜，記録する。
（省略）

注 1)　通常の OS 終了処理やスリープモードへの切替えはせずに，機器側から電源ケーブルを抜くこと。NPC の場合は，電源ケーブルを抜いた上でバッテリを外すことも含む。

図 1　インシデント対応手順（抜粋）

各グループのワークショップの発表結果は，表3のとおりである。

表3　ワークショップの発表結果

シナリオ	グループ1	グループ2	グループ3
1	標的型メール攻撃であるか否かを確認するために，メール本文中の URL をクリックする。クリック後，もし NPC に異常が認められたら，情報セキュリティリーダにインシデントとして報告する。異常が認められなければ，何もしない。	怪しいメールと判断し，メール本文中の URL はクリックしない。インシデントのおそれありと考えられるので，情報セキュリティリーダに報告する。	怪しいメールと判断し，メール本文中の URL はクリックしない。メールをごみ箱に移してから完全に削除する。インシデントのおそれありとは考えられないので，報告は不要と判断する。
2	NPC をネットワークから切り離す。もし，ファイルが勝手に暗号化されるような兆候が認められた場合は，次のようにする。 ・NPC から電源ケーブルを抜く。 ・再起動をしてから，NPC のカバーを閉じて，バッテリを外す。	NPC をネットワークから切り離す。もし，ファイルが勝手に暗号化されるような兆候が認められた場合は，次のようにする。 ・NPC から電源ケーブルを抜く。 ・通常の OS 終了処理は行わず，NPC のカバーを開いたまま，バッテリを外す。	NPC をネットワークから切り離す。もし，ファイルが勝手に暗号化されるような兆候が認められた場合は，次のようにする。 ・NPC から電源ケーブルを抜く。 ・通常の OS 終了処理は行わず，NPC のカバーを閉じて，バッテリを外す。

F さんは，シナリオ1及びシナリオ2について，適切な対応方法を参加者に解説した。その中で，参加者から，なぜ，通常の OS 終了処理ではいけないのかと質問を受けたので，③その理由について説明した。また，演習後に，参加者にアンケートを実施した。

こうして，F さんは，無事にワークショップを終えた。

〔演習結果の振り返り〕

F さんが演習中に参加者から受けた質問と F さんの回答は表 4 のとおりであった。

表 4　参加者からの質問及び F さんの回答（抜粋）

シナリオ	質問	F さんの回答
1，2	サイバーキルチェーンの各段階の対策例を知りたい。	“1 偵察”段階の対策としては，次が考えられる。 ・SNS 利用におけるルールを作成する。 ・ c1 ・ c2 （省略）
1	もし，W 社の偽サイトが発見された場合，会社としてどのような対応を行うのか。	取引先及び顧客が被害に遭わないようにするために，次の対応を行う。 ・ d1 ・ d2 （省略）
2	（省略）	（省略）

〔演習結果の報告〕

F さんは，演習結果，参加者からの質問及び意見，インシデント対応手順の改善案並びに次回の演習に向けての改善案をまとめ，E 部長に報告した。また，F さんは，④ソーラシステム部の組織の状況などを考慮すると，年 1 回の演習だけでは十分とはいえないと考えて，演習の頻度を上げることを E 部長に提案した。E 部長は，F さんからの提案を受け，演習結果とあわせて提案内容を情報セキュリティ委員会に提出した。

情報セキュリティ委員会は，E 部長からの提案を受けて，全社としても，サイバー攻撃を想定した演習を実施することにした。

その後，ソーラシステム部は，大きなインシデントの被害もなく順調に事業を拡大し，W 社全体としても，更なる情報セキュリティの強化を図ることができた。

設問1　〔演習の計画〕について，(1) ～ (3) に答えよ。

(1) 本文中及び表 1 中の［ a ］に入れる具体的な形式はどれか。解答群のうち，最も適切なものを選べ。

a に関する解答群

ア　広域災害対策演習　　イ　情報セキュリティ監査
ウ　脆弱性診断　　エ　パンデミック対策演習
オ　ビジネスインパクト分析　　カ　ファジングテスト
キ　ホワイトボックステスト　　ク　マルウェア解析
ケ　リバースエンジニアリング　　コ　レッドチーム演習

(2) 表 2 中の下線①について，次の (i) ～ (v) のうち，該当する行為だけを全て挙げた組合せを，解答群の中から選べ。

(i) 攻撃者が，WHOIS サイトから，W 社の情報システム管理者名や連絡先などを入手する。

(ii) 攻撃者が，W 社の公開 Web サイトから，HTML ソースのコメント行に残ったシステムのログイン情報などを探す。

(iii) 攻撃者が，W 社の役員が登録している SNS サイトから，攻撃対象の人間関係や趣味などを推定する。

(iv) 攻撃者が，一般的な Web ブラウザからはアクセスできないダーク Web から，W 社のうわさ，内部情報などを探す。

(v) 攻撃者が，インターネットに公開されていない W 社の社内ポータルサイトから，会社の組織図や従業員情報，メールアドレスなどを入手する。

解答群

ア (i), (ii), (iii)　　イ (i), (ii), (iii), (iv)　　ウ (i), (ii), (iii), (v)
エ (i), (ii), (iv)　　オ (i), (ii), (iv), (v)　　カ (i), (iii), (iv), (v)
キ (i), (iv), (v)　　ク (ii), (iii), (iv), (v)　　ケ (ii), (iii), (v)
コ (iii), (iv), (v)

(3) 本文中の［ b1 ］，［ b2 ］に入れる段階の組合せはどれか。b に関する解答群のうち，最も適切なものを選べ。

b に関する解答群

	b1	b2
ア	1 偵察	2 武器化
イ	2 武器化	3 配送
ウ	2 武器化	4 攻撃実行
エ	3 配送	4 攻撃実行
オ	3 配送	5 インストール
カ	4 攻撃実行	5 インストール
キ	4 攻撃実行	6 遠隔制御
ク	5 インストール	6 遠隔制御
ケ	5 インストール	7 目的の実行
コ	6 遠隔制御	7 目的の実行

設問2 〔演習の実施〕について，(1) ～ (4) に答えよ。

(1) 図1中の下線②を表すものはどれか。解答群のうち，最も適切なものを選べ。

解答群

ア Web アプリケーションの脆弱性診断

イ 技術動向の監視

ウ 従業員の情報セキュリティ教育や啓発

エ セキュリティ製品やソリューションの評価

オ セキュリティツールの開発

カ ディジタルフォレンジックス

(2) 表 3 のシナリオ 1 の発表結果について，W 社のインシデント対応手順に沿った対応であるか否かを示す組合せはどれか。解答群のうち，最も適切なものを選べ。ここで，“正”は手順に沿った対応であることを示し，“誤”は手順に沿った対応ではないことを示す。

解答群

	グループ 1	グループ 2	グループ 3
ア	誤	誤	誤
イ	誤	誤	正
ウ	誤	正	誤
エ	誤	正	正
オ	正	誤	誤
カ	正	誤	正
キ	正	正	誤
ク	正	正	正

(3) 表 3 のシナリオ 2 の発表結果について，W 社のインシデント対応手順に沿った対応であるか否かを示す組合せはどれか。解答群のうち，最も適切なものを選べ。ここで，“正”は手順に沿った対応であることを示し，“誤”は手順に沿った対応ではないことを示す。

解答群

	グループ 1	グループ 2	グループ 3
ア	誤	誤	誤
イ	誤	誤	正
ウ	誤	正	誤
エ	誤	正	正
オ	正	誤	誤
カ	正	誤	正
キ	正	正	誤
ク	正	正	正

(4) 本文中の下線③の理由について，次の (i) ～ (v) のうち，該当するものを二つ挙げた組合せを，解答群の中から選べ。

(i) 通常の OS 終了処理を行うと，記憶媒体に異常が生じることがあるから

(ii) 通常の OS 終了処理を行うと，その間にもファイルが暗号化され，被害が拡大することがあるから

(iii) 通常の OS 終了処理を行うと，調査に必要な情報の一部が失われることがあるから

(iv) 通常の OS 終了処理を行うと，バッテリやマザーボードが故障することがあるから

(v) 通常の OS 終了処理を行うと，メーカのサポートを受けられなくなることがあるから

解答群

ア (i), (ii)	イ (i), (iii)	ウ (i), (iv)
エ (i), (v)	オ (ii), (iii)	カ (ii), (iv)
キ (ii), (v)	ク (iii), (iv)	ケ (iii), (v)
コ (iv), (v)		

設問3　〔演習結果の振り返り〕について，(1)，(2)に答えよ。

(1)　表4中の［ c1 ］，［ c2 ］に入れる，次の(i)～(vii)の組合せはどれか。cに関する解答群のうち，最も適切なものを選べ。

(i)　インシデント発生後に迅速な対応ができるように，社内に CSIRT を構築する。

(ii)　インターネット上の匿名掲示板などに社内情報を書き込まないように，従業員に対して情報セキュリティ教育を行う。

(iii)　攻撃者に有用な情報を渡さないように，外部のセキュリティ専門業者に，SNSや匿名掲示板などの監視を依頼する。

(iv)　攻撃者の偵察を検知するために，W 社の社内 Web サーバやプロキシサーバへのアクセス内容をログに記録する。

(v)　実行形式のファイルが添付されたメールを受信したら直ちに削除するように，従業員に対して情報セキュリティ教育を行う。

(vi)　情報漏えいの被害を低減させるために，W 社のファイルサーバのファイルを全て暗号化する。

(vii)　マルウェア感染の被害を低減させるために，W 社の全ての NPC に対して，マルウェア対策ソフトのマルウェア定義ファイルを更新する。

cに関する解答群

	c1	c2
ア	(i)	(ii)
イ	(i)	(vii)
ウ	(ii)	(iii)
エ	(ii)	(iv)
オ	(iii)	(iv)
カ	(iii)	(vi)
キ	(iv)	(v)
ク	(v)	(vi)
ケ	(v)	(vii)
コ	(vi)	(vii)

(2) 表 4 中の [d1] , [d2] に入れる，次の (i) ～ (v) の組合せはどれか。d に関する解答群のうち，最も適切なものを選べ。

(i) 偽サイトが閉鎖されるまでの間，W 社の公開 Web サイトを閉鎖する。

(ii) 偽サイトにアクセスしないように，その存在と危険性について外部に公表する。

(iii) 偽サイトにアクセスできないように，Web フィルタリングを設定する。

(iv) 偽サイトを攻撃するように，外部のセキュリティ専門業者に依頼する。

(v) 偽サイトを閉鎖するように，偽サイトの IP アドレスの割当てを管理しているプロバイダに依頼する。

d に関する解答群

	d1	d2
ア	(i)	(ii)
イ	(i)	(iii)
ウ	(i)	(iv)
エ	(i)	(v)
オ	(ii)	(iii)
カ	(ii)	(iv)
キ	(ii)	(v)
ク	(iii)	(iv)
ケ	(iii)	(v)
コ	(iv)	(v)

設問4　本文中の下線④について，F さんが考えた理由はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　ISMS 認証を取得しているから

イ　オフィスの省エネルギーを推進しているから

ウ　事業に深刻な影響を与えるようなサイバー攻撃を過去に受けたことがあるから

エ　プロフィットセンタであるから

オ　毎月，3～4 名の従業員を採用しているから