次の問1は必須問題です。必ず解答してください。

問1　標的型サイバー攻撃に関する次の記述を読んで，設問1，2に答えよ。

P社は，工場などで使用する制御機器の設計・開発・製造・販売を手掛ける，従業員数約50人の製造業である。P社では，顧客との連絡やファイルのやり取りに電子メール（以下，メールという）を利用している。従業員は一人1台のPCを貸与されており，メールの送受信にはPC上のメールクライアントソフトを使っている。メールの受信にはPOP3，メールの送信にはSMTPを使い，メールの受信だけに利用者IDとパスワードによる認証を行っている。PCはケーブル配線で社内LANに接続され，インターネットへのアクセスはファイアウォール（以下，FWという）でHTTP及びHTTPSによるアクセスだけを許可している。また，社内情報共有のためのポータルサイト用に，社内LAN上のWebサーバを利用している。P社のネットワーク構成の一部を図1に示す。社内LAN及びDMZ上の各機器には，固定のIPアドレスを割り当てている。

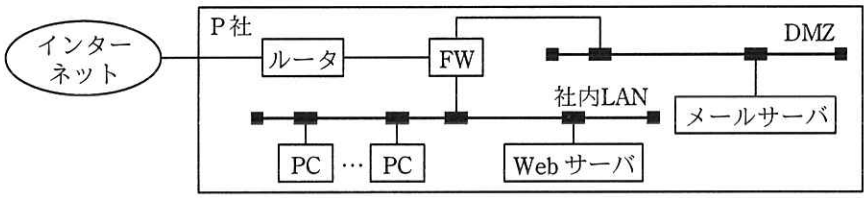

図1　P社のネットワーク構成（一部）

〔P社に届いた不審なメール〕

ある日，“添付ファイルがある不審な内容のメールを受信したがどうしたらよいか”との問合せが，複数の従業員から総務部の情報システム担当に寄せられた。P社に届いた不審なメール（以下，P社に届いた当該メールを，不審メールという）の文面を図2に示す。

P社従業員の皆様
総務部長のXです。
通達でお知らせしたとおり，PCで利用しているアプリケーションソフトウェアの調査を依頼します。このメールに情報収集ツールを添付しましたので，圧縮された添付ファイルを次に示すパスワードを使ってPC上で展開の上，情報収集ツールを実行して，画面の指示に従ってください。

図2　不審メールの文面（抜粋）

情報システム担当の Y さんが不審メールのヘッダを確認したところ，送信元メールアドレスのドメインは P 社以外となっていた。また，総務部の X 部長に確認したところ，そのようなメールは送信していないとのことであった。X 部長は，不審メールの添付ファイルを実行しないように，全従業員に社内のポータルサイト，館内放送及び緊急連絡網で周知するとともに，Y さんに不審メールの調査を指示した。

Y さんが社内の各部署で聞き取り調査を行ったところ，設計部の Z さんも不審メールを受信しており，添付ファイルを展開して実行してしまっていたことが分かった。Y さんは，Z さんが使用していた PC（以下，被疑 PC という）のケーブルを①ネットワークから切り離し，P 社のネットワーク運用を委託している Q 社に調査を依頼した。

Q 社で被疑 PC を調査した結果，不審なプロセスが稼働しており，インターネット上の特定のサーバと不審な通信を試みていたことが判明した。不審な通信は SSH を使っていたので，②特定のサーバとの通信には失敗していた。また，Q 社は［ a ］のログを分析して，不審な通信が被疑 PC 以外には観測されていないので，被害はないと判断した。

Q 社は，今回のインシデントは P 社に対する標的型サイバー攻撃であったと判断し，調査の内容を取りまとめた調査レポートを Y さんに提出した。

〔標的型サイバー攻撃対策の検討〕

Y さんからの報告と Q 社の調査レポートを確認した X 部長は，今回のインシデントの教訓を生かして，情報セキュリティ対策として，図 1 の P 社の社内 LAN のネットワーク構成を変更せずに実施できる技術的対策の検討を Q 社に依頼するよう，Y さんに指示した。Q 社の W 氏は Y さんとともに，P 社で実施済みの情報セキュリティ対策のうち，標的型サイバー攻撃に有効な技術的対策を確認し，表 1 にまとめた。

表 1　標的型サイバー攻撃に有効な P 社で実施済みの情報セキュリティ対策（一部）

対策の名称	対策の内容
FW による遮断	・PC からインターネットへのアクセスには，FW で HTTP 及び HTTPS だけを許可し，それ以外は遮断する。
PC へのマルウェア対策ソフトの導入	・PC にマルウェア対策ソフトを導入し，定期的にパターンファイルの更新と PC 上の全ファイルのチェックを行う。 ・リアルタイムスキャンを有効化する。

W 氏は，表 1 の実施済みの情報セキュリティ対策を踏まえて，図 1 の P 社の社内 LAN のネットワーク構成を変更せずに実施できる技術的対策の検討を進め，表 2 に示す標的型サイバー攻撃に有効な新たな情報セキュリティ対策案を Y さんに示した。

表 2　標的型サイバー攻撃に有効な新たな情報セキュリティ対策案

対策の名称	対策の内容
メールサーバにおけるメール受信対策	・メールサーバ向けマルウェア対策ソフトを導入して，届いたメールの本文や添付ファイルのチェックを行い，不審なメールは隔離する。 ・［ b ］などの送信ドメイン認証を導入する。
メールサーバにおけるメール送信対策	・PC からメールを送信する際にも，利用者認証を行う。
インターネットアクセス対策	・PC から直接インターネットにアクセスすることを禁止（FW で遮断）し，DMZ に新たに設置するプロキシサーバ経由でアクセスさせる。 ・プロキシサーバでは，利用者 ID とパスワードによる利用者認証を導入する。 ・プロキシサーバでは，不正サイトや改ざんなどで侵害されたサイトを遮断する機能を含む URL フィルタリング機能を導入する。
ログ監視対策	・Q 社のログ監視サービスを利用して，FW 及びプロキシサーバのログ監視を行い，不審な通信を検知する。

W 氏は，新たな情報セキュリティ対策案について，Y さんに次のように説明した。

Y さん：メールサーバに導入する送信ドメイン認証は，標的型サイバー攻撃にどのような効果がありますか。

W 氏：　送信ドメイン認証は，メールの［ c ］を検知することができます。導入すれば，今回の不審メールは検知できたと思います。

Y さん：メールサーバで送信する際に利用者認証を行う理由を教えてください。

W 氏：　標的型サイバー攻撃の目的が情報窃取だった場合，メール経由で情報が外部に漏えいするおそれがあります。利用者認証を行うことでそのようなリスクを低減できます。

Y さん：インターネットアクセス対策は，今回の不審な通信に対してどのような効果がありますか。

W 氏：　今回の不審な通信は特定のサーバとの通信に失敗していましたが，マルウェアが使用する通信プロトコルが［ d ］だった場合，サイバー攻撃の被害が拡大していたおそれがありました。その場合でも，表 2 に示したイ

ンターネットアクセス対策を導入することで防げる可能性が高まります。

Yさん：URLフィルタリング機能は，どのようなリスクへの対策ですか。

W氏：　標的型サイバー攻撃はメール経由とは限りません。例えば，③水飲み場攻撃によってマルウェアをダウンロードさせられることがあります。URLフィルタリング機能を用いると，そのような被害を軽減できます。

Yさん：ログ監視対策の目的も教えてください。

W氏：　表2に示したインターネットアクセス対策を導入した場合でも，高度な標的型サイバー攻撃が行われると，④こちらが講じた対策を回避してC&C（Command and Control）サーバと通信されてしまうおそれがあります。その場合に行われる不審な通信を検知するためにログ監視を行います。

W氏から説明を受けたYさんは，Q社から提案された新たな情報セキュリティ対策案をX部長に報告した。報告を受けたX部長は，各対策を導入する計画を立てるとともに，⑤不審なメールの適切な取扱いについて従業員に周知するように，Yさんに指示した。

設問1　〔P社に届いた不審なメール〕について，(1)～(3)に答えよ。

(1)　本文中の下線①で，Yさんが被疑PCをネットワークから切り離した目的を20字以内で述べよ。

(2)　本文中の下線②で，不審なプロセスが特定のサーバとの通信に失敗した理由を20字以内で述べよ。

(3)　本文中の［　a　］に入れる適切な字句を，図1中の構成機器の名称で答えよ。

設問2　〔標的型サイバー攻撃対策の検討〕について，(1)～(5)に答えよ。

(1)　表2中の［　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　OP25B　　イ　PGP　　ウ　S/MIME　　エ　SPF

(2)　本文中の［　c　］，［　d　］に入れる適切な字句を，それぞれ20字以内で答えよ。

(3) 本文中の下線③の水飲み場攻撃では，どこかにあらかじめ仕込んでおいたマルウェアをダウンロードするように仕向ける。マルウェアはどこに仕込まれる可能性が高いか，適切な内容を解答群の中から選び，記号で答えよ。

解答群

ア P社従業員がよく利用するサイト

イ P社従業員の利用が少ないサイト

ウ P社のプロキシサーバ

エ P社のメールサーバ

(4) 本文中の下線④で，C&C サーバが URL フィルタリング機能でアクセスが遮断されないサイトに設置された場合，マルウェアがどのような機能を備えていると対策を回避されてしまうか，適切な内容を解答群の中から選び，記号で答えよ。

解答群

ア PC上のファイルを暗号化する機能

イ 感染後にしばらく潜伏してから攻撃を開始する機能

ウ 自身の亜種を作成する機能

エ プロキシサーバの利用者認証情報を窃取する機能

(5) 本文中の下線⑤で，P 社従業員が不審なメールに気付いた場合，不審なメールに添付されているファイルを展開したり実行したりすることなくとるべき行動として，適切な内容を解答群の中から選び，記号で答えよ。

解答群

ア PCのメールクライアントソフトを再インストールする。

イ 不審なメールが届いたことをP社の情報システム担当に連絡する。

ウ 不審なメールの本文と添付ファイルをPCに保存する。

エ 不審なメールの本文に書かれている URL にアクセスして真偽を確認する。