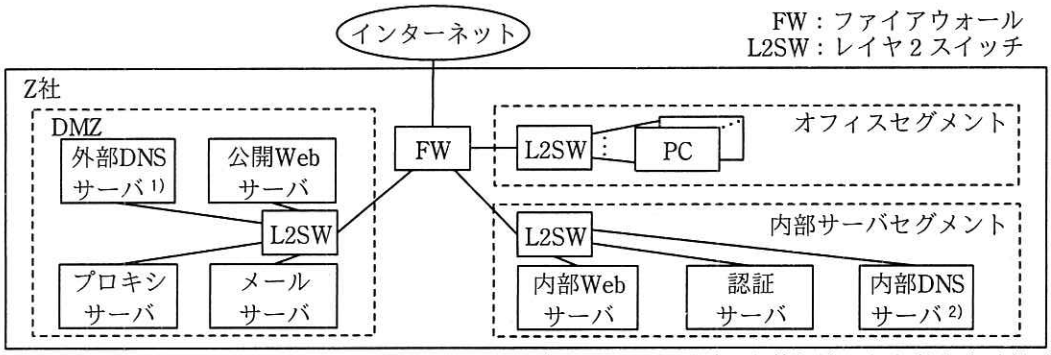
問２　セキュリティインシデント対応におけるサイバーセキュリティ情報の活用に関する次の記述を読んで，設問１，２に答えよ。

Ｚ社は，従業員数150名の金融事業会社である。事業規模は小さいが，多くの個人情報を扱っている。サイバーセキュリティ情報を共有し，サイバー攻撃への防御力を高める目的で活動する組織（ISAC：Information Sharing and Analysis Center）に最近加盟した。Ｚ社には５名で構成されるIT部門があり，ITシステムの運用や管理を行っている。Ｚ社のネットワーク構成を図１に示す。



注記　インターネットからＺ社の公開Webサーバやメールサーバの名前解決を行う外部向け権威DNSサーバの役割は，ドメイン登録サービスが提供するDNSサービスが担っている。ドメイン登録サービスが提供するDNSサービスの記載は省略している。

注1)　外部DNSサーバは，メールサーバ又はプロキシサーバからDNSクエリを受け，インターネット上の権威DNSサーバと通信し，名前解決を行うフルサービスリゾルバとして機能する。

2)　内部DNSサーバは，PCが内部Webサーバ及び公開Webサーバにアクセスするときの名前解決を行う権威DNSサーバとして機能する。

図１　Ｚ社のネットワーク構成

FWのフィルタリングルールを表１に，図１中に記載された機器の詳細を表２に示す。

表１　FWのフィルタリングルール

項番	送信元	宛先	サービス	動作
1	オフィスセグメント	DMZ	HTTP，HTTPS，DNS，POP，SMTP	許可
2	オフィスセグメント	内部サーバセグメント	HTTP，HTTPS，認証サービス，DNS	許可
3	全て	インターネット	DNS	許可
4	インターネット	DMZ	HTTP，HTTPS，SMTP	許可
5	DMZ	インターネット	HTTP，HTTPS，SMTP	許可
6	内部サーバセグメント	オフィスセグメント	認証サービス	許可
7	全て	全て	全て	拒否

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

表2　図1中に記載された機器の詳細（抜粋）

記号	機器	詳細	取得ログ
(a)	PC	1) 次の汎用ソフトウェアを導入している。 ・メールソフト：社内外との電子メール（以下，メールという）の送受信に利用する。 ・文書作成ソフト：文書ファイルの閲覧・作成・編集に利用する。 ・表計算ソフト：表計算ファイルの閲覧・作成・編集に利用する。 ・Web ブラウザ：Web アクセスに利用する。インターネットへの通信は全てプロキシサーバを経由するように設定され，設定は管理者だけが変更可能である。 2) 次のセキュリティ対策ソフトウェアを導入している。設定は管理者だけが変更可能である。 ・マルウェア対策ソフト：メール及びファイルのリアルタイムスキャンを行う。また，1 日 2 回マルウェア定義ファイルを更新し，週 1 回フルスキャンを実行する。 ・EDR（Endpoint Detection and Response）：PC 上のプロセスの起動・終了，ネットワーク通信，ファイル操作，実行ファイルのパスなどを記録し，検索できる。	・マルウェア対策ソフトによるリアルタイム検知情報とフルスキャン結果 ・EDR による記録結果
(b)	FW	ステートフルパケットインスペクション型の FW である。	・動作ログ
(c)	プロキシサーバ	PC からインターネット上の Web サイトへの HTTP 及び HTTPS 通信を中継する。PC からインターネットにアクセスするためには利用者 ID とパスワードによる BASIC 認証（以下，PC からインターネットにアクセスする際にプロキシサーバで実施される BASIC 認証をプロキシ認証という）を必須としている。プロキシ認証に必要なアカウント情報（以下，プロキシ認証情報という）は，プロキシサーバ内に保存されている。	・アクセスログ ・認証結果
(d)	外部 DNS サーバ	（省略）	なし
(e)	メールサーバ	社内外とのメールの送受信に利用する。プロトコルは POP と SMTP を使用する。	・メールの送受信履歴
(f)	認証サーバ	従業員が PC にログインする際に PC に入力された利用者 ID とパスワードで従業員を認証する。認証成功後に PC が利用できる。	・認証結果
(g)	内部 DNS サーバ	（省略）	なし

〔ISAC からの情報提供と対応〕

20XX 年 11 月 19 日，Z 社は ISAC から，サイバーセキュリティ情報の提供を受けた。当該情報の概要を図 2 に示す。

A) 20XX 年 11 月 17 日，金融事業会社 Q 社において従業員が社内で利用している利用者 ID とパスワードが窃取され，某掲示板に掲載されるという攻撃が発見された。

B) 利用者 ID とパスワードの窃取には，マルウェア Y の亜種の一つであるマルウェア P が使用された。

C) 攻撃グループ X は，マルウェア Y とその亜種を使用することで知られており，今回の攻撃も攻撃グループ X による可能性が高い。

D) 攻撃グループ X は，当該掲示板において，マルウェアを利用して Z 社の利用者 ID とパスワードを窃取する計画を立てていた。しかし，会話は途中までしか確認されておらず，実際に計画を実行したかは不明である。

E) 攻撃グループ X の過去の活動について，次のことが確認されている。

（あ）攻撃グループ X は，メールでマルウェアを配信する。同じマルウェアを攻撃対象ごとにファイル名だけ変更して送付することもあれば，挙動は同じだが攻撃対象ごとにコードの一部とファイル名を変更したマルウェアの亜種を送付することもある。

（い）マルウェアは，侵入後，窃取する重要情報を探すため，内部ネットワークの探索を行う。窃取する情報を持ち出す際には，まず，窃取する情報を暗号化し，一定のサイズに分割する。その後，C&C（Command and Control）通信を使用して持ち出す。

（う）C&C 通信には，HTTP 又は DNS プロトコルを使用する。HTTP の場合，Web ブラウザに設定されたプロキシサーバの IP アドレスを確認し，プロキシサーバ経由で C&C サーバと通信する。DNS プロトコルの場合，パブリック DNS サービス L を経由して通信する。攻撃対象となる組織が管理する DNS サーバを経由して C&C サーバと通信する事例は報告されていない。

注記　パブリック DNS サービスとは，インターネット上に公開され，誰でも自由に利用可能なフルサービスリゾルバ型の DNS サービスのことである。

図 2　提供されたサイバーセキュリティ情報の概要

攻撃グループ X が Z 社を攻撃する計画を立てていたことを重く見た Z 社は，実際に攻撃を受けたかの調査を開始した。IT 部門の K 部長がプロジェクトリーダとなり，部下の H さんが調査した。図 3 に H さんの調査結果を示す。

A) 最新のマルウェア定義ファイルを用いてZ社の全PCをスキャンしたが，マルウェアは検知されなかった。

B) ISACから提供されたマルウェアPの情報を用いてEDRで調査したところ，1台のPC（以下，PC-Vという）がマルウェアPに感染しているのを発見した。更に調査したところ，次のことが判明した。

（あ）マルウェアPはAmX3PxvR7.exeというファイル名で，PC-Vのローカルストレージのフォルダ N に配置されていた。

（い）20XX年11月18日 11:09，PC-Vを利用している従業員が，表計算ファイルを装ったメールの添付ファイルをクリックしたことで，PC-VがマルウェアPに感染した。

（う）マルウェアPは，汎用検索サービスA及びグローバルIPアドレスMへのHTTPによる通信を試みたが，①当該通信はZ社のネットワーク環境によって遮断されていたことがプロキシサーバのログに記録されていた。

C) 追加調査から，グローバルIPアドレスMは，攻撃グループXのC&Cサーバに割り当てられたIPアドレスだと判明した。

D) Z社が導入しているEDRでは，DNSプロトコルによる通信を記録しない設定となっていたが，パブリックDNSサービスLに対してDNSプロトコルによる通信が発生すれば，[a]のログに記録される。当該ログを調査したところ，該当する通信がなかったことを確認した。

E) 全PCを対象にグローバルIPアドレスMとの通信の有無について，EDRを使って調査したところ，あるPC（以下，PC-Tという）のローカルストレージのフォルダNにbV6fZq3hi.exeというファイルが配置され，グローバルIPアドレスMとの通信を試みたことを示すログを発見した。更に調査したところ，次のことが判明した。

（あ）bV6fZq3hi.exeについてセキュリティベンダの協力を仰いで調査した結果，マルウェアYの亜種の一つであるマルウェアRであった。

（い）20XX年11月18日 16:15，PC-TはPC-Vと同じ方法で感染した。

（う）マルウェアRは，汎用検索サービスA及びグローバルIPアドレスMへのHTTPによる通信を試みたが，マルウェアPの場合と同様，遮断されていた。

F) ISACから提供された情報を基に，②情報持ち出し成功時に残る痕跡を調査したが，該当する痕跡は確認できなかった。

A)～F)の調査によって，攻撃は受けたが，情報持ち出しは成功していないと判断した。

図3 Hさんの調査結果

K部長は，情報持ち出しは成功していないと判断できたことは不幸中の幸いだったとして，調査は一旦完了とした。③調査で判明した情報はISACに提供した。

〔対策の検討〕

K部長は，様々なC&C通信の手法が今後も使われるであろうと想定し，多層防御の考えに基づいて，C&C通信全般及び各手法への対策案を検討するようHさんに指示した。Hさんが検討したC&C通信全般への対策案を図4に，C&C通信の各手法への対策案を表3に示す。

ディジタル署名が付与されていない実行ファイルからの通信を EDR で遮断する。Z 社の業務で利用しているソフトウェアの実行ファイル（以下，正規実行ファイルという）には，ソフトウェア開発会社がディジタル署名を付与するか，自社で付与することができる。④ディジタル署名を検証すれば，正規実行ファイルか否かを判定できる。

図 4　C&C 通信全般への対策案（抜粋）

表 3　C&C 通信の各手法への対策案（抜粋）

項番	C&C 通信の手法	対策案
1	マルウェアが⑤プロキシ認証情報を窃取して，プロキシ認証を突破し，C&C 通信を行う。	（省略）
2	マルウェアがパブリック DNS サービスを利用して，C&C 通信を行う。	⑥FW のフィルタリングルールを変更することで，C&C 通信を遮断する。
3	攻撃者は，あらかじめ攻撃用ドメインを取得し，[b] を C&C サーバとして，インターネット上に用意しておく。マルウェアが，[c] に攻撃用ドメインについての [d] を送信すると，[c] が C&C サーバに非 [d] を送信する。こうして，マルウェアは C&C 通信を行う。 大量の情報を持ち出す場合，次の特徴が現れる。 ・長いホスト名をもつ DNS クエリの発生 ・[e]	（省略）

対策案は社内で承認され，対策が導入された。

設問 1　〔ISAC からの情報提供と対応〕について，(1)～(4)に答えよ。

(1)　図 3 中の下線①について，通信が遮断された理由を 20 字以内で述べよ。ここで，図 1 で示した Z 社内の機器及び攻撃グループ X の C&C サーバは正常に稼働していたものとする。

(2)　図 3 中の [a] に入れる適切な機器を表 2 中の(a)～(g)から一つ選び，記号で答えよ。

(3)　図 3 中の下線②について，情報持ち出しが成功した可能性が高いと Z 社が判断可能な痕跡は何か。該当する痕跡を二つ挙げ，それぞれ 30 字以内で述べよ。

(4)　本文中の下線③について，ISAC に伝えるべき情報のうち，他社が EDR などセキュリティ対策ソフトウェア又はセキュリティ機器を用いて感染端末を検出する際に有効であり，共有すべき情報を解答群の中から二つ選び，記号で答えよ。

解答群

ア　PC-V と PC-T がマルウェアに感染した日時情報

イ　マルウェア P とマルウェア R が HTTP による通信を試みたグローバル IP アドレス M

ウ　マルウェア P とマルウェア R が配置されていたフォルダ N のパス名

エ　マルウェア P に感染した PC-V のプライベート IP アドレス

オ　マルウェア P のファイル名

カ　マルウェア R に感染した PC-T のプライベート IP アドレス

キ　マルウェア R のファイル名

設問 2　〔対策の検討〕について，(1)～(5)に答えよ。

(1)　図 4 中の下線④について，ソフトウェアのディジタル署名の検証に利用する証明書を解答群の中から選び，記号で答えよ。

解答群

ア　S/MIME 証明書　　イ　TLS クライアント証明書

ウ　TLS サーバ証明書　　エ　コードサイニング証明書

(2)　表 3 中の下線⑤について，プロキシ認証情報の窃取に使用できない攻撃手法を解答群の中から選び，記号で答えよ。

解答群

ア　Web ブラウザのオートコンプリート情報の窃取

イ　キーロガーによる攻撃

ウ　ゴールデンチケットの窃取

エ　総当たり攻撃

オ　偽の BASIC 認証入力フォームの表示とそのフォームへの利用者の誘導

カ　ネットワーク盗聴

(3)　表 3 中の下線⑥について，表 1 のフィルタリングルールを一つ変更することによって対応した。変更すべきフィルタリングルールを項番で答えよ。また，変更後のフィルタリングルールについて，送信元，宛先，サービス，動作を答えよ。

(4)　表 3 中の [b] ～ [d] に入れる適切な字句をそれぞれ 10 字以内で答えよ。

(5)　表 3 中の [e] に入れる適切な特徴を 30 字以内で述べよ。