問３　標的型攻撃への対応に関する次の記述を読んで，設問1～3に答えよ。

J社は，ビッグデータ解析を専門とする，従業員数150名の調査会社である。従業員は，情報収集のためのWebアクセス，並びに営業活動及び情報交換のための社外との電子メール送受信にインターネットを利用している。J社では，情報セキュリティポリシを整備して運用している。

J社では，20XX年3月に標的型攻撃を受け，PCがマルウェアに感染して業務サーバ上の秘密情報を外部に送信してしまった。情報システム部（以下，情シ部という）が感染状況を調査し，感染が確実なPCだけでなく，疑わしいPCも合わせて40台のPCを初期化した。調査を始めてから初期化を完了するまでに48時間掛かり，その間，業務は停止せざるを得なかった。

〔標的型攻撃対策〕

J社は，事態が一段落したところで，情報セキュリティコンサルティング会社のK社に，標的型攻撃への対策についてのアドバイスを求めた。K社の担当コンサルタントである情報処理安全確保支援士（登録セキスペ）のN氏は，標的型攻撃への対応事例を示した上で，感染予防だけでなく，感染拡大防止や情報漏えい防止の対策も取り入れるべきであり，具体的には，マルウェアが，外部のC&C（Command and Control）サーバと通信を開始しようとする段階や，ほかの機器に感染を拡大しようとする段階で検知し対処できれば，情報漏えいの被害を軽減できるとアドバイスした。そこでJ社は，ITサービス会社のP社が提供する監視サービス（以下，Pサービスという）及びマルウェア対策ソフトベンダR社が提供するマルウェア対策製品（以下，Rシステムという）の導入，並びにインシデント対応手順など関係する規則類の改定を決めた。作業は，情シ部のE部長の指示によって，Gさんら3名が担当した。

PサービスとRシステムの導入を終えた20XX年9月時点の，J社情報システムの概要を図1に，J社情報システムの構成要素を表1に示す。また，改定後のインシデント対応手順を図2に示す。

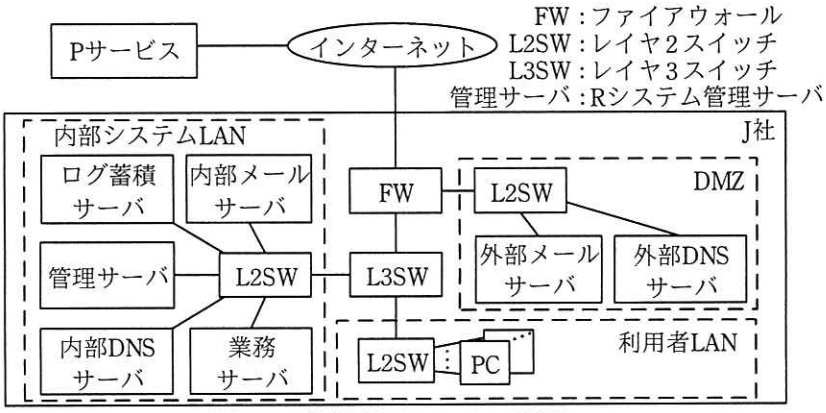

図1　J社情報システムの概要

表1　J社情報システムの構成要素（抜粋）

構成要素	概要
FW	・ステートフルパケットインスペクション型である。 ・フィルタリングルールをもち，送信元 IP アドレス，宛先 IP アドレス，ポートによって不要な通信を拒否する。 ・日時，FW の動作，送信元 IP アドレス，宛先 IP アドレス，ポート，データサイズを，FW のログとして取得し，P サービス及びログ蓄積サーバに syslog で送信する。 ・J 社と P サービスの間を，インターネット VPN で接続する。
業務サーバ及び PC	V 社製のマルウェア対策ソフトを導入しており，次のように設定している。 ・マルウェア定義ファイルを，起動時及び起動後 1 時間ごとに V 社の Web サーバからダウンロードし，更新する。 ・ファイルの読み書き時にリアルタイムスキャンを行う。 ・毎週，月曜日の昼の 12 時にフルスキャンを開始する。 ・マルウェア定義ファイルのダウンロード及び更新，並びにフルスキャンは，いつでも手動で実行できる。
R システム	・管理サーバ及びエージェントプログラムによって構成される。 ・エージェントプログラムは，PC 及び業務サーバに導入している。全てのプロセスの生成から終了までの動作，実行したプログラムのハッシュ値並びに通信の宛先の IP アドレス及びポートを，ログ（以下，R システムで取得するログを R ログという）として取得し，ログ蓄積サーバに syslog で送信する。 ・J 社が社内外からマルウェアのハッシュ値を入手し，管理サーバに登録すると，エージェントプログラムは，そのマルウェアの実行を禁止する。 ・管理サーバには，ログ蓄積サーバに保存された R ログを検索する機能があり，情シ部員は，R ログをマルウェアのハッシュ値で検索することによって，そのマルウェアが実行された痕跡があるかどうか調査することができる。

表1　J社情報システムの構成要素（抜粋）（続き）

構成要素	概要
ログ蓄積サーバ	・syslogで送信された，FWのログ及びRログを蓄積して保存する。
Pサービス	・Pサービスでは，受信したJ社のFWのログを分析する。ただし，FWのログは蓄積しない。過去に遡っての分析は行わない。 ・ログの分析によってC&Cサーバへの通信を検知すると，情シ部員に電子メール及び電話で通知する。 ・通知する内容は，C&Cサーバへの接続日時，送信元のIPアドレス，宛先のC&CサーバのIPアドレス，ポート及びデータサイズの5項目である。

情シ部員が実施する手順
(1) Pサービスからの通知を基に，C&Cサーバと通信したPC（以下，不審PCという）を特定する。
(2) 不審PCの電源が入っていれば，電源を入れたままにしておく。
(3) 不審PCに接続しているLANケーブルを抜き，利用者LANから切り離す。
(4) Pサービスから通知を受けた通信の宛先のC&CサーバのIPアドレスについては，そのIPアドレスへの通信を拒否するフィルタリングルールをFWに登録する。
(5) Pサービスから通知を受けたデータサイズを基に，情報漏えいのおそれがあるかどうかを判断する。
(6) ログ蓄積サーバにあるRログを調査し，マルウェアを特定する。
(7) マルウェアが特定できた場合は，そのハッシュ値を管理サーバに登録し，そのマルウェアの実行を禁止する。
(8) 不審PCからの情報漏えいの可能性が高いと判断した場合は，外部の専門業者に不審PCのメモリやストレージの調査及び分析を依頼する。
(9) (1)～(8)が終了したら，不審PCを必ず初期化する。その後，必要なアプリケーションソフトウェアをインストールして従業員に再配付する。

図2　改定後のインシデント対応手順（抜粋）

〔セキュリティインシデントの検知と対応〕

Pサービスと Rシステムを導入して数週間が経過した20XX年10月8日，C&Cサーバへの通信を検知したという通知をPサービスから受け，Gさんは図2の手順に従って対応した。Gさんによるインシデント対応の記録を表2に示す。

表2　Gさんによるインシデント対応の記録（抜粋）

時刻	対応内容
13:27	Pサービスから，J社内のIPアドレスからC&Cサーバへの通信を検知したという通知を受けた。通知内容は次のとおりであった。 C&Cサーバへの接続日時　20XX年10月8日13:17:15 送信元のIPアドレス　192.168.1.20 宛先のC&CサーバのIPアドレス　w1.x1.y1.z1 [1)] ポート　80/tcp データサイズ　200バイト
13:43	IPアドレス管理台帳で192.168.1.20を調べると，営業部の従業員Lさんの PC（以下，L-PCという）であった。
13:49	Lさんに電話を掛け，L-PCの電源を入れたまま，L-PCからLANケーブルを抜くように指示した。
14:03	宛先がw1.x1.y1.z1の通信を拒否するフィルタリングルールをFWに登録した。
14:28	FWのログを確認したところ，Pサービスからの通知のとおり，C&Cサーバに送信しているデータサイズは200バイトであった。
14:42	13:17:15前後のRログを確認して，C&Cサーバに接続したプログラムをマルウェアMとして特定した。同時にL-PC上で，表3のコマンドがマルウェアMによって，実行されていたことが判明した。
14:58	マルウェアMのハッシュ値を管理サーバに登録した。

注[1)]　w1.x1.y1.z1はグローバルIPアドレスである。

表3　L-PC上で実行されていたコマンド（抜粋）

コマンド	想定される攻撃フェーズ	想定される攻撃者の目的
ipconfig /all	初期調査	a
systeminfo		b
tasklist		c
dir /a	探索活動	秘密情報を含むファイルやフォルダを発見するために一覧を取得する。
net view		d

Gさんは，ここまでの対応を報告書にまとめて，E部長に提出した。

〔インシデント対応手順の改善〕

報告書を読んだ E 部長は，他社での標的型攻撃への対応事例と比較すると，対応が不十分であると考えた。次は，E 部長と G さんの会話である。

E 部長：ほかにもマルウェア M に感染した PC 又はサーバがある場合を想定する必要があるのではないか。

G さん：13:27 以降，P サービスから新たな通知は来ていません。感染したのは，L-PC だけと考えてよいのではないでしょうか。

E 部長：13:17:15 より前の，ログ蓄積サーバ中の FW のログに [e] が含まれているかどうかを確認する必要がある。

G さん：分かりました。早速確認します。

E 部長：ただし，①PC 又はサーバの状態によっては，FW のログを使った確認ではマルウェア M に感染していることを検知できないことがあるので，②R ログを使った確認もする必要がある。

G さん：分かりました。

G さんは，ログを確認し，感染した PC 又はサーバは，ほかに発見されなかったという結果を E 部長に報告した。E 部長は，マルウェアに感染した PC 又はサーバを特定するためのログの調査手順を，インシデント対応手順に追加するよう G さんに指示した。これによって，J 社ではインシデント対応手順を更に改善することができた。

設問１　〔標的型攻撃対策〕について，(1)，(2)に答えよ。

(1)　図２中の(2)のようにする目的を，25字以内で述べよ。

(2)　図２中の(3)について，不審PCを利用者LANから切り離さない場合，マルウェアがどのような活動をすると想定されるか。想定される活動のうち，J社にとって望ましくないものを二つ挙げ，それぞれ20字以内で述べよ。

設問２　表３中の［　a　］～［　d　］に入れる適切なものを解答群の中から選び，記号で答えよ。

解答群

ア　L-PCからその時点で接続可能な端末の一覧を取得する。

イ　L-PC内で悪用できる脆弱(ぜい)性を確認するために，OSのバージョンや脆弱性修正プログラムの適用状況を確認する。

ウ　L-PCのIPアドレス，MACアドレスなどネットワークアダプタの詳細な情報を取得する。

エ　L-PCの秘密情報を含んだファイルを暗号化する。

オ　実行中のプロセス一覧を取得し，マルウェアの解析環境でないか確認する。

カ　パスワードを含む，L-PCにログインするための情報を取得する。

設問３　〔インシデント対応手順の改善〕について，(1)～(3)に答えよ。

(1)　本文中の［　e　］に入れる適切な内容を25字以内で具体的に述べよ。

(2)　本文中の下線①について，検知できないのはPC又はサーバがどういう状態にある場合か。40字以内で述べよ。

(3)　本文中の下線②について，マルウェアMに感染しているPC又はサーバをRログを使って検知する方法を，30字以内で具体的に述べよ。