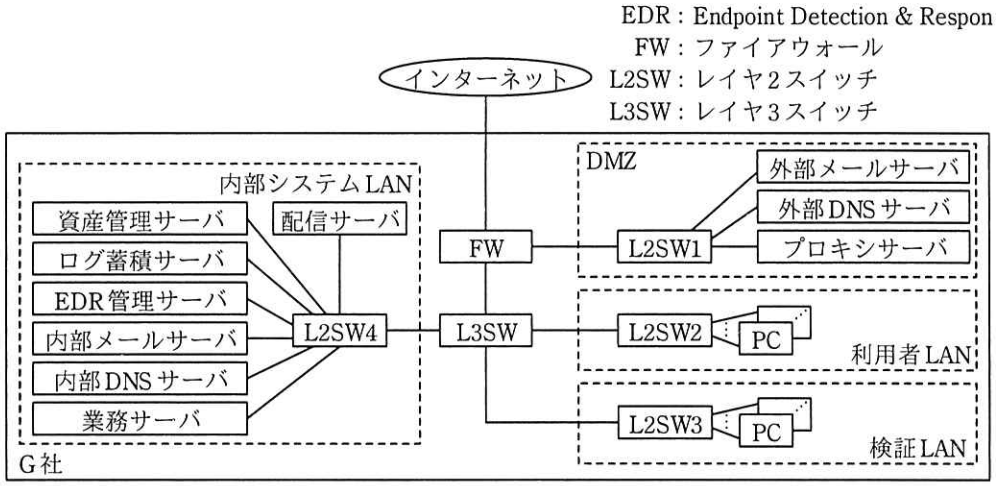
問３　セキュリティ運用に関する次の記述を読んで，設問１～４に答えよ。

G 社は，従業員 1,500 名の製造業であり，研究開発に定評がある。従業員は，Web アクセスによる情報収集並びに電子メール（以下，メールという）による営業活動及び情報交換にインターネットを利用している。G 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。G 社のシステム構成を図１に，機器及びソフトウェアの概要を表１に，OS の脆弱性修正プログラム（以下，セキュリティパッチという）の現状の配信手順を図２に示す。



注記１　全ての PC 及びサーバには，固定 IP アドレスが割り当てられており，PC には，EDR のエージェントプログラム（以下，エージェントという）が導入されている。

注記２　G 社の情報システム部（以下，情シ部という）以外の従業員には，PC の管理者権限を付与していない。

図１　G 社のシステム構成（概要）

表１　G 社の機器及びソフトウェアの概要（抜粋）

機器及びソフトウェア	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，ポートによって通信の許可と拒否を制御する。 ・パケットの送信元 IP アドレス，宛先 IP アドレス，ポート，データサイズと FW の動作を日時とともに FW のログとして取得し，ログ蓄積サーバに syslog で送信する。 ・インターネットとの間の通信を許可しているのは DMZ だけである。

表1　G社の機器及びソフトウェアの概要（抜粋）（続き）

機器及びソフトウェア	概要
配信サーバ	・セキュリティパッチの適用及びソフトウェアの更新を管理する。 ・セキュリティパッチ及び更新用のソフトウェアを取得し配信する。 ・各PCは，セキュリティパッチをOSベンダのサイトから直接ダウンロードするのではなく，配信サーバからダウンロードする。
資産管理サーバ	・エージェントから情報を受け取り，ソフトウェアの資産管理を行う。 ・Wake on LAN（以下，WoLという）の起動パケットを送信する機能をもつ。
ログ蓄積サーバ	・FW，サーバ及びエージェントから送信されるログをsyslogで受信して保存する。
EDR管理サーバ	・エージェントを管理する。 ・社内外からマルウェアのハッシュ値を収集して登録する。
エージェント	・通信，ファイルの操作などのイベントをログとして保存する。ログは直ちにログ蓄積サーバに送信されるとともに，PCにも1週間は保存される。 ・EDR管理サーバで収集されたハッシュ値を基にマルウェアを検知し，検知したマルウェアの起動を抑止する。 ・PC上で起動する全てのプロセスを監視する。指定した時間帯に指定したコマンドが実行された場合，EDR管理サーバとの間の通信を除き，当該PCの全ての通信を遮断する機能をもつ。

(1)　OSベンダがセキュリティパッチをリリースした場合，情シ部のセキュリティパッチ担当者（以下，パッチ担当者という）は，そのリリースノートを確認する。
(2)　パッチ担当者は，セキュリティパッチを検証LANのPCに適用し，社内で利用しているアプリケーションプログラムを2日間動作させて［　a　］を確認する。
(3)　さらに，パッチ担当者は，新たな不具合の情報が公開されていないことを確認した上で，セキュリティパッチを配信サーバに置く。
(4)　PCは，適用すべきセキュリティパッチが配信サーバに存在するかどうかを，起動時に配信サーバに問い合わせるように設定されている。もし，適用すべきセキュリティパッチがあれば，それをダウンロードし，適用する。起動中のPCは，適用状況を配信サーバに数時間ごとに通知する。

図2　セキュリティパッチの現状の配信手順（抜粋）

〔同業他社の事例〕

ある日，情シ部のC主任は，同業他社のH社で発生したセキュリティインシデントの解説記事を見付けた。解説記事の要約を図3に示す。

(1) 8月，H社の1台のPC（以下，PC-Hという）がマルウェアQに感染していたことが分かった。
(2) 各種ログから，PC-Hは外部の不審なサーバに約50Mバイトのデータを送信していたことが分かった。PC-Hでは秘密情報が取り扱われていたことから，H社は，秘密情報が送信された可能性が高いと判断した。
(3) マルウェアQはOSの脆弱性を悪用して感染を広げる。当該脆弱性に対するセキュリティパッチ（以下，パッチQという）は，5月にOSベンダからリリースされており，H社では6月までに，PC-Hを除く全PCに適用されていた。
(4) PC-Hは1月から起動されておらず，7月にPC-Hを起動したときには適用すべきセキュリティパッチが多数あった。そのため，起動後，パッチQの適用完了までに時間が掛かり，その間にマルウェアQに感染したと推測された。
(5) 調査を外部の専門業者に依頼したが，マルウェアQの感染調査に必要なログが一部しか取得されていなかったので調査が難航し，10月まで掛かった。
(6) H社のセキュリティ運用には問題があることが分かった。

図3　解説記事の要約

心配になったC主任はログを調査した。その結果，1か月以上起動していないPCが30台あることが分かった。それらのPCをこのまま数か月起動しないでおくと，PC-Hと同様の問題が発生する可能性があった。図3の内容及びG社の状況を情シ部のB部長に相談した上で，必要な対策を図4のようにまとめ，情シ部のD君とともにそれぞれを具体化することにした。

対策1：マルウェア感染を確認したときに，感染経路及び外部に流出した情報を特定するための手段の導入
対策2：社内におけるセキュリティパッチの配信手順の改善

図4　必要な対策

〔対策1〕

C主任は，対策1については，L2SWのミラーポートに接続するタイプのパケット収集装置を導入し，J社のJサービスを利用して通信内容を分析すればよいと考えた。Jサービスは，インターネットVPN経由でパケット収集装置から必要なパケット情報を取得し，その内容からセキュリティ侵害を検知するサービスである。

C主任は，1台のパケット収集装置を，①マルウェア感染がDMZ又はどのLANで起きてもマルウェアからインターネットへの通信が通過することになるL2SWに接続することに決めた。

〔対策2〕

次は，対策2についてのD君，C主任及びB部長の会話である。

D君　：1か月間起動していないPCを自動的に起動して，セキュリティパッチが適用されるようにすれば図3のようなセキュリティインシデントを防ぐことができます。良い仕組みはありませんか。

C主任：当社のPCは，WoLに対応しています。WoLとは，WoLに対応したPCに対し，特定の起動パケットを送信すると，当該PCが起動するという仕組みです。PCを利用者LANに接続しておけば，資産管理サーバから起動パケットを送信することによって，PCを自動的に起動できます。

B部長：なるほど。では，WoLとセキュリティパッチ適用の動作検証を頼む。

D君は，WoLの動作検証を開始した。まず，検証LANに接続されたPC-XとPC-Yを用いて試すことにした。PC-Xは起動しておき，PC-Yはシャットダウンしておいた。その上で，PC-XからPC-Yに対し，［　b　］に続けて，起動したいPCの［　c　］を16回繰り返したデータを含む起動パケットを送信し，PC-Yが起動することを確認した。その後，資産管理サーバからPC-Yの起動を試みたが，起動しなかった。C主任に相談したところ，②L3SWの設定を変更する必要があるという助言を受けた。D君は，L3SWの設定を変更し，資産管理サーバからPC-Yを起動できることを確認した。続いて，資産管理サーバから利用者LANに接続されたPCを起動できることを確認し，セキュリティパッチが適用されることも確認した。

〔WoLを悪用するマルウェアの脅威〕

WoLについて調べていたD君は，図5に示すマルウェアRの記事を見付けた。

起動していないPCをWoLを使って夜間に起動させ，次の手順で感染拡大を試みる。
(1) 感染するとすぐに，③自身が動作するPCのARPテーブルから下記(2)及び(4)の活動に必要な情報を読み取って保持しておく。
(2) 夜間にARPテーブル中のPC全てにpingコマンドを送信し，PCが起動しているかどうかを確認する。
(3) 起動しているPCに感染拡大を試みる。
(4) 起動していないPCを発見したら，WoLを使ってそれらのPCを起動し，感染拡大を試みる。

図5　マルウェアRの記事（抜粋）

D 君は，昼間は PC が不審な振る舞いをすれば発見し対処できる可能性があるが，夜間は多くの従業員が不在となり発見することは難しいと考えた。そこで，マルウェア R に限らない，WoL を悪用するマルウェアへの対策について，C 主任に相談した。

C 主任は，PC が夜間に不審な振る舞いをしたときに，当該 PC をネットワークから隔離するという対策（以下，対策 3 という）を助言した。D 君は，④対策 3 を G 社で導入済のシステムを用いて実現する方法を立案した。対策 3 は対策 1 及び対策 2 と併せて承認された。各対策は運用を開始し，マルウェア対策が強化された。

設問 1　図 2 中の［　a　］に入れる適切な字句を 20 字以内で具体的に答えよ。

設問 2　本文中の下線①の L2SW を，図 1 中の L2SW1～L2SW4 から選び，答えよ。

設問 3　〔対策 2〕について，(1)～(3)に答えよ。

(1) 本文中の［　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　00:00:00:00:00:00　　イ　00:00:00:FF:FF:FF

ウ　00:FF:00:FF:00:FF　　エ　FF:FF:FF:FF:FF:FF

(2) 本文中の［　c　］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　IP アドレス　　イ　MAC アドレス　　ウ　製造番号

エ　プロダクト ID　　オ　ホスト名

(3) 本文中の下線②に示す設定変更の内容を，30 字以内で具体的に述べよ。

設問 4　〔WoL を悪用するマルウェアの脅威〕について，(1)，(2)に答えよ。

(1) 図 5 中の下線③について，(2)の活動に必要な情報及び(4)の活動に必要な情報を，それぞれ 10 字以内で答えよ。

(2) 本文中の下線④の方法を，55 字以内で具体的に述べよ。