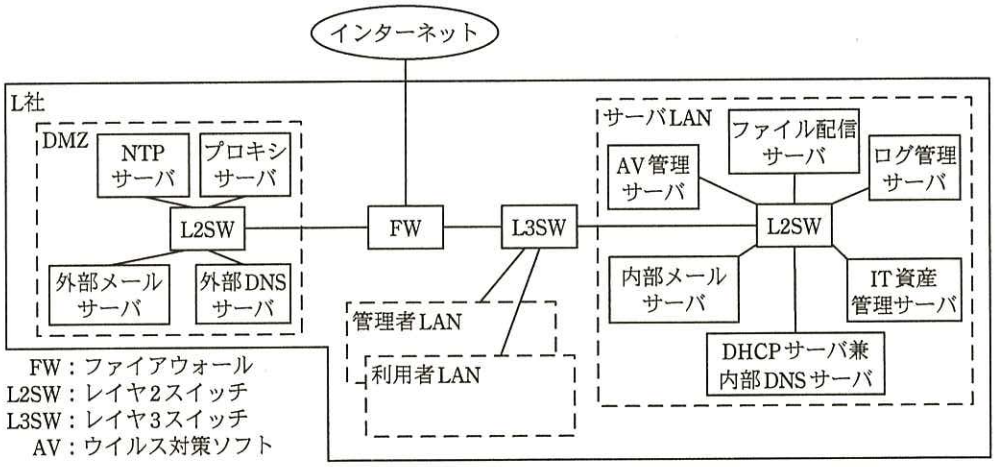
**問２**　情報漏えいインシデントの調査に関する次の記述を読んで，設問 1～3 に答えよ。

L 社は，従業員数 700 名のシステムインテグレータである。L 社のネットワーク構成を図 1 に，主なサーバとその概要を表 1 に示す。




注記１　L3SW のデフォルトゲートウェイは，FW に設定されている。
注記２　L 社の PC は，利用者 LAN 又は管理者 LAN に接続されている。

**図１　L 社のネットワーク構成（概要）**

**表１　主なサーバとその概要**

| サーバ名称 | 概要 |
|---|---|
| プロキシサーバ | ・プロキシ認証機能を使用し，利用者 ID とパスワードで認証する。<br>・ブラックリスト型の URL フィルタリング機能をもつ。 |
| AV 管理サーバ | ・各 PC 及び各サーバ上で稼働している AV は，ウイルス定義ファイルを AV 管理サーバから自動的に取得するよう設定されている。 |
| ファイル配信サーバ | ・パッチの自動配信及びパッチの強制適用に利用されている。 |
| ログ管理サーバ | ・図 1 中のネットワーク機器及びサーバのログを syslog で受信し，直近 3 か月分を保存する。<br>・syslog 受信に必要なポート以外は全て閉じ，リモートからアクセスできないようにしている。 |
| IT 資産管理サーバ | ・各 PC 及び各サーバの次の情報を保管する。<br>- 管理番号<br>- 管理者従業員番号<br>- 型式及びシリアル番号<br>- MAC アドレス<br>- OS 名とそのバージョン |
| 内部 DNS サーバ | ・L 社ネットワーク上にある機器の名前解決を行う。 |
| 外部 DNS サーバ | ・L 社外部メールサーバの MX レコードに関する名前解決，及び L 社ネットワーク外の機器の名前解決を行う。 |

各サーバは，アクセスログ，操作ログ，ミドルウェアのログ及びアプリケーションプログラムのログをログ管理サーバに送信するとともに，各サーバ上でも直近 3 か月分のログを保存している。

FW はステートフルパケットインスペクション型であり，NAPT 機能を使用している。また，許可した通信，拒否した通信ともにログを取得するように設定し，取得したログは全てログ管理サーバに送信している。FW のフィルタリングルールを表 2 に示す。

**表 2　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 | インターネット | 外部メールサーバ | SMTP | 許可 |
| 2 | インターネット | 外部 DNS サーバ | DNS | 許可 |
| 3 | 外部メールサーバ | インターネット | SMTP | 許可 |
| 4 | プロキシサーバ | インターネット | HTTP，HTTPS | 許可 |
| 5 | NTP サーバ | インターネット | NTP | 許可 |
| 6 | 外部 DNS サーバ | インターネット | DNS | 許可 |
| 7 | サーバ LAN | プロキシサーバ | 代替 HTTP | 許可 |
| 8 | 利用者 LAN | プロキシサーバ | 代替 HTTP | 許可 |
| 9 | 管理者 LAN | プロキシサーバ | 代替 HTTP | 許可 |
| 10 | 管理者 LAN | DMZ | SSH | 許可 |
| 11 | DMZ | ログ管理サーバ | syslog | 許可 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 25 | 全て | 全て | 全て | 拒否 |

**注記 1**　項番が小さいルールから順に，最初に合致したルールが適用される。
**注記 2**　項番 12～24 は，送信元及び宛先のどちらもインターネットではないルールである。
**注記 3**　L 社では，代替 HTTP は TCP ポート 8080 を使用している。

L 社ネットワーク上の全てのサーバ，ネットワーク機器及び PC は，NTP サーバと時刻同期を行っている。

L 社での PC に関する環境を図 2 に示す。

- PC は，従業員 1 人につき 1 台貸与されている。
- USB は使用できない設定となっている。
- 光学メディア用のドライブ及びメモリカード用のリーダは，搭載していない。
- DHCP で IP アドレスが動的に付与されるとともに，デフォルトゲートウェイが L3SW に，DNS サーバが内部 DNS サーバに設定される。
- Web ブラウザでのインターネットアクセスは，プロキシサーバを使用するよう設定されている。

**図 2　PC に関する環境（抜粋）**

L 社のサーバ，ネットワーク及び PC は，IT 部が，M 部長の下，リーダの N さんを中心に 10 名で設計，構築，保守・運用を行っている。

L 社では，サーバごとに個別の利用者 ID を IT 部の各従業員に付与しており，サーバの保守・運用時には，その利用者 ID を用いて SSH でサーバに接続し，管理者権限に昇格して作業を行う規則になっている。また，IT 部ではサーバの保守・運用に使用する利用者 ID 及びパスワードの情報を PC に保管してはならない規則となっている。

〔情報漏えいインシデント〕

4 月 23 日に，L 社が加盟しているセキュリティ情報共有団体から L 社に連絡が入った。海外のセキュリティ団体が入手した C&C（Command & Control）サーバの通信履歴の中に，L 社に割り当てられている IP アドレスからの通信が含まれていたとのことであった。セキュリティ情報共有団体からは，C&C サーバの IP アドレス及びポート番号，送信元 IP アドレス並びに C&C サーバ側の受信日時の情報が提供された。受信日時は協定世界時（UTC）で 4 月 16 日 7 時 13 分であった。

〔初期対応〕

M 部長から指示を受け，N さんが確認したところ，送信元 IP アドレスは間違いなく L 社のものであった。また，①この IP アドレスから当該 C&C サーバへの通信が発生していたことも確認できた。送信日時は日本時間で 4 月 16 日 16 時 13 分であった。これらの確認結果を基に，セキュリティ情報共有団体に更なる情報提供を依頼したところ，当該 C&C サーバに送信された情報が提供された。その中には，L 社のファイル配信サーバのホスト名，IT 部の V さんに付与された当該サーバの利用者 ID 及びパスワードが含まれていた。

N さんは，調査結果を M 部長に報告し，次の緊急対応を実施した。

・ファイル配信サーバ上での当該利用者 ID の無効化

・FW による，当該 C&C サーバへの通信の遮断

N さんは M 部長の指示で，漏えい元を特定するために，C&C サーバへの通信の送信元を調査した。その結果を図 3 に示す。

1. 提供された送信元 IP アドレスは，L 社のネットワーク構成から分かるように，[ a ] のものであった。
2. [ a ] のログから，当該 C&C サーバと [ a ] 経由で通信を行っていた機器の IP アドレスを特定したところ，[ b ] のものであった。
3. [ b ] のログから，当該 C&C サーバに [ b ] 経由で HTTP 接続を行っていた機器の IP アドレス，及び [ b ] 接続時の認証に使用した利用者 ID が特定できた。
4. 認証に使用された利用者 ID は，V さんに付与されたものであった。
5. DHCP サーバのログから，上記 3 で特定した IP アドレスが割り当てられていた機器の [ c ] が特定できた。
6. IT 資産管理サーバに保管されている情報によると，当該 [ c ] をもつ機器は，V さんに貸与されている管理番号 0019 の PC であった。
7. V さんは，管理者 LAN に接続した当該 PC から，ファイル配信サーバを含む複数のサーバの保守・運用を行っている。
8. V さんは，これら保守・運用対象のサーバにアクセスするための利用者 ID 及びパスワードを，当該 PC に保管していなかった。

**図 3　C&C サーバへの通信の送信元の調査結果**

N さんは当該 PC をネットワークから切り離した上で，M 部長に図 3 の調査結果を報告した。

〔詳細調査と暫定対応〕

N さんは M 部長の指示で，当該 PC に対するディジタルフォレンジックスによる調査を，セキュリティ専門会社に依頼した。セキュリティ専門会社による調査報告を図 4 に示す。

・当該 PC には，次の 3 種類のマルウェアに感染している痕跡が残っていた。
- ダウンローダ
- キーロガー
- リモートから制御できるトロイの木馬

・これらのマルウェアは，いずれも自ら感染を広げるタイプではない。
・マルウェア内に C&C サーバの FQDN が記述され，C&C サーバへの接続に使用されていた。五つの異なる FQDN が確認できた。
・各マルウェアの C&C サーバとの通信は，次の手順で行われていた。
1. ②プロキシサーバを利用せずに C&C サーバへの接続を試みる。
2. 上記 1 が失敗した場合，Web ブラウザのプロキシ設定を基に，プロキシサーバを利用して接続を試みる。
3. 上記 2 が失敗した場合，PC に保管されている利用者 ID 及びパスワードを窃取して認証突破を試みる。
4. 上記 3 が失敗した場合，ランダムな時間間隔で上記 2 だけを繰り返す。

・最初の感染は 3 月 28 日 13 時 7 分であると考えられる。
・この時刻よりも前にエクスプロイトやマルウェアをダウンロードした痕跡は残っていなかった。
・この時刻よりも後に複数のマルウェアをダウンロードした痕跡が残っていた。
・マルウェアが C&C サーバにアップロードした情報の痕跡は残っていなかった。
・これらのマルウェアは 5 月 14 日時点で L 社が使用していた AV では検知されなかった。

**図 4　セキュリティ専門会社による調査報告（抜粋）**

N さんは，M 部長に図 4 の調査報告を説明した。M 部長は，この調査によって明らかになったマルウェアの特徴から，IP アドレスを基にした FW による通信の遮断では，C&C サーバへの通信を完全には遮断できない可能性があることを指摘した。N さんは，M 部長の指摘に基づき，③この調査で明らかになった C&C サーバへの通信方法を考慮した，新たな遮断方法を検討し，M 部長の承認を得た上で実施した。

〔追加調査〕

N さんは，影響範囲及びマルウェア感染経路を特定するための追加調査を立案し，M 部長から実行承認を得た。追加調査の内容を図 5 に示す。

| | |
|---|---|
| 追加調査 1. | V さんの PC 以外の PC 及びサーバに対する，図 4 で報告されたマルウェアの感染状況調査 |
| 追加調査 2. | ④最初のマルウェア感染後にファイル配信サーバから配信されたファイルの調査 |
| 追加調査 3. | 最初のマルウェア感染後に V さんの利用者 ID でアクセスしたサーバの特定と，アクセス内容の調査 |
| 追加調査 4. | 最初のマルウェア感染前に V さんが受け取った電子メールの調査 |

**図 5　影響範囲及びマルウェア感染経路を特定するための追加調査**

L 社では，AV ベンダとの間で，マルウェアの調査及び対応するウイルス定義ファイルの作成を依頼できる契約を結んでいる。N さんは，図 4 で報告された 3 種類のマルウェアについて，対応するウイルス定義ファイルの作成を AV ベンダに依頼し，そ

のウイルス定義ファイルを用いて追加調査 1 を実施した。その結果，L 社内の他の PC 及びサーバでは，これらのマルウェアの感染は確認されなかった。

N さんは，追加調査 2 として，ファイル配信サーバ上に保存されている操作ログ，アプリケーションプログラムのログ及び配信ファイルのアーカイブを調査した。ファイル配信サーバから 3 月 28 日以降に配信されたファイルは，全て N さんが V さんに指示して配信したものであることが確認できた。

N さんは，追加調査 3 として，L 社内のサーバのうち，V さんの利用者 ID でアクセス可能な全てのサーバ上のアクセスログを調査し，最初のマルウェア感染後に V さんの利用者 ID で当該 PC からアクセスされたサーバを特定した。当該サーバとして，ファイル配信サーバ以外に，NTP サーバ，DHCP サーバ兼内部 DNS サーバ及びプロキシサーバの 3 台が確認できた。これら 3 台のサーバ上の操作ログを更に詳細に確認したところ，各サーバに対する V さんの利用者 ID での操作は，全て N さんの指示に基づく保守・運用作業であり，不正な操作が行われた形跡はなかった。これら 3 台のサーバは，L 社ネットワーク構成において重要であり，サービス停止ができないものであった。N さんは，これらのサーバ上で不正な操作が行われた形跡がなかったこと及びサービス停止ができないことから，⑤これらのサーバ上で実行可能で効果の見込まれる対策を実施した。

N さんは，追加調査 4 として，3 月 1 日から 28 日までに V さんが受け取った電子メールを調査するとともに，V さんへの聞き取りを実施した。その結果，V さんが，3 月 28 日に，インターネットファックスサービスを装った電子メールを受け取り，添付ファイルを開いていたことが判明した。AV ベンダに調査を依頼した結果，このファイルはダウンローダをインストールすることが分かった。

N さんは，これらの結果を M 部長に報告した。

M 部長は，追加調査 3 について，⑥これら 3 台のサーバ上のログに対する改ざんの痕跡が残っていないことを確認したか，N さんに尋ねた。N さんは，ログの改ざんを想定した調査は行っていなかったことを報告し，ログの再調査を実施した。再調査の結果，これら 3 台のサーバ上のログに対する改ざんの痕跡は残っていなかった。N さんは，M 部長に再調査の結果を報告した。

M 部長は，調査結果を了承し，恒久対応としての再発防止策の立案を N さんに指示した。

**設問 1**　〔初期対応〕について，(1)，(2)に答えよ。

(1)　本文中の下線①について，確認の具体的な方法を，30 字以内で述べよ。

(2)　図 3 中の [ a ] ～ [ c ] に入れる適切な字句を，それぞれ 10 字以内で答えよ。

**設問 2**　〔詳細調査と暫定対応〕について，(1)，(2)に答えよ。

(1)　図 4 中の下線②の試みは，L 社の PC からでは必ず失敗するが，FW のログには記録されない。その理由を 35 字以内で述べよ。

(2)　本文中の下線③について，遮断の具体的な方法を 40 字以内で述べよ。

**設問 3**　〔追加調査〕について，(1)～(3)に答えよ。

(1)　図 5 中の下線④の調査は，どのような攻撃を想定したものか。想定した攻撃を 30 字以内で述べよ。

(2)　本文中の下線⑤について，これら 3 台のサーバ上で実施すべき対策を 20 字以内で述べよ。

(3)　本文中の下線⑥について，ログの改ざんの痕跡を確認する方法を 30 字以内で述べよ。