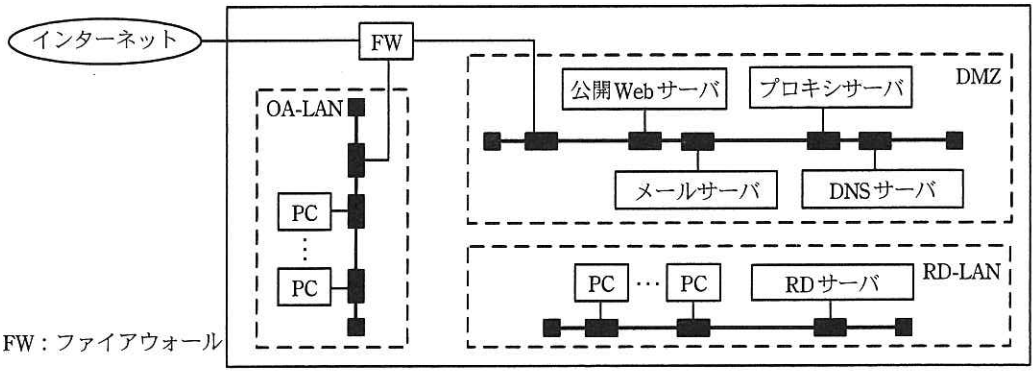
問1　マルウェア解析に関する次の記述を読んで，設問1～3に答えよ。

J社は，新薬の研究開発を行っている従業員数100名の研究所であり，ある特殊な分野の研究開発で世界的に高い評価を受けている。J社のネットワークは，研究開発事業で利用するネットワーク（以下，RD-LANという），外部との情報交換に利用するネットワーク（以下，OA-LANという）及びDMZの三つで構成されている。J社のネットワーク構成を図1に示す。

(1)　RD-LANはRDサーバと十数台のPCで構成されている。RDサーバには，J社において最も機密度が高い情報である新薬の研究報告書が，電子ファイルとして保管されている。機密保護の観点から，RD-LANは，他のネットワークと物理的に隔離されている。RD-LANと他のネットワーク間のデータの受渡しは，J社の情報セキュリティポリシに従ってJ社所有のUSBメモリを介して行われ，必要最小限にとどめられている。

(2)　OA-LANは100台のPCで構成されている。PCは業務に必要な電子メールの送受信及びインターネット上のWebの閲覧に利用されている。

(3)　DMZは，公開Webサーバ，プロキシサーバなどで構成されている。プロキシサーバは，ブラックリストに登録したURLへのWebアクセスを遮断するフィルタリング機能をもっているが，J社では何も登録していない。



注記　OA-LANとRD-LANのネットワークアドレスは異なる。

図1　J社のネットワーク構成

全ての PC，RD サーバ，DMZ の各サーバ及びネットワーク機器には固定の IP アドレスが設定されており，RD-LAN の PC と RD サーバを除いて，デフォルトゲートウェイが設定されている。また，全ての PC，RD サーバ及び DMZ の各サーバにはウイルス対策ソフトがインストールされており，OA-LAN の PC には，Web を閲覧する際に利用する Z ブラウザがインストールされている。現在，最新の Z ブラウザはバージョン 3 であるが，従業員の中には，操作しやすいという理由で，古いバージョン 2 の Z ブラウザを利用している者もいる。また，各サーバではサーバへのアクセスのログを取得している。FW では許可及び拒否する全ての通信のログを取得している。J 社の FW のフィルタリングルールを表 1 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	プロキシサーバ	インターネット	HTTP，HTTPS	許可
2	メールサーバ	インターネット	SMTP	許可
3	DNS サーバ	インターネット	DNS	許可
4	インターネット	公開 Web サーバ	HTTP，HTTPS	許可
5	インターネット	メールサーバ	SMTP	許可
6	インターネット	DNS サーバ	DNS	許可
7	PC	プロキシサーバ	代替 HTTP	許可
8	PC	メールサーバ	SMTP，POP3	許可
9	PC	DNS サーバ	DNS	許可
10	全て	全て	全て	拒否

注記 1　J 社で利用する主要なサービスのポート番号は，次のとおりである。
HTTP : 80，HTTPS : 443，代替 HTTP : 8080，DNS : 53，SMTP : 25，POP3 : 110
注記 2　項番が小さいものから順に，最初に一致したルールが適用される。
注記 3　項番 7～9 の送信元の PC には，RD-LAN 上の PC は含まない。

〔過去のウイルス感染事例〕

J 社では数年前に，公開 Web サーバの情報が愉快犯と思われる攻撃者によって改ざんされるという事件があった。原因は，公開 Web サーバに利用していたミドルウェアが脆(ぜい)弱性のあるバージョンのままとなっていたことにあった。しかも，それだけでなく，公開 Web サーバのウイルス定義ファイルが古かったことから，ウイルスにも感染していた。この時には，J 社のセキュリティ管理者である Y 主任が，セキュリティベンダ X 社の S 氏に協力を仰ぎ，公開 Web サーバのミドルウェアのバージョンを更新するとともにウイルスを駆除した上で，念のため DMZ の全サーバと OA-LAN の全 PC

について最新のウイルス定義ファイルでフルスキャンを行い，ウイルスに感染していないことを確認している。

〔マルウェアの検出〕

今年になって，マルウェアの攻撃による情報漏えい事件の発生が相次いで報道されていることから，S 氏は Y 主任に，マルウェアの感染の有無を確認する検査サービスを提案した。S 氏によると，検査サービスは，専門のアナリストが専用ツールで PC を調査し，疑わしい検体が発見された場合，解析を行うことで，ウイルス対策ソフトでは検出できないマルウェアを検出できるという。Y 主任は，RD-LAN は重要度の高い機密情報が保管されているが，インターネットとは接続されていないので，検査サービスを受けるまでもないと考えた。一方，OA-LAN はインターネットと接続されていることから，念のため OA-LAN の PC のうち 50 台について，検査サービスを受けることにした。検査の結果，5 種類のマルウェアが発見された。Y 主任はマルウェアの影響などを明らかにするために，S 氏にマルウェアの詳細な解析を依頼した。

〔マルウェアの解析結果〕

S 氏は，発見したマルウェア ML1～ML5 の検体を X 社の解析センタに持ち帰り，詳細に解析した。その解析結果の概要を表 2 に示す。

表 2　マルウェアの解析結果の概要

マルウェア名	特徴
ML1	・電子メールに添付された，ML1 が埋め込まれているファイルを PDF 閲覧ソフトで開くと，電子メールの本文の内容に関連する PDF ファイルを表示するとともに，PDF 閲覧ソフトの脆弱性を利用して OS の管理者権限を獲得し，ML2，ML3 を OS のシステムフォルダに配置する。
ML2	・利用者が Z ブラウザのバージョン 2 を利用している場合，Z ブラウザを起動するとその脆弱性を利用して，Z ブラウザのプロセスで動作する。Z ブラウザを終了すると動作を停止する。Z ブラウザがバージョン 3 の場合は，ML2 は動作しない。 ・Z ブラウザで設定されているプロキシサーバの IP アドレス，ポート番号，及びプロキシサーバでの認証の際に利用者が入力した認証情報を窃取し，OS のシステム情報格納領域に保持する。 ・攻撃者が用意しておいた数十の Web サーバ（以下，攻撃者のサーバという）に対して，プロキシサーバ経由で HTTP 通信を試みる。通信に成功すると，ML4 をダウンロードして OS のシステムフォルダに配置する。
ML3	・OS のシステムフォルダに配置されると，攻撃者のサーバに対して，HTTP 通信を試みる。通信に成功すると，ML4 をダウンロードして OS のシステムフォルダに配置する。

表２　マルウェアの解析結果の概要（続き）

マルウェア名	特徴
ML4	・OS のシステムフォルダに配置されると，攻撃者のサーバに，自身をダウンロードしたマルウェアと同じ方法で HTTP 通信を行い，OS の全てのコマンドを，攻撃者のサーバから HTTP 通信を介して遠隔操作可能な状態にする。 ・ML4 に感染した PC と同じネットワークセグメント（以下，セグメントという）内の他の PC，サーバ，ネットワーク機器の存在，空きポート，アプリケーションのバージョンなどの情報を収集し，結果を攻撃者のサーバに送信する。 ・様々なミドルウェアの脆弱性を利用した数百の攻撃用コードをもち，攻撃者の指示によって，ネットワーク上の他の PC，サーバ及びネットワーク機器を攻撃する。攻撃が成功すると，攻撃対象に ML4 自身を感染させる。それと同時に，ML5 を感染させることもできる。
ML5	・ML5 に感染した PC に USB メモリが接続されると，ML5 が自身を USB メモリに感染させる。 ・感染した USB メモリを，未感染の PC に接続したとき，ML5 が自身を感染させ，新たに感染した PC が接続されているセグメント内の PC，サーバ，ネットワーク機器の存在，空きポート，アプリケーションのバージョンなどの情報を収集し，保持する。 ・新たに感染した PC が接続されているセグメント内の PC，サーバなどに ML4 が存在していた場合は，保持している情報を ML4 経由で攻撃者のサーバに送信する。
共通	・ML1～ML5 はパック処理されている。パック処理とは，マルウェア本体をエンコードし，それをデコードするための展開コードを付加して一つのファイルにすることである。ファイル実行時に，展開コードがマルウェア本体をデコードし，実行する。 ・ML3～ML5 は，OS 起動時に自身を自動的に起動するように設定する。 ・ML2～ML5 は，OS のシステムフォルダに配置される際に，ファイルのタイムスタンプを特定のシステムファイルと同じものに書き換える。 ・ML2～ML5 は，感染した PC のパーソナルファイアウォール及び J 社が利用するウイルス対策ソフトのファイアウォール機能を無効にする。

引き続き，S 氏は，OA-LAN の構成機器の情報を調査した。その結果，次の見解に達した。

・4 か月前，複数の従業員に届いた，ML1 が埋め込まれているファイルを，一部の従業員が開いたことで PC がマルウェアに感染した。

・ML1～ML5 は，パック処理に共通した固有の特徴が見られることから，同一の攻撃者によって作られた。

・サーバ，PC がマルウェアに感染すると，その後，攻撃者がマルウェアを削除しても，感染の痕跡が残る。

・痕跡及び①ML3 の活動を示すログが残っていることから，攻撃者が ML3 の活動を隠蔽するために，J 社のある機器のログの改ざんを試みたが，成功しなかった。

・ML4 経由で J 社のネットワーク環境を知った攻撃者によって，ML5 がここ数日の間に送り込まれた。

〔マルウェア解析後の暫定対策〕

解析結果から，S 氏は直ちに対処が必要である旨を，Y 主任に報告した。Y 主任は S 氏の助言を受けて，ML2～ML4 と外部との通信を遮断する設定変更をプロキシサーバで行った。あわせて，②ML2 の活動を阻止するための対策も実施した。Y 主任は，過去のウイルス感染時の対策を参考に，DMZ の全サーバと，OA-LAN の PC のうち検査未実施の 50 台について，マルウェアの検査サービスを依頼したが，S 氏は，“今回はその他に，FW，RD-LAN の PC と RD サーバ及び [a] についても検査すべきである”と助言した。

J 社は S 氏の助言に従ってマルウェアの検査サービスを受けた。その結果，OA-LAN の PC にだけ ML1～ML5 の存在又は感染の痕跡が確認された。

次は，検査の結果に関する Y 主任と S 氏の会話である。

Y 主任：数年前のウイルス感染と同じ攻撃者なのでしょうか。

S 氏　：それは分かりませんが，今回の攻撃は，近年増えている攻撃と特徴がよく似ています。例えば，攻撃者が目的を達成するために，③マルウェアを発見されにくくする工夫をしている点や，侵入先の企業のセキュリティ対策に合わせて攻撃方法を変更している点などです。

Y 主任：侵入先のセキュリティ対策に合わせて攻撃方法を変更するというのは，具体的にはどういうことでしょうか。

S 氏　：ML5 がその代表例と言えます。攻撃者は，ML1～ML4 によって得た情報を基に④J 社のネットワーク構成上のセキュリティ対策を知り，それを突破できるように ML5 を送り込んだのではないかと考えています。仮に今回の攻撃者が，数年前のウイルス感染のような愉快犯であれば，ML5 を送り込まなかったと思います。しかし，今回の攻撃者は目的を達成するために，時間を掛けてでも攻撃を継続するのではないかと考えられます。

Y 主任：当社にとって，どんな被害が想定されるのでしょうか。

S 氏　：過去の同様の攻撃事例，J 社で実施されているリスク評価の結果を踏まえた情報資産の価値，ML5 が送り込まれたことを総合的に考えると，[b] されることが想定されます。

S 氏は更にマルウェアの解析を進め，マルウェアの駆除手順を J 社に提供した。それによって，J 社では OA-LAN の PC からマルウェアを駆除することができた。その後，Y 主任は S 氏の協力を得て，今回のマルウェア感染の根本原因を分析した。その分析結果を基に，PDF 閲覧ソフトのセキュリティパッチ適用，USB メモリへの書出し制限ソフトウェアの導入，従業員教育など，予防的な対策を実施した。

設問 1　〔マルウェアの解析結果〕について，(1)，(2)に答えよ。

(1)　ML4 をダウンロードしたマルウェア名を答えよ。

(2)　攻撃者が ML3 の活動を隠蔽するためにログの改ざんを試みた機器はどれか。マルウェアの特徴と J 社のネットワーク環境を基に答えよ。また，本文中の下線①について，どのような内容のログか。25 字以内で具体的に述べよ。

設問 2　〔マルウェア解析後の暫定対策〕について，(1)～(3)に答えよ。

(1)　本文中の [a] に入れる適切な字句を，本文中の用語を用いて 10 字以内で答えよ。

(2)　ML2～ML4 と外部との通信を遮断するために，Y 主任が行った設定変更を，40 字以内で具体的に述べよ。

(3)　本文中の下線②の対策とはどのようなものか。本文中の記載内容を基に 25 字以内で述べよ。

設問 3　攻撃者の目的について，(1)～(3)に答えよ。

(1)　本文中の下線③の工夫を，マルウェアの機能の観点から二つ挙げ，それぞれ 20 字以内で具体的に述べよ。

(2)　本文中の下線④について，攻撃者が突破を試みた J 社のセキュリティ対策とは何か。30 字以内で具体的に述べよ。

(3)　本文中の [b] に入れる，想定される J 社の被害を 15 字以内で答えよ。