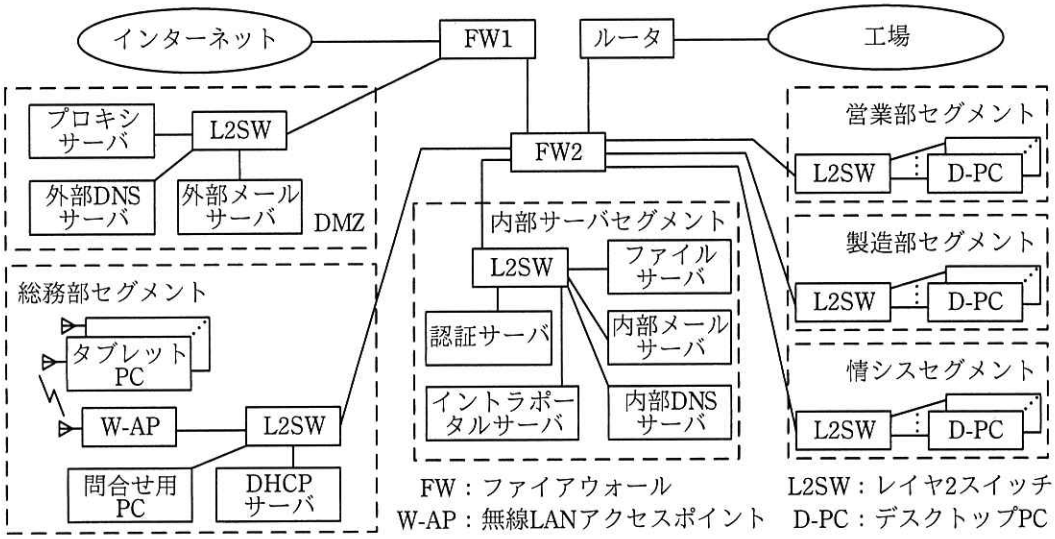
問１　マルウェア感染と対策に関する次の記述を読んで，設問1～6に答えよ。

N社は，従業員数5,000名の化学メーカであり，総務部，営業部，製造部及び情報システム部（以下，情シスという）がある。また，国内に工場がある。N社のLAN構成を図1に示す。



注記1　DMZのサーバには，グローバルIPアドレスが割り当てられている。

注記2　DMZ以外のセグメント及び工場の各機器には，プライベートIPアドレスが割り当てられている。

注記3　タブレットPCには，DHCPサーバによって動的にIPアドレスが割り当てられ，それ以外の機器には，固定IPアドレスが割り当てられている。

図1　N社のLAN構成

N社では，全従業員に一つずつ利用者IDが割り当てられ，その利用者IDとパスワードが認証サーバに登録される。タブレットPC，問合せ用PC及びD-PC（以下この三つを併せて，社内PCという）へのログオン時並びに内部メールサーバ及びファイルサーバへのアクセス時には，認証サーバを使用して認証が実施される。イントラポータルサーバは，認証サーバと連携して，ベーシック認証を使用している。

総務部では，無線LAN接続型のタブレットPCを導入している。無線LANの暗号化では，WPA2を使用している。W-APでは，不正な端末の接続を防ぐための対策として，次の機能を使用している。

・登録済みMACアドレスをもつ端末だけを接続可能とする接続制御

・総務部に所属する従業員の利用者IDだけに接続を許可するIEEE 802.1X認証

IEEE 802.1X認証では，認証サーバと連携して，利用者IDとパスワードを使用している（EAP-PEAP）。

プロキシサーバでは，各機器からの全てのアクセスについて，アクセスログを取得している。

N社では，クラウドサービスを利用して，会社情報や製品情報を公開するWebサイトを運用している。Webサイトには，訪問者からの問合せを受け付けるためのフォームが用意されており，訪問者が問合せ内容を入力すると，その内容が電子メール（以下，メールという）でN社の特定のメールアドレス宛てに送信される。フォームにはファイルを添付する機能はないので，問合せメールにファイルが添付されることはない。万一，このフォーム以外から，この特定のメールアドレス宛てにメールが届いた場合は，そのメールは破棄される。問合せ用PCは，問合せメールを受信するための専用のD-PCで，他の用途には使用していない。また，問合せメールを他の社内PCで受信することはない。問合せ用PCから回答メールを返信する場合，回答メールの送信元メールアドレスには送信専用のメールアドレスを使用している。

FW1のルールを表1に，FW2のルールを表2に示す。

表1　FW1のルール

項番	送信元	宛先	サービス	動作	ログ取得
1	インターネット	外部DNSサーバ	DNS	許可	する
2	インターネット	外部メールサーバ	SMTP，SMTPS	許可	する
3	外部DNSサーバ	インターネット	DNS	許可	する
4	外部メールサーバ	インターネット	SMTP，SMTPS	許可	する
5	外部メールサーバ	内部メールサーバ	SMTP	許可	する
6	内部メールサーバ	外部メールサーバ	SMTP	許可	する
7	内部IP[1)]	プロキシサーバ	代替HTTP	許可	する
8	プロキシサーバ	インターネット	HTTP，HTTPS，FTP	許可	する
⋮	⋮	⋮	⋮	⋮	⋮
15	全て	全て	全て	拒否	する

注記1　SMTPSは，SMTP over TLSを，HTTPSは，HTTP over TLSを示す。

注記2　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[1)]　N社内で使用している全てのプライベートIPアドレスを示す。

表 2　FW2 のルール

項番	送信元	宛先	サービス	動作	ログ取得
1	内部 IP	インターネット	全て	拒否	する
2	内部 IP	プロキシサーバ	代替 HTTP	許可	する
3	内部 IP	内部メールサーバ	SMTP，POP3	許可	する
4	内部 IP	内部 DNS サーバ	DNS	許可	する
5	内部 IP	認証サーバ	LDAP，LDAP over TLS	許可	する
6	問合せ用 PC	全て	全て	拒否	する
7	外部メールサーバ	内部メールサーバ	SMTP	許可	する
8	内部メールサーバ	外部メールサーバ	SMTP	許可	する
⋮	⋮	⋮	⋮	⋮	⋮
22	全て	全て	全て	拒否	する

注記　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。

FW1 と FW2 は，ステートフルパケットインスペクション型である。FW1 には，ペイロードの内容に基づきアプリケーション層での通信の挙動を分析し，マルウェアの動作に伴う不正な通信を検出して遮断できる機能（以下，L7FW 機能という）がある。

〔インシデント発生〕

4 月 12 日 13:00 頃，セキュリティ情報共有団体から，“ある C&C（Command and Control）サーバを調査していたところ，そのサーバに対する N 社からの通信記録を発見した。”との連絡が届き，その通信に関して，表 3 の情報が提供された。

表 3　提供された情報（抜粋）

送信元 IP アドレス	aaa.bbb.ccc.ddd [1]
宛先 IP アドレス	C&C サーバの IP アドレス
宛先 TCP ポート番号	443
通信が開始された時刻	4 月 10 日 14:00:00

注 [1]　aaa.bbb.ccc.ddd は，図 1 中のプロキシサーバの IP アドレスである。

情報提供を受けて，N 社の CSIRT メンバが招集された。N 社の CSIRT のリーダである R 課長は，メンバの P 君に対して，情報処理安全確保支援士（登録セキスペ）である W 主任の支援を受けながら，直ちに状況を確認するよう指示した。P 君は，表 3 の情報の真偽を確かめるために，まず [a] のログを確認して N 社から当

該通信が発信されていたとの確証を得た後，通信を開始した端末を特定するために［　b　］のログを確認した。その結果，問合せ用 PC から C&C サーバに向けて HTTPS と思われるセッションが確立していたことが確認できた。

〔問合せ用 PC の調査〕

状況の報告を受けた R 課長は，問合せ用 PC の調査を指示した。P 君は，決められたインシデント対応手順に従い，まず問合せ用 PC の HDD のコピー（以下，複製 HDD という）を作成した。コピーは①ファイル単位ではなくセクタ単位で全セクタを対象とした。原本である HDD はそのまま保全した。次に，予備の D-PC を新たな問合せ用 PC として設定して，問合せメールへの回答業務を継続できるようにした。

〔感染経路の調査〕

P 君が，複製 HDD の中に残っていた直近 6 か月分の問合せメールについて調査したところ，本文に URL が記載されたメールが幾つかあった。その全ての URL のサイトを調査したが，どのサイトも改ざんの報告はなく，閲覧したとしてもマルウェアに感染するおそれがないサイトだった。

問合せメールによるマルウェア感染が C&C サーバとの通信の原因である可能性は低いと考えた P 君は，調査方針を W 主任に相談し，複製 HDD 内のログ及び関連機器内のログを調査することにした。その結果，図 2 の調査結果が得られた。

(1) 複製 HDD 内のログを調査したところ，4 月 10 日 10:00 に，ある IP アドレス（以下，被疑 IP という）から問合せ用 PC へのリモートデスクトップログオンが成功していた。そのログオンには，総務部の B さんの利用者 ID が使用されていた。
(2) DHCP サーバ内のログを調査したところ，被疑 IP は，4 月 10 日 9:30 から 11:30 までの間，ある PC（以下，被疑 PC という）に割り当てられていた。
(3) W-AP 内のログを調査したところ，4 月 10 日 9:30 に，被疑 PC が発信元である，B さんの利用者 ID を用いた IEEE 802.1X 認証要求が成功していた。
(4) 認証サーバ内のログを調査したところ，4 月 10 日 9:30 及び 10:00 に，B さんの利用者 ID の認証成功の記録があった。一方，4 月 10 日 10:00 から 2 月 1 日まで遡って確認したが，B さんの利用者 ID で認証失敗した記録はなかった。
(5) B さんに話を聞いたところ，4 月 10 日は休暇を取得していたとのことだった。念のために，タブレット PC のログを調査したが，4 月 10 日に使用された形跡はなかった。

図 2　調査結果

この調査結果から，P 君は，攻撃者が B さんの利用者 ID とパスワードを入手し，それらを利用して無線 LAN 経由で問合せ用 PC に不正にログオンしたと判断した。

そこで，W 主任は，不正な PC を W-AP に接続させないための対策として，IEEE 802.1X 認証の方式を EAP-TLS に変更する案を提案した。

また，複製 HDD の分析を続けたところ，マルウェアと思われるファイルが残っており，実行されていた痕跡があった。

〔無線 LAN の脆(ぜい)弱性〕

P 君は，総務部の W-AP は，MAC アドレスによる接続制御をしているのに，攻撃者がなぜ接続できたのか疑問に思い，W 主任に聞いてみた。W 主任は，②WPA2 を使用していても，無線 LAN の通信が傍受されてしまうと B さんが利用しているタブレット PC の MAC アドレスを攻撃者が知ることができることと，③攻撃者が，自分の無線 LAN 端末を総務部の W-AP に接続可能にする方法を P 君に説明した。

また，IEEE 802.1X 認証で使用する B さんの利用者 ID とパスワードを攻撃者が入手する方法について，次のように話した。

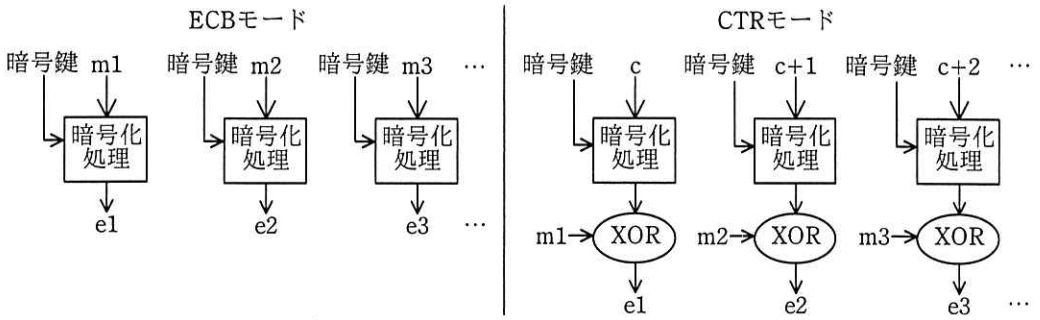
W 主任：最近，KRACKs と呼ばれる WPA2 への攻撃手法が報告され，攻撃用のサンプルコードも公表されている。この攻撃を高い確率で成功させるためには，攻撃者は不正な W-AP を設置し，正規の W-AP と端末との間の中間者として動作させる必要がある。この攻撃が成功すると，WPA2 で暗号化したパケットを解読されるおそれがある。N 社は，4 月 10 日より前に，この攻撃に遭っていながら，攻撃に気付かなかったのではないか。

P 君は，KRACKs について調べてみた。その結果，KRACKs は，攻撃者が特定の通信に介入することによって，WPA-TKIP 及び WPA2 が使用する AES-CCMP というプロトコルの暗号を解読するものであることが分かった。解読の手段は，AES-CCMP の場合，CTR モードにおける初期カウンタ値を強制的に再利用させるものであった。AES-CCMP は，AES というブロック暗号と CTR モードという暗号モードをベースとしている。

〔暗号モード〕

P 君は，暗号モードについても調べてみた。ブロック暗号を利用して長い平文を暗号化するには，平文をブロックに分割し，各ブロックに対して暗号化処理を適用する必要がある。ブロック暗号の適用方法を暗号モードと呼ぶ。最も単純な暗号モードは ECB モードである。

暗号モードのうち，ECB モードと CTR モードの仕組みを図 3 に示す。



注記 1　m1，m2，m3，…はブロック長に分割した平文（以下，平文ブロックという）を，e1，e2，e3，…は平文ブロックを暗号化した暗号文（以下，暗号ブロックという）を，c は初期カウンタ値を表す。

注記 2　XOR は，排他的論理和演算を行うことを示す。

図 3　ECB モードと CTR モードの仕組み

一般的なブロック暗号のブロック長は，64～128 ビット程度なので，暗号化のため TCP/IP パケットをヘッダも含めて平文ブロックに分割すると，④パケットがもつある特徴から，同一端末間の異なるパケットにおいて，同一の平文ブロックが繰り返して現れることが想定される。そのため，その平文の内容は高い確率で推測可能である。仮に TCP/IP パケット全体を ECB モードで暗号化した場合，［　c　］が繰り返して現れることになり，暗号の解読が容易になるおそれがある。

CTR モードでは，暗号ブロックは，［　d　］と［　e　］の排他的論理和である。無線 LAN の場合，攻撃者は暗号化されたパケットを入手可能であるので，その暗号化されたパケットに対応する［　d　］が推測できた場合，［　e　］は容易に算出できる。これらを踏まえると CTR モードでは，初期カウンタ値の再利用の強制によって，同一の［　e　］を使用して異なるパケットの暗号文を作成してしまう可能性がある。

ここまで調べた P 君は，イントラポータルサーバへのアクセスは HTTP であり，かつ，ベーシック認証を使用しているので，WPA2 の通信を解読されると利用者 ID とパスワードの流出に直結してしまうことに気付いた。

〔不審な W-AP の発見と対策〕

無線 LAN 経由で侵入された可能性のある時期には，タブレット PC は KRACKs への対策がされていなかったので，P 君は，KRACKs による攻撃を受けた可能性を調査する必要があると考えた。そこで P 君は，W 主任に相談して，攻撃者が不正な W-AP を設置していないか，N 社の周囲の無線状況を調査した。その結果，総務部の W-AP と同一の SSID が設定された不審な W-AP が，N 社敷地外にあることを発見し，KRACKs による攻撃を受けたと結論付けた。

そこで，W 主任は，KRACKs によって WPA2 の通信が解読された場合でも被害を防ぐ対策として，イントラポータルサーバへのアクセスを HTTPS に変更する案を提案した。

〔L7FW 機能の実効性の確認〕

一方，R 課長は，FW1 には L7FW 機能があることを思い出した。しかし，今回のインシデントでは，FW1 が，マルウェアによる通信を不正な通信として検出した形跡はなく，通過させていた。この件について，R 課長は P 君に調査を指示した。

P 君が，[b] のログを分析したところ，4 月 10 日の 10:00 以降，問合せ用 PC が発信元である HTTPS と思われる通信が，通常よりも大幅に増加していた。これらの通信の大半は，表 3 の C&C サーバの IP アドレスを含む不審な IP アドレスへの通信であったことから，マルウェアによるものと推測された。一方，問合せ用 PC が発信元である HTTP 通信は，ほとんどなかった。

続いて P 君が，FW1 の機能の設定状態を確認したところ，L7FW 機能は有効化されていたが，HTTPS 通信によって送受信されるデータを復号する機能（以下，HTTPS 復号機能という）はライセンスがないので有効化されていなかった。この状態では，HTTPS 通信に対して L7FW 機能は効果がないことも分かった。P 君は，これら一連の内容を R 課長に報告した。

R 課長は，インシデントの調査を終了し，W-AP の IEEE 802.1X 認証の方式を

EAP-TLS に変更する案と，イントラポータルサーバへのアクセスを HTTPS に変更する案を実施するとともに，残りの対策の検討に移ることにした。

〔未知マルウェア対策の改良〕

R 課長は，今後，HTTPS 通信を利用するマルウェアが増えると思われるので，社内 PC について，何らかの対策を打つ必要があると考え，W 主任に検討を指示した。

W 主任は，追加の費用が発生しない範囲で実施できる対策として，プロキシサーバがもつ，特定の URL への接続を禁止するブラックリスト機能の適用を検討した。HTTP 通信の場合，プロキシサーバでは内容を［ f ］ことができる。しかし，HTTPS 通信の場合，社内 PC からプロキシサーバに CONNECT メソッドによって接続要求を送る時点では平文で Web サーバの［ g ］名とポート番号が渡されるが，社内 PC と Web サーバの間で TLS セッションが成立して暗号通信路が確立した後は，プロキシサーバでは内容を［ f ］ことはできない。そのため，HTTPS 通信の場合，実質的にブラックリストに登録できるのが，URL の［ g ］部とポート番号部だけであり，［ h ］部は指定できないことや，そもそもブラックリストに登録すべき URL 情報が必要なタイミングで入手できないことから効果が期待できないとの結論となった。

そこで，追加の費用の発生も視野に入れた対策として，W 主任は，ライセンスの購入による HTTPS 復号機能の有効化（以下，対策 1 という）及び社内 PC のマルウェア対策の強化（以下，対策 2 という）の二つを考えた。それぞれの対策の内容は，表 4 のとおりである。

表 4　検討した対策の内容

項目	対策 1	対策 2
概要	FW1 の HTTPS 復号機能のライセンスを購入し，同機能を有効にする。	未知のマルウェアを検出するソフトウェアを購入し，社内 PC に導入する。
期待する効果	HTTPS 通信であっても，FW1 の L7FW 機能を用いて，マルウェアによる不正通信を検出できる。	（省略）
考慮すべき点	HTTPS 復号機能によって，FW1 の性能低下のおそれがある。 HTTPS 以外の暗号通信には効果がない。	（省略）

W 主任は，⑤マルウェアが窃取した情報を社内 PC から社外に送信する経路が FW1 を経由した HTTPS 以外にもあり，対策 1 と L7FW 機能だけでは全ての経路を検査することはできないので，対策 2 を併せて実施する必要があると考え，P 君に対策 1 及び対策 2 の検討を指示した。

〔対策 1 と対策 2 の検討〕

P 君が，対策 1 と対策 2 の検討に当たり，HTTPS 復号機能の動作の詳細を確認したところ，N 社の LAN では図 4 に示す通信の流れになることが分かった。

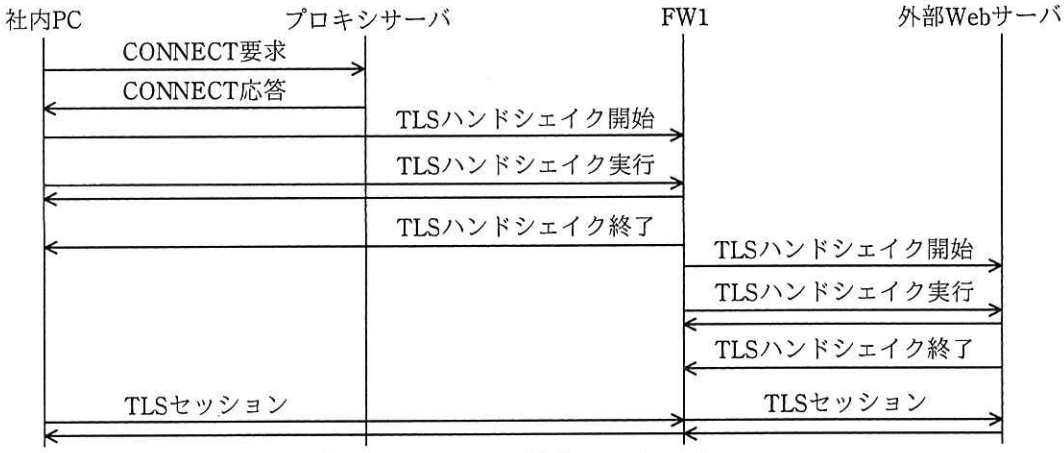


図 4　HTTPS 復号機能の通信の流れ

また，HTTPS 復号機能は，図 5 のとおりになることが分かった。

1. 事前準備
(1) FW1 が発行した自己署名証明書を [i] として全ての社内 PC に登録する。
2. HTTPS 復号機能による外部 Web サーバのディジタル証明書の取扱い
(1) FW1 が，外部 Web サーバへの HTTPS リクエストを検出した際に，宛先 IP アドレスを変換し，FW1 を終端として社内 PC との間で TLS セッションの確立を開始する。
(2) FW1 は，ディジタル証明書及び対応する秘密鍵を作成する。
(3) FW1 は，作成したディジタル証明書及び対応する秘密鍵を利用して社内 PC と FW1 の間で TLS セッションを確立する。
(4) FW1 は社内 PC との TLS セッションの確立とほぼ同時に，クライアントとして外部 Web サーバとの TLS セッションも確立する。
(5) 双方の TLS セッションが確立したら，FW1 はその間で通信内容の転送を行う。
(6) 片方の TLS セッションの確立に失敗した場合は，もう片方の TLS セッションも終了する。

図 5　HTTPS 復号機能の概要

P 君が FW1 の製造元に対策 1 の実施を検討している旨を伝えたところ，無料で 30 日間だけ同機能を利用できる評価用ライセンスの発行を提案されたので，早速，評価用ライセンスを適用し，CSIRT メンバの D-PC から発信される通信で評価してみた。その結果，HTTPS 復号機能には，通信の種類によっては制約があることが分かった。通信の種類と制約を表 5 に示す。

表 5　HTTPS 復号機能における通信の種類と制約（抜粋）

項番	通信の種類	制約の内容	制約の原因
1	j	（省略）	図 4 の流れの中で，FW1 は，社内 PC がもっているクライアント証明書に対応した秘密鍵を利用することができない。
2	外部 Web サーバのサーバ証明書に軽微な不備がある場合に，利用者が不備を無視してアクセスする。	（省略）	外部 Web サーバごとにサーバ証明書の検証条件を変更するということができない。
3	k	（省略）	FW1 には，FW1 の製造元によって安全性が確認された CA のディジタル証明書だけが，信頼されたルート CA のディジタル証明書としてインストールされている。

P 君は，これらの制約の回避方法を運用手順に含めることにした。表 5 の項番 1 の場合は，FW1 の HTTPS 復号機能の例外リストに外部 Web サーバを追加することにした。例外リストに Web サーバを追加すると，例外的に復号機能を適用せず社内 PC と Web サーバの間で直接 HTTPS 通信を行うことができる。例外とする場合には，業務上の必要性があること，及び正当な Web サーバであることを所定の手順で確認することにした。表 5 の項番 2 及び 3 の場合も，必要な内容を運用手順に含めた。

続いて，P 君は，対策 2 の検討を行い，具体策をまとめた。W 主任は，P 君の報告を受けて，対策 1 と対策 2 の実施案をまとめた。実施案は，R 課長から CSIRT 責任者である情シス担当取締役に報告され，承認の上で実施された。以後，N 社では，マルウェアによるインシデントは発生していない。

設問1　本文中の［　a　］，［　b　］に入れる最も適切な機器名を，図1の中から選び答えよ。

設問2　本文中の下線①について，P君がこのようにコピーしたのは，何をどのような手段で調査することを想定したからか。調査する内容を20字以内で，調査の手段を25字以内で具体的に述べよ。

設問3　〔無線LANの脆弱性〕について，(1)，(2)に答えよ。

(1)　本文中の下線②について，知ることができる理由を，30字以内で述べよ。

(2)　本文中の下線③について，具体的な方法を，55字以内で述べよ。

設問4　〔暗号モード〕について，(1)，(2)に答えよ。

(1)　本文中の下線④について，TCP/IPパケットの特徴を，40字以内で述べよ。

(2)　本文中の［　c　］～［　e　］に入れる適切な字句を，それぞれ15字以内で答えよ。

設問5　〔未知マルウェア対策の改良〕について，(1)~(3)に答えよ。

(1)　本文中の［　f　］に入れる適切な字句を，10字以内で答えよ。

(2)　本文中の［　g　］，［　h　］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　インデックス　　イ　サブジェクト　　ウ　シーケンス

エ　ネットワーク　　オ　パス　　カ　ホスト

(3)　本文中の下線⑤について，マルウェアが窃取した情報を社外に送信する方法が複数考えられる。そのうち二つを挙げ，それぞれ35字以内で具体的に述べよ。

設問6　〔対策1と対策2の検討〕について，(1)~(3)に答えよ。

(1)　図5中の［　i　］に入れる適切な字句を，20字以内で答えよ。

(2)　表5中の［　j　］に入れる適切な字句を，40字以内で述べよ。

(3)　表5中の［　k　］に入れる適切な字句を，65字以内で述べよ。