問1　マルウェアの解析に関する次の記述を読んで，設問1～6に答えよ。

R社は，インターネット上でショッピングモール（以下，ECサイトという）を運営する，従業員数3,000名の企業である。ECサイトの総店舗数は5,000店，会員数は300,000名である。

〔R社のネットワーク構成と組織〕

図1は，R社のネットワーク構成である。

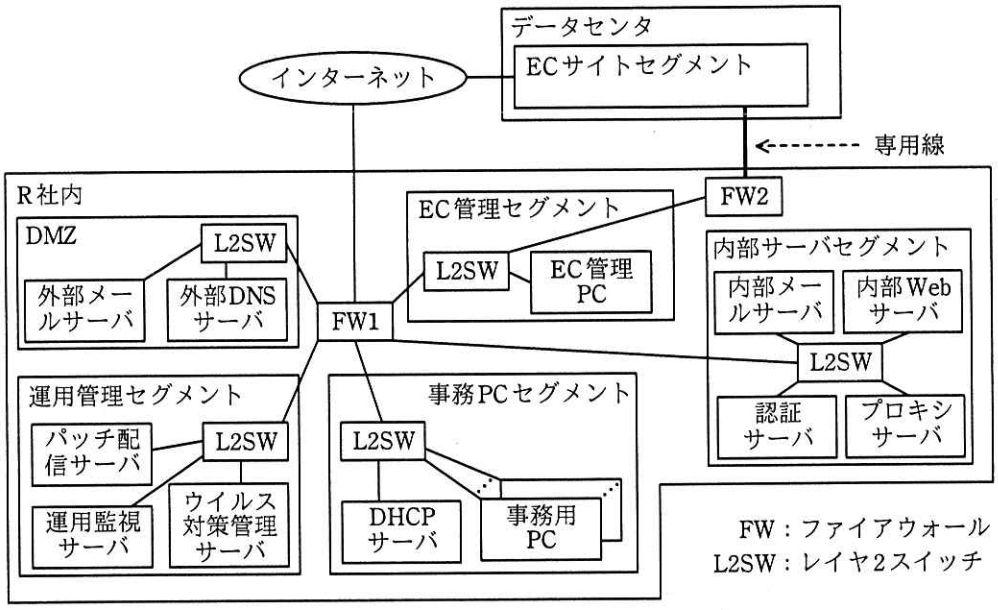


図1　R社のネットワーク構成（抜粋）

R社内では無線LANを使用していない。また，事務用PCとEC管理PCを併せて社内PCと呼んでいる。

R社では，内部Webサーバに対してサーバ証明書を発行するためにプライベートCAを有しており，そのルート証明書を社内PCにインストールしている。プライベートCAは，必要に応じてサーバ証明書を発行することができる。プライベートCAはネットワークに接続されていない。

表1は，R社のネットワーク機器と役割である。

表1　R社のネットワーク機器と役割（抜粋）

機器	役割・仕様	取得しているログ[1]
FW1，2	・各ゾーンの境界を構成して，ゾーン間を接続し，通過するパケットを検査し，許可／遮断を判定する。	・許可ログ ・遮断ログ
外部 DNS サーバ	・社外からの R 社のドメインに対する DNS 問合せに応答する。 ・認証サーバ及び DMZ 内のサーバからの，社外のドメインに対する DNS 問合せを処理する。	なし
外部メールサーバ	・社外からの R 社宛ての電子メール（以下，メールという）を受信し，内部メールサーバに転送する。 ・内部メールサーバからの社外宛てのメールを受信し，社外のメールサーバに転送する。 ・メール転送時にウイルススキャンを行い，検知した場合は転送しない。	・受信したメールの情報 ・転送したメールの情報 ・ウイルススキャンの結果と対処情報
内部 Web サーバ	・従業員に対して，情報提供，勤怠管理などの各種サービスを提供する。	・アクセスログ
認証サーバ	・社内の利用者の認証を処理する。 ・DMZ を除く社内からの DNS 問合せを処理する。R 社のドメインについては自ら応答し，社外のドメインについては，外部 DNS サーバに転送する。	・利用者認証の結果
内部メールサーバ	・社内の利用者のメールボックスを管理するとともに，社内の利用者からのメールの送受信要求を処理する。	・送受信したメールの情報 ・利用者からの送受信要求ログ
プロキシサーバ	・社内 PC から社外の Web サーバへのアクセスを中継する。本サーバ以外から社外の Web サーバへの直接アクセスは，FW1 で遮断される。 ・アクセス先 URL に基づき，アクセス制御を行う。ホワイトリスト／ブラックリストの登録ができる。 ・通信の中継時にウイルススキャンを行い，検知した場合はダウンロードしない。 ・HTTP over TLS（以下，HTTPS という）復号機能はない。	・アクセスログ ・URL フィルタリング結果 ・ウイルススキャンの結果と対処情報
パッチ配信サーバ	・OS と PDF 閲覧ソフトの脆弱性修正プログラムを社内 PC に配信し，適用結果を収集する。	・配信した脆弱性修正プログラムの情報 ・各 PC の脆弱性修正プログラム適用結果
DHCP サーバ	・事務用 PC に対して，DHCP サービスを提供する。 ・IP アドレスのリース期間は，20 時間である。	・DHCP による割当て結果
事務用 PC	・一般事務のために利用される。	なし
EC 管理 PC	・EC サイトを管理するために利用される。	なし

注[1]　機器の障害時や起動時に出力されるログは省略している。

R 社には，情報システム部（以下，IS 部という），開発部，サポート部，営業部及び総務部がある。R 社の各部の役割を表 2 に示す。

表 2　R 社の各部の役割（抜粋）

部署名	役割
IS 部	・R 社のネットワークの構築・運用 ・R 社のネットワークに関する社内規程などの整備 ・R 社のネットワークのセキュリティ監視 ・R 社のセキュリティインシデント（以下，インシデントという）対応 ・プライベート CA の管理
開発部	・EC サイトのアプリケーションソフトウェアの開発と保守
サポート部	・EC サイトの運用管理 ・インシデントを除く障害への対応 ・出店社及び会員向けヘルプデスクの運営

サポート部が EC サイトの運用管理を行う際は，EC 管理 PC を使用している。事務用 PC から FW2 を経由した EC サイトへのアクセスは，FW1 によって遮断される。社内 PC には，パッチ管理プログラムがインストールされていて，パッチ配信サーバから脆弱性修正プログラムの配信を受けると，自動的に脆弱性修正プログラムが適用される。脆弱性修正プログラムは，公表から 1 か月以内に配信する運用としている。社内 PC の利用者には管理者権限を与えておらず，利用者が勝手にプログラムをインストールすることはできない。

〔不審な通信の発見〕

IS 部では，セキュリティ監視業務の一環として 8 時間ごとにプロキシサーバのアクセスログを確認している。ある日の正午過ぎ，その日の午前 4 時から正午までのプロキシサーバのアクセスログの集計情報を確認していた IS 部の U 君は，特定の社内 PC から特定のサーバに多数の HTTPS 通信が行われていることを発見した。U 君は不審に思い，アクセスログを急いで調査した結果，次のことが判明したので，それを午後 0 時 30 分に IS 部の T 部長に報告した。

・1 台の事務用 PC から，社外の同一サーバ（以下，被疑サーバという）に対して多数の HTTPS 通信が，およそ 30 分おきに行われている。

・HTTPS 通信が行われるごとに，数 100k バイトのデータを送信している。

〔インシデントへの初動対応〕

報告を受けた T 部長は，インシデントが発生したと判断して，IS 部内に設置されている CSIRT の責任者である V 課長に対してインシデント対応を開始するよう指示した。V 課長は，CSIRT メンバの M 君を呼び，対応を開始するよう指示した。M 君は，図 2 に示すインシデント対応規程に従って，表 3 の順序で初動対応を行った。

・PC からの不審な通信を発見した場合
(1) 各種のログを調査して，不審な通信の送信元を特定する（以下，特定した送信元を不審 PC という）。
(2) 不審 PC を LAN から切り離す。電源オンの状態のまま移動できる場合は，直ちに解析室へ移動する。電源オンの状態のまま移動できない場合は，①電源をオフにすると消去されてしまう情報について，必要な調査を電源オンの状態で行い，調査終了後，電源をオフにして直ちに解析室へ不審 PC を移動する。
(3) 不審な通信を行っている PC が他にないか確認する。同様の通信を行っている PC を発見した場合は，不審 PC と同じ対処をする。
(4) 解析室内でマルウェア感染の可能性について初期判定を行う。
(5) 不審 PC を利用していた部署に初期判定結果を報告する。
(6) 初期判定でマルウェアの可能性ありと判定したら，マルウェアの動作を特定するために詳細解析を開始する。
(7) 特定されたマルウェアの動作から，被害の有無及び影響範囲を確認するとともに，被害拡大を防ぐために必要な措置を決定し，実施する。

図 2　インシデント対応規程（抜粋）

表 3　M 君の初動対応

順序	概要	詳細
1	送信元特定のためのログ調査	・[a] のログから，被疑サーバを宛先としたエントリを抽出し，送信元 IP アドレスとアクセス時刻を洗い出した。 ・送信元 IP アドレスとアクセス時刻を基に，[b] のログを検索し，アクセス時刻に送信元 IP アドレスを使用していた不審 PC の MAC アドレスを特定した。 ・特定した MAC アドレスを PC 管理台帳中で検索して，不審 PC の利用者，利用部署，設置場所及び不審 PC の管理番号を特定した。不審 PC の利用者は，サポート部の S さんであった。
2	不審 PC の確保	・不審 PC の設置場所に行き，不審 PC に接続されている LAN ケーブルを抜いた。 ・不審 PC はノート PC であったので，電源オンの状態のまま解析室に移動することにした。
3	他の PC からの不審な通信の有無の調査	・移動中，IS 部の U 君に対して，正午以降に不審な通信がないか確認するよう依頼した。U 君の調査の結果，正午から午後 1 時までの不審な通信は，S さんの PC からのものだけであった。

午後1時，不審PCを回収して解析室に設置した後，M君は初期判定を開始した。初期判定は図3に示すIS部のマルウェア初期判定ガイドラインに従って実施した。

1. ゴール
このガイドラインのゴールは，不審PCについて，マルウェアに感染している，感染している疑いがある，感染している疑いが薄いのいずれに当たるかを迅速に判定することである。
2. 方針
不審PCと比較対照用PCを比較して，その差異に基づいて判定する。比較対照用PCとは，OS及びアプリケーションソフトウェアをインストールした後に，最新の脆弱性修正プログラムの適用やウイルス定義ファイルの更新を行った社内PCであり，インシデント対応開始時に作成する。
3. 遵守事項
(a) 不審PCは，解析専用LANだけに接続し，他のLANに接続してはならない。
(b) 比較対照用PCは，比較対照用LAN以外に接続してはならない。また，比較対照用LANには他のPCを接続してはならない。
(c) 不審PCから外部媒体にデータを書き出す場合，又は外部媒体から不審PCにデータを書き込む場合は，所定の手続を経なければならない。
4. 解析チェックリスト
次のチェックリストのうち，不審PCにおいて1件でも該当すれば，マルウェアに感染している疑いがあると判定する。
(1) 動作中のプロセスの一覧を比較対照用PCと突き合わせると，比較対照用PCには存在しないプロセスが存在する。
(2) OSの起動後，操作をしない状態で，比較対照用PCでは発現しない通信が発現する。
(3) OSの起動後，Webブラウザの起動，メールソフトの起動などの操作をした際に，当該操作と関係のない通信が発現する。
(4) OSのシステムファイルの名称，タイムスタンプ及びサイズを比較対照用PCと突き合わせると，差異が存在する。

図3　マルウェア初期判定ガイドライン（抜粋）

M君が図3中の解析チェックリストの(2)について通信の有無を解析したところ，該当する通信を発見した。その通信は，被疑サーバを宛先とした通信であった。M君は，不審PCがマルウェアに感染している疑いがあると判定し，即座にV課長に報告した。不審PCは，マルウェア感染の疑いが濃くなってきたので，CSIRTでは被疑PCという名称で呼ぶことにした。

〔インシデントへの二次対応〕

V課長は，次の指示を出した。

・M君に対して，図3中の解析チェックリストの(3)，(4)について解析した後，詳細

解析を開始すること

・CSIRT メンバの G 君に対して，被疑 PC の利用者及び所属部署に連絡し，聞き取り調査をすること

・CSIRT メンバの Z 君に対して，EC サイトへの影響の有無を調査すること

G 君が，被疑 PC の利用者である S さんから聞き取り調査をした結果は次のとおりであった。

・昨日まで出張が続いていたので，被疑 PC の電源を入れるのは 3 か月ぶりであった。

・朝，被疑 PC の電源を入れ，午前 9 時 30 分までの間，Web ブラウザを開いて幾つか社外の Web ページを閲覧した。その後，今まで会議に出席していたので，それ以外は被疑 PC を操作していなかった。その間，被疑 PC にはログオンしたままであった。被疑 PC は，無操作状態でもスリープ状態にならない設定であった。

・会社から貸与されている出張用スマートフォンでメールを読んでおり，今日は被疑 PC のメールソフトを起動していない。

G 君は，念のため各種ログを調査したが，聞き取り調査の結果との矛盾はなかった。Z 君が実施した調査では，EC サイトへの影響は一切発見できなかった。

〔マルウェアの詳細解析〕

M 君が解析室に戻り，図 3 中の解析チェックリストの (4) についてファイルの差異を解析したところ，不審なファイルを発見した。その後，被疑 PC を図 4 の詳細解析環境に接続し，通信の観測を続けた。表 4 は，詳細解析環境内の各サーバの役割である。

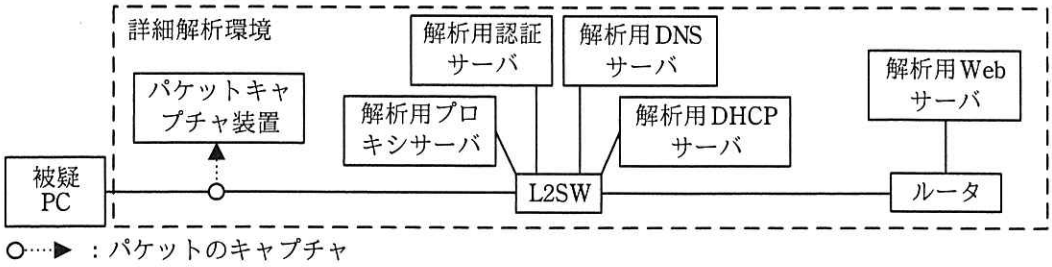


図 4　詳細解析環境

表 4　詳細解析環境内のサーバの役割

サーバ名	役割
解析用プロキシサーバ	社内のプロキシサーバを模する。被疑 PC からの HTTP/HTTPS 通信を中継する。
解析用認証サーバ	社内の認証サーバを模する。被疑 PC の利用者の認証を処理する。また，被疑 PC からの DNS 問合せを処理する。
解析用 DNS サーバ	社内の外部 DNS サーバを模する。解析用プロキシサーバからの DNS 問合せを処理する。任意の DNS 問合せに対して，解析用 Web サーバのアドレスを返す。
解析用 DHCP サーバ	社内の DHCP サーバを模する。被疑 PC に対して，DHCP サービスを提供する。
解析用 Web サーバ	社外の Web サーバを模する。任意の URL に対する HTTP リクエストに対して，同一の HTTP レスポンスを返す。HTTPS にも応答する。

被疑 PC の通信について，観測の結果は次のとおりであった。

(i)　解析用認証サーバに，認証を要求する。

(ii)　解析用プロキシサーバを経由して被疑サーバに HTTPS 通信を行おうとする。

(iii)　被疑サーバ以外を宛先とした HTTP/HTTPS 通信は行わない。

(iv)　被疑 PC と同一サブネット上の IP アドレスに対して，何らかのアクセスをする。

このうち，アクセスの内容が不明であった (iv) を詳細に解析した結果，社内 PC の OS で以前発見された脆弱性（以下，脆弱性 K という）を突いて攻撃を仕掛けていることが判明した。脆弱性 K は，2 か月ほど前に脆弱性修正プログラムと併せて公開されており，R 社でも社内 PC に脆弱性修正プログラムを配信していた。

被疑 PC が (ii)と(iv) の通信を行っている最中に，動いているプロセスを M 君が調査したところ，マルウェアと思われるプロセスを発見した。発見したプロセスは，一通りの処理を終えると自身のファイルの隠蔽処理を行うとともに，自身を所定の時間経過後に起動するための設定を OS に対して組み込み，終了することが判明した。

〔マルウェアの HTTPS 通信の解析〕

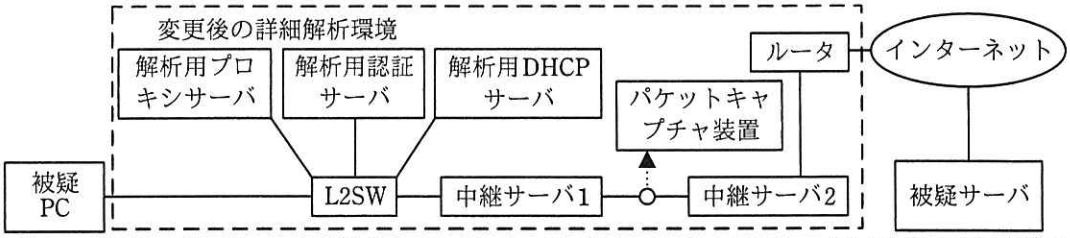
マルウェアのおおよその動きが判明したので，被害の有無を確認するために，被疑サーバにアクセスしている内容を確認すべく，M 君は詳細解析環境を図 5 のように変更した。また，次の三つを行った。

・解析作業による被疑 PC の状態変化を考慮し，被疑 PC の状態を保存するために，

被疑 PC の HDD の複製を作成した。

・解析作業による情報漏えいを防ぐために，被疑 PC 内のファイルのうち，機密情報が含まれているファイルの内容をランダムデータに置き換えた。

・マルウェアが HTTPS 通信を行う際，サーバ証明書の検証を行っている可能性を考慮し，検証が成功するよう，②サーバ証明書を発行し，図 5 の環境に，サーバ証明書と，それに対応する秘密鍵を組み込んだ。



注記　中継サーバ 2 は，R 社が契約している ISP で用意している DNS サーバに DNS 問合せを送る。

図 5　変更後の詳細解析環境

図 5 の環境で被疑 PC が HTTPS 通信を開始した場合の動作は，図 6 のとおりである。

(1) 被疑サーバを宛先とした HTTPS 通信を開始するために，被疑 PC から解析用プロキシサーバにセッション開始要求を送信する。
(2) 解析用プロキシサーバが，HTTPS 通信を中継することによって，被疑 PC と中継サーバ 1 間の通信路が確立する。
(3) 被疑 PC は，確立した通信路を使用して，被疑サーバ宛ての HTTPS 通信でのデータ送受信を開始する。
(4) 中継サーバ 1 は，HTTPS 通信を復号して HTTP 通信に変換した上で，中継サーバ 2 に転送する。応答は，HTTP 通信から HTTPS 通信に変換して解析用プロキシサーバに返す。
(5) 中継サーバ 2 は，HTTP 通信を暗号化して HTTPS 通信に変換した上で，インターネット上の被疑サーバと通信を確立する。応答は，HTTPS 通信から HTTP 通信に変換して中継サーバ 1 に返す。

図 6　変更後の詳細解析環境における通信の概要

M 君は，図 5 の環境で 1～2 時間ほど被疑 PC を稼働させることにした。パケットデータの収集を待つ間，デバッガを用いた解析を行うことにした。

〔デバッガによる解析〕

M 君は，被疑 PC 内の不審なファイルのうち，マルウェアと思われる実行ファイルを所定の手続に従って取り出し，これを検体αと呼ぶことにした。続いて，CSIRT で用意している，デバッガを含むコード解析環境に検体αを投入した。

まず，検体αから読解可能な文字列を探したが，ほとんど存在しなかった。続いて，デバッガによる逆アセンブルを試行した。その結果，得られたアセンブリコードには，通常であれば多数存在するはずのシステムコールの呼出しが少数しかなかった。M 君はブレークポイントを指定して検体αを実行してみたが，コードの冒頭部分が実行されただけで，何ら不正な動作をすることなく終了してしまった。

解析に行き詰まった M 君が V 課長に相談したところ，検体αにはデバッガ環境下で実行していることを検知して実行を停止する機能が組み込まれているのであろうという説明を受けた。マルウェアがデバッガ環境下であることを検知する方法としては，デバッガ環境下であるかどうかを調べるシステムコールを実行する方法があるが，③その他にも幾つかの方法が知られている。

M 君は，検体αのアセンブリコードを読んで，デバッガ検知機能を発見し，これを無効化することに成功した。無効化後の検体を検体α2 と呼ぶことにし，M 君は，検体α2 の解析を次の手法で進めた。

・検体α2 をデバッガにロードした時点で，逆アセンブルを行い，システムコールの呼出し全てにブレークポイントを設定する。
・ブレークするごとにシステムコールの内容を記録し，検体αの動作を推測する。

この結果判明したシステムコールの呼出し回数はごく僅かで，動作の推測には至らなかった。ごく僅かの回数ブレークした後は，ブレークすることなく検体α2 の実行が続き，他の PC を感染させるための通信を試みた上で終了した。この通信を行うには，システムコールの呼出しが必要なはずであるが，ブレークすることはなかった。

またもや解析に行き詰まった M 君が V 課長に相談したところ，パッカーが使われている可能性が高いとの説明を受けた。V 課長は，パッカーの一般的な仕組みについて図 7 と図 8 を使って説明した。

(1) 図 8 の三つの図は，いずれもメモリ上のメモリブロックを表しており，プログラムカウンタ（以下，カウンタという）は上から下へと移動していく。
(2) マルウェアがメモリにロードされた時点では，図 8 のマルウェアのロード時の状態になる。デバッガにロードされたときも同じ状態である。
(3) マルウェアが動作を始めると，図 8 のアンパック処理時の状態になる。この時点で，暗号化済みコード部のデータは実行プログラム部によって復号されて，見せかけのデータ部に書き込まれる。
(4) 見せかけのデータ部への書込みが完了すると，図 8 の本体の実行開始時の状態になる。この時点で，見せかけのデータ部が，マルウェア本体に変わり，攻撃者の意図した動作を開始する。
(5) このようなマルウェアは，ウイルス定義ファイルに基づくウイルススキャンでの検知が著しく難しい。

図 7　パッカーに関する説明

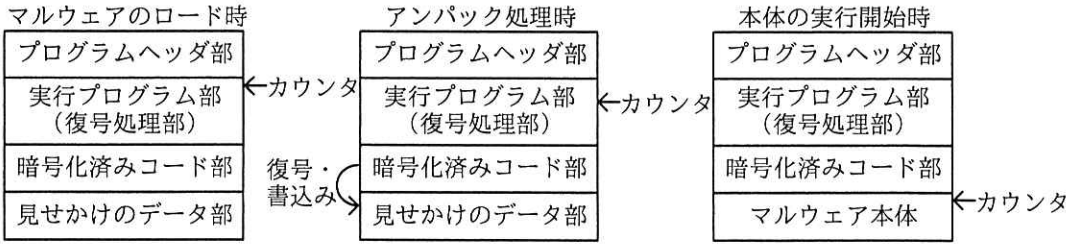


図 8　パッカーの説明図

M 君は，パッカーによる動作を解析して，検体 $\alpha 2$ のマルウェア本体のコードを手に入れることができた。

〔応急措置の決定と実施〕

M 君がデバッガを使って検体 $\alpha 2$ を解析している間に，図 5 の環境において十分なパケットデータが取得できた。このパケットデータから，被疑サーバに送信していた情報が判明した。情報は暗号化されていたが，検体 $\alpha 2$ のマルウェア本体から取り出した鍵を使って復号したところ，平文を得ることができた。

その結果，次の三つが被疑サーバに送信されていることが確認できた。

・被疑 PC 内に一時的に保存された認証情報（利用者 ID と，パスワードのハッシュ値を含む）
・解析用認証サーバから取得した認証情報（利用者 ID だけを含み，パスワードのハッシュ値を含まない）
・OS の設定情報及びシステムファイルのファイル名の一覧

M 君の報告を受けた V 課長は，マルウェアの動作の特定並びに被害の有無及び影響範囲の確認ができたと考え，これ以上の被害拡大を防ぐために，表 5 の応急措置を即時実施することを T 部長に進言した。

表 5　インシデントに対する応急措置

措置の目的	マルウェアの動作に対応した応急措置
被疑サーバへの HTTPS アクセスの禁止	・[c] に被疑サーバを登録するとともに，念のため FW1 のルールを変更する。
マルウェアの感染の防止	・全ての社内 PC について，[d]。
マルウェアによる不正なプロセスの実行の禁止	・解析の結果，判明したマルウェアのプログラム名を，社内 PC の OS に，実行禁止プログラムとして登録する。
窃取されたアカウント情報の悪用の防止	・被疑 PC 内にキャッシュされていた認証情報に含まれる利用者のアカウントについて，[e] を行う。

〔感染経路の特定と対処〕

V 課長は，再感染を防止するために，M 君に感染経路を特定するよう指示した。M 君は，S さんからの聞き取り調査の内容から，被疑 PC が社外の Web ページを閲覧した際にマルウェアに感染した可能性が高いと考え，表 6 の手順で感染経路の特定を目指した。

表 6　感染経路の特定手順

順序	概要	詳細
1	被疑 PC の IP アドレスの特定	・初動対応において特定済みである。
2	アクセス先 URL の一覧取得	・[a] のログを参照し，今日被疑 PC がアクセスした社外の URL の一覧を作成する。
3	URL の内容確認	・URL の一覧中の各 URL について，URL の安全性を評価する Web サイトで評価結果を確認する。 ・URL の一覧中の各 URL にアクセスし，不審な内容が存在しないか確認する。

確認したところ，URL の一覧に記載された Web サイトの中で，インターネット上の EC サービスに関するニュースを提供している Q 社の Web サイト内の 1 ページ（以下，N ページという）に，不自然な形でスクリプトが埋め込まれていることが発見された。このスクリプトは複雑であり，M 君が読んでも動作を把握することがで

きなかった。そこで V 課長が N ページを分析してみたところ，次のことが分かった。

・N ページを Web ブラウザで開くと，Q 社のドメイン外のサイトから PDF ファイルをダウンロードして，PDF 閲覧ソフトで開く。

・N ページから不自然なスクリプトを削除したページを Web ブラウザで開くと，N ページと表示に違いはないが，PDF ファイルはダウンロードされない。

V 課長と M 君は，N ページが改ざんされ，マルウェアを配布していると推測した。しかし，比較対照用 PC をインターネットにアクセスできる環境とした上で N ページを開いても，PDF の内容が表示されるだけで，不審なファイルや不審なプロセスが生成されることはなく，マルウェアに感染しなかった。

困った M 君が V 課長に相談したところ，④比較対照用 PC の状態と，今日の勤務開始時刻時点の被疑 PC の状態では，重要な点が異なっている可能性が高いので，[f] のログを確認してみるようアドバイスを受けた。[f] のログを確認した M 君は，比較対照用 PC の状態を，今日の勤務開始時刻時点の被疑 PC と同一の状態にした上で，もう一度 N ページにアクセスした。その結果，不審なプロセスや検体 α などの不審なファイルが生成されていた。このことによって，マルウェア（以下，マルウェア L という）に感染したことが分かった。

この時点で，マルウェア L の感染経路は N ページを閲覧したことによるものと判断することができた。この報告を受けた V 課長は，次の対応策の実施を T 部長に進言した。

・当面の間，社内 PC から Q 社の Web サイトへのアクセスを遮断する。

・過去 1 週間の [a] のログを調査し，Q 社の Web サイトを閲覧した社内 PC を洗い出し，それらの PC について，[a] のログと [f] のログを突き合わせ，⑤マルウェア L に感染する可能性があったかどうか判断する。

・Q 社に対して適切な方法で，Web サイトが改ざんされている旨を伝える。

調査の結果，S さんの PC 以外に感染した社内 PC は存在しないことが確認できた。最後に，検体及び複製 HDD を消去し，インシデント対応を無事終了した。

〔インシデント対応の事後評価〕

V 課長は，今回のインシデント対応を振り返り，1 日以内に全ての対応を完了したこと，マルウェア L に感染した PC も 1 台だけであり，拡大を防げたことから，対応は成功したと考えた。

後日，V 課長は，今回のインシデント対応に当たったメンバを招集し，事後評価を実施した。その結果，⑥ディジタルフォレンジックスという観点から，実施するタイミングを見直す必要がある作業があること，⑦被疑 PC の利用者の業務継続を考慮して対応する必要があることが課題として挙げられた。さらに，今回のマルウェア L の場合，図 3 中の解析チェックリストではマルウェア感染を発見できない場合があるので，解析チェックリストの項目に，“ g を比較対照用 PC と突き合わせると，差異が存在する”という項目を追加する必要があるとの結論に至った。

その後，Q 社から Web サイトの改ざんの原因の判明と復旧の連絡が届いたので，内容を確認後，Q 社 Web サイトへのアクセス遮断を解除した。

設問 1　〔インシデントへの初動対応〕について，(1)，(2)に答えよ。

(1)　図 2 中の下線①について，該当する情報を，解答群の中から全て選び，記号で答えよ。

解答群

ア　HDD のパーティションテーブルの情報

イ　OS のバージョンの情報

ウ　画面に表示されているウィンドウの名称一覧

エ　起動しているプロセスの一覧

オ　脆弱性修正プログラムの適用状況

(2)　表 3，表 6 及び本文中の a ，表 3 中の b に入れる適切な字句を，図 1 中の構成要素から選び，答えよ。

設問 2　〔マルウェアの HTTPS 通信の解析〕について，(1)～(3)に答えよ。

(1)　本文中の下線②について，発行する証明書において，サブジェクトのコモンネームは，どのサーバの何を組み込むべきか。15 字以内で答えよ。

(2)　本文中の下線②について，発行した証明書と対応する秘密鍵を組み込むべきサーバの名称を，図 5 中の機器から選び，答えよ。

(3) 図 5 の解析環境を正常に動作させるためには，図 5 中の解析用プロキシサーバ上で特別な設定を行う必要がある。その設定内容を，45 字以内で述べよ。

設問3 〔デバッガによる解析〕について，(1)，(2)に答えよ。

(1) 本文中の下線③について，どのような方法があるか。40 字以内で述べよ。

(2) 図 7 の(5)について，検知が著しく難しい理由を，60 字以内で述べよ。

設問4 〔応急措置の決定と実施〕について，(1)～(3)に答えよ。

(1) 表 5 中の [c] に入れる適切な字句を，20 字以内で述べよ。

(2) 表 5 中の [d] に入れる適切な措置を，新規にソフトウェアや機器を調達しない前提で，30 字以内で述べよ。

(3) 表 5 中の [e] に入れる適切な字句を，10 字以内で答えよ。

設問5 〔感染経路の特定と対処〕について，(1)～(3)に答えよ。

(1) 本文中の下線④について，どのような点が異なっていたか。30 字以内で述べよ。

(2) 本文中の [f] に入れる適切な機器名称を，表 1 中の機器から選び，答えよ。

(3) 本文中の下線⑤について，どのような場合に感染の可能性があったと判断するか。55 字以内で具体的に述べよ。

設問6 〔インシデント対応の事後評価〕について，(1)～(3)に答えよ。

(1) 本文中の下線⑥について，実施するタイミングを見直す必要がある作業とは何か。20 字以内で述べよ。

(2) 本文中の下線⑦について，どのような対応をすべきか。25 字以内で具体的に述べよ。

(3) 本文中の [g] に入れる適切な内容を 40 字以内で述べよ。