平成 29 年度 春期 情報処理安全確保支援士

＜午後Ⅱ 解答・解説＞

＜問１＞ マルウェアの解析

■設問１

〔試験センターによる解答例〕

(1) ウ，エ

(2) a：プロキシサーバ

b：DHCP サーバ

（1）

ア　HDD のパーティションテーブルの情報は OS が常に保持している（ディスクに書き込まれている）ため，電源をオフしても消去されることはない。

イ　OS のバージョン情報は OS が常に保持しているため，電源をオフしても消去されることはない。

ウ　画面に表示されているウィンドウの名称はメモリにしか存在しないため，電源をオフすると消去される。

エ　起動しているプロセスの情報はメモリにしか存在しないため，電源をオフすると消去される。

オ　脆弱性修正プログラムの適用状況は OS が常に保持しているため，電源をオフしても消去されることはない。

（2）

a：被疑サーバを宛先とした送信元 IP アドレスとアクセス記録を洗い出し，被疑 PC がアクセスした社外の URL の一覧を作成するには，プロキシサーバのアクセスログが必要であ

る。

b：送信元 IP アドレスとアクセス時刻を基に，当該 IP アドレスを使用していた不審 PC の MAC アドレスを特定するには，DHCP サーバのログが必要である。

■設問２

〔試験センターによる解答例〕

(1)　被疑サーバの FQDN（10 字）

(2)　中継サーバ１

(3)　被疑サーバへの HTTPS 接続要求を，中継サーバ１に到達するようにする。(35 字)

(1)　マルウェアは被疑サーバとの HTTPS 通信を行うように組み込まれているので，当該 HTTPS 通信の確立時の検証を成功させるには，サーバ証明書のサブジェクトのコモンネームを被疑サーバの FQDN にしておく必要がある。

(2)　図 6 の（2）に「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」とあるように，図 5 の解析環境においては，被疑 PC が，中継サーバ 1 を被疑サーバと誤認識して通信を行うようにしている。したがって，発行した証明書と対応する秘密鍵は中継サーバ 1 に組み込んでおく必要がある。

(3)　上記 (2) で，中継サーバ 1 にサーバ証明書と対応する秘密鍵を組み込んでおいても，それだけで被疑 PC と被疑サーバの通信をコントロールすることはできない。被疑 PC は，インターネット上の被疑サーバに対する HTTPS 接続要求を解析用プロキシサーバに送ってくるが，解析用プロキシサーバには，この要求が中継サーバ 1 に到達するように設定しておく必要がある。

■設問３

〔試験センターによる解答例〕

(1) 実行中プロセスの一覧から既知のデバッガのプロセス名を探す。(29 字)

(2) 暗号鍵を変えてパック処理すると暗号化済みコード部が変化し，ウイルス定義ファイルに登録されていないファイルとなるから (57 字)

(1) マルウェアが自己防衛のためにデバッガの存在を検知する方法として，次のようなものがある。

・開かれているウィンドウの名前を取得し，既知のデバッガを探す

・実行中のプロセスの一覧を取得し，既知のデバッガのプロセス名を探す

・OS の API を使用してデバッガの存在を検知する

(2) ウイルス定義ファイルに基づくウイルススキャンはマルウェアのロード時に行われるが，この時点ではマルウェアの本体は暗号化され，暗号済みコード部に格納されている状態である。マルウェア対策ベンダに提供された検体についてはウイルス定義ファイルに登録されるが，暗号鍵を変えてパック処理をすれば暗号化済みのコード部は全く異なるものに変化するため，無数のパターンが存在し得る。そのため，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困難になる。

■設問 4

〔試験センターによる解答例〕

(1) c：プロキシサーバのブラックリスト (15 字)

(2) d：脆弱性 K に対応した脆弱性修正プログラムを適用する (24 字)

(3) e：パスワードの変更 (8 字)

(1) 表 1 のプロキシサーバの役割・仕様に「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」とある。R 社のネットワーク構成で被疑サーバへの HTTPS アクセスを禁止するには，FW1 のルールを変更するか，プロキシサーバのブラックリストに被疑サーバを登録することになる。表 5 に「…とともに，念

のため FW1 のルールを変更する」とあることから，［ c ］にはプロキシサーバのブラックリストが入る。

（2） 〔マルウェアの詳細解析〕に「詳細に解析した結果，脆弱性 K 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」とある。新規に機器やソフトウェアを調達しない前提であることからも，マルウェアの感染防止のために行う応急措置は，全ての社内 PC について，脆弱性 K に対応した脆弱性修正プログラムを適用することである。

（3） 窃取されたアカウント情報の悪用を防止するためには，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，パスワードを変更する必要がある。

■設問 5

〔試験センターによる解答例〕

（1） PDF 閲覧ソフトの脆弱性修正プログラムの適用状況（24 字）

（2） f：パッチ配信サーバ

（3） PDF 閲覧ソフトの脆弱性修正プログラムを適用する以前に，Q 社の Web サイトを閲覧した場合（45 字）

（1） V 課長が分析した結果，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 閲覧ソフトで開くが，N ページから不自然なスクリプトを削除すると PDF ファイルはダウンロードされない，ということから，この PDF ファイルが PDF 閲覧ソフトの脆弱性を突いて感染するタイプのマルウェアであると推測できる。

比較対照用 PC 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がないのは，PDF 閲覧ソフトの脆弱性が修正済みであり，今日の勤務開始時点の被疑 PC とは PDF 閲覧ソフトの脆弱性修正プログラムの適用状況が異なっていたと考えられる。

（2） 表 1 より，各 PC の脆弱性修正プログラムの適用結果については，パッチ配信サーバのログで確認できることがわかる。

（3） 上記（1）より，PDF 閲覧ソフトの脆弱性修正プログラムを適用する前に，Q 社の Web サイトを閲覧した場合にマルウェア L に感染する可能性があったと判断できる。

■設問 6

〔試験センターによる解答例〕

（1） 被疑 PC の HDD の複製作業（13 字）

（2） 被疑 PC の解析中に使用する代替 PC の払出し（21 字）

（3） g：PC 起動時や所定の時刻などに特定のプログラムを自動的に起動する設定内容（35 字）

（1） マルウェア感染の可能性がある PC 等に何らかの調査行為を行った結果，証拠となるデータが更新されたり，失われたりする可能性がある。そのため，ディジタルフォレンジックスの観点からは，PC がマルウェアに感染した可能性があると判明した時点で，一刻も早く当該 PC のメモリダンプを取得したり，HDD を複製したりする等して，解析の対象となるデータの保全を図るべきである。しかし，R 社では今回のインシデント対応において，〔インシデントへの初動対応〕で不審 PC を回収した時点では解析データの保全を行っておらず，〔マルウェアの HTTPS 通信の解析〕の段階でようやく被疑 PC の HDD の複製作業を行っている。上記の理由により，被疑 PC の HDD 複製作業を PC 回収の時点で行うなど，手順の見直しが必要である。

（2）被疑 PC の解析及び復旧には長時間を要する可能性が高いため，業務の継続を考慮し，被疑 PC の回収時に，当該 PC の利用者に代替 PC を貸与する必要がある。

（3） 〔マルウェアの詳細解析〕で，マルウェアと思われるプロセスを発見し，調査した結果，当該プロセスは，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。この挙動では，外部への通信は発生せず，OS のシステムファイルに変更がなく，終了後はプロセスとしても検出されないため，図 3 の項番 4 の解析チェックリストで

はマルウェアの感染を発見できない可能性がある。これを改善するには，今回のマルウェアの挙動を踏まえ，「PC 起動時や所定の時刻などに特定のプログラムを自動的に起動する設定内容を比較対象用 PC と突き合わせると，差異が存在する」という項目を解析チェックリストに追加する必要がある。

＜問２＞　社内システムの情報セキュリティ対策強化

■設問１

〔試験センターによる解答例〕

(1)　a：SMTP over TLS

(2)　b：ウ

　　d：ア

(3)　c：内部メールサーバ

（1）　サーバ証明書を用いて SMTP 通信をセキュアにする方式であるから，該当するのは「SMTP over TLS」である。これにより，内部メールサーバと外部メールサーバとの通信を TLS によってセキュアに行うことができる。

（2）
b：解答群の中で，メールの転送を行うのは MTA である。

d：解答群の中で，メールをメールボックスに格納するのは MDA である。そのほかは次の通り。

・MSA：メールの投稿受付け，ユーザ認証等を行う。

・MUA：クライアント環境でメールの発信（投稿），受信等を行う。（一般的なメールクライアントソフトウェア）

（3）　宛先メールアドレスが A 社ドメイン名，A 社サブドメイン名であった場合に外部メ

ールサーバがメールを転送する先であるから，該当するのは内部メールサーバである。

■設問 2

〔試験センターによる解答例〕

(1) e：プロキシサーバ

f：URL がマルウェア X 中に保持された URL である（23 字）

(2) g：外部メールサーバ

h：インターネット上のサーバに転送された（18 字）

(3) 外部 DNS サーバの設定変更内容：内部 DNS サーバからの DNS 問合せを拒否する。（23 字）

内部 DNS サーバの設定変更内容：インターネット上のサーバ名についての DNS 問合せを拒否する。（30 字）

(4) i：社内専用のドメイン名以外の FQDN が書かれている（24 字）

（1） 表 2 の概要にあるように，各サーバからインターネット上の C&C サーバへの HTTP 通信及び HTTP over TLS 通信の有無を確認するには，プロキシサーバのログを確認する必要がある。図 2 の（2）より，マルウェア X はダウンロード型であり，内部に C&C サーバの URL を保持していることがわかる。したがって，ログに記録された URL がマルウェア X 中に保持されている URL と合致することを条件としてログを抽出すればよい。

（2） マルウェア Y によるメール送信を確認するには，外部メールサーバのログを，マルウェア Y によって送信されたメールが「インターネット上のサーバに転送された」という条件で抽出する必要がある。

（3） 図 2 のマルウェア Y に関する次の情報に着目して対策を考察する。

・マルウェア中に多数の FQDN が保持されている。

・OS の設定で指定された DNS サーバに対して，マルウェアに保持された FQDN の全ての TXT レコードを問い合わせ，得られた文字列を指示として解釈し，動作する。

これは，DNS の TXT レコードによって指令を受け取るタイプのマルウェアであり，近年実際にその存在が確認されている。

このようなマルウェアに対抗するためには，外部 DNS サーバ，内部 DNS サーバの DNS 問合せに関する設定を次のように変更するべきである。

＜外部 DNS サーバ＞
社内 PC はプロキシサーバ経由でインターネット上のサーバ名についての DNS 問合せができるため，内部 DNS サーバからの DNS 問合せを拒否する。

＜内部 DNS サーバ＞
上記と同じ理由により，内部 DNS サーバは社内環境の名前解決のみを行うこととし，インターネット上のサーバ名についての DNS 問合せを拒否する。

（4） マルウェア Y は自身が保持するインターネット上の FQDN に対して TXT レコードを問い合わせるという特徴があるので，内部 DNS サーバのログから，社内専用のドメイン名以外の FQDN が書かれているログを抽出することで検出することが可能である。

■設問 3

〔試験センターによる解答例〕

（1） ファイルを暗号化しない。（12 字）

（2） サーバ及び PC でのウイルス検出結果をシステム部運用グループに通知する機能（36 字）

（1） 問題点（あ）に「SMTP ウイルススキャンでは，暗号化されたファイルについてウイルス検出ができない」とあることからわかるように，図 3 中の（4）のウイルススキャン機能を有効なものとするためには，ファイルを暗号化せずにアップロードする必要がある。

（2） PC 利用者からのマルウェア感染の申告に基づく対応では遅すぎるという問題への対応策としてウイルス対策集中管理ソフトを導入するのであるから，求めるのは，サーバや PC でのウイルス検出結果を集中管理し，それを速やかにシステム部運用グループに通知する機能である。

■設問 4

〔試験センターによる解答例〕

j：PC-LAN

表 5 の内部メールサーバの設定では，項番 3 で，A 社ドメイン名，もしくは A 社サブドメイン名以外の宛先（インターネット宛て）のメールについて，転送元が A 社が利用しているプライベートアドレスであれば，外部メールサーバに転送していた。そのため，図 2 (6) のように，マルウェア Y によってコンテンツ管理 Web サーバからインターネット上のサーバに対して不審なメールが転送されるのを防ぐことができなかった。

これを改善し，内部 DNS サーバ及び業務 LAN のサーバから内部メールサーバに転送されるインターネット宛てのメールを拒否するには，表 7 の項番 2, 3 の転送元 IP アドレスの条件として，［ j ］に「PC-LAN」を設定するのが有効である。

■設問 5

〔試験センターによる解答例〕

業務 LAN の全てのサーバにホスト型 IPS ソフトウェアを導入する。(32 字)

業務サーバ間の必要な通信を維持しながら業務 LAN サーバ間のマルウェア感染を防止するには，ホスト型 IPS ソフトウェア（HIPS）が有効である。HIPS は，サーバ装置等のホスト上で動作し，当該ホストに対する不審な通信を遮断したり，不正なプロセスの実行を防いだりする機能等がある。これを業務 LAN の全てのサーバに導入することで，必要な通信を維持しながらセキュリティを高めることが可能となる。HIPS はクライアント PC 環境等で動作するパーソナルファイアウォールと同様な働きをするが，製品によってはファイアウォールや他のセキュリティ対策製品との連携機能を持つものなどもある。