はじめに

本記事では「令和元年度 秋季 情報処理安全確保支援士試験 午後I問題」の解説を行います。

問題文へのリンクは 令和元年度 秋季 情報処理安全確保支援士試験 午後I問題 です。

注意

出展: 令和元年度 秋季 情報処理安全確保支援士試験 午後I

問1 電子メールのセキュリティ対策

設問1

メールの送信元であるFROMアドレスには、いわゆる一般的なメールクライアント上で表示されるようなHeader-FROMアドレスと、メール配送に関する問題が発生した際の返送先となるEnvelope-FROMアドレスの2種類があります(TOアドレスも同様に2種類存在します)。

さて、SMTPコマンドを用いてメールを送信する際の流れの一例を以下に示します。

```
EHLO <SMTP ClientのFQDN>
MAIL FROM: <Envelope-FROMアドレス>
RCPT TO: <Envelope-TOアドレス>
DATA
<メール本文>
.
QUIT
```

上記から分かるように、Envelope-FROMアドレスの指定にあたっては`MAIL FROM`コマンドを利用します。

よって、空欄aには**MAIL FROM**が入ります。

設問2

(1)

SPF(Sender Policy Framework)は、電子メールにおける送信元ドメインの認証技術です。具体的には、以下のようにして送信元ドメインの認証が行われます。

- 送信側は、自ドメインを管理するDNSサーバのSPFレコードにメールの送信元として有効であるサーバのIPアドレスを登録する。

- 受信側は、受信したメールの送信元アドレスに対応するDNSサーバへSPFレコードを問い合わせ、登録されているIPアドレスと一致するかどうか検証する。

上記の流れを考慮すると、SPFによる認証を行うには以下の条件が必要です。

- 送信側のDNSサーバにSPFレコードが登録されている。
- 受信側のメールサーバでSPFの検証が行われている。

さて、図3に示されている攻撃を簡潔にまとめると以下のようになります。

- 攻撃1 N社でのなりすましメールの**受信**。
- 攻撃2 N社を起点とするなりすましメールの**送信**。

まず、項番4について考えます。

- 攻撃1(受信)は防げません。なぜなら、取引先のDNSサーバはSPFへの対応を行なっていないため、N社のメールサーバにおいてSPFレコードの検証ができないからです。よって空欄bは×です。
- 攻撃2(送信)も防げません。なぜなら、取引先のメールサーバはSPFの検証を行わないからです。よって空欄cは×です。

次に、項番6について考えます。

- 攻撃1(受信)は防げません。なぜなら、N社のメールサーバはSPFの検証を行わないからです。よって空欄dは×です。
- 攻撃2(送信)も防げません。なぜなら、取引先のメールサーバはSPFの検証を行わないからです。よって空欄eは×です。

次に、項番7について考えます。

- 攻撃1(受信)は防げません。なぜなら、N社のメールサーバはSPFの検証を行わない上に、取引先のDNSサーバはSPFへの対応を行なっていないからです。よって空欄fは×です。
- 攻撃2(送信)は防ぐことができます。なぜなら、N社のDNSサーバはSPFへの対応を行なっており、かつ取引先のメールサーバはSPFの検証を行うからです。よって空欄gは○です。

最後に、項番13について考えます。

- 攻撃1(受信)は防げません。なぜなら、N社のメールサーバはSPFの検証を行わないからです。よって空欄hは×です。
- 攻撃2(送信)も防げません。なぜなら、N社のDNSサーバはSPFへの対応を行なっていないため、取引先のメールサーバにおいてSPFレコードの検証ができないからです。よって空欄iは×です。

(2)

SPFレコードは、DNSにおいてTXTレコードとして公開します(SPFレコードも存在しますが、互換性等の関係でTXTレコードが用いられることが一般的です)。

SPFレコードの書式は以下の通りです。

```
<FQDN> IN TXT "<バージョン> <定義>"
e.g. example.com. IN TXT "v=spf1 +ip4:x.y.z.w -all"
```

このうち、バージョンは問題文の`v=spf1`の部分です。

さて、肝心の定義の部分は`+ip4:[ j ] -all`と記述されています。

このうち、`-all`とは「設定された以外のアドレスを当該ドメインのメールサーバとして一切認証しない」という設定です(ちなみに、正当なメールであっても認証に失敗する恐れがあることを示すための`~all`といった緩めの設定もあり、これはSoftFailと呼ばれます)。

前半の部分は`ip4:`と書かれていることからわかるように、IPv4のIPアドレスを設定します。図2からわかるように、N社のグローバルIPアドレスは`x1.y1.z1.1`であるため、空欄jは**x1.y1.z1.1**です。

(3)

「... (メールが転送される) その間でSPFに対応している別のメールサーバがEnvelope-FROMを変えずにメールをそのまま転送する場合は、メール受信側のメールサーバにおいて、SPF認証が失敗してしまう」理由について考えます。

問題を簡潔に捉えるために、以下のような場合を想定します。なお、各サーバはカッコ内に示すSPFレコードを適切にDNSサーバへ登録しているものとします。

```
[ メールサーバA ] a.com (v=spf1 +ip4:x.y.z.1 -all)
        |
        |
[ メールサーバB ] b.com (v=spf1 +ip4:x.y.z.2 -all)
        |
        |
[ メールサーバC ] c.com (v=spf1 +ip4:x.y.z.3 -all)
```

ここで、`foo@a.com`から`bar@b.com`にメールを送信すると`bar@c.com`に転送されるとします。

まず、メールをメールサーバAからメールサーバBに送信します。そうすると、メールサーバBはSPFの検証に成功します。なぜなら、Envelope-FROMのアドレスが`x.y.z.1`であり、かつSMTP接続元IPアドレスにおけるDNSサーバのSPFレコードの値(`x.y.z.1`)が一致するからです。

次に、メールはメールサーバBからメールサーバCに転送されます。ここで、メールサーバCはSPFの検証に失敗します。なぜなら。転送を行うメールサーバがEnvelope-FROMの値を変えないために、Envelope-FROMのアドレスは`x.y.z.1`のままになるからです。そのため、SMTPの接続元IPアドレスにおけるDNSサーバのSPFレコードの値(`x.y.z.2`)とは一致しません。

よって、本問の理由は「**送信側のDNSサーバに設定されたIPアドレスとSMTP接続元のIPアドレスが一致しないから**」だと言えます。

(4)

「... メール本文とメールヘッダをもとに生成したハッシュ値を用いて、DKIM-Signatureヘッダに付与されているディジタル署名を検証する」ことによって、メールの送信元の正当性以外に確認できる事項を考えます。

ディジタル署名は、メール本文とメールヘッダをもとに生成したハッシュ値を送信者の秘密鍵で署名したものです。つまり、送信者の本当の秘密鍵で署名されていなかったり、メール本文とメールヘッダがハッシ

ュ値生成時の内容から変更されていたりすると受信側で検証に失敗します。

このうち、「メールの送信元の正当性」は「送信者の本当の秘密鍵で署名されたかどうか」によって確認できます。

では「メール本文とメールヘッダがハッシュ値生成時の内容から変更されていないかどうか」によって確認できることはなんでしょうか。それは「メール本文とメールヘッダが改ざんされていないこと」だと言えます。

よって、本問の答えは「**メール本文及びメールヘッダの改ざんの有無**」です。

このように、ディジタル署名を用いることで「送信者の検証」に加えて「完全性の検証」も行えることを覚えておくと良いでしょう(なお「否認防止」も可能です)。

設問3

図7の1行目はMXレコードであり、空欄kにはドメイン`a-sub.n-sha.co.jp`のメールサーバのホスト名を指定します。問題文にある通り、`a-sub.n-sha.co.jp`のメールサーバのホスト名は`mail.x-sha.co.jp`であるため、空欄kは**mail.x-sha.co.jp.**です。末尾に`.`(ドット)を付与することを忘れないでください。

図7の2行目はSPFレコードであり、空欄lにはドメイン`a-sub.n-sha.co.jp`におけるSPFのIPアドレスを設定します。問題文にある通り、メールサーバ(`mail.x-sha.co.jp`)のIPアドレスは`x2.y2.z2.1`であるため、空欄lは**x2.y2.z2.1**です。なお、`x2.y2.z2.2`はSPF検証時に問い合わせ先となるDNSサーバのグローバルIPアドレスです。空欄lには当てはまりません。

空欄mでは、DMARCの`p`タグを設定します。表2にある通り、`p`タグでは「送信側が指定する受信側でのメールの取り扱いに関するポリシ」を設定します。問題分より、受信側で検証に失敗したメールは隔離するポリシとするため、空欄mには**quarantine**を指定します。

空欄mでは、DMARCの`aspf`タグを設定します。表2にある通り、`aspf`タグは「SPF認証の調整パラメタ」です。問題文より、ニュースレターはX社のメールサーバから配信され、Header-FROMにはN社ドメイン名のメールアドレスが、Envelope-FROMにはN社のサブドメイン名のメールアドレスが設定されます。そのため、もし`aspf`タグに`s`(strict)が設定されている場合、Header-FROMとEnvelope-FROMに用いられているFQDNが一致しないため認証に失敗してしまいます。よって、空欄mには組織ドメイン(サブドメイン)が一致していれば認証に成功する**r**(relaxed)を指定します。

設問4

ここまでを通して見てきたように、SPF、DKIM及びDMARCを用いることで送信元ドメインを偽るような、いわゆるなりすまし攻撃を防ぐことができます。

これは、裏を返せば、送信元ドメインを偽っていないような攻撃は防ぐことができないと言えます。

例えば、取引先の正規のメールアドレスが`foobar@torihiki.com`である場合を想定します。

この時、攻撃者が送信元メールアドレスを`foobar@torihiki.com`であると詐称した場合は、検証を通してその詐称を検知することができます。

しかしながら、攻撃者が`tor1hiki.com`のような人間が見間違えそうなドメイン名を取得した上で送信ドメイン認証技術の設定を行い、そのドメイン名を用いて送信元メールアドレスを`foobar@tor1hiki.com`のように設定したとします。この場合、送信ドメインの認証においては何ら問題はない(不一致が発生しない)た

め、N社メールサーバにおける検証が成功します(なお、このように人が勘違いしそうな、正規のドメイン名に類似したものを利用する攻撃をTyposquattingと言います)。

このように、送信ドメイン認証技術の設定を行った上で送信元ドメインを偽らずにメールを送信することで、送信ドメインの認証を成功させつつも攻撃を行うことができると言えます。よって、設問4の答えは「**N社の取引先と似たメールアドレスから送信ドメイン認証技術を利用してメールを送信する。**」であると言えます。

以上。

問2 セキュリティインシデント対応におけるサイバーセキュリティ情報の活用

設問1

(1)

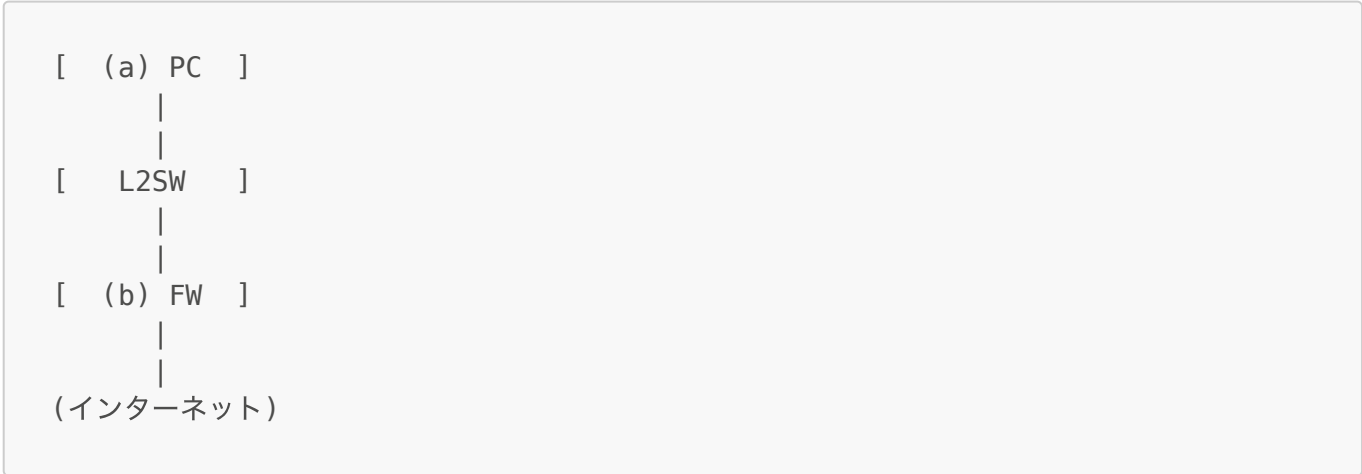
「(マルウェアによるHTTP)通信がZ社のネットワーク環境によって遮断されていた」理由を考えます。」

表2の(a)によると、PCからのインターネットアクセスは全てプロキシサーバを経由するように設定されています。また、(c)によると、プロキシサーバはPCからインターネットへのHTTP通信を中継する際に、利用者IDとパスワードによるBASIC認証を必須としています。これらの認証情報はプロキシサーバ内に保存されているため、その認証情報が窃取されたような場合を除いては、正規のユーザしか知り得ない情報だと言えます。当然マルウェアはこの認証情報を知り得ないため、プロキシサーバを介したインターネットへのHTTP通信は行えません。

よって、本問の答えは「**プロキシ認証に失敗したから**」だと言えます。

(2)

パブリックDNSサービスLに対してDNSプロトコルによる通信が発生した際、その通信は以下のような流れをたどります。なお、DNS通信の場合はHTTP通信の場合とは違って、プロキシサーバによって通信が中継されないことに注意してください。



このうち、(a)のPCに導入されているEDRではDNSプロトコルによる通信を記録しない設定となっていたため、ログは残りません。一方で、(b)のFWにおいては、表2の取得ログの列において動作ログを取得すること

が明記されています。よって、もしマルウェアによるDNS通信が発生したのであれば、FWの動作ログに残されているでしょう。

よって、空欄aは**(b)**です。

(3)

マルウェアによる情報持ち出し成功時に残る痕跡を考えます。

図2に示されている通り、当該マルウェアは以下のようにして情報を持ち出します。

> (い) マルウェアは、 ... 窃取する情報を持ち出す際には ... C&C通信を使用して持ち出す。 (う) C&C通信には、HTTP又はDNSプロトコルを使用する。 HTTPの場合、 ... C&Cサーバと通信する。DNSプロトコルの場合、パブリックDNSサービスLを経由して通信する。 ...

また、図3のC)から分かる通り、グローバルIPアドレスMは、攻撃グループXのC&Cサーバに割り当てられたIPアドレスです。

以上の情報から考えると、マルウェアは以下のどちらかの手段によって、情報を持ち出すと言えます。

- グローバルIPアドレスMへのHTTP通信。
- パブリックDNSサービスLへのDNS通信。

よって、もし情報の持ち出しに成功したのであれば、上記のどちらかの通信に成功したという旨のログが痕跡として残ると言えます。

そのため、本問の答えである「該当する痕跡」は以下の二つであると言えます。

- グローバルIPアドレスMへのHTTP通信成功のログ
- パブリックDNSサービスLへのDNS通信成功のログ

(4)

当該マルウェアへのセキュリティ上の対策として共有すべき情報について、選択肢を一つずつ検討していきます。

- ア PC-VとPC-Tがマルウェアに感染した日時情報

共有しても意味がありません。当然のことながら、「何日の何時何分にマルウェアに感染したのか」を知ったとしても対策に活かすことはできないでしょう。

- イ マルウェアPとマルウェアRがHTTPによる通信を試みたグローバルIPアドレスM

共有すべきでしょう。図2によると、当該マルウェアはHTTP通信によって情報を持ち出すことが示されていますが、その通信先C&Cサーバの詳細までは提示されていません。本情報が共有されれば「グローバルIPアドレスMをHTTP通信におけるブラックリストとして登録する」といった措置が可能となるでしょう。

- ウ マルウェアPとマルウェアRが配置されていたフォルダNのパス名

共有すべきでしょう。図3によると、マルウェアPとマルウェアRは同一のフォルダであるフォルダNに配置されています。これらの共通点から、当該マルウェアは、(観測できる範囲では)全ての場合においてフォ

ルダNに配置されるものと言えます。本情報が共有されれば「フォルダNが存在していないか、そのフォルダに不審なファイルが存在しないか」といったチェックが可能となるでしょう。

- エ マルウェアPに感染したPC-VのプライベートIPアドレス

　共有しても意味がありません。マルウェアPはIPアドレスをベースに感染を行うのではなく、メールの添付ファイルとして配信されるからです。

- オ マルウェアPのファイル名

　共有しても意味がありません。図2によると、当該マルウェアは攻撃対象ごとに異なるファイル名のものが送付されることが示唆されています。よって、ファイル名をベースとした当該マルウェアの検知といった対策は困難だと言えます。

- カ マルウェアRに感染したPC-TのプライベートIPアドレス

　共有しても意味がありません。エと同様の理由です。

- キ マルウェアRのファイル名

　共有しても意味がありません。カと同様の理由です。

　以上より、答えは**イ**と**ウ**です。

設問2

(1)

　正規実行ファイルに付与すべき証明書の種類を考えます。

　解答から述べると、これは**(エ) コードサイニング証明書**です。コードサイニング証明書とは、主にソフトウェアに対して発行する証明書で、ソフトウェア配布元や改ざんの有無等の検証を行うことができます。

　なお、(ア) S/MIME証明書は電子メールにおけるS/MIMEに用いられる証明書で、(イ) TLSクライアント証明書及び(ウ)TLSサーバ証明書は、HTTPS等のTLS通信で用いられる証明書です。ソフトウェアに対する証明書としては適切ではありません。

(2)

　マルウェアがプロキシ認証情報を窃取する際に使用できない攻撃手法について、選択肢を一つずつ検討していきます。

- ア Webブラウザのオートコンプリート情報の窃取

　窃取が可能です。BASIC認証用の認証情報がブラウザによって自動入力される場合、自動入力されたその内容を窃取することで達成されます。

- イ キーロガーによる攻撃

窃取が可能です。正規のユーザによる認証情報の入力内容を窃取することで達成されます。

- ウ ゴールデンチケットの窃取

窃取はできません。ゴールデンチケットとは、Active DirectoryにおけるKerberos認証の認証情報を使用して作成される、任意の権限や有効期限が設定されたチケット認可チケット(TGT)のことです。本問の状況とは適合しません。

- エ 総当たり攻撃

窃取が可能です。現実的な時間において可能であるかどうかはさておき、無限のリソースと時間を前提とするならば、いつかは試行する認証情報が正規のものと一致すると言えます。

- オ 偽のBASIC認証入力フォームの表示とそのフォームへの利用者の誘導

窃取が可能です。選択肢の文章の通り、正規の認証情報を知っているユーザに対してフィッシングを仕掛け、それを入力させることで窃取が可能です。

- カ ネットワーク盗聴

窃取が可能です。PCとプロキシサーバ間でやりとりされるBASIC認証の通信内容は暗号化されていないからです。

よって、答えは**ウ**です。

(3)

C&C通信を遮断するためには、FWにおいてパブリックDNSサービスとの通信を拒否する必要があります。

さて、表1によると項番3において任意の送信元からインターネットへのDNS通信が許可されています。よって、このルールを変更する必要があります。

さて、本来Z社のネットワーク構成において、インターネットを宛先としたDNS通信を行う必要があるのは以下の2パターンです。

- 外部DNSサーバがインターネット上の権威DNSサーバと通信を行う場合。
- PCがプロキシサーバ経由でインターネットへのWebアクセスを行う場合。

これらを考慮すると、インターネットへのDNS通信を許可する送信元はDMZに限定するだけで良いと言えます。なぜなら、上記のどちらのパターンも「DMZに配置されたサーバがインターネットに向けたDNS通信を行う」ものだからです。

よって、変更すべきフィルタリングルールは以下の通りです。

```
| 項番 | 送信元 | 宛先          | サービス | 動作 |
|  3   |  DMZ   | インターネット| DNS      | 許可 |
```

このように変更することで、マルウェアによるPCからパブリックDNSサーバへの直接的な通信をFWにて拒否することができるようになります。

(4)

空欄b,c,dに入る字句を考えます。

表3の項番3のC＆C通信の手法においては「攻撃用ドメイン」や「長いホスト名を持つDNSクエリの発生」といった内容が見られます。よって、項番3で示されている手法はDNS通信を用いたものだと推察されます。

さて、前述の「長いホスト名を持つDNSクエリの発生」とはどういう状況において起こり得るのでしょうか。

ここで、攻撃者の攻撃用ドメインが`attacker.com`であり、攻撃者がそのドメインの名前解決を行う権威DNSサーバを用意していたとしましょう。この時、名前解決を行うキャッシュサーバであるDNSサーバ(以下、キャッシュDNSサーバ)に`xxx.attacker.com`のようなホスト名の名前解決を依頼すると、そのDNSサーバは攻撃者が用意した権威DNSサーバにクエリを送信します。この時、当然ながら攻撃者は権威DNSサーバのログを参照することで`xxx`の部分を閲覧することができます。

これを利用することで、例えば`</etc/passwdの内容>.attacker.com`のようなホスト名の名前解決をキャッシュDNSサーバに依頼することで、攻撃者の権威DNSサーバにその名前解決クエリが送信され、結果として攻撃者に`/etc/passwd`の内容が知れ渡ってしまいます。

つまり、「長いホスト名を持つDNSクエリ」は、ホスト名に窃取したい情報を記述している場合に発生するものだと考えられます。

以上を考慮すると、空欄bは、C&Cサーバとして名前解決を待ち受ける**権威DNSサーバ**だと言えるでしょう。

また、空欄cは、キャッシュDNSサーバであり、問題文に登場する用語を使うのであれば**外部DNSサーバ**が適切でしょう。

そして、空欄dは、DNS通信において送信されるクエリを表す語が入ると考えられます。ここで、問題文をまとめると以下のようになります。

- マルウェアは外部DNSサーバに攻撃用ドメインについての`[ d ]`を送信する。
- 外部DNSサーバはC&Cサーバ(権威DNSサーバ)に`非[ d ]`を送信する。

ここで、クライアントからキャッシュDNSサーバに送信されるクエリを再帰的クエリ、キャッシュDNSサーバから権威DNSサーバに送信されるクエリを非再帰的クエリと言います。これらを考慮すると、空欄dは**再帰的クエリ**が適切でしょう。

(5)

(4)で考察した攻撃において「長いホスト名をもつDNSクエリの発生」以外にどのような特徴が現れると言えるのでしょうか。

当然のことながら、DNSクエリのパケットサイズには上限があります。そのため、持ち出したい情報のデータサイズがその上限を超える場合、パケットを分割する必要があります(本問題のマルウェアにおいてもこのような動作が行われることが図2の(い)で示唆されています)。

その場合、以下のようなDNSクエリのパケットが連続して観測されるでしょう。

```
<窃取する情報(part 1/N)>.attacker.com の名前解決クエリ
<窃取する情報(part 2/N)>.attacker.com の名前解決クエリ
...
<窃取する情報(part N/N)>.attacker.com の名前解決クエリ
```

よって、空欄eには「**特定のドメインに対する多数のDNSクエリの発生**」が当てはまります。

以上。

問3 標的型攻撃への対応

設問1

(1)

不審PC(C&Cサーバと通信したPC)の電源を入れたままにしておく理由を考えます。

さて、電源を入れたままにするということは、電源を消してしまうと何か不都合が発生するのだと考えられます。電源を消すことで失われる情報としてもっとも先に挙げられるものは、揮発性メモリ(いわゆる通常のメモリ)上の情報です。

当然ながら、マルウェアはソフトウェアの一種であるため、実行するコードやそこで扱われるデータはメモリ上に展開されます。マルウェアの解析に当たっては、これらのメモリ上の情報を必要とします。これらの情報を用いることで、マルウェアがどのようなコードを実行しているのか、どのようなデータを扱っているのかを詳細に解析することができます。

一方で、電源を消してしまうと当然メモリ上のデータは失われるため、前述のような解析が困難になってしまいます。

よって、不審PCの電源を入れたままにしておく理由は、「**メモリ上の情報が失われないようにするため**」であると言えます。

(2)

不審PCを利用者LANから切り離さない場合に想定されるマルウェアの活動のうち、J社にとって望ましくないものを考えます。

さて、マルウェアの目標を端的に述べると「感染したホストにおいて目的とするコマンドを実行したり、機密情報を窃取して、インターネット上で待ち受ける攻撃者のサーバにそれを送信したりすること」だと言えます。また、攻撃の影響範囲を広げるために「ネットワークを介して感染を拡大させること」も副次的な目標だと言えるでしょう。

これらを考慮すると、利用者LAN(ネットワーク)から切り離さない場合に想定されるマルウェアの活動のうち、J社にとって望ましくないものとは以下の2点であると言えます。

- **J社情報システムに感染を拡大する。**
- **インターネットに情報を送信する。**

不審PCを利用者LANから切り離すことでネットワークアクセスそのものが失われるため、これら2点の懸念事項は同時に解消されます。

設問2

表3中の空欄a,b,c,dに入れる適切な文章を考えます。

表3に示されているコマンドは、いずれもWindowsにおいて実行可能なコマンドです。それぞれのコマンドの動作内容を考えることで、各空欄に入る攻撃者の目的を導出することができるでしょう。

まず、`ipconfig`はネットワーク環境に関する情報を確認するためのコマンドです。 また`/all`オプションを指定することで、ネットワーク設定が詳細に表示されます。よって、空欄aには「**ウ L-PCのIPアドレス、MACアドレスなどネットワークアダプタの詳細な情報を取得する。**」が当てはまります。

次の`systeminfo`はその名の通りシステムの情報を確認するためのコマンドです。例えば、ホスト名や所有者の情報、OSの詳細情報、システムの情報といったものを閲覧することができます。よって、空欄bには「**イ L-PC内で悪用できる脆弱性を確認するために、OSのバージョンや脆弱性修正プログラムの適用状況を確認する。**」が当てはまります。

次の`tasklist`はコンピュータ上で実行中のプロセスの情報を確認するためのコマンドです。例えば、実行中のプロセスの名前や、そのプロセスのPID値を確認することができます。よって、空欄cには「**オ 実行中のプロセス一覧を取得し、マルウェアの解析環境でないか確認する。**」が当てはまります。

最後の`net view`はLAN内のネットワークコンピュータの情報を表示するためのコマンドです。つまり、当該PCから接続可能なコンピュータを一覧表示するコマンドです。よって、空欄dには「**ア L-PCからその時点で接続可能な端末の一覧を取得する。**」が当てはまります。

なお、解答群のエに当てはまる動作を行うコマンドは表3中にはありません。

設問3

(1)

空欄eに当てはまる文章を考えます。

なお、空欄eには「マルウェアが13:17:15より前に他のマシンに感染していた場合に、FWのログに含まれているであろう情報」が当てはまります。

インシデント対応手順の改善の章においてE部長が懸念しているのは「Pサービスから通知を受けるより前にマルウェアMに感染したPC又はサーバがあるのではないか」ということです。もし、PC又はサーバがマルウェアMに感染している場合、マルウェアMのC&Cサーバである`w1.x1.y1.z1`との通信が発生しているはずです。

ここで、もし実際にC&Cサーバとの通信が発生しているのであれば、FWにおいてLAN上のマシンと`w1.x1.y1.z1`との間で発生する通信の履歴がログとして取得され、ログ蓄積サーバに送信されているはずです。

よって、空欄eには「**IPアドレスw1.x1.y1.z1との通信履歴**」が当てはまります。

(2)

「PC又はサーバの状態によっては、FWのログを使った確認ではマルウェアMに感染していることを検知できない」について、検知できないPC又はサーバの状態について考えます。

さて、「マルウェアMに感染しているにも関わらずFWにログが残らない」状況は、どのような場合において発生するのでしょうか。

マルウェアMが正しく動作していることを前提とすると、マシンとC&Cサーバ間で通信が行われていない理由は、マルウェアが通信をしようとした時にネットワークアクセスが存在していなかったためであると推察されます。例えば、マルウェアが感染し、C&Cサーバへの通信が発生する前にマシンからLANケーブルが取り外された場合においては、当然のことながらC&Cサーバへの通信は発生し得ません。

よって、その状態とは「**感染をしたが、C&Cサーバと通信する前にネットワークから切り離された状態。**」だと言えます。

(3)

では、(2)のような状態のPC又はサーバについて、マルウェアに感染していることをRログを使って検知するにはどのすれば良いのでしょうか。

表1のRシステムの行に示されている通り、RログとはRシステムによって取得されるログです。そのログの内容は、以下の通りであると述べられています。

> 全てのプロセスの生成から終了までの動作、実行したプログラムのハッシュ値並びに通信の宛先のIPアドレス及びポート

このうち、通信が発生していないので「通信の宛先のIPアドレス及びポート」は利用できません。よって、利用するのは「プロセスの生成から終了までの動作」か「実行したプログラムのハッシュ値」のどちらかになります。

ここで、改めて表1のRシステムの行を確認すると、Rシステムの機能として以下の事柄が述べられています。

> ... Rログをマルウェアのハッシュ値で検索することによって、そのマルウェアが実行された痕跡があるかどうか調査することができる。

よって、Rログで収集される「実行したプログラムのハッシュ値」に基づいたマルウェアの検索を行うことで、対象のPC及びサーバがマルウェアMに感染しているかどうかを確認することができます。

以上より、Rログを使った検知方法とは、「**Rログをマルウェアのハッシュ値で検索する。**」ことだと言えます。

以上。