これを踏まえ、図 4 の通信シーケンスを考察する。

図 4 で、スマートフォンがトークンなしで SaaS Q にアクセス要求を行った場合は、SaaS Q から認証サーバ B1 が発行したトークン要求が返ることになるため、［ a ］にはカが入る。

図 4 の 3 つ目の通信シーケンスでスマートフォンで認証サーバ B1 へのアクセスに必要な VPN クライアントを起動しているので、次に続くのは、スマートフォンと VPN サーバ間での端末認証である。したがって、［ b ］にはウの接続要求、［ c ］にはイのクライアント証明書の要求、［ d ］にはアのクライアント証明書が入る。

VPN サーバへの接続が完了した後の通信シーケンスは、スマートフォンと認証サーバ B1 間での利用者認証及びトークンの発行である。

まず、スマートフォンから認証サーバ B1 に対してトークンの発行要求が行われると、同サーバから利用者 ID 及びパスワードの入力要求が返るので、スマートフォンは利用者 ID 及びパスワードを同サーバに送る。したがって、［ e ］にはオ、［ f ］にはク、［ g ］にはキが入る。

図 4 のように、その後は認証サーバ B1 と認証サーバ A1 間で利用者 ID 及びパスワードの検証が行われた後、スマートフォンのパッチ適用状況及びセキュリティ設定の確認が行われ、問題なければ認証サーバ B1 からスマートフォンにトークンが発行される。したがって［ h ］にはエが入る。

＜問２＞　セキュリティインシデントへの対応

■設問 1

［試験センターによる解答例］

(1) a：エ
　　b：イ
　　※a，b は順不同

(2) c：ケ
　　d：ウ
　　e：コ

(1) NIST の文書 SP 800-61「コンピュータセキュリティインシデント対応ガイド」では、インシデント対応チームが提供するサービスの例として、侵入検知、脆弱性や脅威に

ついてのアドバイザリの配信、教育と意識向上、及び社内外での情報共有の推進を挙げている。したがって [a] , [b] には、イ、エが入る。(順不同)

(2) NIST SP 800-61 の内容を知らなくても、インシデント対応ポリシに記載する項目の例であるから、空欄の前後の内容から正解が導き出せると思われる。[c] は、インシデント対応ポリシで責任表明するのであるから、ケの「マネジメント層」が入る。[d] は、インシデント対応ポリシで定義する対象であり、深刻度評価を行う対象となるものであるから、ウの「インシデント」が入る。[e] は、インシデントについて、深刻度評価と並んで行うものであるから、コの「優先順位付け」が入る。

■設問２

［試験センターによる解答例］

(1) f：ログを取得する機器（9 字）
g：取得するログの種類（9 字）
h：保存期間（4 字）
※f，g は順不同

(2) i：タイムゾーン（6 字）
j：統一（2 字）

(3) ネットワークトラフィック量と比較して異常を検知する。(26 字)

(1) 図 3 の(6)d に「開発部はログ取得を定めた規程をもたず、開発部が管理する機器のうちログを取得していたものは少数だった。また、取得していたログの種類や保存期間にはばらつきがあった。」とある。このような課題を解決するために定める要件であるから、要件１の取得するログについての要件における [f] , [g] には、「ログを取得する機器」と「取得するログの種類」が入る。(順不同)
また、要件 2 の取得したログについての要件における [h] には、「保存期間」が入る。

(2) 各機器が出力するログに記録する時刻情報について行うべき設定であるから、該当するのは [i] が「タイムゾーン」、[j] が「統一」である。タイムゾーン（時間帯）とは、同じ標準時を使う地域のことであり、UTC（Coordinated Universal Time：

協定世界時）を基準として、その差分で表される。

(3) 通常時のネットワークトラフィック量や日、週、月、年の中でのその推移などの情報を把握しておくことで、サイバー攻撃により、ネットワークトラフィック量が通常時よりも大幅に増加した等の異常を検知することが可能となる。

■設問３

［試験センターによる解答例］

(1) プロキシサーバのログからアクセス先がサイト M のエントリを抽出し、このエントリから PC-A の IP アドレスを得た。(55 字)

(2) HTTP リクエストによる活動：C&C サーバへのコマンド要求又は応答（18 字）
HTTP レスポンスによる活動：C&C サーバからのコマンド受信（15 字）

(3) 問題：PC のネットワークインタフェースや通信の状態についての情報が失われること（36 字）
措置：メモリダンプを取得する。(12 字)

(4) k：プロキシサーバのログから、IPn のサイトにアクセスした機器がほかにないか（36 字）

(5) 7 回

(6) l：ハッシュ値（5 字）

(7) 行番号：28 行目
役立つ情報：プロキシサーバがインターネットに送信したデータのサイズ（27 字）

(1) 問題文の「サイト M のログに残っていたアクセス元の IP アドレスは A 社のプロキシサーバのものだった」という記述からもわかるように、サイト M にはプロキシサーバを経由して接続しているため、プロキシサーバのログからサイト M にアクセスした PC を特定することが可能である。具体的には、プロキシサーバのログからアクセス先がサイト M のエントリを抽出し、当該エントリの送信元 IP アドレスを確認する。続いて、

当該送信元 IP アドレスが割り当てられた PC を確認すればよい。

(2) マルウェアに感染した PC-A が特定のサイトにアクセスし、その後頻繁に同じサイトにアクセスを繰り返したということは、特定のサイトが C&C サーバ(Command and Control sever：指令サーバ) であり、そこから指令コマンドを受け取った可能性が高い。このアクセスにおいて、HTTP リクエストと HTTP レスポンスによってマルウェアが行っていた活動としては、HTTP リクエストでは C&C サーバに対するコマンドの要求や応答、HTTP レスポンスでは C&C サーバからのコマンドの受信、と考えられる。

(3) インシデント調査の観点からすると、マルウェアが活動している状態をそのまま維持しておくことが望ましい。特に、活動している不正なプロセスに関する情報、ネットワークインタフェースや通信の状態、メモリの内容などはマルウェアの特性や活動内容を調査する上で重要な情報となるが、感染 PC をネットワークから切断すると、これらの情報が失われる可能性がある。この問題を軽減するためには、感染 PC をネットワークから切断する前に、メモリの内容を記録しておくため、メモリダンプを取得しておくとよい。そのためには、マルウェア感染等のインシデントに備え、あらかじめ各 PC にメモリダンプ取得用のツールをインストールし、手順書等を作成しておくことが望ましい。

(4) 図 6 からわかるように、マルウェア K に感染した PC-A が頻繁にアクセスを繰り返していたサイトの IP アドレスは IPn である。したがって、プロキシサーバのログからから IPn のサイトにアクセスした機器がほかにないかを調査することで、マルウェア K がほかの機器にも感染している可能性を簡易に確認することが可能である。

(5) 図 8、図 9 で、9 月 5 日 10 時 35 分から 45 分までの時間帯における PC-B 上での last コマンド、lastb コマンドの実行結果を見ると、攻撃者は 9 月 5 日 10 時 35 分から 10:40 までに 7 回ログインに失敗した後、10:41 にログインに成功していることがわかる。

(6) ファイル名が異なっていた場合であっても、目的とするファイルと同じ内容であることを確認するには、各ファイルのハッシュ値を照合するとよい。ハッシュ値はファイルの名称は影響されず、内容によって出力結果が変わる。同じ手法でハッシュ値を出力した場合、ファイルの内容が同一であれば出力されるハッシュ値も常に同じだが、比較対象となるファイルの内容がわずか 1 バイトでも異なれば、出力されるハッシュ値は大きく異なる。

(7) 表 1 にあるように、"new3.exe"は、指定されたファイルを HTTP の POST メソッドを用

いて IPn のサイトに送信する機能をもっている。図 6 で、9 月 8 日 3 時 35 分以降のログを見ると、行番号 27～30 の 4 行が該当するが、この中で、行番号 28 だけが POST メソッドであり、レスポンスメッセージのサイズも"35618"と大きな値となっている。したがって、行番号 28 がファイルを社外に送信した可能性を示す記録である。また、プロキシサーバ又は FW が取得できる情報のうち、図 6 中に示された情報以外で、合わせて見ることによってファイル送信の有無を判断するのに役立つ情報としては、プロキシサーバがインターネットに送信したデータのサイズが挙げられる。マルウェアの挙動によってはファイルを小さなサイズに分割し、何度かに分けて外部のサイトに送信するケースも多いが、その場合であっても、感染が疑われる PC が特定のサイトに対して送信したデータのサイズを確認することで、情報流出の有無を判断する手掛かりとなる。

■設問４

［試験センターによる解答例］

(1) ア：9/4 14:31
　　イ：9/4 14:37
　　ウ：9/5 10:41

(2) m：タ
　　n：コ
　　o：ソ
　　p：ケ
　　q：シ
　　r：カ
　　s：オ

(1) ア：図 7 の D さんへのヒアリング内容によると、D さんは 9 月 4 日午後に ZIP 形式の"samplebun.zip"をダウンロードしている。図6のプロキシサーバのログを見ると、4 行目に HTTP で"samplebun.zip"にアクセスした記録が残っていることがわかる。このログが出力された日時は"9/4 14:31"である。

イ：図 6 のプロキシサーバのログより、マルウェア K による IPn のサイトとの頻繁な通信が開始されたのは 8 行目であり、その日時は"9/4 14:37"である。

ウ：設問３の(5)の解説にあるように、攻撃者が PC-B へのログインに成功したのは″9/5 10:41″である。

(2) m：表 1 にあるように、ファイル W はダウンローダの機能をもつマルウェア L である。したがって［ m ］にはタが入る。

n：マルウェア L がアクセスし、″new3.exe″をダウンロードするサイトはサイト M である。したがって［ n ］にはコが入る。

o，p：表 1 にあるように、″new3.exe″は遠隔操作の機能をもつマルウェア K であり、実行されると IPn のサイトにアクセスし、そのレスポンスに従って動作する。したがって［ o ］にはソ、［ p ］にはケが入る。

q：図 7 にあるように、攻撃者は PC-B へのログインに成功した後、9 月 7 日 4:15 までに、漏えいが疑われるファイルのコピーとファイル A を、PC-B のローカルディスクに作成している。したがって［ q ］にはシ、［ r ］にはカが入る。

s：問題文にあるように、C さんがフォレンジックツールを用いてファイル A のファイルサイズとハッシュ値をキーにしてファイルを検索した結果、PC-A において、9 月 8 日 3:35 にファイル A と同じ内容のファイルが作成されていたことがわかった。したがって［ s ］にはオが入る。

■設問５

［試験センターによる解答例］

課題：b
措置：**インシデント対応の作業手順書を作成する。**（20 字）

図 3 中の(6)に示された課題 a～d は概ね次の通りである。

a. インシデント対応についての各部の責任や役割が曖昧
b. インシデント対応についての作業手順が不明確
c. インシデント対応の経験をもつ者又はスキルをもつ者がいない

d. ログ取得を定めた規程がなく、取得するログの種類や保存期間にばらつきがある

これらのうち、a の課題についてはインシデント対応ポリシを策定し、A-CSIRT 及び各部の役割、責任及び権限レベルを規定することで改善を図っている。
c の課題については、各部で A-CSIRT の構成メンバを見直すとともに、システム部所属のメンバを増やしている。加えて定期的に勉強会を開催し、外部の研修に参加する方針を立てる等して改善を図ている。
d の課題については、ログを取得する機器、取得するログの種類、ログの保存期間等の要件を定めたログ管理ポリシを作成し、情報セキュリティ委員会から各部に同ポリシに従った運用を指示することで改善を図っている。

残る b の課題については特に措置が講じられておらず、未対応となっている。b の課題を解決するには、インシデント対応の作業手順書を作成する必要がある。