＜問２＞　マルウェア感染への対処

●設問１

［試験センターによる解答例］

(1) a：ア
　　b：イ
　　c：イ
　　d：ウ

(2) e：CRYPTREC（8 字）

＜解説＞

(1) a：テレワークの推進に必要な人材・資源を確保するために、必要な予算を割り当てるのは経営者の役割である。

b, c：セキュリティ維持に必要な技術的対策を講じたり、社内システムに強度の低いパスワードが用いられないように制限を掛けたりするのはシステム管理者の役割である。

d：他人に推測されにくいパスワードを設定し、パスワードの使い回しを避けるのはテレワーク勤務者の役割である。

(2) 電子政府における調達の際に参照される暗号リスト（英字）であるから、該当するのは"CRYPTREC"である。

●設問２

［試験センターによる解答例］

(1) エ

(2) B サービスのアクセス制限機能によって通信が拒否されたから（28 字）

＜解説＞

(1) 下線①のようなネットワーク構成を示すのは「ローカルブレイクアウト」である。ローカルブレイクアウトは、特定のクラウドサービスへの通信ついては、DC などに設けられたインターネットとの接続口を経由せず、各拠点等から直接アクセスするネットワーク構成である。

(2) 表 1 にあるように、B サービスでは、アクセス制限機能によって、アクセス元 IP アドレスが UTM のグローバルアドレスの場合だけアクセスが許可されるようになっている。そのため、UTM を経由しない新 NW での B サービスへのアクセスは拒否されたのである。

●設問３

［試験センターによる解答例］

(1) マルウェア内に FQDN で指定した C&C サーバの IP アドレスの変更（32 字）

(2) C&C サーバとの通信時に DNS への問合せを実行しない場合があるから（33 字）

(3) f：イベントログの消去を示すログ（14 字）

(4) 横展開機能と待機機能だけを実行していた場合（21 字）

(5) UTM の IDS 機能によって攻撃が検知でき、システム管理者に連絡がされるから（37 字）

＜解説＞

(1) マルウェアに埋め込まれていた FQDN に対応する IP アドレスについては、攻撃者が後から自由に変更することが可能である。そのため、ある時点での当該 FQDN の DNS の正引き結果の IP アドレスへの通信を UTM で拒否したとしても、上記の変更が行われた場合には、マルウェア α やマルウェア β の通信を遮断できなくなる。

(2) DNS シンクホール機能を有効化することで、危険リストに登録されている FQDN への DNS クエリを検知して遮断することができる。しかし、マルウェア α とマルウェア β には C&C サーバの IP アドレスが埋め込まれていたことから、DNS への問合せを実行せずに C&C サーバとの通信が行われる場合もある。そのため、DNS シンクホール機能を有効化しても、UTM での通信拒否が必要である。

(3) 図 8 の〔攻撃者の特徴〕に、「一部の業務 PC では、全てのイベントログが消去された痕跡があった。全てのイベントログが消去された後、イベントログの消去を示すログが記録されていた。」とあることから、イベントログに、イベントログの消去を示すログが存在するかどうかもチェックすべきである。

(4) 表 2 のマルウェア β の特徴にあるように、(1)～(3)の機能のうち、イベントログに記録されるのは(3)の遠隔操作機能が実行されたときである。したがって、マルウェア β

が横展開機能と待機機能だけを実行していた場合はイベントログには記録されず、確認ツールを実行しても問題がないと判定されてしまう。

(5) 連携サーバを DC の DMZ に移設すると、表 1 にある UTM の機能で防護されることになる。インターネットから連携サーバが攻撃を受けた場合には、UTM の IDS 機能で検知し、システム管理者に通知されることにより、迅速な対応が可能となる。

●設問４

［試験センターによる解答例］

(1) g：7 月 14 日

(2) h：IP リストに登録された IP アドレス（17 字）

(3) 連携端末以外の IP アドレスを送信元とする通信記録（24 字）

(4) 連携端末を一時的にネットワークから切り離した対応（24 字）

＜解説＞

(1) 図 8 の初期調査結果にあるように、7 月 14 日に攻撃者はマルウェア α を添付したメールを送信しており、F さんがそれを開いた結果、F さんの業務 PC がマルウェア α に感染し、その後マルウェア β にも感染している。そのため、マルウェア β の横展開機能により、同日には連携サーバに細工されたファイルが置かれていた可能性がある。したがって、調査 1 の対象期間の開始日は 7 月 14 日にする必要がある。

(2) マルウェアへの感染が疑われるのは、マルウェア α とマルウェア β に埋め込まれていた C&C サーバの IP アドレスと FQDN を DNS で正引きした結果の IP アドレスを登録した IP リストの IP アドレスへの通信記録が存在する PC である。

(3) 連携端末からほかの PC やサーバへの感染拡大した場合には、連携端末以外の IP アドレスを送信元とした、IP リストに登録された IP アドレスへの通信記録が会員 FW のログに記録されるはずである。したがって、この条件に合致する会員への対処を優先すればよい。

(4) 問題文の〔連携サーバ経由の感染状況の確認と感染拡大防止〕にあるように、E さんは、運営責任者を通して化学コンの全会員に連携端末を一時的にネットワークから切り離してもらうよう連絡し、全ての会員で対応が完了したことを即日確認している。した

がって、IP リストに登録された IP アドレスへの通信記録が連携端末以外にはなかった会員については、感染を拡大させるリスクは低いと考えることができる。