平成 28 年度 春期 情報セキュリティスペシャリスト

＜午後Ⅱ 解答・解説＞

＜問1＞ CSIRT 構築とセキュリティ設計

■設問 1

〔試験センターによる解答例〕

a：対応の要否（5 字）

重要度や優先度を考慮して判断することであり，その結果によって次のステップである番号 3（調査依頼検討）に進むか，番号 6（完了）に進むかが決定するため，［ a ］に該当するのは「**対応の要否**」である。

■設問 2

〔試験センターによる解答例〕

(1) b：報告すべきインシデントの範囲（14 字）

(2) インシデントが A 社全体に与える影響度に基づいた対応を指示するため（32 字）

(1)〔A 社 IRT の現状〕に現状の A 社 IRT における問題点について記述があるが，これらの中で明らかに「不明確である」のは，A 社 IRT に「**報告すべきインシデントの範囲**」である。この問題と A 社 IRT 自体の周知不足により，本来は表 1 の番号 1，2 にあるように，A 社 IRT が報告を受け，対応要否を判断すべきところが，A 社 IRT への報告が行われず，事業部内で対応や判断が行われているケースもあった。

(2)インシデントへの対応指示が事業部内で行われた場合，A 社全体への影響度は考慮されず，表 2 の「対応指示手順」にあるように，事業部の都合を優先させた対応となる可能性が高い。本来は，表 1 の番号 5 に記載の通り，A 社 IRT が**インシデントの全社への影響度に基づいて対応内容を決定し，対応を指示する**必要がある。そのため，A 社 IRT が対応指示を直接行えるようにしたのである。

■設問３

〔試験センターによる解答例〕

(1) IT 部の OA 用 PC に攻撃メールが送信され，PC がマルウェアに感染し，起動したマルウェアがサーバ LAN に不正アクセスする攻撃（61 字）

(2) IT 部運用チームのメンバの LDAP ID 以外によるログイン要求の検知（34 字）

※文字数には空白を含む

(1)〔A 社のシステム運用〕にあるように，サーバ LAN のサーバなどの運用保守は，IT 部の OA 用 PC から管理画面にアクセスし，実施している。この環境では，標的型攻撃等によって IT 部の OA 用 PC に感染したマルウェアが，サーバ LAN のサーバの管理画面に不正アクセスする攻撃等を防ぐことができない。運用管理セグメントを新設することにより，同セグメント以外の PC からサーバ LAN のサーバの管理ポートへのアクセスは禁止され，運用管理 PC へのアクセスも禁止される。これにより，上記のような攻撃を防ぐことが可能となる。

(2)リバースブルートフォース攻撃とは，パスワードを固定して何通りものユーザ ID の組合せを試行する手法である。表 3 の「LDAP サーバ」の「概要」にあるように，LDAP サーバの管理画面には IT 部の運用チーム 4 名の LDAP ID でだけログインできる。したがって，**これら 4 名の LDAP ID 以外によるログイン要求を検知する**ことで，LDAP サーバの管理画面でのリバースブルートフォース攻撃を検知することが可能である。

■設問４

〔試験センターによる解答例〕

(1) A 社 IRT が収集すべき脆弱性情報を把握するため（23 字）

(2) A 社 IRT が，各部署のインシデント発生時や対策時の，影響範囲の特定に活用する。（39 字）

(1)図 5 の課題 1 にあるように，現状では情報機器の構成情報を正しく把握していない部署がある。構成情報が把握できていなければ，収集すべき脆弱性情報を把握することもできず，収集すべき情報が漏れてしまったり，無用な情報を収集することに工数を割くことになったりする可能性がある。各部署の情報機器の現状が示された構成管理情報を活用することにより，A 社 **IRT が収集すべき脆弱性情報が明確**になり，上記のような問題が発生するの

を防ぐことができる。

(2)インシデントハンドリングにおいては，A 社 IRT は当該インシデントによる影響範囲を可能な限り正確に把握する必要があるが，情報機器の構成情報が把握できていない状況では非常に困難である。インシデントによる影響範囲がわからなければ，A 社 IRT は各部署に対して適切な対応指示を行うことができない。**A 社 IRT は，各部署の情報機器の構成管理情報を，各部署のインシデント発生時や，その対応時の影響範囲を特定するために活用する**ことができる。

■設問５

〔試験センターによる解答例〕

各部署が収集している脆弱性情報の提供を受ける。(23 字)

〔脆弱性情報ハンドリング〕に「各部署が独自に管理する情報機器の脆弱性情報の収集や脆弱性修正プログラムの適用は，…」「A 社 IRT が収集し，各部署に発信することによって，各部署が脆弱性情報を収集する負担を低減し，…」とあるように，現状では各部署が独自に脆弱性情報を収集している。A 社 IRT が各部署と連携し，**各部署が独自に収集している脆弱性情報の提供を受ける**ことで，A 社 IRT における脆弱性情報収集にかかる工数の発生を最小限に抑えることができる。

■設問６

〔試験センターによる解答例〕

(1) 現状評価基準

(2) c：ネットワーク

d：ローカル

e：FW1

(1)ゼロデイ攻撃とは，OS やソフトウェアに脆弱性が発見された際に，パッチが提供されるよりも前に当該脆弱性を悪用して行われる攻撃である。“基本評価基準”は攻撃元の特性からスコアが算出されるため，ゼロデイ攻撃が可能かどうかは関係しない。一方，“現状評価基準”は，攻撃コードの出現有無や対策情報が利用可能であるかどうかを基にした評価基準

であるため，ゼロデイ攻撃が可能かどうかがスコアに大きく反映される。また，“環境評価基準”は，脆弱性が存在する情報機器の設定や環境によって異なるため，ゼロデイ攻撃が可能かどうかによるスコアへの影響は“**現状評価基準**”のように大きくない。

(2)
c：表 3 にあるように，FW1 は，外部業者の担当者が遠隔地からインターネットを経由して保守作業を行っている。したがって，攻撃者はネットワーク経由でリモートから攻撃可能であり，攻撃元区分は「**ネットワーク**」となる。

d：表 3 にあるように，FW2 は，コンソールポートに常時接続された MPC からのみ保守作業を行うことが可能である。したがって，攻撃者はローカル環境から攻撃する必要があり，攻撃元区分は「**ローカル**」となる。

e：攻撃元区分が「ローカル」の FW2 よりも，「ネットワーク」である **FW1** の方が脆弱で攻撃を受ける可能性が高く，“環境評価基準”のスコアは高くなる。

＜問 2＞ テレワークのセキュリティ

■設問 1

〔試験センターによる解答例〕

(1) UA が DL2 以外の場合には“404 Not Found”を返す。(32 字)

※文字数には空白を含む

(2)・J プロキシの URL フィルタ機能（15 字）

・J プロキシの RH フィルタ機能（14 字）

(1)C&C サーバとの通信では，UA が DL2 の場合には“200 OK”が返っていたが，標準ブラウザからアクセスした場合には“404 Not Found”が返ってきていた。このことから，**UA が DL2 以外の場合には，“404 Not Found”を返す**仕組みになっていると考えられる。

(2)マルウェアによるモバイル PC から C&C サーバへの通信をブロックするには，経路上にあるプロキシサーバでフィルタリングするのが有効である。表 1 の「J 社セキュアプロキシ（J プロキシ）」の機能概要を見ると，**URL フィルタ機能**，**RH フィルタ機能**が提供されていることがわかる。したがって，これらの機能でブロックするのが有効である。

■設問２

〔試験センターによる解答例〕

a：DLL（3 字）

このように，システムディレクトリ等に不正なコードを含むファイルを埋め込み，ブラウザなどの既存のプログラムに利用者が意図していない振る舞いをさせる手口を，**DLL**（Dynamic Link Library）インジェクション攻撃と呼ぶ。

■設問３

〔試験センターによる解答例〕

(1) b：ドライブバイ（6 字）

c：分割（2 字）

(2) d，e：※下記は順不同

・H 社 Web メール（8 字）

・N コラボ（4 字）

・可搬記憶媒体（6 字）

・P 社 CRM ツール（8 字）

(1)

b：ユーザが気付かないうちにインターネット上の悪意ある Web サイト等にアクセスしてマルウェアをダウンロードし，実行する手法を**ドライブバイダウンロード**（drive-by-download）攻撃と呼ぶ。また，このような振る舞いをするマルウェアを「ダウンローダ型マルウェア」，あるいは単に「ダウンローダ」と呼ぶ。

c：圧縮状態で 200k バイト以上あったファイルを 2k バイト未満で送るのであるから，考えられるのは当該ファイルを「**分割**」することである。これは，マルウェアが外部に情報を流出させる際の典型的な振る舞いの一つである。

(2)問題文に示されているモバイラのテレワーク環境において，モバイル PC のハードディスク以外で PJ 情報が格納される可能性のある場所を考えればよい。まず表 1 のクラウドサ

ービスの中で，「**H 社 Web メール**」「**N コラボ**」「**P 社 CRM ツール**」が挙げられる。さらに，表 2 の「**可搬記憶媒体**」も挙げられるので，これらの中から二つ解答すればよい。

■設問４

〔試験センターによる解答例〕

f：見直し（3 字）

〔侵入経路と被害状況の調査〕に，「ビューア V は以前に業務上必要があったので標準ソフトとして導入されていたが，現在では必要性はなくなっていた」とあるように，必要がなくなったのにもかかわらず，依然として標準ソフトになっていたことが根本的な問題である。したがって，その対策としては，ビューア V を含む標準ソフトの「**見直し**」を定期的に行うことが求められる。

■設問５

〔試験センターによる解答例〕

(1) マルウェアからハードディスク内の情報が透過的に見えてしまうから（31 字）

(2)・AM のマルウェア定義ファイルが初期状態に戻る。(23 字)

・セキュリティパッチが適用前の状態に戻る。(20 字)

(3) 画面などの情報からのデータの窃取（16 字）

(4)

項目：3

変更後の案：VDI サーバ及び社内 LAN からの HTTP 及び HTTPS 通信によるアクセスだけを許可するよう設定する。(50 字)

(1)表 2 の「ハードディスク暗号化」にあるように，OS 起動時の認証に成功すると，ハードディスクへの書き込み時の暗号化と読み出し時の復号を透過的に行うようになり，OS からは，ハードディスク内にデータが平文で格納されているかのようにアクセスできる。これは，OS 上で動作するその他のソフトウェアやマルウェアから見ても同様であり，**ハードディスク内の情報が透過的に見えてしまう**ことになる。

(2)PC 起動時に，読取り専用領域に保存されたブートイメージから動作環境を復元する方式では，動作後に OS やソフトウェアに行った更新内容は破棄されることになる。表 2 にあるように，Q 社のモバイル PC では，**AM のマルウェア定義ファイルが自動的に更新される**とともに，OS の修正パッチ（セキュリティパッチ）も自動的に適用される。表 5 の項番 1 の実装方式では，PC を起動するたびにこれらの更新内容が破棄され，**更新前（適用前）の状態に戻る**ことになる。

(3)要件 2 にあるように，仮想端末と VDI 端末との間では，画面及びキーボード・マウスの操作データだけが送受信される。この環境において，VDI 端末上のマルウェアが窃取可能なデータは，画面の情報，もしくはキーボードからの入力内容である。問題文には「仮想端末からの情報窃取」とあるので，**画面などの情報からのデータの窃取**が該当する。

(4)VDI を実装したとしても，図 1 の項目 1，2 については特に変更する必要はない。VDI を実装すると，Q 社貸与のモバイル PC からクラウドサービスにアクセスすることはなくなり，代わって VDI サーバ（上のゲスト OS）から同サービスにアクセスすることになる。したがって，項目 3 については，「**VDI サーバ及び社内 LAN からの HTTP 及び HTTPS 通信によるアクセスだけを許可するよう設定する**」といった内容に変更する必要がある。