平成 27 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＞ ウイルス対策

■設問 1

〔試験センターによる解答例〕

(1) a：DNSSEC（6 字）

(2) b：オープン（4 字）

　　c：エンベロープ（6 字）

(3) d：n-sha. co. jp

(1) DNS の拡張仕様であり，公開鍵暗号方式によるディジタル署名の DNS レコードの付加と，DNS 応答のディジタル署名の検証が可能である，という記述から，［a］に該当するのは **DNSSEC**（DNS Security Extensions）である。

(2)

b：インターネットからの再帰的な名前解決問合せなど，問合せ元のアドレスや問合せ対象ドメインの制限なく名前解決問合せに応じる DNS サーバは「**オープンリゾルバ**」と呼ばれる。オープンリゾルバは DNS リフレクション（DNS amp）攻撃の踏み台として利用される可能性があるほか，DNS キャッシュポイズニング攻撃に対しても脆弱である。

c：メールの宛先情報としては，SMTP の「RCPT TO」コマンドで指定したエンベロープアドレスと，メールヘッダの To アドレスとがある。これらのうち，SMTP のメール転送においては**エンベロープ**中の宛先情報が用いられる。

(3) N 社の外部メールサーバが内部メールサーバに転送するメールのドメイン名であるから，N 社のドメイン名が入る。N 社のドメイン名は，表 1 より「**n-sha.co.jp**」であることが分かる。

■設問 2

〔試験センターによる解答例〕

e：送信者メールアドレス（10 字）

図 3 の(2)にあるように，PC から送信されたメールの場合は，送信者メールアドレスに通知メールを送信する。一方，外部メールサーバから転送されたメールの場合は，宛先のメールアドレスに送信している。 e は宛先のメールアドレス以外のアドレスであり，通知メールを送信すると迷惑メールになる可能性があるアドレスであるから，該当するのは「**送信者メールアドレス**」である。例えば，標的型攻撃メールでは送信者のメールアドレスが実在する第三者のものに詐称されていることもある。そのような場合に，送信者メールアドレスに通知メールを送信すると迷惑メールになってしまう可能性がある。

■設問３

〔試験センターによる解答例〕

脆弱性修正プログラム及びウイルス定義ファイルを提供するサイトに制限する。(36 字)

問題文〔PC の管理方法〕にあるように，PC の初期設定では，次のような作業を行う。

① OS，ウイルス対策ソフトなど N 社で定めたソフトウェアのインストール
② 脆弱性修正プログラムの適用
③ ウイルス定義ファイルの更新
④ Web ブラウザの設定及びメールソフトの設定

これらの中で，初期設定用ネットワークを設置した場合に外部のサイトに接続する必要があるのは②と③である。そのため，初期設定用ネットワークからの接続サイトを，**脆弱性修正プログラム及びウイルス定義ファイルを提供するサイトに制限する**設定を追加すべきである。

■設問４

〔試験センターによる解答例〕

(1) 初期設定用ネットワークに接続し，W 社の駆除ツールをダウンロードして適用した。(38 字)

(2) 中継サーバのサーバ名を部分一致でマッチさせる。(23 字)

(3) G さん以外の広報グループのメンバに届いたメールを調査し，マルウェア X を含むメールを削除した。(46 字)

(4) スキャン不能の場合も通知するようにした。(20 字)

(1) 先頃改善された N 社の環境を活用してマルウェア X を駆除する方法であり，他の PC やサーバへのネットワークを経由した感染を防ぐことができるのであるから，該当するのは初期設定用ネットワークの活用である。図 5 より，W 社の駆除ツールを適用すれば，マルウェア X を駆除し，感染によって改ざんされた OS の設定を復元できること，当該駆除ツールは W 社の Web サーバからダウンロードできることが分かる。したがって，解答としては，**初期設定用ネットワークに接続し，W 社の駆除ツールをダウンロードして適用した**，となる。

(2) 中継サーバを経由するアクセスを防止する対策として，プロキシサーバのサーバ管理者用ブラックリストに追加する具体的な設定の内容が問われている。そこで，表 2 のプロキシサーバの概要を見ると，URL フィルタリング機能のサーバ管理者用ブラックリストでは，パターンマッチングの方式と文字列を登録できる，とある。また，パターンマッチングの方式としては，完全一致，部分一致，前方一致，後方一致のいずれかを指定する，とある。したがって，中継サーバのサーバ名である"server.example.net"を文字列として登録し，パターンマッチングの方式としては，部分一致を指定すればよい。

(3) 図 5 の(1)にあるように，G さんは広報問合せ用のメールアドレスあてのメールに添付されていたファイルを開いたことによってマルウェア X に感染している。表 1 にあるように，広報問合せ用メールアドレスあてに届いたメールは営業部広報グループのメンバのメールアドレスあてに同報されているため，他の広報グループのメンバが G さんと同様に添付ファイルを開き，マルウェア X に感染する可能性がある。したがって，F さんは，追加の調査と対処として，**G さん以外の広報グループのメンバに届いたメールを調査し，マルウェア X を含むメールを削除した**と考えられる。

(4) 図 3 にあるように，N 社の SMTP ウイルススキャンでは，暗号化されたファイルはスキャン不能と判定され，その場合には結果を通知しない設定となっている。これに対し，E 主任は，パスワードを用いて暗号化されたファイルを添付したメールがインターネットから届いた場合に，メール受信者に注意を喚起する必要があると指摘している。この指摘に対応するには，**スキャン不能の場合にもメール受信者に結果を通知する**ように設定を変更すればよい。

■設問 5

〔試験センターによる解答例〕

- **1 週間を超えてフルスキャンが実行されない PC を指定して，フルスキャンを実行させる。(41 字)**
- **ウイルス定義ファイルが更新されない PC を指定して，ウイルス定義ファイルを更新させる。(42 字)**
- **アップロードされるウイルス感染情報を基に感染した PC を特定し，ウイルスを駆除する。(41 字)**

D 部長の指示は，ウイルス感染防止のためのウイルス対策集中管理ソフトの活用方法を考えるように，とのことである。そこで，図 6 より，活用方法を検討する。まず，ウイルス感染防止のためには，①ウイルス定義ファイルが遅滞なく更新されること，②フルスキャンが定期的に実行されること，が求められる。

①については，ウイルス対策集中管理ソフトに各 PC のウイルス定義ファイルの更新時刻及びバージョン情報がアップロードされており，同ソフトには，ウイルス定義ファイルをダウンロードして更新するように PC に対して動作指示を送信する機能がある。表 3 にあるように，PC のウイルス定義ファイルは起動時及び起動後 1 時間ごとに更新する設定となっている。そのため，ウイルス対策集中管理ソフトの機能を活用し，**ウイルス定義ファイルが一定時間更新されない PC を指定して，ウイルス定義ファイルを更新させる**のが有効である。

②についても，ウイルス対策集中管理ソフトに各 PC のフルスキャン実行結果がアップロードされており，同ソフトには，フルスキャンを実行するように PC に対して動作指示を送信する機能がある。表 3 にあるように，PC のフルスキャンは毎週月曜日の昼の 12 時に開始する設定となっている。そのため，ウイルス対策集中管理ソフトの機能を活用し，**1 週間を超えてフルスキャンが実行されない PC を指定して，フルスキャンを実行させる**のが有効である。

また，ウイルス対策集中管理ソフトには，各 PC のウイルス感染情報もアップロードされている。そのため，この情報からウイルスに感染した PC を特定し，速やかにウイルスを駆除することも考えられる。とはいえ，ウイルス対策集中管理ソフトの機能のみで確実にウイルスを駆除できるとは限らないため，別途対応手順を検討する必要がある。これは，ウイルス感染による被害の拡大を防ぐ上で有効な策である。

■設問６

〔試験センターによる解答例〕

(1) 連絡先メールアドレス：攻撃対象のメールアドレス（12 字）

お問合せ内容：誘導する Web サイトの URL（14 字）

(2) f：・hhttp://ttp（11 字）

・hhttp://ttps（12 字）

・hhttps://ttp（12 字）

・hhttps://ttps（13 字）

※上記のような文字列の中から一つ。

(1) 図 8 を見ると，Web フォームの連絡用メールアドレスに入力されたメールアドレスがそのまま To アドレスとなり，受付通知メールが送信される仕組みになっている。連絡用メールアドレスにはどのようなアドレスでも入力可能であるため，攻撃者が不正なメールを送信する目的で悪用することが可能である。また，図 9 及び F さんと H さんの会話にあるように，お問合せ内容として任意の URL を入力した場合には，それがそのままメールの本文に表示される。そのため，攻撃者は，Web フォームの連絡先メールアドレスに**攻撃対象のメールアドレス**を入力し，お問合せ内容に誘導する Web サイトの URL を入力することで，任意の相手に対し，不正な Web サイトに誘導するメールを送信することができる。

(2) 図 10 にあるように，メール送信プログラムに追加した処理では，与えられた文字列の中から，大文字と小文字の区別をせずに，"http://"，"https://"を削除する。しかし，この仕様では，例えば"http://"の文字列内に"http://"を挿入し，"hhttp://ttp://"という文字列にした場合などは，2 文字目からの"http://"が削除された後に"http://"が残るため，クリック可能な URL として表示されてしまう。

"http://"の先頭と末尾以外であれば"http://"をどこに挿入してもよいため，下記のように様々なパターンが考えられる。

・hthttp://tp://
・htthttp://p://
・httphttp://://

また，次のように，削除される文字列，残す文字列を"https"にしてもよい。

・hhttp://ttps://

・hhttps://ttp://
・hhttps://ttps://

こうした様々なパターンの中からいずれか一つを [f] の表記に合わせ，末尾の"://"を除いた文字列を解答すればよい。

＜問2＞ 製造業におけるネットワーク構築

■設問１

〔試験センターによる解答例〕

a：事務系 LAN への接続時にマルウェアに感染した転送用 PC を，その状態のままで製造系 LAN へ接続すると，製造装置へマルウェアの感染が広がる。(68 字)

表 2 にあるように，脆弱性攻撃型マルウェアは，同一 LAN 上の他のコンピュータに対し，OS の脆弱性を悪用する攻撃を試み，攻撃に成功すると当該コンピュータを同マルウェアに感染させる。そのため，転送用 PC を事務系 LAN に接続している間に，同 LAN 上の事務用 PC に感染した脆弱性攻撃型マルウェアの攻撃により，転送用 PC が同マルウェアに感染する可能性がある。そして，その状態のまま転送用 PC を製造系 LAN へ接続すると，製造装置へマルウェアの感染が広がる可能性がある。

■設問２

〔試験センターによる解答例〕

(1) b：操作禁止状態に（7 字）

c：他人が推測できない（9 字）

d：知られないように（8 字）

(2) e：影響を評価し，必要であれば脆弱性修正プログラムを適用する（28 字）

(1)

b：他人による接続端末の利用を防止するために，利用者が接続端末から離れる場合に実施すべきこととしては，次のような方法で**操作禁止状態に**することである。

・パスワードロックされた状態でスクリーンセーバを起動する
・OS からログアウト（ログオフ）する
・OS をシャットダウンする

c：パスワードの設定において，どのようなパスワードを使用するべきかが問われている。パスワードが他人に利用されないようにするためには，英大文字，英小文字，数字，記号など複数の文字種を混在させて十分な長さの文字列にするなどして，複雑で**他人が推測できない**ものを使用する必要がある。そして，それを利用者に指導するだけでなく，OS の機能等を用いてシステム的に強制することが望ましい。

d：パスワードの管理においては，パスワードのメモを人目につく場所に置いたり，教えたりせず，他人に**知られないように**する必要がある。

(2) e：接続端末に関する脆弱性が公表された場合には，速やかに脆弱性修正プログラムを適用する必要がある。ただし，〔K 工場の工場内ネットワークの構成と運用〕に「脆弱性修正プログラムの適用に当たっては，事前に K 工場内で動作検証を行っており，……」という記述があるように，適用したことによってシステムが動作不良を引き起こさないように，事前に適用による影響を検証し，その結果を踏まえて判断すべきである。

■設問３

〔試験センターによる解答例〕

f：情報共有系 LAN と製造系 LAN の間で通信が成立することがない。(31 字)

g：情報共有系 LAN 上の機器へ実行形式ファイルが書き込まれても，製造系 LAN にファイルが転送されることがない。(53 字)

f：前述のように，脆弱性攻撃型マルウェアは，同一 LAN 上の他のコンピュータに対し，OS の脆弱性を悪用する攻撃を試み，攻撃に成功すると当該コンピュータを同マルウェアに感染させる。図 4 にあるように，K サーバの接続された情報共有系 LAN と製造装置の接続された製造系 LAN とは，FC スイッチを介して接続されている。ただし，〔K サーバの設計・構築〕の(2)にあるように，K サーバが FC を経由して利用できる機能は単方向レプリケーションによってコピーされたボリュームをマウントする機能だけである。そのため**情報共有系 LAN と製造系 LAN の間で通信が成立することはなく**，製造装置への脆弱性攻撃型マルウェアの感染を防止できる。

g：一方，ファイルばらまき型マルウェアは，表 2 にあるように，同マルウェアに感染するような実行形式ファイルを共有ディスクや外部記憶媒体上に書き込むことで感染を広げる。そのため，FC スイッチを介して接続された SAN ストレージ内のボリュームに実行形式ファイルが書き込まれる可能性がある。ただし，マルウェアが実行形式ファイルを書き込むのは単方向レプリケーション機能によってコピーされたボリュームであるため，当該ファイルが製造系 LAN に転送されることはなく，製造装置へのファイルばらまき型マルウェアの感染を防止できる。

■設問４

〔試験センターによる解答例〕

(1) ・IP アドレスが動的に割り当てられるインターネット回線を利用している協力会社に対応できない。(45 字)

・プロキシサーバを利用している協力会社の場合，社内の接続端末の個別識別ができない。(40 字)

(2) h：K 工場

i：K 工場

j：J 社本社

k：K 工場

l：J 社本社

(3) K サーバへのアクセスだけに使用する鍵ペアだから（23 字）

(4) ①・証明書に対応した秘密鍵の漏えいが疑われる場合（22 字）

②・接続端末を廃棄する場合（11 字）

(1) 表 6 の「接続端末の限定」に，「K サーバを利用する端末を限定する」とあるが，これが実現できないと P さんが考えた根拠が問われている。これは，〔K サーバの設計・構築〕の「(3)協力会社からのアクセス方法」の次の記述から解答が導き出せる。

①インターネットとの接続は，協力会社各社の既設設備を使用できるように，回線種別，固定 IP アドレスが割り当てられるか否かについて限定しない。
②協力会社内の LAN 構成については特に制限せず，プロキシサーバの有無及び NAT，NAPT の利用の有無にかかわらず利用できる。

①より，**IP アドレスが動的に割り当てられるインターネット回線を利用している協力会社の場合には，接続端末を特定することができない**。そのため，K サーバを利用する端末を限定することができない。
また，②より，**プロキシサーバを利用している協力会社の場合には，K サーバは常にプロキシサーバと通信することになり，社内の接続端末の個別識別ができない**。そのため，K サーバを利用する端末を限定することができない。また，NAT や NAPT を利用している協力会社の場合も，接続元の IP アドレスがすべてブロードバンドルータやファイアウォール等のアドレスになるため，接続端末を特定することができない。

(2) CA の機能のうち，通常 IA と RA は主に次のような役割分担となる。

＜IA の主な役割＞
・利用者の公開鍵に対してディジタル署名を付与し，証明書を発行する
・CRL（証明書失効リスト）を発行する
＜RA の主な役割＞
・証明書発行や失効などの資格審査を実施する
・証明書利用者情報を登録する

上記のように，証明書の発行可否を判断するのは RA の役割であり，ディジタル署名を付与し，証明書を発行するのが IA の役割である。
これと図 5 の証明書の流れをもとに，［ h ］～［ l ］について考察する。

h：図 5 の注記にあるように，接続端末ごとに，一意の識別名をもたせるため，証明書を発行する前に，識別名の一意性が確保されていることを確実にする必要がある。これは，図 5 では K 工場が(2)で証明書の発行依頼を行う前に実施すべきことであるため，RA である **K 工場**の役割である。

i：上記のように，証明書の発行可否を判断するのは RA である **K 工場**の役割である。

j：上記のように，証明書の発行者としてディジタル署名を付与するのは IA である **J 本社**の役割である。

k：K サーバへアクセスしてきた接続端末が提示した証明書の有効性検証を行うのは K サーバである。K サーバは K 工場に設置されているため，この役割は **K 工場**の役割である。

l：上記のように，CRL を発行するのは IA である **J 社本社**の役割である。

(3) 接続端末用の証明書は，J 社本社のプライベート CA が発行するものであり，その用途は，K 工場が管理する K サーバへのアクセスにおける端末認証である。また，J 社本社のプライベート CA はルート CA であり，証明書発行業務を一切，他に委託していない。このように，**証明書も鍵ペアも K 工場が管理する K サーバへのアクセスだけに使用するもの**であり，協力会社では，これらを他の用途に利用することはできない。したがって，鍵ペアを K 工場で作成しても問題はない。

(4) 証明書の失効処理は，利用者が当該サービスの利用をとりやめる場合以外に，証明書の誤発行，秘密鍵の漏えいなどの不測事態が発生した場合に実施する必要がある。**証明書に対応した鍵ペアが第三者に漏えいした場合**には，なりすましによって不正な端末認証が成立する可能性があるため，その疑いがあれば直ちに該当する証明書を失効させる必

要がある。
上記以外に，証明書は接続端末ごとに発行された一意のものであるため，**接続端末を廃棄する**場合にも当該証明書を失効させる必要がある。これを行っておかないと，廃棄された接続端末に保存されていた証明書や秘密鍵が第三者によって不正利用される恐れがある。