令和 3 年度 春期 情報処理安全確保支援士
＜午後Ⅱ解答・解説＞

＜問1＞ インシデント対応体制の整備

●設問 1

[試験センターによる解答例]

(1) 外部から入手した利用者 ID とパスワードの組みのリストを使ってログインを試行する攻撃（41 字）
(2) 他のサービスで利用したパスワードとは別のものを設定すること（29 字）
(3)・IP アドレスから分かる地理的位置について、過去のログインのものとの違いを確認する。(41 字)
・Web ブラウザの Cookie を利用し、過去にログインした端末かを判定する。(37 字)
(4) a：タイムゾーン（6 字）
(5) b：9

＜解説＞

(1) パスワードリスト攻撃とは、利用者の多くが複数のサイトで同一のユーザ ID とパスワードを使い回している状況に目を付け、何らかの手段で外部から不正に入手したユーザ ID とパスワードの組みのリストを使い、それらを自動的に連続入力するプログラムなどを用いて会員向けサイト等へのログインを試行する攻撃である。なお、パスワードリスト攻撃は別名で「クレデンシャルスタッフィング攻撃」とも呼ばれる。クレデンシャルとはユーザ ID、パスワード、メールアドレス等、ユーザ認証に使われる情報の総称である。

(2) パスワードリスト攻撃に使われるユーザ ID とパスワードは、利用者の PC からではなく、多くの場合、会員向けサービスを提供しているいずれかのサイトのサーバ等から盗み取られている。そのため、利用者がいかにパスワードを厳重に管理していたとしても、複数のサイトやサービスで同一のパスワードを使い回している限り、この攻撃により被害を受ける可能性がある。したがって、利用しているすべての会員向けサイトやサービスにおいて、異なるパスワードを設定することである。

(3) なりすましによる不正ログインや不正利用を検知する上で、ログインが行われた環境を都度確認し、普段と異なる場合にその旨を通知することは有効な対策である。ログインが普段と異なる環境から行われたことを判定する技術的手法の例を次に挙げる。

・送信元の IP アドレスから地理的位置を割り出し、過去のログイン時との違いを確認する。
・Web ブラウザの Cookie を確認し、過去にログインした端末であるかを判定する
・端末の種類、ブラウザの種類等の情報を確認し、過去のログイン時の端末と同環境であるかを判定する。

(4)　日本標準時（JST：Japan Standard Time）、協定世界時（UTC：Coordinated Universal Time）等、同じ時刻を使う地域の集合をタイムゾーン（時間帯、等時帯）という。

(5)　日本標準時は、協定世界時に対し、9 時間進んでいる。

●設問２

[試験センターによる解答例]

マルウェアに感染した USB メモリを介して管理用 PC に侵入し、さらに店舗管理サーバへ侵入する。(46 字)

＜解説＞

図 2 の注記 2 にあるように、店舗管理システムと社内 LAN との間でデータの受渡しが必要な場合は USB メモリを用いることになっている。このデータ受渡しの際に、社内 LAN に侵入したマルウェアが USB メモリを介して管理用 PC に侵入し、そこからさらに店舗管理サーバにまで侵入する可能性がある。

●設問３

[試験センターによる解答例]

(1)　c：オ
(2)　d：イ
　　e：カ
　　f：ウ
※d と e は順不同。

＜解説＞

(1)　問題文の冒頭に「N 社は、情報セキュリティ委員会を設置している。同委員会は、経営陣が委員となり、情報セキュリティについての基本方針及び重要な課題を取り扱う。」とあることからわかるように、［ c ］にはオの“情報セキュリティ委員会”が入る。

(2)　図 7 に示されたインシデント対応のライフサイクルにおいて、準備と事後活動に挟まれた 2 つの枠内で行うのは、発生したインシデントを検知し、復旧させるまでのインシデントハンドリング業務である。左側枠内の［ d ］［ e ］は、インシデント発生直後に行うべき対応であるから、イの“検知”、カの“分析”が入る（順不同）。

　一方、右側枠内の［ f ］はインシデントの封じ込めと復旧の間に行うべき対応であるから、ウの“根絶”が入る。

●設問４

[試験センターによる解答例]

(1)　5
(2)　脆弱性 M を悪用しても一般利用者権限での操作であるが、“/etc/shadow”ファイルの閲覧には管理者権限が必要であるから（61 字）
(3)　攻撃の接続元 IP アドレスを“etc/hosts.allow”ファイルに追加する。(40 字)
(4)　24
(5)　FW2 において、インターネットからのインバウンド通信は N 社と V 社からの通信だけを許可する。(45 字)

＜解説＞

(1)　図 2 の注記 4 に、N 社、V 社に割り当てられたグローバル IP アドレスの範囲はそれぞれ、“x1.y1.z1.0/28”、“x2.y2.z2.128/30”とあることから、接続元 IP アドレスが次の範囲にある場合は正常なアクセスと判断できる。

N 社：x1.y1.z1.0～15
V 社：x2.y2.z2.128～131

また、不正ログインは SSH で行われていたので、図 9 のインバウンド通信の中で、SSH かつ N 社、V 社に該当しない接続元 IP アドレスを抽出すると次のようになる。

x1.y1.z1.100
x2.y2.z2.60
x1.y1.z1.240
x2.y2.z2.58
a2.b2.c2.d2

したがって、不正ログインを行ったと推測される接続元 IP アドレスは 5 個である。

(2)　表 3 にあるように、脆弱性 M は、細工された HTTP リクエストを送信することによって、開発支援ツール J を実行している利用者アカウントの権限で任意のコマンドを実行できるというものである。また、図 3 の(2)にあるように、開発支援ツール J は、OS の一般利用者権限を割り当てた利用者アカウントで動作している。

認証情報を格納した“/etc/shadow”ファイルを参照するには管理者権限が必要であるため、脆弱性 M だけを悪用しても、同ファイルを参照することはできない。

(3)　図 3 の(3)にあるように、R1 サーバへの“etc/hosts.allow”ファイルの設定において、SSH 接続の接続元は N 社と V 社に限定されている。そこで、攻撃者は R1 サーバをインターネット経由で操作するため、自身の接続元 IP アドレスを“etc/hosts.allow”ファイルに追加したと考えられる。

(4)　図 10 の(3)にあるように、攻撃者はスキャン結果を F1、F2 の二つのファイルに格納して自身のサーバにアップロードした。これを示すログが、図 9 の通信量 960k バイト、320k バイトのアウトバウンド通信である。320k バイトの F1 ファイルには 8 個の IP アドレスをスキャンした結果が固定長で格納されていたことから、1 つの IP アドレスのスキャン結果は 40k バイトであることがわかる。図 9 のログから F2 ファイルのサイズは 960k バイトと推定されるので、格納されていた IP アドレスのスキャン結果は 24 個である。

(5)　図 3 の(1)にあるように、従前の開発用システムの接続制御では、FW2 において、インターネットから各サーバへのインバウンド通信として SSH 接続及び HTTP 接続が許可されており、接続元 IP アドレスによる制限は行われていなかったことがわかる。開発用システムに接続する必要があるのは N 社と V 社のみであるため、インターネットからのインバウンド通信については N 社と V 社からのみ許可するよう FW2 の設定を変更することで、SSH 接続及び HTTP 接続を使った攻撃から開発用システムを保護することができる。

●設問 5

[試験センターによる解答例]

・複数の脆弱性が同時に悪用される可能性の観点（21 字）
・対応を見送った脆弱性の影響の観点（16 字）

＜解説＞

インシデント Q では、それ単体としてはそれほど大きな影響はないとして対応を見送っていた二つの脆弱性を組み合わせた攻撃により、R1 サーバが不正にログインされる結果となった。図 4 の N 社の脆弱性管理プロセスでは、（イ）で個々の脆弱性について悪用される可能性を評価しているが、複数の脆弱性が同時に悪用される可能性につ

いては考慮しておらず、この観点からの評価が不足していたといえる。また、図 4 の（ウ）では、悪用される可能性が高いと判断した場合は N システムへの影響を評価していたが、対応を見送った脆弱性による影響については評価しておらず、この観点も不足していたといえる。

＜問2＞ クラウドセキュリティ

●設問 1

[試験センターによる解答例]

(1) オ

(2) 多くの個人所有機器を C 社内 LAN に接続することによって、IP アドレスが枯渇するという問題が引き起こされた。(53 字)

(3) 稼働させたまま行う方法:L2SW にミラーポートを設定し、そのポートに LAN モニタを接続して DHCP OFFER の数を確認する。(50 字)
停止させて行う方法：DHCP による IP アドレスの配付がないことを確認する。(27 字)

＜解説＞

(1) 上位 2 オクテットが“169.254”に設定された IP アドレスは、固定アドレスが設定されておらず、DHCP サーバからの動的なアドレスも配付されない場合に自動的に設定される IP アドレスで、リンクローカルアドレスという。リンクローカルアドレスは、OS に実装された APIPA（Automatic Private IP Addressing）という機能により、169.254.0.1～169.254.255.254 の範囲で他の機器と重複しない IP アドレスがランダムに設定される。リンクローカルアドレスはネットワークセグメントを越えてユニークであることが保証されないため、同アドレスからの通信データをルータは中継しない。そのため実質的にネットワークを使用することができない状態となる。

(2) 上述のように、リンクローカルアドレスは固定アドレスが設定されておらず、DHCP サーバからの動的なアドレスも配付されない場合に設定される。問題文にあるように、C 社では個人所有機器の C 社内 LAN への接続は統制しておらず、多くの従業員が同機器を AP に接続して使用している。また、DHCP サーバが配付する IP アドレスは“192.168.1.20”～“192.168.0.240”の 221 個であり、150 名の従業員に 1 人 1 台の C-PC を貸与していることがわかる。