令和 3 年度 秋期 情報処理安全確保支援士

＜午後Ⅰ解答・解説＞

＜問 1＞ セキュリティインシデント

●設問 1

［試験センターによる解答例］

(1) a：接続先が保守用中継サーバではない（16 字）

(2) 操作ログの改ざんや削除を防止するため（18 字）

(3) b：保守 PC-A
　　c：インターネット

＜解説＞

(1) SSH 接続する際に警告が表示され、接続が切断された場合、保守用中継サーバのフィンガプリントが変わった以外の理由としては、接続しようとした相手が本来の保守用中継サーバではなかったことが考えられる。

(2) 図 2 の中で、利用者の権限と"操作ログ"についての記述を探すと、「ログ」に第 2 項、第 3 項に「保守用中継サーバと顧客管理サーバでのコマンド実行及びその結果が保守用中継サーバ上に操作ログとして記録される」「操作ログへのアクセスには特権利用者の権限が必要」とある。これらの内容から、保守員に割り当てる保守用中継サーバの利用者 ID に一般利用者の権限を与える目的は、保守員によって同サーバ上の操作ログが改ざんされたり削除されたりすることを防止するためであることがわかる。

(3)b：表 1 の項番 3 で保守用中継サーバに対する SSH 接続を許可する必要があるのは保守 PC-A, B, C であるが、図 1, 2 にあるように、これらの中で固定の IP アドレスが付与されているのは保守 PC-A のみである。したがって、［ b ］には「保守 PC-A」が入る。

c：表 2 の項番 4 で保守用中継サーバへの SSH 接続を拒否するのは、保守 PC-B, C の IP アドレス以外のインターネットの全ての IP アドレスである。なお、欄外の注 1)にあるように、保守 PC-B, C については、保守作業の際に事前申請された作業時間だけ、J 社のシステム管理者が"許可"に変更することになっている。したがって、通常はインターネットの全ての IP アドレスを拒否すればよいため、［ c ］には「インターネット」が入る。

●設問２

［試験センターによる解答例］

(1) 6

(2) 6 月 14 日の 7 時 0 分から 6 月 14 日の 9 時 30 分まで

＜解説＞

(1) 保守用中継サーバは DMZ にあり、そこからインターネット上のサーバへの通信の試みであるから、表 1 のルールでこれに該当し、ログに記録するのは項番 6 である。

(2) 前述のように、表 1 の項番 4 のルールによって通常はインターネットから保守用中継サーバへの SSH 通信は拒否されているが、保守作業の際に事前申請された作業時間だけ、J 社のシステム管理者が当該ルールを"許可"に変更することになっている。そのため、この作業時間帯は第三者が保守用中継サーバに SSH 接続することが可能となる。図 3 の冒頭にあるように、今回のセキュリティインシデントが発生した際の保守作業は、6 月 14 日の 7 時 0 分から 6 月 14 日の 9 時 30 分に行うと事前申請されている。したがって、この時間帯は第三者が保守用中継サーバに SSH 接続することが可能であったことがわかる。

●設問３

［試験センターによる解答例］

(1) **・保守員以外が不正に秘密鍵を利用できないようにするため（26 字）**
・秘密鍵が盗まれても悪用できないようにするため（22 字）

(2) **d：パスワード認証（7 字）**

(3) **e：秘密鍵（3 字）**

(4) **f：送信元 IP アドレスを固定にする（15 字）**

＜解説＞

(1) 鍵ペアを作成する際にパスフレーズを設定すると、秘密鍵を利用する際には当該パスフレーズの入力が必要になる。そのため、十分な強度のパスフレーズを設定することで、保守員以外の第三者が秘密鍵を利用できないようにすることができる。また、マルウェア感染等によって秘密鍵が盗まれた場合であっても、その悪用を防ぐことができる。したがって、これらが秘密鍵にパスフレーズを設定する目的に該当する。

(2) SSH 接続の認証方式をパスワード認証から公開鍵認証に変更するのであるから、無効にする必要があるのは「パスワード認証」である。

(3) SSH Agent Forwarding とは、公開鍵認証方式が設定された SSH サーバへの接続時に、"ssh Agent"が秘密鍵に設定されているパスフレーズの入力を代行する仕組みである。J 社では、保守 PC から保守用中継サーバに SSH 接続した後、顧客管理サーバに SSH 接続して保守作業を行う方式である。このとき、接続に必要な秘密鍵とパスフレーズを保守 PC の"ssh Agent"に登録しておくことで、顧客管理サーバへの SSH 接続に用いる秘密鍵を保守用中継サーバに保存する必要がなくなる。これにより、保守用中継サーバが不正アクセスされたとしても、顧客管理サーバへの SSH 接続に必要な秘密鍵を不正利用されるのを防ぐことができる。

(4) 現状では、保守 PC-B, C に固定の IP アドレスが付与されていないため、保守作業時間帯は表 1 の項番 4 が送信元 IP アドレスの制限なく"許可"になり、第三者による不正アクセスのリスクが高まる。問題文では、保守 PC-B, C から保守用中継サーバへの接続を、VPN 装置を介して直接行う方式か、M 社内のネットワークに接続させた後に、インターネット経由でアクセスさせる方式が検討されている。これらは、保守 PC-B, C の送信元 IP アドレスを固定にし、表 1 の項番 4 のルールを特定の IP アドレスのみ許可するよう変更することで、不正アクセスのリスクを低減させることを目的としている。

＜問２＞　システム開発での情報漏えい対策

●設問１

［試験センターによる解答例］
a：P パスワードの変更（9 字）
b：PC にコピー（6 字）

＜解説＞

a：プロジェクトメンバは P パスワードを知っているため、離任後であっても設計秘密にアクセスが可能である。離任後の元プロジェクトメンバが設計秘密にアクセスできないようにするためには、P パスワードを変更する必要がある。

b：〔設計秘密の管理〕にあるように、R 社の規則では、設計秘密は W ソフトを使って PC 上で作成及び暗号化を行い、R 社のネットワーク内のファイルサーバだけに保管することとなっている。この規則に反して、プロジェクト参加期間中にプロジェクトメンバが設計機密を PC にコピーしていたとすれば、当該メンバは離任後も設計機密を参照できてしまう。