平成 29 年度 春期 情報処理安全確保支援士

＜午後 I 解答・解説＞

＜問 1＞ 社内で発生した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：カ

b：オ

c：エ

(2) d：5

(3) 送信元：ケ

宛先：カ

サービス：キ

(1)

a：**ARP ポイズニング**とは，パケット盗聴などを目的として，攻撃者自身の MAC アドレスと正規のホストの IP アドレスとを組み合わせた偽の ARP 応答パケットを送信することで，ARP テーブル（ARP キャッシュ）の内容を書き換える手法であり，ARP スプーフィング，ARP キャッシュポイズニングとも呼ばれる。多くの OS が，ARP 応答パケットを受け取ると無条件に ARP テーブルを更新することを悪用した攻撃である。

表 2 で，管理用 PC と（キ）の PC の MAC アドレスが，いずれも（カ）の PC の MAC アドレスとなっていることから，マルウェアに感染した A さんの PC は（カ）である。したがって，表 3 の管理用 PC の ARP テーブルの FW の IP アドレスに対する MAC アドレスも同様に（カ）となっていると推測できる。

b：A さんの PC については ARP テーブルを書き換える必要はないため，本来のアドレス

となっている。したがって，管理用 PC の MAC アドレスは（オ）である。

c：b と同様に，FW の PC セグメント側の MAC アドレスは（エ）である。

（2） PC セグメントにある A さんの PC から総当たりで管理用の IP アドレスを推測しようとした場合，表 1 の項番 5 のフィルタリングルールにより，サーバセグメントへの通信が拒否され，ログに記録されることになる。

（3） 管理用 PC 固有の通信を盗聴すれば，管理用 PC の IP アドレスを特定することが可能である。問題本文に「利用者 ID 作成などのサーバの運用は…（中略）…管理用 PC から SSH でサーバにログインして行っている」とあるように，サーバに対して SSH 通信が許可されるのは管理用 PC であると推測できるため，攻撃者はそれを盗聴したと考えられる。解答群でこれに該当するのは，送信元が管理用 PC（ケ），宛先が LDAP サーバ（カ），サービスが SSH（キ）である。

■設問２

［試験センターによる解答例］

攻撃名：中間者攻撃（5 字）

機器名：CRM サーバ

その他（A さんの PC 以外）の PC から CRM サーバにアクセスした際の通信からの情報窃取する方法として考えられるのは，中間者攻撃である。具体的には，盗聴の対象となる PC（ターゲット PC）と CRM サーバとの通信に攻撃者が介在し，ターゲット PC に対しては CRM サーバに，CRM サーバに対してはターゲット PC になりすまし，HTTP over TLS 通信を攻撃者が一旦復号して盗聴する。ただし，その場合，HTTP over TLS 通信確立時にサーバからターゲット PC に提示されるのは，攻撃者が用意した偽のサーバ証明書であるため，Web ブラウザは検証に失敗する。

D 社内の Web ブラウザは，サーバ証明書の検証に失敗した場合は接続しない設定となっているため，このような攻撃への対策となる。

■設問３

［試験センターによる解答例］

(1)　PC セグメント内に管理用 PC とサーバ間の通信が流れなくなるから（31 字）

(2) SYN パケット：(C) → (A)

SYN-ACK パケット：(A) → (B)

(1)　サーバ管理セグメントと PC セグメントを分割することにより，ARP などのブロードキャスト通信は各々のセグメント内にしか流れなくなる。また，表 5 からも，サーバ管理セグメントと PC セグメント間の通信は全て拒否となっていることがわかる。そのため，図 3 の 6 のように，A さんの PC 上で通信を盗聴して管理用 PC の IP アドレスを特定することはできなくなる。

(2)　PC セグメントにある A さんの PC 上で管理用 PC の IP アドレスを詐称して，サーバセグメントのサーバと TCP コネクションを確立しようとした場合には, SYN パケットは（C）→（A）の経路をたどる。

それを受け取ったサーバセグメントのサーバは，管理用 PC の IP アドレスに対して SYN-ACK パケットを返す。当該パケットは FW によってサーバ管理セグメントの正当な管理用 PC に中継されるため，TCP コネクションは確立しない。したがって，このときの SYN-ACK パケットがたどる経路は（A）→（B）である。

＜問２＞　Web サイトのセキュリティ対策

■設問１

［試験センターによる解答例］

L 氏に確認した内容：L 氏が今日ログインしたと言っている回数（19 字）

ログイン記録：L 氏の利用者 ID を用いた今日のログイン回数（21 字）

L 氏のアカウントで少なくとも今日は不正ログインされていないとの結論に至るには，L 氏が今日ログインしたと言っている回数を確認し，その回数と，L 氏の利用者 ID を用いた

今日のログイン回数とが一致していることが確認できればよい。

■設問２

［試験センターによる解答例］

(1)　a：クロスサイトリクエストフォージェリ（17 字）

(2) b：3

(3) c：現在のパスワード（8 字）

d：知り得ない（5 字）

(4) e：confirm（7 字）

f：submit（6 字）

（1）　表 2 では，本来の画面遷移を経ずに（お）の処理を実行することにより，脆弱性 1 を確認している。このように，本来の画面遷移を経ずに処理の実行を許してしまう Web アプリケーションソフトウェアの脆弱性は，クロスサイトリクエストフォージェリ（CSRF）である。

（2）　表 2 の項番 3 では，POST データとして"action_id=submit"を送ったのみで退会完了の画面が表示されていることから，ここに CSRF の脆弱性があることがわかる。図 2 はこれと同じような動作を Web ブラウザに実行させるための HTML である。

（3）　表 1 の（い）の PC での操作例にあるように，パスワード変更画面では現在のパスワードと新しいパスワードの入力が求められるが，攻撃者は現在のパスワードは知り得ない情報である。また，画面遷移（お）のような実装の不備もないことから，問題ないと判断できる。

（4）図 2 の HTML は項番 3 のような動作を Web ブラウザに実行させるものであるから，8～12 行目では，画面遷移（え）のような処理，13～16 行目では（お）のような処理を実行していることがわかる。［ e ］は，画面遷移（え）の"action_id"に格納する文字列であ

るから，表 1 の（え）より，該当するのは"confirm"である。同様に，［ f ］は，画面遷移（お）の"action_id"に格納する文字列であるから，表 1 の（お）より，該当するのは"submit"である。

■設問３

［試験センターによる解答例］

（1） カ，キ

（2） g：セッションハイジャック（11 字）

（3） h：タグの中で利用できる属性を制限する（17 字）

（1） "on"から名前が始まるタグ属性は「イベント属性」もしくは「イベントハンドラ」と呼ばれるもので，スクリプトを記述し，実行することが可能である。"<b>"タグには，次のようなイベント属性を指定することが可能である。

・onclick
・ondblclick
・onkeydown
・onkeypress
・onkeyup
・onmousedown
・onmousemove
・onmouseup
・onmouseout
・onmouseover

解答群でこれに該当するのはカ，キである。

（2） 攻撃者は，プロフィール入力・変更画面で Cookie の情報を盗むことにより，本来の利用者のセッションを乗っ取り，勝手にプロフィールを閲覧したり，変更したりすることが可能となる。このような攻撃手法は「セッションハイジャック」と呼ばれる。「

(3) 利用者が入力できる HTML の要素の制限は変えずにクロスサイトスクリプティングの脆弱性に対処するには，タグの中で指定可能な属性のうち，イベント属性のようにスクリプトの実行が可能な属性の使用を制限することである。

＜問３＞ プロキシサーバによるマルウェア対策

■設問１

［試験センターによる解答例］

接続元 IP アドレスが F 社のグローバル IP アドレスではないこと（30 字）

F 社からのログインであれば F 社のグローバル IP アドレスが送信元 IP アドレスになっている。したがって，F 社以外からのログイン記録を特定するには，送信元 IP アドレスが F 社のグローバル IP アドレスでないものを抽出すればよい。

■設問２

［試験センターによる解答例］

(1) a：ウ

b：エ

c：ア

e：イ

(2) e：処理 1

f：処理 4

(3) g：ウ

(4) h：IdP（3 字）

i : 改ざん（3 字）

(5)　認証に関する情報を Web ブラウザが中継するから（23 字）

(1)

a : (1) で［　b　］からのサービス要求を受け，(10) でサービスを提供していることから，［　a　］は SP である。

b : (1) で SP にサービスを要求し，(10) でサービスの提供を受けていることから，［　b　］は利用者端末の Web ブラウザである。

c : 問題文本文に「SAML を用いることによって，利用者にサービスを提供する SP と，IdP との間で利用者の認証結果などの情報を安全に連携することができる」とあることからわかるように，［　c　］は IdP である。

d : IdP からの認証要求に対して認証結果を返している［　d　］は LDAP サーバである。

(2)

e : URL を生成して送出する処理であるから，表 1 の処理内容で該当するのは処理 1 である。

f : IdP のディジタル証明書が必要な処理であるから，表 1 の処理内容で該当するのは，ディジタル署名の検証を行う処理 4 である。

(3)

解答群の中で，URL 内に含まれるのはクエリ文字列である。なお，クエリ文字列は「クエリストリング」，「URL パラメタ」などとも呼ばれる。

(4)

h : 処理 4 では SAML Response に含まれるディジタル署名を検証している。当該署名を行うのは，処理 3 でディジタル署名を含めた SAML Response を生成する IdP である。

i : ディジタル署名を検証することにより，署名の対象となったデータ，文書ファイル等について次の点を確認することができる。

・なりすまし等がなく，正当な発信者によるものであること
・送信経路上で改ざんされていないこと

（5） 図 1 にあるように，SP と IdP 間の認証情報の送受信は，利用者端末の Web ブラウザによって中継されている。SAML による認証システムでは，このような仕組みにより，SP と IdP が直接通信できなくとも連携が成立するのである。

■設問３

＜交通費精算サービス＞

［試験センターによる解答例］

番号：(3)
理由：社外から IdP への通信がファイアウォールによって遮断されるから（31 字）

＜グループウェアサービス＞

［試験センターによる解答例］

番号：(1)
理由：クラウドサービス側で接続元 IP アドレスの制限が行われているから（31 字）

問題文の冒頭に「社外から社内ネットワークへの通信はファイアウォールによって禁止されている」とある。また，〔暫定対策の実施と根本的な対策の検討〕に「F 社で利用しているクラウドサービスのうち，グループウェアサービスだけは，接続元 IP アドレスを制限する機能を備えていたので，その機能を有効化し，社内からだけログインできるように設定した」とある。

社外から交通費精算サービスにアクセスした場合には，図 1 の（1），（2）のシーケンスまでは実行されるが，（3）の社外から社内の IdP への通信がファイアウォールによって遮断される。

一方，社外からグループウェアサービスにアクセスした場合には，接続元 IP アドレスの制限により，図 1 の（1）で SP への通信に失敗する。