平成 26 年度 秋期 情報セキュリティスペシャリスト

＜午後Ⅱ 解答･解説＞

＜問1＞ 利用者 ID 管理システム及び認証システムの設計

■設問 1

〔試験センターによる解答例〕

(1) a：認証 Cookie

(2) b：アジアポータル

(3) 承認が行われず，社内システムにアクセスする必要がない者も ID を登録できてしまう。(40 字)

(1) 図 1 の [a] に続く「の発行」,「の検証」を手掛かりに問題文と照らし合わせてみる。すると，「日本認証サーバは，利用者認証が成功すると，認証 Cookie を発行し，……」「日本ポータルは，認証 Cookie の検証を行う」「日本社内システムは，認証 Cookie の検証を行った後,……」といった表記がある。したがって,[a] に入るのは「**認証 Cookie**」である。

(2) 図 3 の [b] に続くのが「の URI」であることから，アクセス先のサーバやシステムの名称が入ることが分かる。図 3 と問題文を照らし合わせてみると,「利用者が，アジア PC にログオンして，ブラウザを立ち上げると，ブラウザは，ホームページとして設定されたアジアポータルにアクセスしようとする」という表記がある。
また，図 3 の中段の [b] の HTTP 要求はアジアポータルに対して行われており，続くシーケンスでは HTTP 応答としてポータル画面が返されている。したがって，[b] に入るのは「**アジアポータル**」である。

(3) 問題文に「正社員及び契約社員は，アジア社内システムにアクセスする必要が生じた際に，自ら ID とパスワードの登録をアジア地域の情報システム部に依頼している」「情報システム部は，依頼内容に沿ってアジア LDS に ID とパスワードを登録する」とあるように，正社員や契約社員が自らアジア LDS への ID とパスワードの登録を依頼し，情報システム部はそれをそのまま登録している。
これに対し，日本での IC カード発行のプロセスを見ると，正社員の場合は「人事管理手続きに基づき，正社員情報の確認と登録の承認が行われた後，人事システムに登録される」とあり，契約社員の場合は「管理者が所属長に対して当該契約社員のシステム利用申請を行い，承認を得る」とある。この「承認」のプロセスがアジア LDS への正社員

及び契約社員の ID 登録手順にはないため，**社内システムにアクセスする必要がない者も ID を登録できてしまう**可能性がある。

■設問２

〔試験センターによる解答例〕

(1) G ポータルや G システムからエージェントを呼び出すための変更（29 字）

(2) GDS と各地域の DS 間で信頼関係を結ぶ。（20 字）

(3) 日本と欧米地域の ID に重複があるという問題（21 字）

(1) 問題文の〔日本における ID 管理・認証の方式〕にあるように，エージェントは日本認証サーバと併せて開発された Java プログラムであり，認証 Cookie の検証時にアプリケーションプログラムからメソッドとして呼び出される。市販のパッケージ製品を採用した G ポータルや G システムに上記のような認証方式を実装するためには，**エージェントを呼び出すための変更**が必要となる。

(2) SPNEGO による SSO を利用している欧米地域では，欧米 DS1 に欧米 PC のコンピュータ名及び欧米地域の ID が，欧米 DS2 には欧米地域の各サーバのコンピュータ名がそれぞれ登録されており，欧米 DS1 と欧米 DS2 間で信頼関係が結ばれている。
図 2 の注記 2 にあるように，この DS 間の信頼関係は利用者認証が正しく動作するための条件となっているが，現在 N 社の中の DS 間で信頼関係が結ばれているのは欧米 DS1 と欧米 DS2 間だけである。GDS には認証サブシステム，ID 管理サブシステム及び G ポータルの各サーバのコンピュータ名が登録されるとあることから，欧米 DS2 と同様の役割を担うことが分かる。これに対し，各地域の DS には ID が登録されており，欧米 DS1 と同様の役割を担うことになるので，利用者認証が正しく動作するためには **GDS との間で信頼関係を結ぶ**必要がある。

(3) 図 2 の注記 2 にあるように，SPNEGO による SSO で利用者認証が正しく動作するためには，DS 間の信頼関係に加え，各 DS がもつドメイン名，登録されている ID 及びコンピュータ名が重複していないことが条件となる。しかし，問題文の〔欧米地域における ID 管理・認証の方式〕にあるように，**欧米地域における ID の体系は日本と同じであり，日本と重複している ID がある**ため，上記の条件を満たすことができない。したがって，GIAM システムで SPNEGO による SSO を実現するためには，上記の ID 重複の問題を解決する必要がある。

■設問３

〔試験センターによる解答例〕

(1) 契約社員の利用者情報が取り込まれない点（19 字）

(2) ①・日本 DS

②・欧米 DS1

③・アジア LDS

(1) 下線④より，ID 管理サブシステムの設計において，利用者情報の収集の不十分な点があることが分かる。そこで，問題文の〔G システムにおける ID 管理・認証の設計〕の「ID 管理サブシステム」の概要を見ると，「日次で各地域の人事システムから正社員の利用者情報を収集し，新たに登録された正社員に対して，GID と初期パスワードを生成して GLDS に登録する」とある。つまり，ID 管理サブシステムが収集しているのは正社員の利用者情報のみであり，各地域の**契約社員の情報については収集できていない**。これが，Z 主任が指摘した不十分な点である。

(2) 各地域の正社員及び契約社員の利用者情報が登録されているサーバを確認する。日本では「情報システム部は，当該正社員の証明書を発行し，ID と証明書を日本 DS に登録し，……」「情報システム部は，当該契約社員の証明書を発行し，ID と証明書を日本 DS に登録し，……」とあるように，日本 DS に登録されている。したがって，**日本 DS** から利用者情報を収集するのが適切である。

欧米地域では「欧米地域の情報システム部は，新しい正社員又は契約社員の ID と初期パスワードを欧米 DS1 に登録し，……」とあるように，欧米 DS1 に登録されている。したがって，**欧米 DS1** から利用者情報を収集するのが適切である。

アジア地域では，すべての正社員及び契約社員の ID がアジア DS に登録されており，アジア社内システムにアクセスする正社員及び契約社員の ID とパスワードはアジア LDS に登録されている。つまり，アジア地域では二つの DS に利用者の情報が登録されているため，そのどちらから収集するべきか考察する必要がある。ここで〔G システムにおける ID 管理・認証の設計〕の「G ポータル」の概要を見ると，「GID 及び GLDS に登録された利用者属性に基づいて（中略）当該利用者が所属する地域のポータルサーバへのリンクを表示する」とあるように，必要なのは各地域のポータルサーバにアクセスする利用者の情報である。したがって，アジア地域では**アジア LDS** から利用者情報を収集するのが適切である。

■設問４

〔試験センターによる解答例〕

地域：日本

サーバ名：日本認証サーバ

前述のように，G ポータルの画面中のリンクには利用者が所属する地域のポータルサーバへのリンクが表示されるが，Z 主任は一部の地域ではこのリンクからのアクセスが失敗すると指摘している。そこで各地域の利用者認証の通信シーケンスを確認すると，日本では〔日本における ID 管理・認証の方式〕の本文及び図 1 にあるように，日本ポータルへのアクセス時に認証 Cookie の検証が行われるが，GIAM システムでは日本ポータルへのリンクを表示する前に認証 Cookie は発行されないため，そのままではアクセスに失敗することが分かる。これに対し，欧米地域とアジア地域では認証 Cookie の検証プロセスなどはなく，G ポータルの画面中のリンクによって各地域のポータルサーバにアクセスすることが可能である。

続いて，上記の問題を解決するためにポータル画面に載せるリンクについて考察する。〔日本における ID 管理・認証の方式〕の本文及び図 1 にあるように，日本 PC のブラウザは SPNEGO による SSO に対応しており，日本認証サーバにアクセスして利用者認証が成功すると，認証 Cookie が発行される仕組みになっている。したがって，G ポータルのポータル画面には**日本認証サーバ**へのリンクを載せればよい。

■設問５

〔試験センターによる解答例〕

(1) ①・パスワード（5 字）

②・OTP トークン（7 字）

(2) 多種の個人所有機器での利用者認証の動作検証（21 字）

(3) ネットワーク遅延が大きいことから，仮想デスクトップの操作に対するレスポンスが悪化する。（43 字）

(1) 問題文にあるように，拡張 GIAM システムでは，個人所有機器の業務利用を希望する利用者に VPN 接続用の ID とパスワードが割り当てられ，ハードウェア型の OTP トークンが貸与される。そして，図 7 の通信シーケンスを見ると，個人所有機器からシンクライアントサーバにアクセスする際には VPN 接続後，ログオン要求として ID，パスワード，OTP が送信され，そのうち ID と OTP が OTP 認証サーバに，ID とパスワードが DS に送られ，二段階で認証が行われていることが分かる。

一般的に，利用者を認証する方式として「バイオメトリクスによる認証」「所有物による

認証」「記憶や秘密による認証」があるが，二要素認証は，これらのうち二つの方式（要素）を組み合わせたものである。GIAM では，パスワードが「記憶や秘密による認証」，OTP トークンが「所有物による認証」に該当する（OTP トークンで使用する OTP は利用者が記憶するものではないため，「記憶や秘密による認証」には該当しない）。
したがって，GIAM システムの二要素認証において使われる認証要素は，**パスワード**と**OTP トークン**である。

(2) 〔日本における ID 管理・認証の方式〕にあるように，IC カードリーダは日本 PC 専用に開発されたものであり，日本 PC は一括調達したものである。一方，拡張 GIAM システムでは，〔欧米地域からの要望への対応〕にあるように，自宅又は出張先にいる利用者が個人所有機器から VPN サーバ経由で自分が所属する地域のシンクライアントサーバにアクセスし，そこから G システム，ポータルサーバ，社内システム等にアクセスすることになる。利用者の個人所有機器は多種に及ぶため，IC カードによる利用者認証を採用した場合，IC カードリーダの追加導入や持ち運びが必要になる上，テスト工程で**多種の個人所有機器での利用者認証の動作検証**が必要となり，多くの期間と工数を要すると考えられる。

(3) 拡張 GIAM システムでは，シンクライアントサーバから，利用者が所属する地域のポータルサーバ及び同社内システムにアクセスする。そのため，利用者が他の地域のシンクライアントサーバからアクセスした場合には，そこから広域イーサネットを介して所属する地域のポータルサーバ及び同社内システムにアクセスすることになる。そうなると，**ネットワークの物理的な距離や経路上に存在する機器の多さから遅延が発生し，仮想デスクトップの操作に対するレスポンスが悪化する**可能性がある。

■設問６

〔試験センターによる解答例〕

(1) アジア地域

(2)

構成要素	設定内容
①アジア認証サーバ	SPNEGO の設定をする。(13 字)
②アジア PC	SPNEGO の設定をする。(13 字)

※①と②は順不同

(1) 問題文に「Y さんは，利用者が各地域の PC から G システムにアクセスする場合の通信シーケンスは，図 8 中の仮想デスクトップを各地域の PC に置き換えたものになると考えた」とあるように，拡張 GIAM システムで各地域の利用者が PC による利用者認証の

後，G ポータル及び地域のポータルサーバにアクセスする際の通信シーケンスを図 8 で確認する。
すると，各地域の PC（図中は仮想デスクトップ）は G 認証サーバに HTTP 要求を送ると，G 認証サーバから HTTP 応答として，ステータスコード 401, Negotiate の値をもつ WWW-Authenticate ヘッダ，ID とパスワードの入力画面が返り，SPNEGO によるシングルサインオンが行われていることが分かる。表 1 や各地域の通信シーケンス等にあるように，日本と欧米地域については SPNEGO による PC と社内システムにおける SSO が実現できている。一方，アジア地域では，アジア認証サーバは SPNEGO ではなくフォーム認証を利用しており，アジア PC にも SPNEGO の設定はされていないため，PC と社内システムにおける SSO が実現できていない。そのため，**アジア地域**では，PC における利用者認証の後，G ポータル及びアジアポータルにアクセスしようとしたときにフォーム認証（ID とパスワードの再入力）が必要となる。

(2) アジア地域で SPNEGO による PC と社内システムにおける SSO を実現するためには，他の地域と同様に **SPNEGO の設定**を行う必要がある。設定が必要な構成要素は，SPNEGO に対応した他の地域の通信シーケンス及び問題文の「アジア認証サーバは，SPNEGO ではなくフォーム認証を利用しており，アジア地域の PC に SPNEGO の設定はされていない」という記述から分かるように，**アジア認証サーバ**と**アジア PC** である。

＜問1＞ Web サイトのセキュリティ

■設問 1

〔試験センターによる解答例〕

(1) a：ウ

b：ク

(2) c：/GoodsDetail（12 字）

d：goodsNo（7 字）

(3) 残り 3 画面に SQL インジェクションの脆弱性があるかもしれないから（32 字）

(4) A 社情報システム部に事故発生後にすぐ報告していない点（26 字）

(1) 表 2 のアクセスログの中で，同じ URI のパス名に対して複数のパターンが試行されているものとして，ログ番号 4～7，8～11，12～14 があるが，4～7 と 8～11 については応答サイズに変化がないため除外する。12～14 の中で，ステータスコードが 200 で SQL インジェクションの代表的なパターン（例えば「1＝1」のように，常に真になる条件式など）が試行されているのはログ番号 14 である。これに対し，通常のアクセスとなって

いるのはログ番号 12 であるため，この二つの応答サイズを比較すると次のようになる。

1806 ÷ 1798 ≒ 100.4%

したがって，［ a ］にはウの「**14**」が，［ b ］にはクの「**95～105%**」が入る。

(2) 脆弱性があると考えられるのはログ番号 12～14 であるから，その URI のパス名は「**/GoodsDetail**」であり，クエリ文字列中のパラメタ名は「**goodsNo**」である。

(3) 〔F 社ショッピングサイトαへの攻撃〕にあるように，サイトαの携帯サイトは 30 画面である。このうち，攻撃が行われたのは 27 画面だが，**残り 3 画面にも SQL インジェクションの脆弱性があるかもしれない**。そのため，攻撃が行われた 27 画面だけでなく，携帯サイト全体に対して SQL インジェクションの対策を行う必要がある。

(4) サイトα担当者から連絡を受けた N さんは，X 社に調査を依頼した後，その結果を受けて数日後に携帯サイトの脆弱性対策が完了し，携帯サイトを再開する段階になってから A 社情報システム部に報告している。これは，〔セキュリティ対策プロジェクトの立上げ〕のセキュリティ対策推進計画の(4)にある「セキュリティ事故が発生した直後の A 社情報システム部への報告」に反する対応であり，改善が必要である。

■設問２

〔試験センターによる解答例〕

(1) e：診断ツールの IP アドレス（12 字）

(2) f：ファイアウォールで遮断されているポート番号の通信に関わる脆弱性（31 字）

(3) 修正によって新たな脆弱性が発生していないこと（22 字）

(1) IPS（Intrusion Prevention System）や WAF（Web Application Firewall）は，攻撃の疑いがある通信を検知して遮断する機能がある。この機能により，診断を行う端末やツールの IP アドレスからの通信が遮断されると，対象 Web サイトの脆弱性を検出できなくなってしまう。そのため，**診断を行う端末やツールの IP アドレス**からの通信は遮断しないように設定した上で診断する必要がある。

(2) ファイアウォールの内側から行った診断で検出された脆弱性であり，深刻な脆弱性であっても対策の優先順位を下げてもよいということであるから，当該脆弱性に対する攻撃はファイアウォールによって遮断されているということである。このような脆弱性を「ファイアウォール」と「ポート」の二つの用語を用いて表現すると，「**ファイアウォールで遮断されているポート番号の通信に関わる脆弱性**」となる。

(3) ある脆弱性を修正したとしても，その方法が適切でなかったり，単純なコーディングミス等により，新たな脆弱性が発生してしまったりする場合がある。そのため，脆弱性の修正完了後には，当該脆弱性が適切に修正されたこと，また，それによって**新たな脆弱性が発生していないこと**を確認するため，公開前に診断を再度実施する必要がある。

■設問３

〔試験センターによる解答例〕

(1) g：#

h：</script>

(2) 診断方法：スクリプトを含むデータを Web アプリに入力し，それが Web サイトからの応答中に出力されているかを確認する。(53 字)

理由：Web サイトからの応答中に不正なスクリプトが含まれていないから (31 字)

(3) サイト：サイト 5，サイト 6

変更内容：X-FRAME-OPTIONS ヘッダの DENY を SAMEORIGIN にする。(38 字)

(4) i：ウ

(5) j：ブラウザのアドレスバーの情報で，https で通信していることを確認する (35 字)

(6) 初回にブラウザで Web サイトへ http でアクセスした場合 (28 字)

(1) DOM とは，HTML 文書や XML 文書を構成するテキスト，タグ，属性などの各種要素をオブジェクトとみなし，それらの論理的構造やアプリケーションから操作（追加，変更，削除等）するための仕組み（API）である。DOM を通じた HTML 操作の結果として，意図しないスクリプトが実行されることや，それを許す脆弱性のことを「DOM ベースの XSS」という。

問題文に示された DM ベースの XSS は，図 3 の URI にブラウザからアクセスすると，図 2 の HTML の 4 行目の記述により，図 3 の [g] 以降の部分が実行され，その結果"1"という警告ダイアログが表示される。

図 2 の 4 行目の「hash」は，記号の"#"のことであり，「location.hash」で"#"以降の部分の文字列を取得し，「decodeURIComponent」でデコードし，「document.write」でブラウザに表示する。したがって，[g]には"**#**"が入る。そして，[h] には，右側のスクリプトを閉じるための文字列である"**</script>**"が入る。

(2) 反射型の XSS とは，悪意ある Web サイトやメールに貼り付けられたスクリプトを含むリンクを利用者（クライアント）がクリックし，それが XSS 脆弱性をもつターゲット

Web サイトに送られた結果，その応答として有効なスクリプトが利用者に返され，ブラウザで実行されてしまうというものである。
反射型の XSS の診断では，上記と同様に，**スクリプトを含むデータを対象となる Web アプリに入力し，その結果，Web サイトからの応答中に有効なスクリプトとして出力されているかどうかを確認する**ことで脆弱性の有無を判定する。
一方，DOM ベースの XSS では，問題文にあるように，反射型の XSS とは異なり，**攻撃者が注入するデータ（不正なスクリプト等）が Web サイトからの応答中に出力されない**。そのため，反射型の XSS と同じ方法では診断できない。

(3) 下線④の文にあるように，HTTP 応答ヘッダで"X-FRAME-OPTIONS"に DENY を指定すると，自サイトをフレームで表示させないようにすることができる。しかし，これにより，フレーム内でページの表示を行っているサイトでは当該ページを表示することができなくなり，正規の利用において不具合が発生する。表 3 を見ると，**サイト 5** とサイト 6 では同じドメインページ内でフレーム内にページを表示しているため，上記の不具合が発生することになる。
これを改善するには，**"X-FRAME-OPTIONS"ヘッダの"DENY"を"SAMEORIGIN"にすればよい**。"DENY"がフレーム内でページを表示することを一切禁止するのに対し，"SAMEORIGIN"は，アドレスバーに表示されたドメインと同じドメインのページである場合のみフレーム内で表示することを許可する。

(4) HSTS が"HTTP Strict Transport Security"の略であることから推測できるように，
[i] に入る応答ヘッダフィールド名は"**Strict-Transport-Security**"である。HSTS は，Web サイトが，HTTPS でアクセスしたブラウザに対し，当該ドメイン（サブドメインにも適用可能）への次回以降のアクセスにおいて，"max-age"で指定した有効期限（秒単位）まで，HTTPS の使用を強制させる機能である。

(5) 問題文にあるように，[j] に入るのは，中間者攻撃によってブラウザが HTTP 通信で接続していることを気付くために利用者が毎回すべきことであり，それを徹底させるのは難しいと考えられることである。**ブラウザで接続しているプロトコルの情報は，アドレスバー等で目視確認できる**ため，利用者がこれを毎回実施すれば，上記の攻撃を受けても気付くことが可能であるが，徹底させることは難しい。

(6) 図 4 及び上記(4)の解説にあるように，HSTS が有効になるのは，ブラウザが HTTPS でアクセスした場合である。そのため，**初回にブラウザが HTTP で Web サイトにアクセスした場合**には HSTS が有効にならず，下線⑤の事象が発生する場合がある。