平成 28 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＞ IC カードを用いた認証システム

■設問 1

〔試験センターによる解答例〕

(1) a：ウ

b：オ

c：ス

k：エ

l：イ

(2) 認証対象者が，認証カードと PIN を他人に又貸しして使わせる行為（31 字）

(3) d：ウ

e：カ

f：ク

(4) ア，イ，エ，キ，ク，ケ

(5) g：イ

h：オ

i：ア

j：セ

(1)

a：パスワードを用いる利用者認証で確認しているのはログインする人の「**記憶**」である。

b：認証カードを利用する利用者認証では，認証カードの「**所持**」を確認する。

c：2 種類の方法を組み合わせた認証方式は「**複数要素認証**」である。他の呼称として「二要素認証」「多要素認証」などがある。

k：認証が成立するためには，鍵の生成等に用いられる技術が陳腐化したり，脆弱性が発見される等して「**危たい化**」していないことが必要である。

l：CRL の配布とは別に，証明書の失効情報をリアルタイムに提供している仕組みとして **OCSP**（Online Certificate Status Protocol）がある。OCSP を実装したサーバを OCSP レスポンダ（OCSP サーバ）といい，CA（Certification Authority）や VA（Validation Authority）が運営する。クライアントは OCSP レスポンダに問い合わせることによって，自力で CRL を取得したり照合したりする手間を省くことができる。

(2) 認証カードと PIN を組み合わせた複数要素認証を採用してセキュリティを高めていたとしても，当の**認証対象者が，認証カードと PIN を他人に又貸しして使わせていた場合**等には無意味なものとなる。

(3)
d，e：図 1 の第 2 項にあるように，利用者認証の対象者（**認証対象者**）は業務上，いずれかの**事業用システム**を利用する必要があるグループ従業員及び取引先の従業員であり，これが要求者 A に相当し，事業用システムが検証者 B に相当する。

f：図 1 の第 3 項にあるように，認証対象者に本人用の公開鍵証明書（利用者証明書）を発行し，利用者証明書と，対応する秘密鍵とを格納した認証カードを貸与する。したがって，「**利用者証明書**」が入る。

(4) 解答群の中で，次に示す CRYPTREC 暗号リストに掲載されているのは，**AES**，**Camelia**，**ECDSA**，**RSA-OAEP**，**SHA-256**，**SHA-512** である。

電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）
https://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

(5)
g：図 2 にあるように，ディジタル署名生成関数“sign(x,y)”の“x”は要求者 A の秘密鍵であり，「**Ks**」が該当する。

h：図 2 にあるように，ディジタル署名生成関数“sign(x,y)”の“y”は，署名対象データで

あり，これはディジタル署名検証関数“verify（s,t,u）”の署名対象データ“u”と同じである。図 2 の項番 7 にあるように，署名対象データは「**Ra||Rb||Sn**」である。

i：図 2 にあるように，ディジタル署名検証関数“verify（s,t,u）”の“s”は要求者 A の公開鍵であり，「**Kp**」が該当する。

j：図 2 にあるように，ディジタル署名検証関数“verify（s,t,u）”の“t”は署名値であり，「**X**」が該当する。

■設問２

〔試験センターによる解答例〕

(1)①・申請者に認証カードを貸与済みでないこと（19 字）

②・申請者が事業用システムの利用を業務上必要としていること（27 字）

(2) ア

(3)

改善すべき不備：失効の申請がされてから失効情報の開示まで最短でも 2 日掛かるという不備（34 字）

失効事由の値：ア，ウ

(1) 図 1 の第 2 項に「業務上，いずれかの事業用システムを利用する必要があるグループ従業員及び取引先の従業者に限る」とあることから，**申請者が事業用システムの利用を業務上必要としていること**を確認する必要がある。また，図 1 の第 4 項に「グループ従業員に貸与する認証カードは，一人 1 枚とする」とあることから，**申請者に認証カードを貸与済みでないこと**を確認する必要がある。

(2) 利用者ア証明書の subject フィールドには，グループ従業員を一意に識別できる情報が必要不可欠であるが，問題文の冒頭にあるように，**グループ従業員番号**がこれに該当する。一方，解答群のその他の項目は必要不可欠ではなく，利用者証明書の有効期間（5 年）中に変わる可能性もあるため，記載するべきではない。

(3) 図 4 の項番 3 にあるように，システム部は毎週火曜日に，前週の月曜日から前々日の日曜日までの受付分について，利用者証明書の失効を失効情報サーバに登録して公開する。つ

まり，**失効の申請がされてから失効情報が開示されるまでに最短でも 2 日**，最長で 8 日掛かることになる。事業用システムの不正利用を防ぐため，失効情報は可能な限り迅速に開示する必要があり，改善が必要である。

失効事由が，認証カード自体は利用可能な状態でありながら失効させる必要がある場合に事業用システムの不正利用に結び付く可能性が高い。これに該当する失効事由は「退職又は事業用システムの利用終了」「認証カードの紛失」「鍵の不正利用のおそれ」であり，失効事由の値は「**affiliationChanged**」，「**keyCompromise**」である。

■設問 3

〔試験センターによる解答例〕

(1) サーバ証明書の正当性を確認できず警告が表示される。(25 字)

(2) PC の Web ブラウザが不正なサーバ証明書を信頼し，不正なサーバにアクセスするリスク (41 字)

(1) グループ従業員が使用する PC のブラウザは，CA-3 が発行したサーバ証明書を受け取ると，その正当性を確認するため，CA-3 の上位 CA である D 社ルート CA の公開鍵証明書の公開鍵を用いてサーバ証明書に付与されたディジタル署名を検証する。D 社ルート CA の公開鍵証明書が PC に登録されていないと，**サーバ証明書の正当性を確認することができず，警告が表示される**ことになる。

(2) D 社ルート CA の公開鍵証明書が信頼する認証局の証明書として登録されていると，万一 D 社の認証局が何らかの原因で不正操作された場合，**取引先の PC の Web ブラウザが不正なサーバ証明書を信頼し，不正なサーバにアクセスしてしまうリスク**がある。取引先においては，D 社ルート CA の公開鍵証明書を専用の PC にインストールすることで，上記のリスクを軽減することができる。

■設問 4

〔試験センターによる解答例〕

(1) 認証を成功させても，事業用システムの利用の認可が得られないから (31 字)

(2)①・事業部門は管理責任者の役割を担わず，認証カードの配布・回収を担当しないから (37 字)

②・プロジェクトをまたいで認証カードが共用され，配布・回収の回数が少ないから（36 字）

(3) 入退室に必要なため，認証カードの置き忘れ及び現場事務所内での保管がなくなる。（38 字）

(1) 取引先の従業者が，回収の遅れや漏れのあった認証カードを用いて事業用システムを不正利用するには，J システムで認証を成功させた後，目的とする事業用システムの利用を認可される必要がある。表 3 の「システムの権限管理」にあるように，事業用システムの利用権限は，事業部門がプロジェクトの参加期間だけ有効となるようにシステムに登録している。そのため，取引先の従業者が回収の遅れや漏れのあった認証カードを用いて事業用システムを不正利用しようとした場合，J システムで**認証に成功しても，事業用システムの利用の認可を得ることができない**。

(2) 問題文にあるように，取引先に認証カードを貸与する方式の選択に際して優先させる非機能要件は，第 1 に事業部門での管理工数が少ないこと，第 2 にシステム部での管理工数が少ないことである。方式 A と方式 B を比較した場合，方式 B は，**事業部門は管理責任者の役割を担わないため，認証カードの配布及び貸与対象者からの回収等に工数を割く必要がなく**，非機能要件に適合している。

また，取引先の従業者によっては最多で五つのプロジェクトに同時参加していたり，3 割程度が 1 か月以内に次のプロジェクトに参加したりするという実態からすると，プロジェクトごとに従業者に認証カードを貸与する方式 A では，認証カードの配布及び回収が頻繁に発生し，多くの工数を要すると考えられる。それに対し方式 B は，**プロジェクトをまたいで認証カードが共用され**，半年以内に次のプロジェクトへの参加が見込まれる場合は貸与を継続するため，**認証カードの配布及び回収等の工数を削減することができ**，非機能要件に適合している。

(3) グループ従業員が認証カードをオフィスに置き忘れたり，現場事務所に保管したりするのは，認証カードを携帯する必要がないからであり，それが問題文にあるような不正利用につながっている。認証カードを入退室カードとしても利用するようになれば，外出時や帰宅時に携帯することになるため，**置き忘れや現場事務所での保管がなくなる**はずである。

＜問2＞ 脆弱性対策

■設問１

〔試験センターによる解答例〕

(1) ウ

(2) 脆弱性が発見された特定のバージョンのソフトウェアが導入された機器を迅速に特定するため（42 字）

(1) 項番 1 の「機器の重要度レベルの定義」は，「社外からアクセスできる」「重要情報を扱っている」ことから「重要度レベル高」となる。また，項番 2 の「脆弱性レベルの定義」は，X 脆弱性の CVSS 基本値が 6.5 であることから「脆弱性レベル低」となる。

したがって，項番 3 の「リスクレベルの定義」は「**リスクレベル 2**」となる。

(2) 固定資産管理台帳には各機器に搭載された OS，サーバソフトウェアやミドルウェアなどのソフトウェアの名称とバージョンは記載されていなかったため，X 脆弱性の対応において，ソフトウェア M を導入している機器の調査に多くの時間を要した。これを改善するため，新台帳にはバージョンを含むソフトウェアの情報も記載することにしたのである。

■設問２

〔試験センターによる解答例〕

(1) ウ

(2) ウ

(3) a：HTTP リクエスト（9 字）

(4) () { echo test; }; /usr/bin/cat /etc/passwd

(1) 図 7 の(2)にあるように，Web ブラウザからの HTTP リクエストによって Web サーバ上で Web アプリ B が起動され，bash が呼び出される。また，問題文に「典型的な Web サーバでは，Web サーバ（httpd）が［ a ］ヘッダの④フィールド値を環境変数として設定してから Web アプリ B を起動するので，攻撃者は，Y 脆弱性を悪用して Web サーバで任意のコードを実行することができる」とある。Y 脆弱性を悪用される条件に TLS や Cookie は関係ないことからも，必要な条件に該当するのは「**Web サーバに Y 脆弱性がある bash が導入されていること**」である。

(2) コマンドの実行権限は，そのコマンドを呼び出したソフトウェアやアプリケーションプログラムの実行時の権限になる。図 7 にあるように，bash を呼び出しているのは Web アプリ B であるため，cat コマンドは「**Web アプリ B の実行時の権限**」となる。

(3) Web 通信におけるヘッダ（HTTP メッセージヘッダ）には，HTTP リクエスト時に送信される HTTP リクエストヘッダ，HTTP レスポンス時に送信される HTTP レスポンスヘッダがある。［ a ］は HTTP リクエスト時に送信されるヘッダであるため，「**HTTP リクエスト**」が入る。

(4) 下線④の前後にあるように，Web サーバ（httpd）が HTTP リクエストヘッダのフィールド値を環境変数として設定することで，攻撃者は Y 脆弱性を悪用して Web サーバで任意のコードを実行することが可能となる。つまり，フィールド値には環境変数として設定する文字列が入る。図 6 のファイル/etc/passwd を不正に参照する際のコマンドの例の中で，環境変数に設定する文字列である「**() { echo test; }; /usr/bin/cat /etc/passwd**」を HTTP ヘッダフィールドのフィールド値として設定すればよい。

■設問３

〔試験センターによる解答例〕

(1) b：パターンマッチング（9 字）

(2) WAF の場合，検証作業の試験項目がパッチ適用のときよりも少なくて済むから（36 字）

(3) c：ウ

d：イ

(4) 通信量の上限の切替えで WAF の能力変更が随時可能，かつ作業工数やコストの観点から無駄がない。（46 字）

(1) WAF のシグネチャとは，攻撃の特徴を示す文字列である。シグネチャを用いて攻撃を検知する手法を**パターンマッチング**と呼ぶ。

(2) 通常サーバへパッチを適用する場合には，事前に検証用環境にパッチを適用し，当該脆弱性が修正されたことを確認するとともに，パッチ適用後もサーバで動作するアプリケーションプログラムの全ての機能が正常に動作することを検証する必要がある。それに対し，

WAF による対応の場合は，目的とする攻撃を正しく検知することができることを検証できればよいため，**サーバへのパッチ適用よりも実施期間を短くすることが可能**である。

(3) 表 1 にあるように，クラウド型の WAF では，公開 Web サーバの別名としてサービス事業者に指定された FQDN を設定する。設定するサーバは **DNS サーバ**であり，別名を設定するリソースレコードは **CNAME** である。

(4) 問題文にあるように，β製品本部の Y 脆弱性がある公開 Web サーバには，新製品の発表時などに，購入希望者からのアクセスが通常時の 100 倍程度まで一時的に増大するものがあり，かつ，次の新製品発表が 3 週間後に予定されているという状況である。クラウド型の WAF であれば，機器を購入する必要がないため，短期間での導入が可能であるとともに，**サービス利用契約を随時更新して通信量の上限を切り替えることができる**。加えて，設定とログ解析もサービス事業者が実施するため，オンプレミス型に比べ，A 社の**作業工数のコストを低減することが可能**である。

■設問 4

〔試験センターによる解答例〕

(1) f：社内 Web サーバの URL（12 字）

(2) e：オ

g：ア

h：キ

(3) プロキシサーバを通じて攻撃者のサイトと通信する機能（25 字）

(1) 社外の攻撃者が社内 Web サーバに対する Y 脆弱性を悪用した攻撃を成功させるためには，攻撃者が**社内 Web サーバの URL** を知ることができ，その情報を図 8 の(2)の攻撃コードに組み込むことができる必要がある。

(2) 近年多くの Web サイトで，JavaScript などのスクリプト言語を使ってサーバと非同期通信を行うことで，Web ページ全体を再描画することなく，ページの必要な箇所だけを部分的に更新することを可能にする Ajax（Asynchronous JavaScript + XML）が利用されている。

Ajax でサーバと通信を行う際には **XMLHttpRequest（XHR）**を用いる。XHR は，各種

ブラウザに実装されている組込みオブジェクト（API）であり，同期通信，非同期通信の双方をサポートしている。

XHR を用いることにより，サーバとの通信をスクリプトで制御することが可能となる。ただし，悪意のあるサイトに対し，不用意にクッキーや個人情報を送ってしまわないようにするなど，セキュリティ上の理由から，当初の XHR ではドメインの異なるサイトに対してリクエストを送信（クロスドメインリクエスト）できないように制限されていた。これを「Same-Origin ポリシ」あるいは「**同一生成元ポリシ**」と呼ぶ。

しかし，その後多くのブラウザに実装された XHR Level2 では，受信する Web サーバの HTTP レスポンスヘッダに「**Access-Control-Allow-Origin**」が付加されている場合において，クロスドメインリクエストが可能となった。

上記より，［ e ］には**オ**，［ g ］には**ア**，［ h ］には**キ**が入る。

(3) 問題文で F 氏が「攻撃者が A 社のプロキシサーバを利用するために必要な情報を知ることができた場合には，図 8 中の(4)，(5)とは別の手法を用いることで，社内 Web サーバの情報が攻撃者のサイトに送信されるおそれがある」と指摘していることから，「**プロキシサーバを通じて攻撃者のサイトと通信する機能**」が該当する。

■設問５

〔試験センターによる解答例〕

(1) i：中

(2) ア，ク

(3) j：重要情報が漏えいする（10 字）

k：社外から侵入される（9 字）

※j，k は順不同

(1) 問題文に「Q 主任は，重要情報を扱ってはいないが社外からアクセスできる機器，及び社外からアクセスできないが重要情報を扱っている機器も，場合によっては直ちに脆弱性に対応する必要があると考えた」とある。

これらのうち，後者については図 10 の「機器の重要度レベルの定義」が「重要度レベル中」となっており，かつ，「リスクレベルの定義」で「脆弱性レベル高」の場合に「リスクレベル 2 又は 3」となることからわかるように，［ i ］には「**中**」が入る。

(2) 図 9 の案では，リスクレベル 2 の場合に V チームによる評価を行うことにしている。図 4 でリスクレベル 2 となる条件は次の 4 つである。
「重要情報を扱っている」「社外からアクセスできる」「脆弱性レベル低」
「重要情報を扱っている」「社外からアクセスできない」「脆弱性レベル高」
「重要情報を扱っていない」「社外からアクセスできる」「脆弱性レベル高」
「重要情報を扱っていない」「社外からアクセスできない」「脆弱性レベル高」

解答群でこれに該当するのは，ア，ウ，オ，クである。
これに対し，図 10 の案では「重要度レベル中」「脆弱性レベル高」の場合に V チームによる評価を行うこととしているため，この条件に合致するのは次の 2 つである。

「重要情報を扱っている」「社外からアクセスできない」「脆弱性レベル高」
「重要情報を扱っていない」「社外からアクセスできる」「脆弱性レベル高」

つまり，図 10 の修正案では，解答群のウ，オのみが V チームによる評価を行う対象となり，**ア**，**ク**については対象外となる。

(3) 実際のリスクレベルは各機器の接続環境，構成，実装，設定等によって異なるため，それらを十分評価する必要がある。評価を行う条件としては，**社外からの侵入**，**重要情報の漏えい**，といったリスクが高い場合が挙げられる。