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。