●平成31年度春期
午後問題 解答・解説

問1　クラウドサービスの利用者認証（情報セキュリティ）（H31春-FE 午後問1）

【解答】

［設問1］　a－カ，b－イ，c－ウ

［設問2］　d－エ，e－イ

【解説】

クラウドサービスの利用者認証に関する出題である。これまで，基本情報技術者試験の午後問題でそれほど問われなかったIdPやLDAPなどのキーワードが登場し，認証の流れが非常に細かく説明されている。内容としては，クラウドサービスのシングルサインオン用に広く普及しているSAML2.0を題材にしている

問題文の内容を理解するのにひと苦労する難問だったであろう。しかし，選択式であるメリットを生かし，矛盾しているの選択肢を消去法で消していくと，自然に正解が絞られる。必須問題であることから，分からないなりに最後まであきらめずに解き切ってほしい。

［設問1］

・空欄a：〔クラウドサービスの利用者認証〕の(3)には「利用者が本人であることを確認するためにA社認証サーバで用いる［a］は，B社クラウドサービスには送信しない」とある。ヒントは，「利用者が本人であることを確認するため」の部分である。本人認証をするには，「利用者ID」と「パスワード」が必要である。図1の後にも「業務システムの利用者認証は，A社認証サーバでの利用者IDとパスワードの検証」と記述されている。

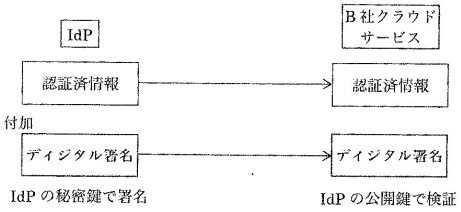
　では，「利用者ID」と「パスワード」のどちらを送信しないのだろうか。セキュリティの観点で考えると，インターネットにはパスワードを送信したくない，というのが通常の感覚であろう。〔B社クラウドサービスが利用可能になるまでの処理の手順〕の⑨でも，「Webブラウザは，⑧の転送指示に従い，認証済情報をB社クラウドサービスに送信する」とある。利用者認証情報ではなく，「認証済情報」を送っており，パスワードは送信していない。認証済情報とは〔クラウドサービスの利用者認証〕に「認証結果，認証有効期限及び利用者ID（以下，これら三つを併せて認証済情報という）」とあり，ここからも確認できる。つまり，「利用者ID」は送信するが，（カ）の「パスワード」は送信しない。

・空欄b：〔クラウドサービスの利用者認証〕には「B社クラウドサービスは，付加されているディジタル署名を使って，受信した認証済情報に［b］がないことを検証する」とある。この記述から，「ディジタル署名」によって実現できる機能である「改ざん防止」，「（他人による）なりすまし防止」，「（本人による）否認防止」の三つに着目すると正解に近づく。この中で，選択肢にあるものは（イ）の「改ざん」だけである。事前知識がなかったとしても，前後の文脈から，「改ざん」を選ぶことができた受験者もいただろう。

　なお，「（本人による）否認防止」とは，行為や事象について，後から否定しようとしたり，取り消そうとしたりすることを防ぐことである。

・空欄c：空欄bの後に「このために，IdPの［c］をB社クラウドサービスに登録しておく」とある。正解を導くには，その前の「IdPは，（中略）ディジタル署名を付加して」，「B社クラウドサービスは，付加されているディジタル署名を使って，受信した認証済情報に［b］（改ざん）がないことを検証する」の部分が重要になる。

　整理すると，IdPとB社クラウドサービスのディジタル署名の流れは図Aのようになり，B社クラウドサービスは，IdPが付加したディジタル署名を検証する必要がある。

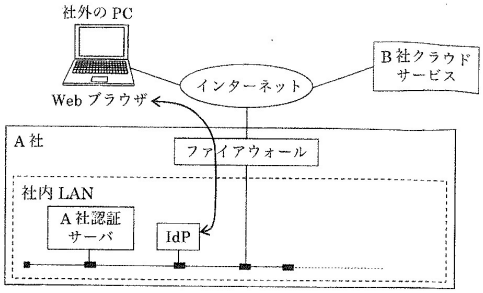


図A

　ディジタル署名を付加しているのはIdPなので，IdPの秘密鍵で署名されている。これを検証するには，IdPの公開鍵が必要になる。したがって，空欄cには（ウ）の「公開鍵」が入る。

［設問2］

・空欄d：まず，B社クラウドサービスに移行した後の構成図を図Bで考えてみよう。分かりやすくするため，該当する機器だけを記述している。〔クラウドサービスの利用者認証〕に「IDプロバイダ（以下，IdPという）を社内LANに設置することにした」とあるように，IdPは社内LANに設置される。



図B

　ここでは，〔B社クラウドサービスが利用可能になるまでの処理の手順〕の①～⑩に沿って，Webブラウザから，B社クラウドサービスを利用することを考える。

　設問の「図2中の［e］の送信で失敗」の部分がヒントである。図1の後にはセキュリティポリシが記述されており，通信を禁止するものを問題文から探すと，ファイアウォールしかない。

　次に，図2を確認すると，通信をしているのは「B社クラウドサービス」，「Webブラウザ」，「IdP」，「A社認証サーバ」の四つである。図Bを見ていくと，「B社クラウドサービス」と「Webブラウザ」（図Bの社外のPC）は，どちらも社外にあり，ファイアウォールで通信が禁止されることはない。同様に，「IdP」と「A社認証サーバ」も，どちらもA社の社内LANにあるので，ファイアウォールで通信は禁止されない。禁止される可能性があるのは，Webブラウザと IdPだけであると考えられる。

　図2の処理の流れを確認すると，Webブラウザと IdPは通信をする必要がある。しかし，セキュリティポリシに基づき「社外からインターネットを介した社内LANへの通信は，全てファイアウォールによって禁止されて」，通信ができない。このため，社外からB社のクラウドサービスを利用しようとしても，失敗することになる。

　したがって，空欄dには（エ）の「Webブラウザが，IdPと通信する」が入る。

　他の選択肢も見ておこう。

ア：「B社クラウドサービスが，IdPと直接通信する」とあるが，図2を見ても，直接通信をする必要がない。

イ：「B社クラウドサービスが，利用者認証情報を検証し，Webブラウザに返信する」とあるが，B社クラウドサービスが検証するのは利用者認証情報ではなく認証済情報である。また，「B社クラウドサービス」，「Webブラウザ」のどちらも社外にあり，A社のファイアウォールでは禁止できない。

ウ：「IdPが，利用者に代わって，利用者認証情報をB社クラウドサービスに送信する」とあるが，図2を見ても，そのような通信は存在しない。

・空欄e：設問には，「図2中の［e］の送信で失敗し，利用者認証されないからである」とある。空欄dで解説したように，Webブラウザと IdPは通信をする必要があるが，ファイアウォールによって通信が禁止されている。このため，利用者認証がされない。では，この通信は図2の中のどれに当たるか。該当する番号は，③と⑤である。先に行われる③で失敗するので，⑤は実施されない。したがって，（イ）の「③」が正解である。