される。

(2) 図 7 の（あ）の画面は SP であるサイト Q のサーバから送られた HTML が表示されたものである。続く（い）の画面は IdP であるサイト S のサーバから送られた HTML が表示されたものである。そして（う）の画面は、表示されている内容からも、SP であるサイト Q のサーバから送られた HTML が表示されたものである。

(3) アカウントの紐付け時も基本的な流れは図 7 と同様である。まず、図 8 の（え）（お）の画面は SP であるサイト Q のサーバから送られた HTML が表示されたものである。続く（か）（き）の画面は IdP であるサイト S のサーバから送られた HTML が表示されたものである。そして、（く）（け）の画面は、サイト S のアカウントが作成され、サイト Q アカウントとの紐付けが行われた後、IdP から SP であるサイト Q のサーバに結果が連携され、それに基づいてサイト Q のサーバから送られた HTML が表示されたものである。したがって、（え）（く）が“SP”、（か）（き）が“IdP”となる。

＜問 2＞　クラウドサービスを活用したテレワーク環境

●設問 1

[試験センターによる解答例]

(1) イ
(2) 第三者の OTP アプリで不正に OTP を生成される。(24 字)
(3) a：ウ
　　b：エ
　　c：イ
　　d：ア
　　e：カ
　　f：オ

＜解説＞

(1) 問題文のスマホアプリ方式の説明にあるように、OTP アプリは TOTP に従って OTP を QR コードで表示する。この OTP が第三者によって推測されないようにするた

め、QR コードには、秘密情報を含める必要がある。解答群でそれに該当するのはシェアードシークレットである。

(2) 要件 2 は、T 環境へのログインパスワードが見破られても、それだけでは不正アクセスできないようにすることであり、そのために IDaaS-Y の OTP アプリを用いて OTP を生成し、2 要素認証を行う方式を E 社は採用した。仮に T 環境へのログインパスワードが見破られており、かつ IDaaS-Y の OTP アプリ初期設定用の QR コードを表示する機能へのアクセスが E 社以外のネットワークからも可能であったとすれば、第三者によって OTP アプリが悪用され、不正に OTP を生成される可能性がある。

(3) OpenID Connect は、API 連携技術により、サードパーティアプリケーションが認証サーバとの間で認証連携する技術である。OpenID Connect では、認証連携に必要な認証情報をやり取りするためにトークンを用いる。

まず、図 3 の空欄は [d] のみであるが、前後の流れと解答群から、会議ツール Z による「トークンを検証」であることがわかる。したがって [d] にはアが入る。
続いて図 2 を見ると、[d] の前に [a] ～ [c] があるが、[d] は SaaS-X による「トークンを検証」であるため、その前にはトークンに関する通信メッセージや処理が入ることがわかる。
[a] では、SaaS-X が IDaaS-Y と認証連携するため、トークンエンドポイントに認可コード等を提示し、トークンを要求する。したがって [a] にはウが入る。
トークン要求を受けたトークンエンドポイントは、SaaS-X から提示された認可コードを検証する。したがって [b] にはエが入る。
トークンエンドポイントは、認可コードの検証結果に問題がなければ SaaS-X にトークンを返す。したがって [c] にはイが入る。
[d] でのトークンの検証後、SaaS-X はユーザ情報エンドポイントにユーザ情報を要求する。それを受け、ユーザ情報エンドポイントが SaaS-X にユーザ情報を返す。したがって [e] にはカ、[f] にはオが入る。

●設問 2

[試験センターによる解答例]

社内情報を表示した画面をカメラで撮影するという方法（25 字）

＜解説＞

問題文の〔要件 4 への対応〕にある設定が行われていれば、ノート PC からネットワークや USB デバイス等を介して社内情報が持ち出されるリスクは極めて低くなる。しかし、画面に表示される社内情報をカメラ等で撮影し、社外に持ち出すことは可能であり、それを技術的な対策で防ぐことは難しい。

●設問 3

[試験センターによる解答例]

(1) 社内情報を表示した画面のスクリーンショットを取るという方法（29 字）
(2) ア、ウ、エ

＜解説＞

(1) VD とノート PC との間でクリップボード及びディスクを共有できないように設定されており、ノート PC 自体には社内情報は存在しないため、ノート PC にマルウェアが感染しても、PC や VD のハードディスクから取得することはできない。しかし、問 2 の手法と同様に、利用者が社内情報を画面に表示しているときに、マルウェアが PC のスクリーンショット機能を悪用して社内情報を取得し、社外に持ち出される可能性がある。

(2)・DaaS-V は、PC が業務を行うための VD 基盤を提供しており、T 環境内のノート PC からのアクセスを許可する必要がある。
・EDR-U はクラウド上の DaaS-V がオプションとして提供してサービスであり、T 環境内からアクセスする必要はない。
・IDaaS-Y は T 環境へのログイン時の認証に使用するため、T 環境内からのアクセスを許可する必要がある。
・MDM-W は、ノート PC とスマホにインストールしたデバイス用ソフトウェアが通信するため、T 環境内からのアクセスを許可する必要がある。
・SaaS-X は、クラウド上の VD 環境（DaaD-V）から利用するサービスであるため、T 環境内からアクセスする必要はない。
・会議ツール Z は、SaaS-X と同様にクラウド上の VD 環境（DaaD-V）から利用するサービスであるため、T 環境内からアクセスする必要はない。

したがって、T 環境内からのアクセスを許可する必要があるのはア、ウ、エである。

●設問 4

［試験センターによる解答例］

セキュリティ対策についての第三者による監査報告書で確認するという方法
（34 字）

＜解説＞

問題文の〔クラウドサービス固有の課題〕にあるように、CSP のような IT サービス基盤に対して、その利用者である企業等が直接脆弱性検査を実施しようとしても許可されないケースが大半である。とはいえ、通常 CSP は自社で第三者によるセキュリティ監査や脆弱性検査を実施しているため、CSP に依頼してその報告書を閲覧することで確認する方法がある。

●設問 5

［試験センターによる解答例］

DaaS-V でのクライアント証明書によるデバイス認証（26 字）

＜解説＞

DaaS-V のフィッシングサイトで T 環境実験メンバの入力した内容が詐取された場合、第三者がそれを悪用して実験メンバになりすまし、T 環境への不正アクセスを試みる可能性がある。しかし、これについては問題文〔要件 3 への対応〕にあるように、DaaS-V でクライアント証明書によるデバイス認証を行うことで、貸与するノート PC 以外のデバイスからの T 環境への不正アクセスを防ぐことができる。

●設問 6

［試験センターによる解答例］

（1）g：パスワードの推測によってログイン（16 字）
（2）容易に推測可能な PIN コードを設定する。（20 字）
（3）クライアント証明書によるデバイス認証を行う仕組み（24 字）

＜解説＞

（1）OS に搭載されたディスク暗号機能を使ったとしても、紛失したノート PC を取得

した第三者が、パスワードを推測することによって当該 PC にログインすることができれば、ディスクは復号されるため、そこに保存された営業資料を悪用することが可能である。

(2) システム管理者がランダムな PIN コードを設定する方式に対し、利用者が設定した場合の問題として、容易に推測可能な PIN コードが設定されてしまうことが考えられる。

(3) 要望 X が許可されると、第三者によってインターネット VPN 経由で E 社のネットワークに侵入される可能性がある。こうした第三者による不正アクセスに対し、DaaS-V では、クライアント証明書によるデバイス認証を行うことで、貸与するノート PC からのみ接続できるようにしている。E 社のインターネット VPN においても、これと同等のセキュリティを実現するため、FW の VPN 機能にクライアント証明書によるデバイス認証を行う仕組みが必要である。