問2　クラウドサービスを活用したテレワーク環境に関する次の記述を読んで，設問 1～6 に答えよ。

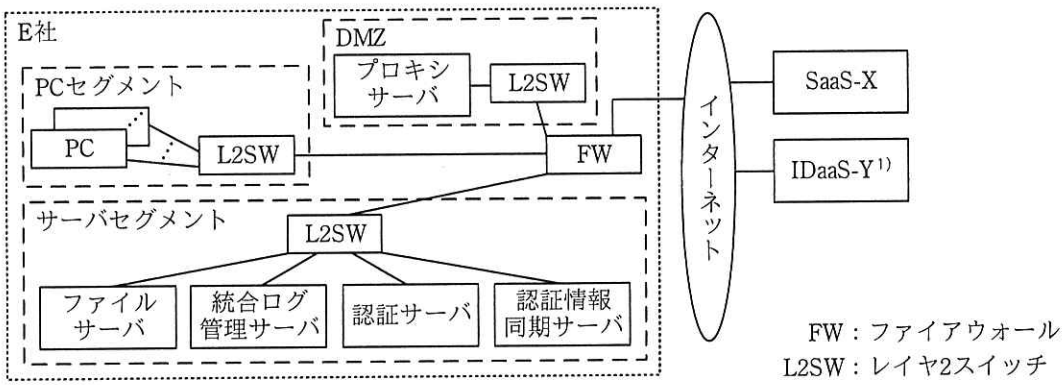
E 社は，従業員数 5,000 名の IT 企業である。E 社では，働き方改革の一環として，テレワーク環境を整備することになった。テレワーク環境について検討すべき重要なテーマの一つに，テレワーク環境経由での情報漏えいを起こさないためのセキュリティ確保がある。そこで，テレワーク環境の整備をシステム企画部長の指示の下，情報処理安全確保支援士（登録セキスペ）でもあるシステム企画部の F 次長，及び部下の G さんが担当することになった。

現在 E 社では，次のクラウドサービスを利用している。

・電子メールの送受信及びスケジュールの管理のための基盤を提供する，X 社のクラウドサービス（以下，SaaS-X という）

・クラウドサービスの認証基盤を提供する，Y 社のクラウドサービス（以下，IDaaS-Y という）

E 社のネットワーク構成を図 1 に示す。



注 1)　SaaS-X の認証に利用している。

図 1　E 社のネットワーク構成（概要）

IDaaS-Y を用いても，社内と同じ利用者 ID とパスワードで認証できるように，サーバセグメントに設置した認証情報同期サーバを経由して認証サーバと IDaaS-Y の認証情報を同期している。

F 次長は，全社に展開する前に，まずテレワーク実証実験環境（以下，T 環境という）を構築し，一部の従業員（以下，実験に参加する従業員を実験メンバという）に実際に利用してもらい，結果を経営陣に報告することにした。

〔T 環境の要件〕

T 環境においては，E 社の従業員の多くが実施している次の業務を，自宅や出張先から実施できるようにすることにした。

業務 1：電子メールの送受信及びスケジュールの管理を行う。

業務 2：業務文書を作成し，ファイルサーバ上に保存する。また，その業務文書を閲覧・編集する。

業務 3：従業員間でテレカンファレンスを実施する。

F 次長は，業務 1～3 を実施できるよう，T 環境を，次のように整備する方針とした。

・T 環境の構成要素の一部として，各実験メンバにスマートフォン（以下，スマホという）及びノート PC を貸与する。スマホは，ノート PC をインターネットに接続するために利用する。

・実験メンバは，仮想デスクトップ（以下，VD という）で業務を行う。そのために，VD 基盤を提供する V 社のクラウドサービス（以下，DaaS-V という）を利用する。

・FW の VPN 機能を利用して，DaaS-V と E 社のネットワークをインターネット VPN で接続する。

・VD では文書作成ソフトによる業務文書の作成・閲覧・編集・保存を行えるようにする。

・テレカンファレンスは，コミュニケーション基盤を提供する Z 社のクラウドサービス（以下，会議ツール Z という）を利用し，E 社のネットワークからのアクセスだけを許可する。VD には会議ツール Z のクライアントソフトを導入する。

F次長は，T環境におけるセキュリティ要件を，次のように定め，対応するための対策を検討した。

要件1：スマホ及びノートPCには，インストール可能なアプリケーションソフトウェアの制限及び必要な設定の強制をする。

要件2：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，2要素認証を行う。

要件3：T環境へは，貸与するノートPCからだけログインできるようにする。

要件4：T環境からの情報の持ち出しは禁止する。

要件5：T環境でマルウェア感染を検知・防止する。

要件6：T環境では認証ログ，操作ログを記録する。

〔要件1への対応〕

要件1への対応として，モバイルデバイス管理基盤とデバイス用ソフトウェアを提供するW社のクラウドサービス（以下，MDM-Wという）を利用することにし，貸与するスマホとノートPCにデバイス用ソフトウェアをインストールすることにした。また，MDM-Wの認証は，IDaaS-Yを利用することにした。

MDM-Wは，ノートPCの脆弱性修正プログラム及びマルウェア対策ソフトのインストール並びにマルウェア定義ファイルの更新にも利用することにした。

〔要件2への対応〕

要件2への対応として，IDaaS-Yを利用することにした。

まず，IDaaS-Yが対応している2要素認証について調査した。パスワード方式による認証に追加可能なものは次の4方式であった。

SMS方式　：事前登録した電話番号にSMSでワンタイムパスワード（以下，OTPという）を送付する。

自動音声方式　：事前登録した電話番号に自動音声でOTPを通知する。

スマホアプリ方式：OTP表示用のスマホアプリケーションソフトウェア（以下，OTPアプリという）を利用する。OTPアプリはTOTP（Time-Based One-Time Password Algorithm）に従ってOTPを表示する。

FIDO方式　：事前登録したデバイスでFIDO認証を行う。

費用を抑えたいが，SMS 方式及び自動音声方式は認証の都度料金が発生する。また，FIDO 方式は，FIDO 認証に対応したスマホが必要となるが，貸与予定のスマホは FIDO 認証に対応していない。そこで，スマホアプリ方式を採用することにした。

OTP アプリは事前に次のようにして設定する。

1. PC から Web ブラウザで IDaaS-Y にログインする。
2. IDaaS-Y の OTP アプリ初期設定用の QR コードを表示する機能にアクセスし，OTP アプリ初期設定用の QR コードを表示させる。
3. ①当該 QR コードを OTP アプリで読み込む。

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は，E 社の利用者 ID でログインするときには，②E 社のネットワークからのアクセスだけに制限することにした。

次に，IDaaS-Y と各クラウドサービス間の認証連携について検討した。ノート PC から VD へアクセスする際の，VD と IDaaS-Y との認証連携は，RADIUS で行うことにした。VD から SaaS-X にアクセスする際の，SaaS-X と IDaaS-Y との認証連携は，図 2 のように OpenID Connect の認可コードフローでこれまでと同様に行うことにした。VD から会議ツール Z にアクセスする際の，会議ツール Z と IDaaS-Y との認証連携は，図 3 のように Implicit フローで行うことにした。

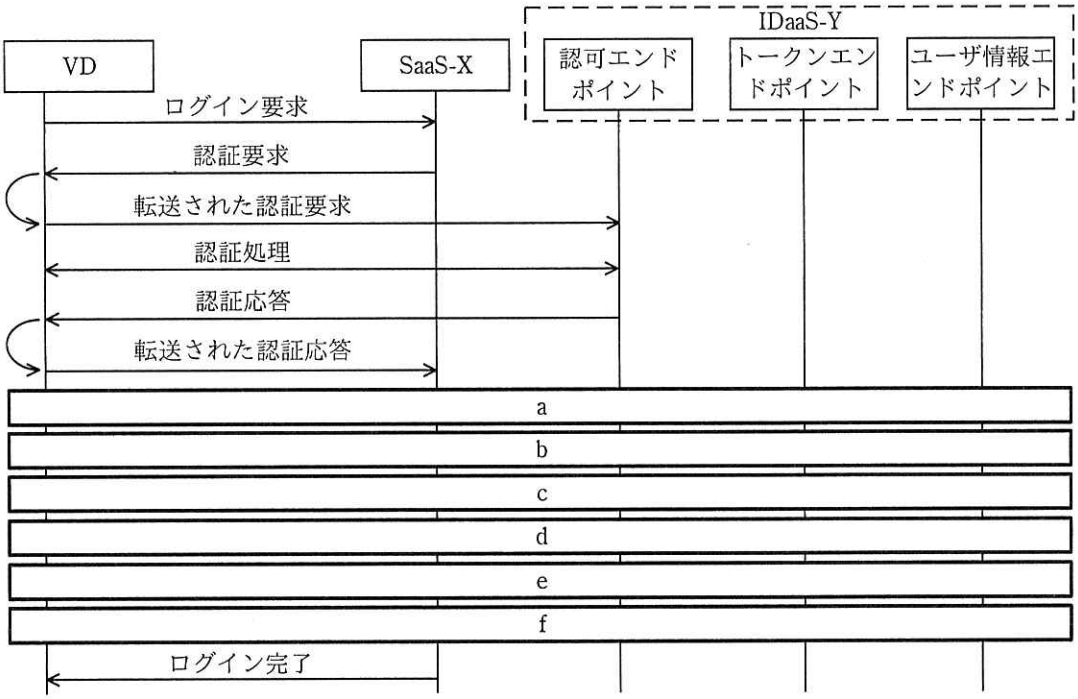


図 2　SaaS-X と IDaaS-Y との認証連携

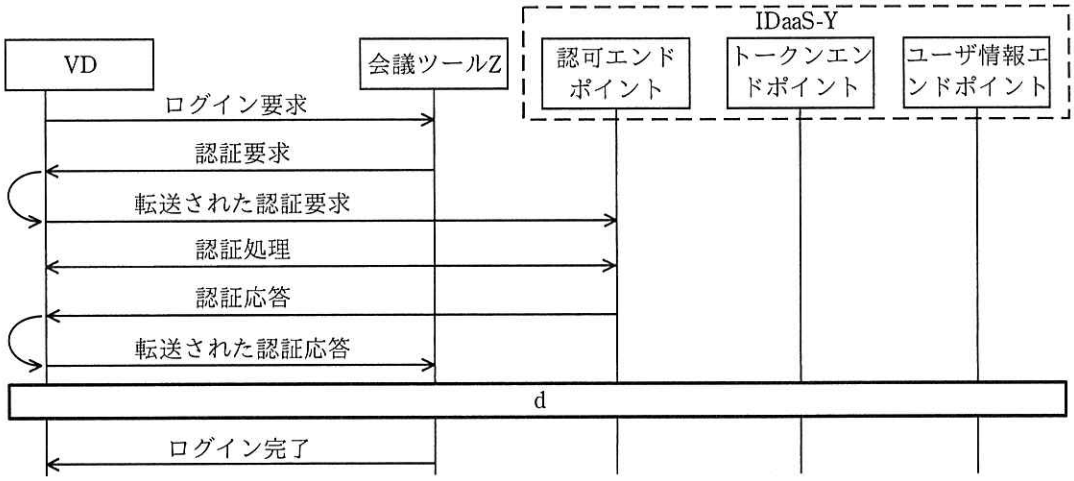


図 3　会議ツール Z と IDaaS-Y との認証連携

〔要件 3 への対応〕

要件 3 への対応として，DaaS-V の利用時は，IDaaS-Y による 2 要素認証に加えて，クライアント証明書によるデバイス認証を DaaS-V で行うことにした。社内にプライベート認証局を構築し，当該認証局の証明書によるクライアント証明書の検証が行

われるようにDaaS-Vを設定することにした。クライアント証明書はMDM-Wを利用して，ノートPCのTPM（Trusted Platform Module）に格納することにした。

〔要件4への対応〕

要件4への対応として，VDからインターネットへのアクセスは，全てE社のネットワークを経由させることによってアクセス先の制限とアクセスの監視を行うことにした。

また，VDとノートPCとの間でクリップボード及びディスクの共有を禁止するようにDaaS-Vを設定することにした。Gさんが設定してみたところ，ノートPCからは，VDの閲覧，キーボード及びマウスによる操作，並びにマイク及びスピーカによる会話しかできなくなることが確認できた。しかし，この設定であっても③利用者が故意に社内情報を持ち出すおそれがある。これについては，簡単には技術的対策ができないので，利用規程で禁止することにした。

〔要件5への対応〕

要件5への対応として，VD，ノートPC及びスマホに対するマルウェア感染の対策を検討した。

VDでは，電子メールの添付ファイル開封及びWebアクセスによるマルウェア感染のおそれがある。仮にVDがマルウェアに感染した場合に被害調査のためのディジタルフォレンジックスを行おうとしても，マルウェア感染したVDのディスクイメージを取得するのに時間が掛かったり，提供してもらえなかったりすることも考えられる。そこでDaaS-VがオプションとしてU社のクラウド型エンドポイント検知対応サービス（以下，EDR-Uという）も契約し，マルウェアの検知及び駆除並びに調査に必要な情報の常時収集をすることにした。

ノートPCについては，自由なWebアクセスを許可した場合，マルウェアに感染するリスク，及び利用者がVDを利用中に④マルウェアが社内情報を取得して持ち出すリスクが高くなる。そこで，それらのリスクを低減するために，MDM-Wでは，ノートPCからT環境へのアクセスだけを許可し，⑤T環境内のアクセスも必要最小限にする設定を行うことにした。

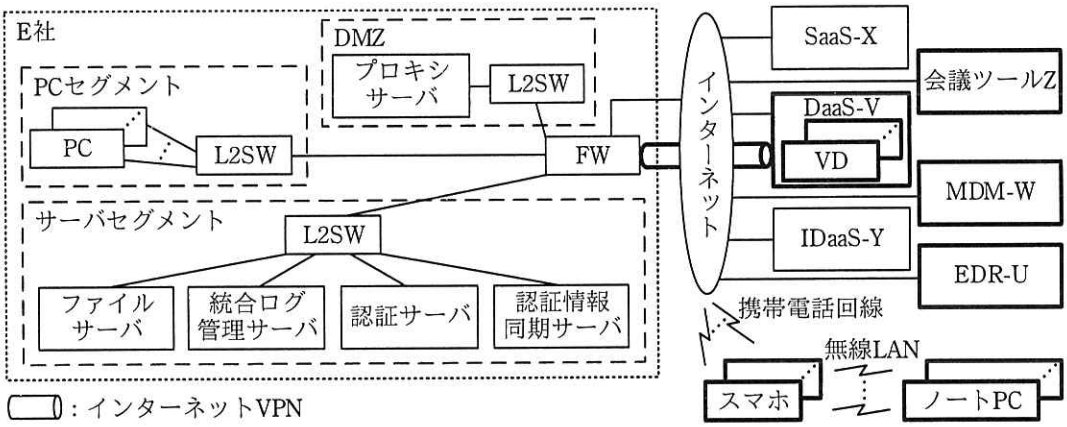
スマホについては，自由なWebアクセスを許可した場合でもマルウェア感染のリ

スクは十分低いと考えられたので，追加の対応は行わないことにした。

〔要件 6 への対応〕

要件 6 への対応として，ノート PC，スマホ及び各クラウドサービスで認証ログ，操作ログの記録を有効化することにした。また，各クラウドサービスにおいて記録した認証ログ，操作ログを取り出すための Web API が用意されていたので，統合ログ管理サーバにログを取り込み，ログ監視を一元的に行うことにした。

要件 1～6 に対応した T 環境のネットワーク構成を図 4 に示す。



注記　太線は T 環境構築に当たって追加されるものを示す。

図 4　T 環境のネットワーク構成（概要）

〔クラウドサービス固有の課題〕

T 環境で利用するクラウドサービスに脆弱性があれば，それを悪用する攻撃によって，E 社のセキュリティが侵害されるおそれがある。そこで，各クラウドサービスプロバイダ（以下，CSP という）に，脆弱性対策の状況についてのヒアリング及びサービスの基盤についての脆弱性検査を実施させてもらえないか確認した。そうしたところ，各 CSP ともヒアリングには対応するが，利用者による脆弱性検査は，サービス提供に影響を及ぼすおそれがあるので許可していないとの回答だった。そこで F 次長は，脆弱性検査を⑥別の方法とヒアリングで代替することにした。

〔実証実験の実施〕

各 CSP の脆弱性対策には大きな問題がなかった。そこで，図 4 の T 環境を構築し，システム企画部，人事部，営業部から実験メンバをそれぞれ 20 名ずつ計 60 名募った。実験メンバには，T 環境を利用できるように設定したスマホとノート PC を貸与し，期間を 3 か月間として，実証実験を開始した。

実証実験後，実験メンバにアンケートを採ったところ，多くの実験メンバから，これまでより利便性・生産性が向上したとの意見が集まった。また，二つの要望が出た。

〔公衆無線 LAN の利用〕

一つ目の要望は，出張の移動中又は宿泊先でスマホの通信回線が利用できなかった場合，公衆無線 LAN を利用したいというものである。国内の多くの公衆無線 LAN 環境では，無線 LAN アクセスポイントへの接続時に Web で利用者登録画面や利用規約同意画面が表示され，利用者が利用者情報を登録したり，利用規約への同意をしたりした後にインターネット接続が許可される仕組みになっている。ノート PC ではアクセス先を T 環境宛に制限していたので，これらの画面が表示されず，公衆無線 LAN を利用できなかったということであった。

そこで，F 次長は，ノート PC のアクセス先制限を緩和して利用者が公衆無線 LAN 環境に接続できるようにした場合のリスクを評価した。その結果，フィッシングサイトなどに誘導されるリスクが高まると考えられたが，仮に DaaS-V のフィッシングサイトで，利用者の入力が詐取されたとしても，その情報を悪用した不正アクセスは⑦検討済みの他の対策で防止できるので，ノート PC のアクセス先制限を緩和することにした。

〔業務文書のノート PC へのダウンロード〕

二つ目の要望（以下，要望 X という）は，営業部の実験メンバから，顧客を訪問した際の業務文書の閲覧・作成について挙がったものである。持込端末のインターネット接続が禁止されている顧客を訪問した際は，VD にアクセスできない。そこで，会社を出た後，訪問前にファイルサーバ上の営業資料をノート PC にダウンロードしておき，それを閲覧したり，ノート PC 上で顧客打合せの議事録の文書を作成し，訪

問後，会社に戻る前にその文書をファイルサーバにアップロードしたりしたいということであった。

要望Xを実現すると，ノートPCに対する盗難・紛失時の情報漏えい対策が必要になる。次は，この件についてのGさんとF次長の会話である。

Gさん：ノートPCの盗難・紛失時の情報漏えい対策としては，OSに搭載されたディスク暗号化機能を使えばよいのではないでしょうか。

F次長：そうだな。しかし，紛失したノートPCを第三者に取得されたときに，［ g ］されてディスクが復号されてしまうおそれがある。ディスク暗号化機能だけでは不十分だ。

Gさん：追加の対策はあるのでしょうか。

F次長：PINコードを利用したログイン方式を強制した場合を考えてみよう。PINコードを利用したログイン方式は，TPMを利用する。正しいPINコードが入力された場合，ディスクが復号される。今回，⑧PINコードは，6桁の数字とし，システム管理者が事前にランダムなものを設定することにしよう。

Gさん：6桁の数字だと総当たり攻撃で破られそうですが，大丈夫なのでしょうか。

F次長：誤った入力が5回連続で行われると管理者が回復用のパスワードを入力しない限りログインできなくなるように設定し，回復用のパスワードには推測困難な十分に長いランダムな文字列を設定する方法もある。

Gさん：なるほど。

F次長は，検討の結果，要望Xには原則として対応しないが，希望者には個別に申請してもらい，⑨申請が許可された利用者のノートPCについては，E社のネットワークとのインターネットVPNでの接続を可能とする方針にした。

F次長は，実証実験の結果，実験メンバからの要望及びそれへの対応，並びに残存するリスク及びその低減策についてシステム企画部長と経営陣に報告した。経営陣はテレワーク環境を全社に展開することを決めた。

設問1　〔要件2への対応〕について，(1)～(3)に答えよ。

(1)　本文中の下線①について，QRコードに含まれ，OTPアプリがOTPの生成に使用する情報を，解答群の中から選び，記号で答えよ。

解答群

ア　cookie　　イ　シェアードシークレット

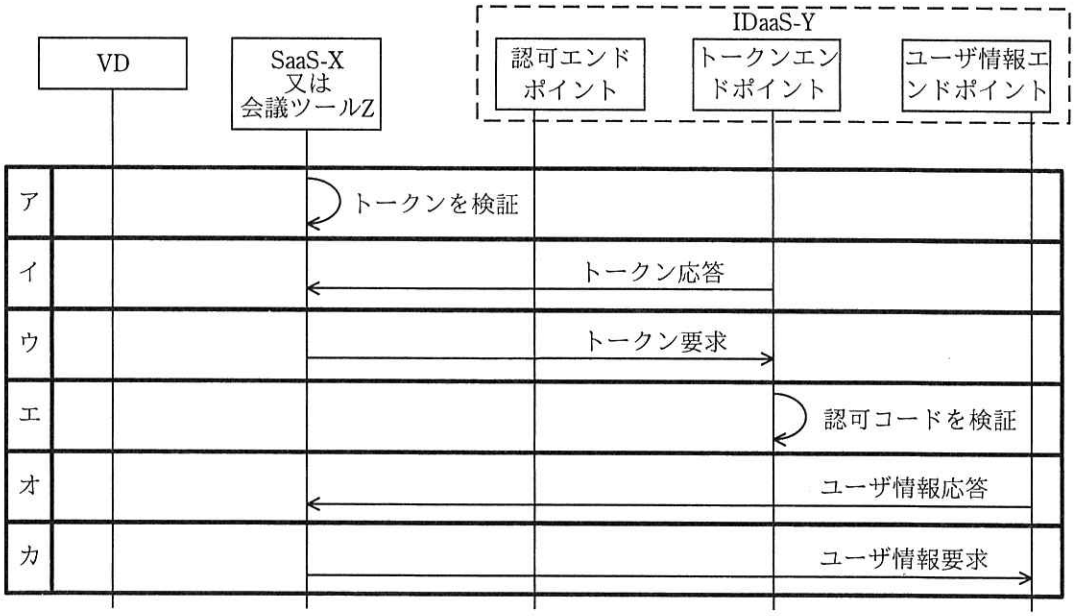
ウ　シリアル番号　　エ　タイムスタンプ

オ　ディジタル署名　　カ　フィンガプリント

(2)　本文中の下線②について，E社のネットワークからのアクセスだけに制限しなかった場合，OTPについてどのような問題が起きると考えられるか。起きると考えられる問題を30字以内で述べよ。

(3)　図2及び図3中の［　a　］～［　f　］に入れる適切な通信メッセージ又は処理を，解答群の中から選び，ア～カの記号で答えよ。

解答群



設問2　本文中の下線③について，ノートPCを介して持ち出す方法を30字以内で具体的に述べよ。

設問3　〔要件5への対応〕について，(1)，(2)に答えよ。

(1)　本文中の下線④について，マルウェアが社内情報を取得する方法を35字以内で具体的に述べよ。

(2) 本文中の下線⑤について，T 環境内のアクセスも必要最小限にする場合，許可するアクセス先を解答群の中から全て選び，記号で答えよ。

解答群

ア DaaS-V	イ EDR-U	ウ IDaaS-Y
エ MDM-W	オ SaaS-X	カ 会議ツール Z

設問4 本文中の下線⑥について，どのような方法か。35 字以内で述べよ。

設問5 本文中の下線⑦について，該当する対策を本文中の用語を用いて 35 字以内で述べよ。

設問6 〔業務文書のノート PC へのダウンロード〕について，(1)～(3)に答えよ。

(1) 本文中の［ g ］に入れる適切な字句を，20 字以内で述べよ。

(2) 本文中の下線⑧について，利用者に設定させるとどのような問題が起きると考えられるか。起きると考えられる問題を 25 字以内で具体的に述べよ。

(3) 本文中の下線⑨について，DaaS-V へのアクセスと同等のセキュリティを実現するためには，FW の VPN 機能にどのような仕組みが必要か。必要な仕組みを 30 字以内で具体的に述べよ。