SC

令和２年度
情報処理安全確保支援士試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問１，問２
選択方法	１問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問２を選択した場合の例〕

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　百貨店における Web サイトの統合に関する次の記述を読んで，設問 1～5 に答えよ。

C 社は，半年ほど前に旧 A 社と旧 B 社が合併してできた会社である。旧 B 社が存続会社となり，旧 A 社の事業を承継した上で，C 社に改称した。C 社は，旧 A 社の 10 店舗の百貨店（以下，A 百貨店という）と，旧 B 社の 5 店舗の百貨店（以下，B 百貨店という）を運営している。

C 社は，旧 A 社が発行していたクレジットカードの会員向け Web サイト（以下，サイト P という），A 百貨店の取扱商品を販売するオンラインストア Web サイト（以下，サイト Q という），及び旧 B 社のポイントカードを保有する会員向け Web サイト（以下，サイト R という）を運営している。

合併後，旧 A 社クレジットカードの B 百貨店での利用を促進したり，旧 B 社ポイントカードの A 百貨店での利用を可能にしたりするなど，両社の顧客サービスの融合に力を入れている。表 1 は，サイト P，Q，R の概要である。

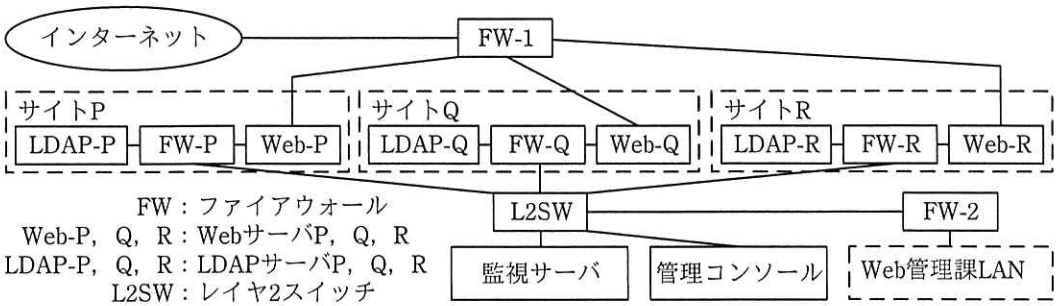
表 1　各サイトの概要

サイト名	機能	利用者 ID
サイト P	・利用明細の表示 ・クレジットカード利用ポイントの残高確認，商品又は他社のポイントとの交換申請 ・各種申請書類の送付依頼 ・アカウント管理（新規登録，パスワード変更，登録事項変更など）	英数字 8～16 字の文字列を利用者が設定する。
サイト Q	・A 百貨店の商品の購入 ・購入履歴の表示 ・アカウント管理（新規登録，パスワード変更，決済用クレジットカード登録など）	英数字 8～16 字の文字列を利用者が設定する。
サイト R	・ポイント獲得履歴，利用履歴の表示 ・ポイント獲得履歴から購買傾向を分析し，傾向に基づいたお買い得情報の表示 ・キャンペーンへの応募，応募履歴の表示 ・アカウント管理（新規登録，パスワード変更，パスワード失念時の処理など）	ポイントカードに記載されている数字 8 桁の会員番号が割り当てられる。

〔機器の集約と運用作業の効率化〕

C 社では，運用作業を効率化するために，別々の場所に設置されていた各サイトを構成する機器を 1 か所のデータセンタに集約するとともに，これらの機器を管理する

Web管理課を新設した。機器集約後のネットワーク構成は図1のとおりである。



注記　FW-1では，サイトP，Q，R相互間の通信を禁止している。

図1　機器集約後のネットワーク構成（抜粋）

サイトP，Q，Rは，それぞれ独立して運営されている。いずれのサイトも，アカウント情報はサイトごとに設置したLDAPサーバのユーザエントリとして管理しており，ログイン時の認証には，各LDAPサーバのユーザエントリ内の利用者IDとパスワードを利用している。

〔サイト間でのアカウントの共通利用〕

C社では経営戦略の一環として，三つのサイトで収集した情報から顧客の購買傾向を分析することにした。そこで，サイトP，Q，Rでクロス分析などの手法を用いて購買傾向を分析する上で，各サイト間で同一の顧客を特定するために，サイトP，Q，R相互間でのアカウントの共通利用を実現することにした。

アカウントの共通利用では，次の三つの利用方法のいずれかを各顧客に選択してもらうことにした。

(1) サイトPのアカウントを親アカウントとし，サイトQ，Rのアカウントを子アカウントとして，子アカウントを親アカウントに紐付(ひも)ける。主に旧A社の顧客向けである。

(2) サイトRのアカウントを親アカウントとし，サイトP，Qのアカウントを子アカウントとして，子アカウントを親アカウントに紐付ける。主に旧B社の顧客向けである。

(3) アカウントの共通利用をしない。

顧客がアカウントの紐付けを設定すれば，子アカウントの代わりに親アカウントを用いて各サイトにログインできる。

〔アカウントの共通利用の設計〕

Web 管理課の J 主任は，アカウントの共通利用の設計を任された。J 主任は，アカウントの共通利用を実現するために，次の四つを行うことにした。

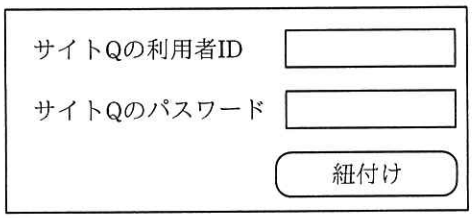
(1) サイト P，Q，R のログイン処理を変更する。

(2) LDAP-P，LDAP-R で管理するアカウント情報に，紐付け情報を保存する。具体的には，LDAP-P のユーザエントリに siteQid，siteRid 属性を追加して，当該アカウントに紐付けた子アカウントの利用者 ID を保存する。LDAP-R のユーザエントリには，sitePid，siteQid 属性を追加する。

なお，紐付け前の sitePid，siteQid，siteRid には，空文字列が設定される。

(3) Web-P，Web-R の Web アプリケーションプログラム（以下，Web アプリケーションプログラムを Web アプリという）に，アカウントの紐付け機能を追加する。

サイト P のアカウントを親アカウントとし，サイト Q のアカウントを子アカウントとして紐付けるときのサイト P の画面と処理内容は図 2 のとおりである。



［紐付け］ボタンが押された場合の処理
(i) Web-PのWebアプリが，LDAP-Qに問合せて，入力されたサイトQの利用者IDとパスワードを用いて認証を行う。
(ii) 認証に失敗したら，エラー画面を表示する。
(iii) Web-PのWebアプリが，LDAP-Pの該当するユーザエントリのsiteQid属性に，サイトQの利用者IDを書き込んで完了画面を表示する。

注記　サイト P にログイン済みである。

図 2　サイト P におけるサイト Q のアカウントの紐付けの画面と処理内容

(4) FW-P，Q，R のルールに対して必要な変更を行う。例えば，変更後の FW-P のルールは，表 2 のようにする。

表 2　変更後の FW-P のルール

項番	送信元	宛先	プロトコル	動作
1	監視サーバ，管理コンソール，Web 管理課 LAN	Web-P，LDAP-P	管理用プロトコル	許可
2	Web-Q，Web-R	LDAP-P	LDAP	許可
3	Web-P	a	b	許可
⋮	⋮	⋮	⋮	⋮
15	全て	全て	全て	拒否

注記 1　FW-P は，ステートフルパケットインスペクション型である。
注記 2　項番が小さいルールから順に，最初に合致したルールが適用される。
注記 3　項番 4～14 には，LDAP に関するルールは記述されていない。

〔個人情報の取扱い〕

J 主任は，C 社の法務担当の M さんに，アカウントの共通利用について説明し，個人情報の取扱いの観点から問題がないかどうか相談した。M さんは，合併前後の個人情報の利用目的の内容について確認した。

確認後，M さんは，アカウントの共通利用には，顧客に対して利用目的の変更を通知して，同意を得る必要があると指摘した。

指摘を受け，J 主任は，顧客がアカウントの共通利用を選択したときに，個人情報の利用目的の変更を通知するとともに，変更後の利用目的を明示して同意を得る機能を加えることにした。

〔コードレビュー〕

アカウントの共通利用の設計を終えた J 主任は，サイト P の Web アプリの改修に着手した。

図 3 及び図 4 は，サイト P のアカウントにサイト Q のアカウントを紐付ける場合のサイト P 上での紐付け処理の Java ソースコードである。

利用者が，サイト P にログイン後，図 2 の画面を操作し，“紐付け”ボタンをクリックした場合，図 4 の行番号 101 の siteID にサイトの識別文字列として“siteQ”が代入された状態で図 4 のコードの実行が開始される。図 4 のコードが正常に終了したら，紐付けが完了したことを表示する。

```
   (省略)    // パッケージ宣言，インポート宣言
             // インポート宣言には，javax.naming.NamingException を含む。
 1: public class AccountLink {
 2:     boolean childChecked;   // 子アカウントの利用者 ID のチェック完了フラグ
 3:     String childSite;       // 子アカウントのサイトの識別文字列
 4:     String childID;         // 子アカウントの利用者 ID
 5:     String childPW;         // 子アカウントのパスワード
 6:     String parentID;        // 親アカウントの利用者 ID
 7:     public static final int NO_ERROR = 0;                  // 正常終了コード
 8:     public static final int ERROR_SITE_UNAVAILABLE = -101; // エラーコード
 9:     public static final int ERROR_ID_OR_PW = -102;         // エラーコード
10:     public static final int ERROR_LINK_FAILED = -103;      // エラーコード

11:     public AccountLink(String site, String id, String pw, String loginID) {
12:         childChecked = false;
13:         childSite = site;
14:         childID = id;
15:         childPW = pw;
16:         parentID = loginID;
17:     }

18:     public int checkChild() throws NamingException {
            // サイトの識別文字列のチェック
19:         childChecked = childSite.equals("siteQ") || childSite.equals("siteR");
20:         if (!childChecked) {     // サイトの識別文字列が正当でなかった場合
21:             return ERROR_SITE_UNAVAILABLE;
22:         }
23:         switch (childSite) {
24:         case "siteQ":
25:             try {
                    // 認証情報チェック
26:                 if (siteQAuth(childID, childPW) == NO_ERROR) {
27:                     childChecked = true;    // 認証成功
28:                 } else {
29:                     childChecked = false;   // 認証失敗
30:                 }
31:             } catch (NamingException e) {   // 認証が実行できなかった場合
32:                 throw e;
33:             }
34:             if (!childChecked) {
35:                 return ERROR_ID_OR_PW;
36:             } else {
37:                 return NO_ERROR;
38:             }
```

図3　Web-P の Web アプリにおける AccountLink のクラス定義

```
39:         case "siteR":
                (省略) // サイトRに対して認証を行い，結果に応じてERROR_ID_OR_PW又は
                       // NO_ERROR を返して終了する。
40:         default:
                (省略) // ERROR_SITE_UNAVAILABLE を返して終了する。
41:         }
42:     }

43:     public int makeLink() throws NamingException {
            (省略) // LDAP-P 上の parentID のユーザエントリの属性 siteQid 又は siteRid
                   // に childID を書き込む。
44:     }

45:     private int siteQAuth(String qID, String qPW) throws NamingException {
            (省略) // 認証情報を確認し，認証成功なら NO_ERROR を，認証失敗なら NO_ERROR
                   // 以外の値を返す。必要な通信ができないなど，認証そのものが実行
                   // できない場合，例外 NamingException を投げる。
46:     }
        (省略) // その他のメソッドなどの定義
47: }
```

図3　Web-P の Web アプリにおける AccountLink のクラス定義（続き）

```
101:    AccountLink idPair = new AccountLink(siteID, userID, userPassword, loginId);
          // 各変数には次の内容が代入されている。
          //   siteID には，紐付けるアカウントのサイトの識別文字列
          //   userID には，紐付けるアカウントの利用者 ID
          //   userPassword には，紐付けるアカウントのパスワード
          //   loginId には，現在サイトPにログインしている利用者 ID
102:    int result = AccountLink.NO_ERROR;
103:    for (int retryCount = 1; retryCount < 4; retryCount++) {
104:        try {
                // サイトの識別文字列，利用者 ID/パスワードの組みを確認する。
105:            result = idPair.checkChild();
106:            if (result == AccountLink.NO_ERROR) {
107:                break;
108:            } else {
                    (省略) // result の値に従った適切な処理を実施する。
109:            }
110:        } catch (NamingException e) {
                (省略) // 再試行のために，一定時間待つ。
111:        }
112:    }
113:    if (!idPair.childChecked) {
114:        return AccountLink.ERROR_LINK_FAILED;
115:    }
```

図4　Web-P の Web アプリにおける AccountLink のメソッドを呼んでいる部分

```
116:     try {
117:         idPair.makeLink();          // アカウントの紐付けを実施する。
118:     } catch (NamingException e) {
             （省略）// 例外処理
119:     }
```

図4　Web-P の Web アプリにおける AccountLink のメソッドを呼んでいる部分（続き）

J主任は，情報処理安全確保支援士（登録セキスペ）のK主任とともにコードレビューを実施した。K主任は，次のような特定の状況では，サイトPのある利用者のアカウントに，サイトQの他人のアカウントが紐付いてしまうと指摘した。

(1)　図2で，サイトQの利用者ID欄に誤った利用者IDを入力する。

(2)　図4のコードが呼び出され，［　c　］に誤った利用者IDが代入されたまま，［　d　］が呼び出される。

(3)　何らかの理由で，［　d　］中の図3中の行番号［　e　］で［　f　］が発生し，結果として［　d　］が再試行される。

(4)　［　d　］が3回試行され，全て同じく［　f　］が発生すると，［　g　］の値はtrueなので，図4中の行番号［　h　］に進み，紐付けが行われる。

K主任は，図3の32行目前後に着目し，［　i　］という修正案を提示した。

〔サイトRでのインシデント〕

リリースに向けて準備を進めていたところ，インシデント発生の報告があった。発端は，ある顧客からの指摘で，その内容は，“サイトRのキャンペーン応募履歴を見たら，3月のキャンペーンに応募したことになっているが，身に覚えがない。3月にはサイトRに一度もアクセスしていないはずだ。”というものであった。

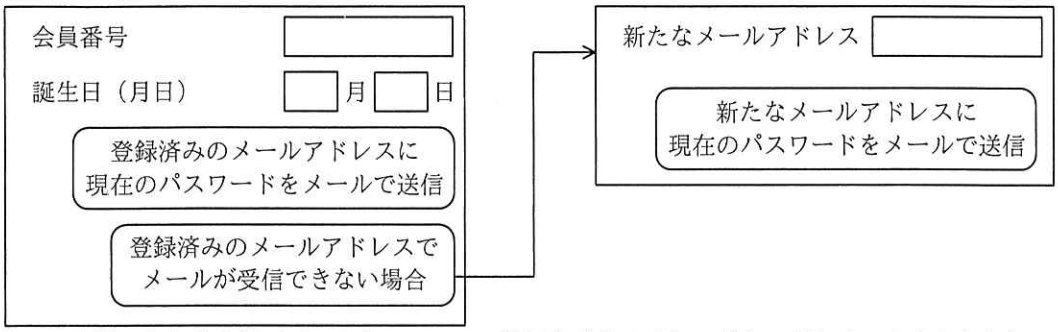
J主任が，サイトRのアクセスログを確認したところ，次のことが分かった。

・3月30日に，当該顧客のアカウントでキャンペーンに応募していた。

・応募の直前にパスワード失念時の処理を実行し，パスワードを電子メール（以下，メールという）で未登録のメールアドレスに送信した記録がある。

・3月25日から3月31日に掛けて，サイトRへの通信量が増加傾向にあった。

図5は，サイトRのパスワード失念時の操作画面である。



注記　実線の矢印は当該画面の入力フォームに適切な値を入力してボタンがクリックされたときの遷移を示す。

図5　サイトRのパスワード失念時の操作画面

J主任は，攻撃者がパスワード失念時の処理を悪用して，会員番号及び誕生日を総当たりで入力し，たまたま合致した当該顧客のアカウントを乗っ取ったものと判断した。J主任は，このインシデントについてWeb管理課のL課長に報告した。L課長は旧A社出身で，この報告でサイトRのパスワード失念時の操作を初めて知った。次は，その報告の時のL課長とJ主任の会話である。

L課長：サイトRのパスワード失念時の処理には，三つの問題があるね。一つ目は，本人であることを確認するための情報が少なすぎるという問題だ。そこは後で解決するとしよう。二つ目は，パスワードそのものをメールで送るという問題だ。三つ目は，［　j　］という問題だ。二つ目と三つ目の問題の解決には，［　k　］ように改修すべきだ。この方法では，一部の利用者はパスワード失念時にログインできなくなるが，その場合はコールセンタで対応することにしよう。

J主任　：はい。分かりました。

L課長：サイトRでは，攻撃者がアカウントを乗っ取ったとしても，あまり経済的利益を得られないので，今回のような被害で済んだと考えられるが，直ちに改修を完了させてほしい。もしもこれらの問題に気付かずにアカウントの共通利用を提供していたら，①利用者に更に大きな被害が発生するところ

だった。アカウントの共通利用の設計，及びリリースまでのスケジュールも見直してほしい。

〔アカウントの共通利用の設計の見直し〕

J主任は，次のように全面的に設計を見直し，承認を得た。

・サイトSを立ち上げ，新たにサイトSのアカウントを発行して管理する。

・アカウントの共通利用に当たり，アカウントの紐付け時とサイトP，Q，Rへのログイン時には，SAMLプロトコルのWeb Browser SSO Profileを用いる。サイトSが，IdP（Identity Provider）となり，サイトP，Q，Rは，SP（Service Provider）となる。

・サイトQには，サイトQのアカウントでも，サイトQのアカウントと紐付けたサイトSのアカウントでもログインできる。サイトP，Rも同様である。

図6は，Web Browser SSO Profileの基本的な通信の流れである。

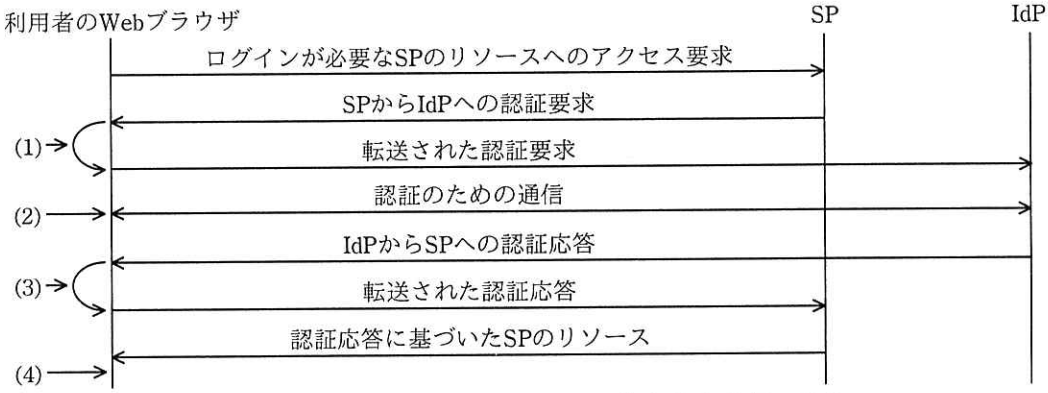
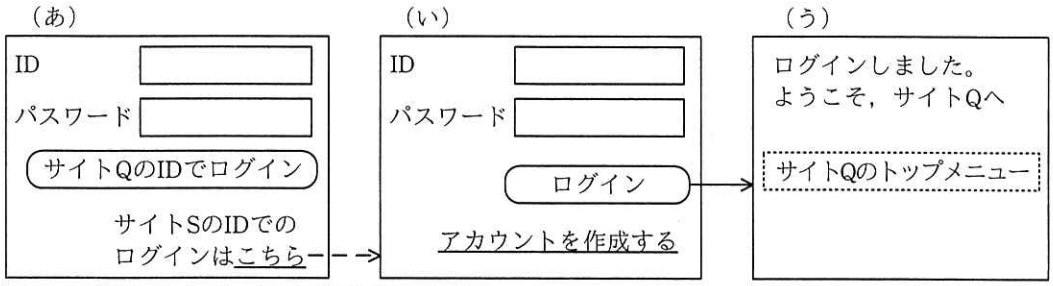


図6　Web Browser SSO Profileの基本的な通信の流れ

図7は，紐付け済みのサイトSのアカウントでサイトQにログインするときの画面遷移図である。

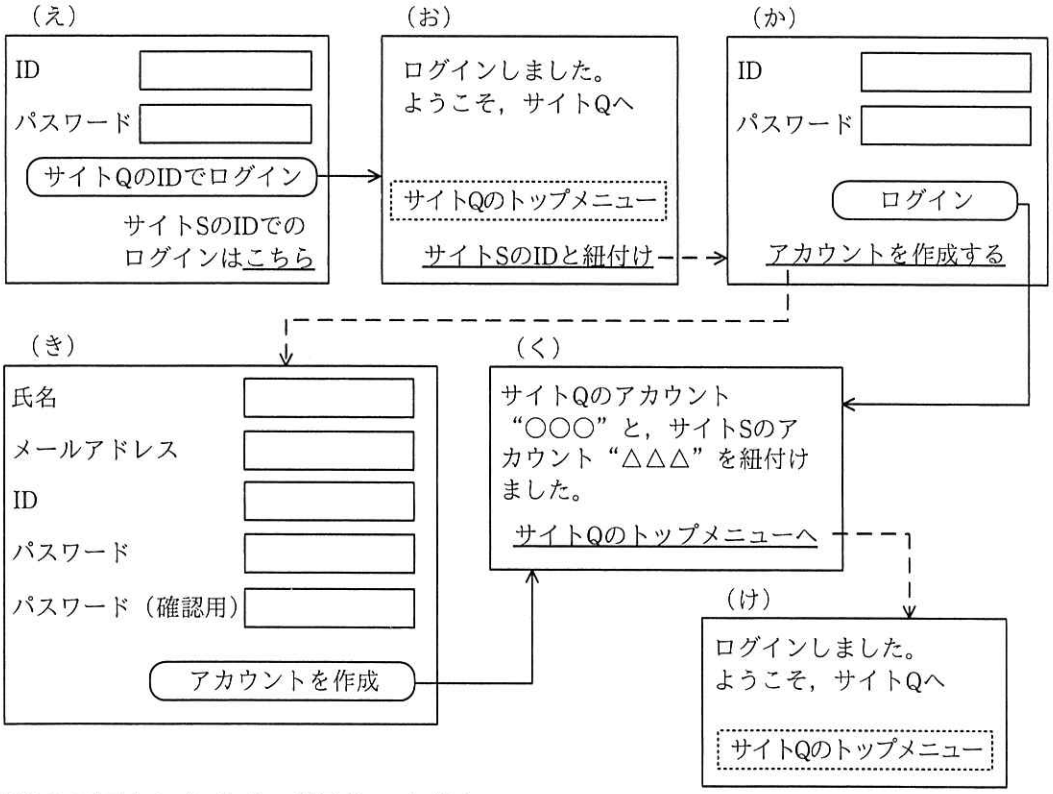


注記 1 画面内の“ID”は，利用者 ID を指す。

注記 2 実線の矢印は当該画面の入力フォームに適切な値を入力してボタンがクリックされたときの遷移を示す。破線の矢印はリンクがクリックされたときの遷移を示す。

図 7　サイト S のアカウントでサイト Q にログインするときの画面遷移図

図 8 は，サイト Q のアカウントとサイト S のアカウントを紐付けるときの画面遷移図である。



注記 1 画面内の“ID”は，利用者 ID を指す。

注記 2 実線の矢印は当該画面の入力フォームに適切な値を入力してボタンがクリックされたときの遷移を示す。破線の矢印はリンクがクリックされたときの遷移を示す。

図 8　サイト Q のアカウントとサイト S のアカウントを紐付けるときの画面遷移図

〔見直し後のアカウント共通利用の提供開始〕

C 社は，サイト P，Q，R の改修とサイト S の開発を完了して，アカウント共通利用の提供を開始し，順調に運用を続けた。サイト P，Q，R のアカウントの廃止，及びサイト S のアカウントへの統合を目指している。この統合が実現すれば，図 7 の（あ）や，図 8 の（え），（お）などの画面は不要となり，より使いやすいサイトを実現できる。

設問 1　表 2 中の［ a ］，［ b ］に入れる適切な字句を答えよ。

設問 2　〔個人情報の取扱い〕について，旧 A 社と旧 B 社の合併による C 社への事業承継に伴って取得した個人情報の取扱いに関し，個人情報保護法に定められている禁止事項は何か。70 字以内で述べよ。

設問 3　〔コードレビュー〕について，(1)～(3)に答えよ。

(1) 本文中の［ c ］，［ d ］，［ f ］，［ g ］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア idPair.checkChild()	イ idPair.childChecked
ウ idPair.childID	エ idPair.childPW
オ idPair.childSite	カ idPair.makeLink()
キ idPair.parentID	ク idPair.siteQAuth()
ケ NamingException	コ return ERROR_ID_OR_PW
サ return NO_ERROR	

(2) 本文中の［ e ］，［ h ］に入れる適切な図 3 又は図 4 中の行番号を，解答群の中から選び，記号で答えよ。

解答群

ア 20	イ 23	ウ 26	エ 34
オ 105	カ 106	キ 117	ク 118

(3) 本文中の［ i ］に入れる適切な処理内容を 50 字以内で具体的に述べよ。

設問 4　〔サイト R でのインシデント〕について，(1)～(3)に答えよ。

(1) 本文中の［ j ］に入れる適切な内容を 40 字以内で述べよ。

(2) 本文中の［ k ］に入れる適切な内容を 40 字以内で述べよ。

(3) 本文中の下線①について，更に大きな被害とは何か。具体的な被害を二つ挙げ，それぞれ 30 字以内で述べよ。

設問５ 〔アカウントの共通利用の設計の見直し〕について，(1)～(3)に答えよ。

(1) 利用者の操作によって，図 7 のとおりに画面が遷移した場合，（い）（う）の画面は，図 6 の(1)～(4)のどの時点で表示されるか。それぞれ，(1)～(4)の記号で答えよ。

(2) 利用者の操作によって，図 7 のとおりに画面が遷移した場合，（あ）（い）（う）の各画面では，どのサーバから送られた HTML を表示するか。それぞれ，答案用紙の“SP”，“IdP”のいずれかを○印で囲んで示せ。

(3) 利用者の操作によって，図 8 の（え）（お）（か）（き）（く）（け）の順に画面が遷移した場合，（え）（か）（き）（く）の各画面では，どのサーバから送られた HTML を表示するか。それぞれ，答案用紙の“SP”，“IdP”のいずれかを○印で囲んで示せ。

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。

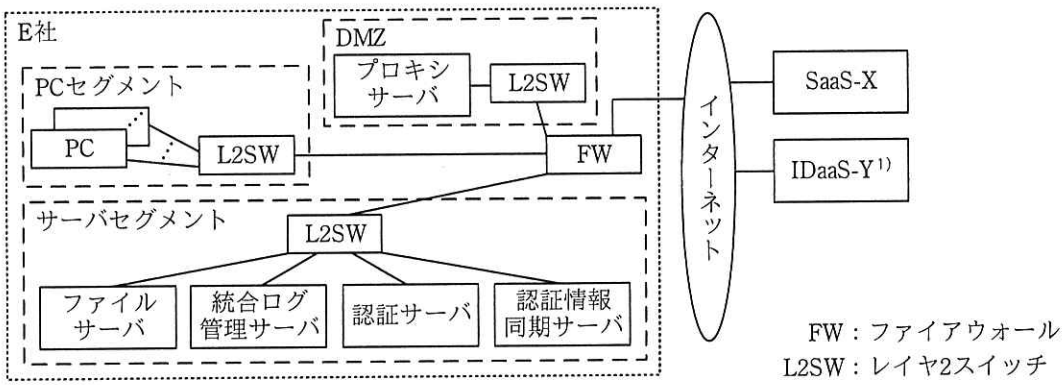
E 社は，従業員数 5,000 名の IT 企業である。E 社では，働き方改革の一環として，テレワーク環境を整備することになった。テレワーク環境について検討すべき重要なテーマの一つに，テレワーク環境経由での情報漏えいを起こさないためのセキュリティ確保がある。そこで，テレワーク環境の整備をシステム企画部長の指示の下，情報処理安全確保支援士（登録セキスペ）でもあるシステム企画部の F 次長，及び部下の G さんが担当することになった。

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。

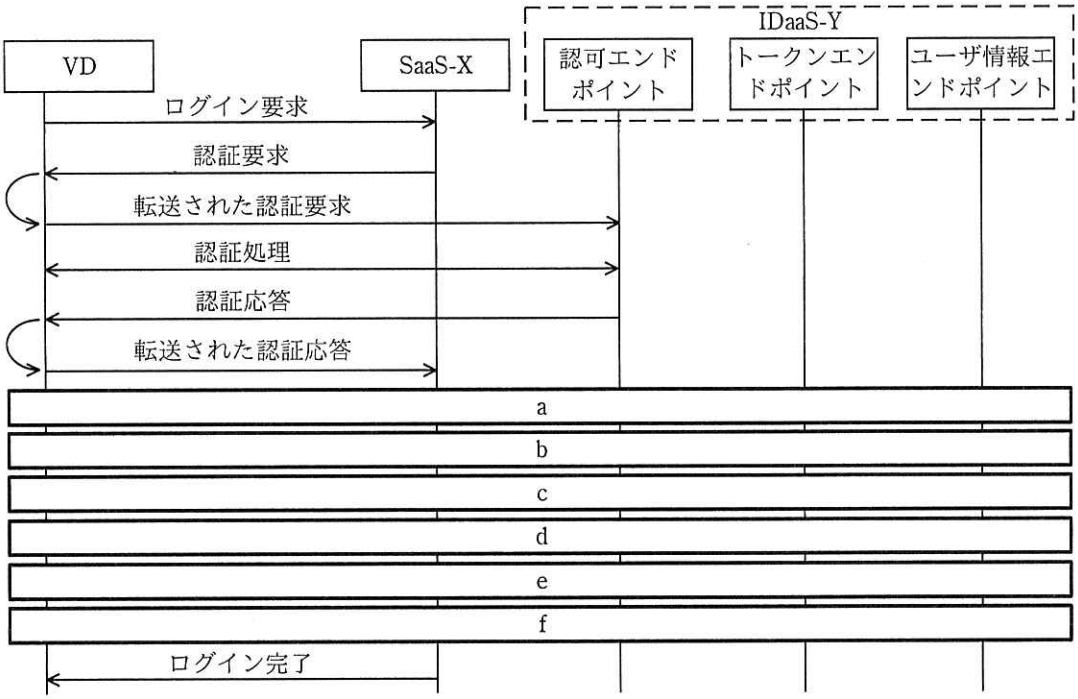


図 2　SaaS-X と IDaaS-Y との認証連携

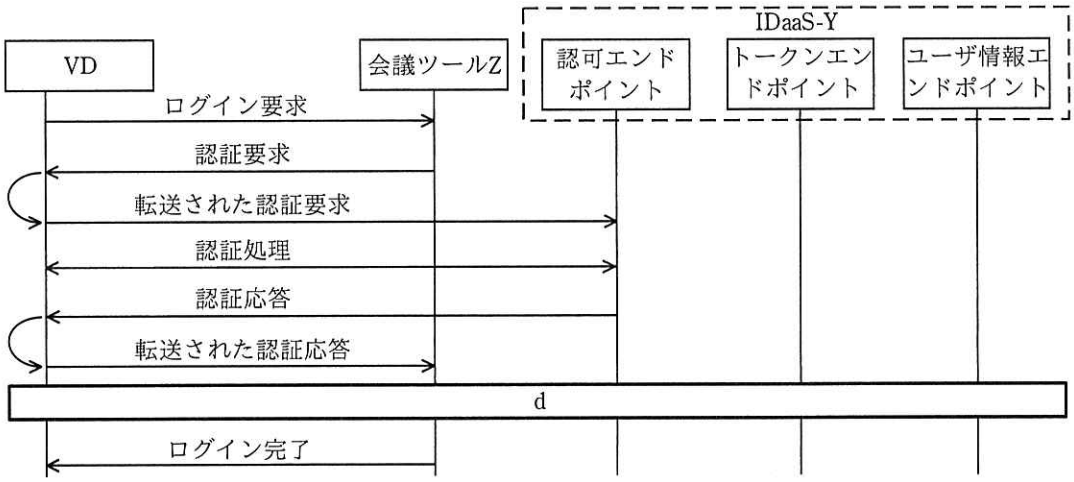


図 3　会議ツール Z と IDaaS-Y との認証連携

〔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。

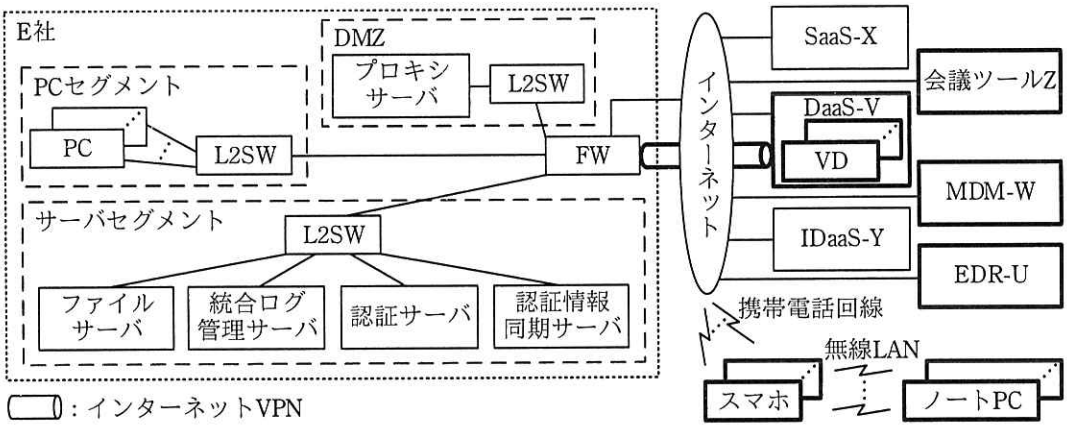
スマホについては，自由なWebアクセスを許可した場合でもマルウェア感染のリ

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

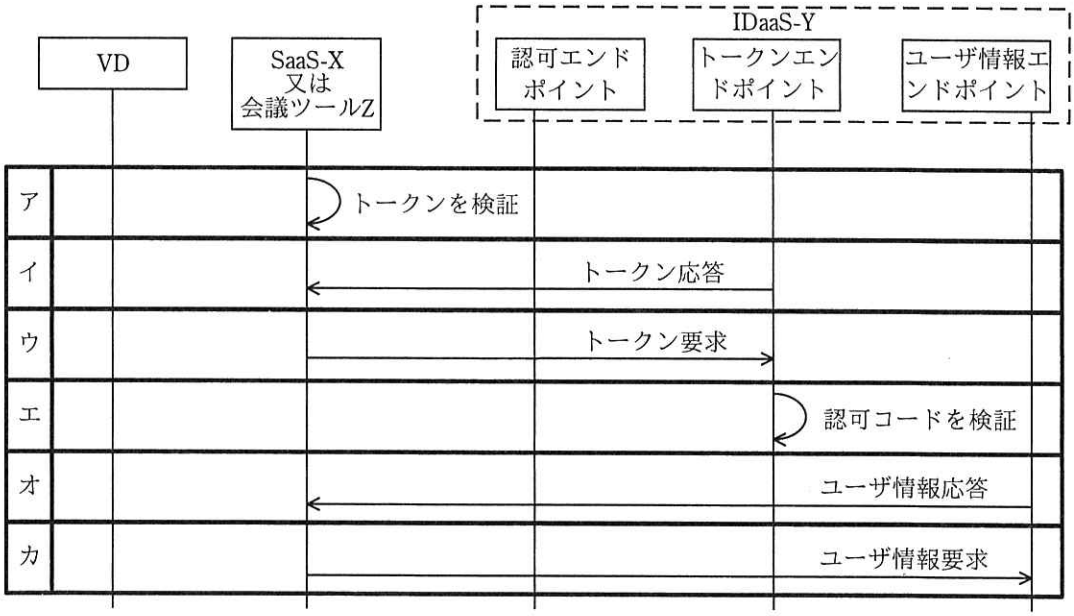
ウ　シリアル番号　　エ　タイムスタンプ

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。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。