SC

令和７年度　秋期
情報処理安全確保支援士試験
午後　問題

試験時間	12:30 ～ 15:00（2 時間 30 分）

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４
選択方法	２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。3 問以上○印で囲んだ場合は，はじめの 2 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１，問３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　コンサルティング業務で利用する SaaS に関する次の記述を読んで，設問に答えよ。

H 社では，コンサルティング業務で利用する SaaS（以下，S サービスという）を提供している。コンサルティング業務を行う企業 50 社程度が S サービスを利用しており，総利用者数は 1,000 名程度である。

〔S サービスの概要〕

S サービスでは，利用企業ごとに複数のプロジェクトを登録できる。S サービスの利用者には 2 種類のロールがある。自社の全てのプロジェクトの情報にアクセスできる管理者と，自身に割り当てられているプロジェクトの情報だけにアクセスできる一般利用者である。

S サービスには，プロジェクトを管理する機能（以下，プロジェクト管理機能という）のほか，利用者がプロジェクト内で特定の話題ごとに“スレッド”と呼ばれるページを作成する機能（以下，スレッド作成機能という），スレッドに文章を投稿したりファイルをアップロードしたりする機能（以下，スレッド投稿機能という）などが設けられている。

S サービスの主な機能を表 1 に示す。

表1　Sサービスの主な機能（抜粋）

機能名	機能概要	備考
ログイン	（省略）	（省略）
利用者管理	管理者が，利用者の登録，変更及び削除を行う。	登録された利用者には，利用企業内で一意となる利用者 ID が発行される。利用者 ID の形式は次のとおりである。 “U”と数字 8 桁をつなげた文字列
ロール管理	管理者が，利用者のロールを設定する。	処理の流れは次のとおりである。 1. ログイン後の画面からロール管理機能を選択すると，パス“/management/role”にリクエストが GET メソッドで送信される。csrf_token という一時的でランダムな文字列のトークンが発行され，ロール設定画面が表示される。 2. ロール設定画面で任意の利用者のロールを変更し，確定ボタンをクリックすると，パス“/management/roleset”に対して，パラメータ csrf_token，is_admin 及び user_id を含むリクエストが POST メソッドで送信される。パラメータ is_admin は指定した利用者のロールに応じて次のいずれかが設定される。 - 管理者：is_admin=1 - 一般利用者：is_admin=0
プロジェクト管理	管理者が，プロジェクトの登録及び変更を行う。また，プロジェクトに一般利用者を割り当てる。	プロジェクトには，利用企業内で一意となるプロジェクト ID が発行される。プロジェクト ID の形式は次のとおりである。 “P”と数字 8 桁をつなげた文字列
タスク管理	利用者が，プロジェクトのタスク管理画面からタスクを登録し，タスクの担当者を割り当てる。また，タスクの更新を行う。	タスクには，次の項目を設定する。 ・タスク名 ・タスクの詳細説明 ・タスクの担当者 ・タスクの締切日 ・タスクの進捗状況 ・タスクの完了フラグ
スレッド作成	利用者が，スレッドを作成する。	スレッドの作成時は，アクセスできる一般利用者を指定する。管理者は利用企業内の全てのスレッドにアクセスできる。
スレッド投稿	利用者が，アクセスできるスレッドに文章の投稿とファイルのアップロードを行う。アップロードされたファイルは，ファイル識別子が一意になるように変更されてからサーバに保存される。	アップロードできるファイルの拡張子は，docx，xlsx，pptx，pdf，jpg，gif 及び png の 7 種類である。アップロードされたファイルは，スレッドにアクセスできる利用者だけがアクセスできる。ファイルの参照時及びダウンロード時のパスは次のとおりである。 /files/[一意のファイル識別子].[拡張子]
プロジェクト進捗管理	利用者が，プロジェクトの進捗を管理する。スケジュールの作成及び管理並びにタスクの進捗確認を行う。	未完了のタスクのうち締切日を過ぎたものは，プロジェクト進捗管理画面にそのタスク名と締切日からの経過日数が表示される。

S サービスでは，半年ごと及び新機能リリース前に診断ツール X による脆弱性診断を実施することにしている。診断ツール X は，送信したリクエストとそれに対するレスポンスから脆弱性を検出する。

S サービスでは，HTTP レスポンスヘッダーに Content Security Policy（CSP）を設定している。図 1 に，S サービスの HTTP レスポンスヘッダーの例を示す。

```
HTTP/1.1 200 OK
Cache-Control: no-store
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: （省略）
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: JSESSIONID=e962879ef251f2117460cf0d5ce714e3; Secure; HttpOnly
Content-Security-Policy: default-src 'self';
Content-Length: 31337
```

図 1　S サービスの HTTP レスポンスヘッダーの例

図 1 の設定では，リソースの読込みとスクリプトの実行に関する動作は次のようになる。

・S サービス以外のドメインからのリソースの読込み：［　a　］

・script タグ内に直接記述されたスクリプトの実行：［　b　］

〔インシデントの発生とその調査〕

ある日，S サービスを利用している B 社の管理者から H 社に対して，“S サービスの一般利用者であった元従業員 Z のローカル PC 上に，元従業員 Z が割り当てられていなかったプロジェクトのファイルが保存されていたので，S サービスに不具合がないか調査してほしい”との依頼があった。

S サービスのシステム担当者である U さんは，ログを確認するとともに，B 社の許可を得た上で，B 社の管理者の利用者 ID を使ってログインし，幾つかの画面を確認した。そのうち，プロジェクト進捗管理画面の HTML を図 2 に，その HTML が参照していた F1234567890.xlsx というファイルをテキストエディターで開いたときの内容を図 3 に示す。

```
<html>
<head>
    <meta charset="UTF-8">
    <title>プロジェクト進捗管理</title>
    <link href="/static/css/style.css" rel="stylesheet" type="text/css">
    <script src="/static/js/action.js"></script>
</head>
<body>
    <h1>プロジェクト進捗管理（プロジェクト ID：P00395000）</h1>
（省略）
    <div name="alert">
        <div name="alert-title">期限切れタスク一覧</div>
        <div name="alert-description">
            次のタスクが締切日を過ぎています。<br>
        </div>
        <ul className="delayed-task">
            <li>G 社のコンペ資料作成（締切日過ぎ 1 日）</li>
            <li>G 社の業界分析（締切日過ぎ 4 日）</li>
            <li>個人タスク<script src="/files/F1234567890.xlsx"></script>（締切日過
ぎ 5 日）</li>
        </ul>
    </div>
（省略）
</body>
</html>
```

図 2　プロジェクト進捗管理画面の HTML

```
(async function() {
    const response = await fetch("/management/role");
    const text = await response.text();
    // 次の 2 行で csrf_token を取得
    const tokenMatch = text.match(/id="csrf_token"[^>]*value="([^"]+)"/);
    const csrfToken = tokenMatch[1];
    await fetch("/management/roleset", {
        method: "POST",
        // POST メソッドのリクエスト body
        body: new URLSearchParams({
            "csrf_token": csrfToken,
            "is_admin": "1",
            "user_id": "U00331001"
        })
    });
})();
```

注記　整形とコメントの追記は，U さんによるものである。

図 3　F1234567890.xlsx の内容

Uさんは，調査の結果，図4に示す攻撃が実行されていたことを確認した。

1. 元従業員Zの利用者IDでアクセスできるスレッドに，F1234567890.xlsxをアップロードした。
2. 当該利用者IDで，タスク管理画面から［ c ］に次の文字列を指定して，タスクを登録した。
   文字列：［ d ］
3. その後，2で登録したタスクが次の条件を満たしたときに，［ e ］がプロジェクト進捗管理画面にアクセスした。
   条件：未完了の状態で，かつ，［ f ］
4. 3の結果，図2のHTMLが［ e ］のWebブラウザに出力された。
5. 4の結果，図3のスクリプトが実行された。
6. 5の結果，元従業員Zの利用者IDであったU00331001に対して次の処理が行われた。
   処理：［ g ］

（省略）

8. 元従業員Zの利用者IDで，調査依頼の発端となったファイルをダウンロードした。

図4　実行されていた攻撃

Uさんは，図4の項番2と類似した文字列が指定されたタスクが登録されていないかどうかを確認したところ，完了済みタスクの中に類似したものがあることを確認した。しかし，このタスクによる攻撃は，CSPの設定で防御できていた。

Uさんは，攻撃者がこの失敗の原因を分析し，失敗したときに使用した文字列に①工夫を加えることによって図4の項番2の文字列を作成し，攻撃を成功させたと推測した。

〔インシデントへの対応及び攻撃への対策〕

Uさんは，まず必要なインシデント対応を行った。その結果，図4以外に成功した攻撃はないことが分かった。Uさんは，結果をB社の管理者に報告した。また，ほかの利用企業で同様の攻撃がなかったかどうかを調査したところ，なかったことも分かった。

次に，図4と同様の攻撃を防止するために，次の対策を行った。

(1) 図4の項番1については，アップロードされたファイルが許可された拡張子であることのチェックに加えて，次の処理を追加する。

処理：［ h ］

(2) 図4の項番4について，類似の問題がないかどうか，Sサービス全体を確認したところ，問題は1箇所だけだったので，表1の機能のうち，［ i ］について，②必要な処理を追加する。なお，この処理が行われていないという脆弱性は，診断ツールXでは検知されない。

〔開発プロセスの見直し検討〕

Uさんは，図4の項番4の脆弱性のように診断ツールXで検知されないものであっても，検知できる可能性のある検査として，次の二つも実施するという開発プロセスの見直し案を作成した。

・SAST

・［ j ］

Uさんは，開発プロセスの見直し案について承認を得て，見直しに着手した。

設問1　本文中の［ a ］，［ b ］に入れる適切な字句を，“できる”，“できない”のいずれかでそれぞれ答えよ。

設問2　〔インシデントの発生とその調査〕について答えよ。

(1) 図3のスクリプトは，表1中のどの機能を悪用するものか。機能名を答えよ。

(2) 図4中の［ c ］に入れる適切なタスクの項目を，表1中の字句を用いて答えよ。

(3) 図4中の［ d ］に入れる適切な文字列を，図2から抜き出して答えよ。

(4) 図4中の［ e ］～［ g ］に入れる適切な字句を答えよ。

(5) 本文中の下線①について，工夫の内容を，具体的に答えよ。

設問3　〔インシデントへの対応及び攻撃への対策〕について答えよ。

(1) 本文中の［ h ］に入れる追加すべき処理の内容を，具体的に答えよ。

(2) 本文中の［ i ］に入れる適切な機能名を答えよ。

(3) 本文中の下線②について，追加すべき処理の内容を，具体的に答えよ。

設問4　本文中の［ j ］に入れる適切な検査方法を，具体的に答えよ。

問２　暗号資産交換業におけるセキュリティに関する次の記述を読んで，設問に答えよ。

A 社は従業員 50 名の暗号資産交換業者である。A 社では，3 年前から暗号資産 B コインを取り扱っており，20 万人の顧客が暗号資産口座を開設している。A 社には財務部があり，顧客の預けた時価 200 億円相当の B コインを顧客に代わって保有し管理している。

〔B コインの仕組み〕

B コインは，楕円曲線暗号を用いたデジタル署名方式を用いて，分散型台帳で管理される。B コインの保有者が，別の者に B コインを送ることを移転という。B コインを移転する際は，まず，B コインの移転先，移転数量などを含むバイナリ形式で表現された B コインの移転指示情報（以下，移転情報という）に対して，移転元の署名鍵を用いてデジタル署名し，次に，そのデジタル署名済みの移転情報を B コインの分散型台帳を保存するサーバ（以下，B コインノードという）の一つに送付する。デジタル署名済みの移転情報は，移転元の署名鍵に対応する検証鍵を用いて検証することができる。同一の移転情報は一度しか分散型台帳に記録されず，重複して B コインが移転されることはない。B コインノードは，誰でも自由にインターネット上に立ち上げることができる。

〔A 社のシステム構成〕

A 社のシステム構成を図 1 に，機器の概要を表 1 にそれぞれ示す。

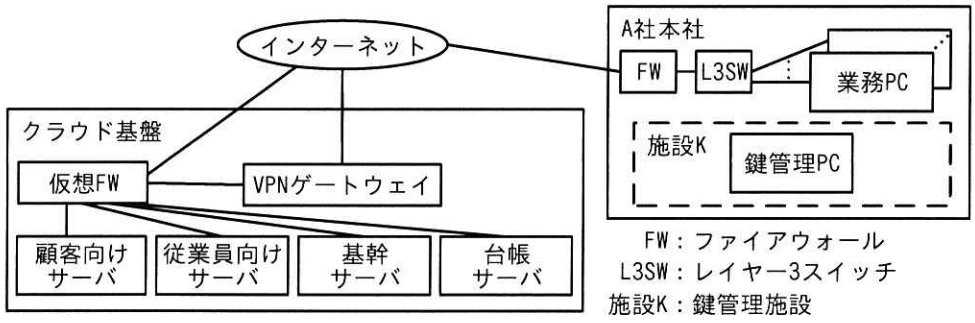


図 1　A 社のシステム構成（抜粋）

表1　A社の機器の概要（抜粋）

名称	概要
VPNゲートウェイ	A社本社内の業務PCからのVPN接続を終端する。
顧客向けサーバ	A社の顧客向けの機能を提供する。提供する機能には，出庫[1)]依頼などがある。
従業員向けサーバ	A社の従業員向けにBコインを管理する機能を提供する。
基幹サーバ	顧客の暗号資産口座に関する情報を集中的に管理する。
台帳サーバ	Bコインノードのうちの1台である。台帳サーバは，インターネット上の他のBコインノードとピアツーピア通信を行う。
業務PC	A社の各従業員に貸与されている。FWでは，インターネット上のWebサイトと通信が許可されている。業務に必要なアプリケーションソフトウェア及びマルウェア対策ソフトがインストールされている。TLSクライアント認証を用いたVPNゲートウェイへのVPN接続を利用できる。
鍵管理PC	Bコインの移転時に用いるA社開発のアプリケーションソフトウェア（以下，署名アプリという）がインストールされている。鍵管理PCの製造元から調達して以降，一度もネットワークに接続しておらず，他の機器とのデータの授受にはUSBメモリだけを用いている。
仮想FW	ステートフルパケットインスペクション型FWである。インターネットからは，顧客向けサーバへの通信だけを許可する。VPNゲートウェイからは，従業員向けサーバへの通信だけを許可する。基幹サーバからは，顧客向けサーバ，従業員向けサーバ及び台帳サーバへの通信だけを許可する。台帳サーバからは，インターネットへの通信だけを許可する。顧客向けサーバ及び従業員向けサーバからは，全ての通信を禁止する。

注[1)]　顧客のA社に預けているBコインを顧客自身に移転することを出庫という。

施設Kには鍵管理PCと監視カメラだけが設置してあり，施設Kはネットワークから遮断されている。監視カメラの映像は，監視カメラの内蔵ストレージに保存され，定期的に内蔵ストレージから別の媒体にコピーして保管される。施設Kの出入口には金属探知機がある。A社が保有し管理するBコインの署名鍵（以下，署名鍵Sという）は鍵管理PCに保存してあり，対応する検証鍵（以下，検証鍵Vという）は基幹サーバに保存してある。施設Kには，①サイドチャネル攻撃を防ぐ対策が施されている。A社は施設Kについて平常時の運用ルールを図2のとおり定めている。

1. 財務部の従業員だけに入室を許可する。
2. 電子機器の持込み及び持出しは，会社の用意したUSBメモリ（以下，業務用メディアという）の持込み及び持出しだけを許可する。

図2　施設Kの平常時の運用ルール（抜粋）

出庫依頼は平均して1日5件あり，毎営業日に出庫依頼の処理（以下，出庫業務という）が行われる。出庫業務の処理手順を図3に示す。

手順1　午前9時，基幹サーバが，未処理の出庫依頼を顧客向けサーバから取り出す。そして，移転情報を記録したファイルを出庫依頼ごとに一つずつ生成し，従業員向けサーバに全てアップロードする。
手順2　午前10時，当日の出庫業務の担当者（以下，当日担当者という）が，次の作業を行う。
(i) 自身の業務PCを用いて，手順1で生成された各ファイルを従業員向けサーバから全てダウンロードし，所定の場所から取り出した空の業務用メディアに全て保存する。手順1で生成されたファイルが一つもない場合は，出庫業務を終了する。
(ii) 業務PCから業務用メディアを取り外し，業務用メディアを持って施設Kに入室する。
(iii) 鍵管理PCの電源を入れ，業務用メディアを接続し，署名アプリを起動する。
(iv) 業務用メディア内の移転情報を記録した各ファイルを署名アプリに読み込み，移転情報に対して署名鍵Sを用いてデジタル署名する。デジタル署名済みの移転情報を記録した各ファイルを業務用メディアに保存する。
(v) 鍵管理PCから業務用メディアを取り外し，鍵管理PCの電源を切る。
(vi) 業務用メディアを持って施設Kから退室し，自身の業務PCに業務用メディアを接続する。
(vii) 自身の業務PCを用いて，業務用メディア内のデジタル署名済みの移転情報を記録した各ファイルを，従業員向けサーバに全てアップロードする。
(viii) 業務用メディア内のデータを全て消去し，所定の場所に返却する。
手順3　午後1時，基幹サーバが，手順2(vii)でアップロードされた各ファイルを従業員向けサーバから全てダウンロードして，各ファイルに記録された移転情報と手順1で生成したファイルに記録された移転情報が一致するかどうかを検査する。また，各移転情報に付与されたデジタル署名を検証鍵Vで検証する。異常がない場合，全てのデジタル署名済みの移転情報を台帳サーバに送付する。移転情報が一致しなかった場合又はデジタル署名の検証に失敗した場合，処理を中止し，財務部の従業員全員に電子メールで警告する。

注記　財務部には複数の従業員がおり，営業日ごとの出庫業務の担当者を事前に割り当てている。

図3　出庫業務の処理手順（概要）

〔Bコインの不正移転への対策強化〕

A社の経営陣は，保有し管理するBコインの不正移転のうち，第三者の攻撃によるもの及び従業員一人の不正によるものの防止策を強化したいと考えた。そこで，セキュリティ部に所属する情報処理安全確保支援士（登録セキスペ）のJさんに，そういった不正移転の想定事例をまとめるよう指示した。Jさんは図4のとおり想定事例をまとめた。

想定事例(a) 第三者の攻撃

当日担当者が標的型攻撃メールを受信し，マルウェアを含む添付ファイル（以下，添付ファイルに含まれていたマルウェアをマルウェアXという）を業務PCで開いてしまい，業務PCがマルウェア X に感染する。マルウェア X は，マルウェア対策ソフトに検知されず，攻撃者の指示に従って，PC 上の任意のファイルの書換えやインターネット通信を行うことが可能であるとする。

図3の手順2(iv)では，デジタル署名しようとする移転情報の内容を当日担当者が確認していない。そこで攻撃者が，②図3の手順2(i)と(ii)の間及び(vi)と(vii)の間のそれぞれにおいてマルウェアXに特定の処理をさせる。その結果，図3の手順3で警告の電子メールが送られないまま，Bコインが攻撃者に移転される。

想定事例(b) 従業員一人の不正

当日担当者が，図3の手順2(iv)の作業中に署名鍵Sを業務用メディアにコピーする。当日担当者は，図3の手順2(vi)の後，業務PCで業務用メディアから署名鍵Sを取り出し，自身の個人メールアドレスに送付する。後日，自宅で，自身にA社のBコインを移転させる移転情報を作成してデジタル署名し，インターネット上に自身で設置したBコインノードにこの移転情報を送付する。その結果，Bコインが当日担当者に移転される。

図4　想定事例

A 社の経営陣は出庫業務の処理手順を見直すよう財務部に指示した。財務部は，想定事例(a)に対しては，不正な移転情報を検知できるように，図 5 に示すシステム及び手順の改修案を考えた。

・手順1において，基幹サーバは，移転情報を記録したファイルに対してメッセージダイジェストを計算し，移転情報を記録したファイルの名称とメッセージダイジェストとの対応のリストを記録した一つのテキストファイル（以下，照合ファイルという）を生成し，照合ファイルも従業員向けサーバにアップロードするように改修する。
・手順2(i)において，照合ファイルも従業員向けサーバからダウンロードし，業務用メディアに保存するように改修する。
・手順2(iv)において，当日担当者は，移転情報を記録したファイル数が当日の出庫依頼の件数と一致することを確認し，不一致の場合はデジタル署名せずに出庫業務を終了する作業を追加する。
・署名アプリは，移転情報を記録したファイルに重複がなく，移転情報を記録した各ファイルのメッセージダイジェストが照合ファイルに記録されたものと一致した場合だけ移転情報にデジタル署名し，それ以外の場合には警告画面を表示するように改修する。

図5　システム及び手順の改修案

A 社の経営陣がこの改修案を J さんにレビューさせたところ，J さんは，この改修案では，正規の移転情報を記録したファイルの一つを不正な移転情報に書き換えた上で，メッセージダイジェストが一致するように照合ファイルを書き換えることが

できてしまうと指摘し，改修案において，照合ファイルにメッセージダイジェストを記録する代わりに基幹サーバ及び署名アプリに共通鍵をもたせ，その共通鍵を使った［　a　］を記録するよう提言した。

想定事例(b)に対して財務部は，出庫業務の担当者に対する研修を強化する対策に加えて，③図3の手順2の作業中における不正行為の機会を減らす対策を講じることにした。

A社の経営陣がセキュリティ部に業務PCのログと監視カメラの映像を分析させたところ，事業開始以来，流出事案につながる不正の兆候は発見されなかった。

〔M社によるA社の買収〕

半年後，従業員200名で暗号資産交換業を営むM社がA社を買収し，A社の事業はM社に統合されることになった。M社では，M社の署名鍵をT社製ハードウェアセキュリティモジュール（以下，HSMという）に格納し，HSMをHSM管理用のサーバ（以下，HSM管理サーバという）にUSBケーブルで接続してから操作している。HSM管理サーバは，M社内のLANに接続されている。

事業統合に伴って，施設Kを閉鎖し，署名鍵SをM社に移管する方針になった。M社では署名鍵のネットワーク経由での送信を禁止する業務規程がある。そこでM社はA社に，図6に示す署名鍵Sの移送及び確認方法を提案した。

作業1 鍵の移送用のUSBメモリ（以下，移送用メディアという）を用意しておく。A社の財務部の従業員とM社の従業員が施設K内で，鍵管理PCを用いて署名鍵Sをパスワード[1]付き圧縮ファイルに圧縮し，この圧縮ファイルを空の移送用メディアに保存する。パスワードは紙に書き留める。
作業2 A社の従業員とM社の従業員が移送用メディア及びパスワードを書き留めた紙をM社まで持ち運ぶ。
作業3 A社の従業員とM社の従業員が，HSM管理サーバに移送用メディアを接続して，紙に書き留められたパスワードを使って移送用メディア内で圧縮ファイルを展開する。その後HSMに署名鍵Sを読み込んで登録する。
作業4 A社の従業員とM社の従業員が，HSMで署名鍵Sを使って移転情報にデジタル署名を付与し，A社が保有し管理していたBコインがその移転情報を使って移転できるかどうかをテストする。
作業5 A社の従業員とM社の従業員が，移送用メディアの内容を消去する。

注記1　移送作業中，M社の従業員は施設Kへの入室を許可されるものとする。

注記2　A社の従業員とM社の従業員がそろってミスをする又は不正行為を共謀するリスクは無視できるほど低いものとする。

注[1]　パスワードは，オフライン解析を試みる攻撃に対して十分な強度のものを選ぶ。

図6　署名鍵Sの移送及び確認方法

A社の経営陣から指示があり，Jさんがこの方法によって安全に署名鍵Sを移送できるかどうかを検討したところ，図6の方法には④幾つかの問題点があることが分かった。そこで，Jさんは，図7を起案した。

作業1　M社の従業員が，A社の財務部の従業員の立会いの下，HSM管理サーバを操作してHSM内に3,072ビットのRSA暗号の鍵ペアとして暗号鍵（以下，暗号鍵Eという）及び復号鍵（以下，復号鍵Dという）を生成し，暗号鍵EをHSM管理サーバに接続した空の移送用メディアに保存する。
作業2　A社の従業員とM社の従業員が共同で，移送用メディアを施設Kまで持ち運ぶ。
作業3　A社の従業員とM社の従業員が，施設K内の鍵管理PCで，移送用メディアから暗号鍵Eを読み込む。そして，［　b　］を［　c　］で［　あ　］し，生成されたデータを移送用メディアに保存する。移送用メディアから暗号鍵Eを削除する。
作業4　A社の従業員とM社の従業員が共同で，移送用メディアをHSM管理サーバまで持ち運ぶ。
作業5　A社の従業員とM社の従業員が，移送用メディアをHSM管理サーバに接続する。
作業6　A社の従業員とM社の従業員が，移送用メディアから読み込んだデータをHSMにアップロードする。HSM内でこのデータを［　d　］で［　い　］し，得られた［　e　］をHSMに登録する。
作業7　（図6の作業4と同じ）
作業8　（図6の作業5と同じ）

注記1　移送作業中，M社の従業員は施設Kへの入室を許可されるものとする。
注記2　A社の従業員とM社の従業員がそろってミスをする又は不正行為を共謀するリスクは無視できるほど低いものとする。

図7　Jさんの案

Jさんは当初，図7の案では，⑤図7の作業4で移送用メディアが盗難に遭ったとしても署名鍵Sは漏えいしないと考えていた。しかし，Jさんが図7の案を詳細に検討したところ，作業2及び4で移送用メディアを安全に持ち運びできたとしても，HSM管理サーバが仮にマルウェアに感染し，その結果，攻撃者の指示によって⑥図7の作業1で移送用メディアに保存されるファイルが書き換えられ，かつ，図7の作業5で移送用メディアの内容を読み取られてしまった場合には，署名鍵Sが攻撃者に漏えいするリスクがあると分かった。

そこでJさんは，HSMの機能を利用して，移送用メディアに保存されるファイルの改ざんを検知できるように改良した手順をA社及びM社の経営陣に提案した。その結果，改良した手順を用いて施設KからHSMまで署名鍵Sを移送することが決定した。

設問１　楕円曲線暗号を用いたデジタル署名アルゴリズムを解答群の中から全て選び，記号で答えよ。

解答群

ア　AES　　イ　ECDH　　ウ　ECDSA　　エ　EdDSA

オ　RSA　　カ　SHA-256

設問２　本文中の下線①について，攻撃にはどのような手法が考えられるか。手法を具体的に答えよ。

設問３　〔B コインの不正移転への対策強化〕について答えよ。

(1)　図 4 中の下線②について，どのような処理をさせるのか。処理の内容を答えよ。

(2)　本文中の［　a　］に入れる共通鍵を使った適切な暗号技術を答えよ。

(3)　本文中の下線③について，対策を具体的に答えよ。

設問４　〔M 社による A 社の買収〕について答えよ。

(1)　本文中の下線④について，問題点のうちリスクの最も高いものを答えよ。

(2)　図 7 中の［　b　］～［　e　］に入れる適切な字句を b～e の解答群の中から，［　あ　］，［　い　］に入れる適切な字句をあ，いの解答群の中から，それぞれ選び，記号で答えよ。なお，解答は重複して選んでもよい。

b～e の解答群

ア　暗号鍵 E　　イ　検証鍵 V　　ウ　署名鍵 S　　エ　復号鍵 D

あ，いの解答群

オ　暗号化　　カ　検証　　キ　デジタル署名　　ク　復号

(3)　本文中の下線⑤について，J さんが考えていた根拠を答えよ。

(4)　本文中の下線⑥について，攻撃者はファイルを何に書き換えるか。書換え後のファイルの内容を答えよ。

問３　情報システムのセキュリティ強化に関する次の記述を読んで，設問に答えよ。

P 社は，従業員 100 名の機械部品商社である。P 社には，総務部，営業部，技術部が，また，総務部には経理係と情報システム係がある。

従業員には，一人 1 台の社有 PC 及び社有スマートフォン（以下，両者を併せて情報端末といい，スマートフォンをスマホという）を貸与している。さらに，社有スマホの故障，災害発生などの緊急時については，個人所有のスマホの利用を許可している。

情報端末以外の P 社の情報システムの管理は，総務部の H 部長配下の情報システム係の T 主任と F さんが行っている。各部には，情報システム係をサポートする情報セキュリティ推進者がいる。

P 社では，表 1 に示す情報端末などの利用規程を定めている。

表 1　情報端末などの利用規程（抜粋）

項番	情報端末など	項目	規程
1	社有 PC	(1)初期設定	・次の初期設定を情報システム係が P 社内で行う。 - Q 社のマルウェア対策ソフトを導入し，リアルタイムスキャンを有効にする。 - 起動時及び起動後 1 時間ごとに Q 社のマルウェア定義ファイル配布サイトに接続して更新するように設定する。
		(2)OS	・ベンダーがサポートしているバージョン X 又はバージョン Y [1]を利用する。 ・利用者は，脆弱性修正プログラムがリリースされたら，OS のアップデート機能を用いて，2 週間以内に適用する。
		(3)確認	・各部の情報セキュリティ推進者が，利用者が項番 1(2)に従って適切に利用しているかどうかを毎月確認する。
2	社有スマホ，緊急時に利用する個人所有のスマホ	(1)OS	・利用者は，脆弱性修正プログラムがリリースされたら 1 週間以内に適用する。
		(2)アプリケーションプログラム（以下，アプリという）	・利用者は，毎週スマホのアプリ管理機能で最新化を行う。 ・利用者は，アプリ内での認証機能には，可能であれば，生体認証を利用する。
		(3)スマホのスクリーンロック	・一定時間操作がない場合は，スクリーンロックが行われるように設定する。 ・スクリーンロックの解除には，可能であれば，生体認証を利用する。

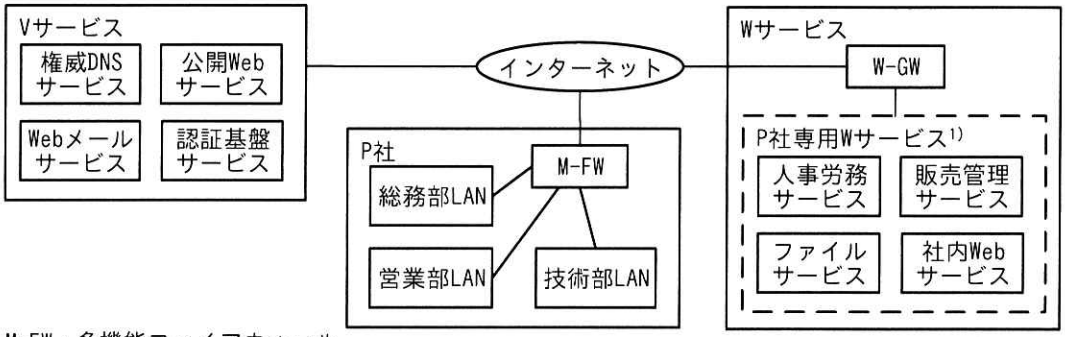
注 [1]　バージョン X は 1 年後にサポート終了を迎える。バージョン Y はその後継である。

〔社有 PC の OS の現状〕

社有 PC は，バージョン X から，バージョン Y への OS の移行中である。移行は，各部の情報セキュリティ推進者の管理の下，6 か月以内に完了させることになっている。

〔情報システムの現状〕

P 社では，V 社の SaaS（以下，V サービスという）及び W 社の SaaS（以下，W サービスという）を使っている。オンプレミスの情報システムはない。P 社のネットワーク図を図 1 に示す。



M-FW：多機能ファイアウォール
W-GW：Wサービスのレイヤー3ゲートウェイ
注記　総務部 LAN，営業部 LAN，技術部 LAN では，レイヤー2 スイッチ，無線ルータ及び情報端末の記載は省略している。社有 PC は，P 社内の LAN のいずれかのレイヤー2 スイッチ又は無線ルータに接続して業務を行う。
注 1)　P 社専用に提供される四つのサービスを指す。

図 1　P 社のネットワーク図（抜粋）

M-FW は，ステートフルパケットインスペクション型のファイアウォール機能，DNS キャッシュサーバ機能及び Web プロキシ機能をもつ。

V サービスの構成要素の概要を表 2 に示す。

表2　V サービスの構成要素の概要（抜粋）

構成要素	構成要素の概要
権威 DNS サービス	・権威 DNS サーバ機能を提供している。 ・次のプロトコルにも対応している。 - [a] ：応答にデジタル署名を付与する。 - [b] ：HTTPS を用いて DNS 通信する。 - DoT：[c] を用いて DNS 通信を暗号化する。
認証基盤サービス	・多要素認証（以下，MFA という）の利用が可能である。MFA の認証方式は次の 3 通りである。どれを使うかは契約企業の管理者が設定する。 認証方式 1：利用者ごとにあらかじめ登録した 1 件の電話番号への SMS 通知による認証 認証方式 2：利用者ごとにあらかじめ登録した 1 台のスマホでの認証アプリを用いた認証 認証方式 3：認証の都度，利用者が認証方式 1 又は 2 のいずれかを選択 P 社では認証方式 2 を設定している。 ・契約企業の管理者又は利用者は，認証基盤サービスの設定画面（以下，MFA 設定画面という）にアクセスし，必要な情報を設定する。 ・MFA 設定画面への接続元 IP アドレス制限が可能である。

W-GW には，ファイアウォール機能があり，P 社専用 W サービスに接続可能なのは M-FW のグローバル IP アドレスに制限されている。

P 社が利用しているグローバル IP アドレスを表 3 に示す。

表3　P 社が利用しているグローバル IP アドレス（抜粋）

機器又はサービス	IP アドレス
M-FW のインターネット側インタフェース	a1.b1.c1.d1
P 社専用 W サービス	a8.b8.c8.1～a8.b8.c8.4
V サービスの認証基盤サービス	a9.b9.c9.d9

営業部及び技術部では，取引先から指定された Web サービス（以下，取引先サービスという）を利用することがある。取引先サービスは複数あり，各取引先サービスで接続元 IP アドレス制限を行っている。各取引先サービスでは，M-FW のグローバル IP アドレスからの接続は許可されている。

情報システム係は，社有 PC の初期設定後に，図 2 に示す追加作業を行っている。

1. OS ベンダーの OS アップデート配布サイト，Q 社のマルウェア定義ファイル配布サイト，V サービス，P 社専用 W サービス（以下，四つを併せて基本サイトという）及び取引先サービスにアクセスし，正しく初期設定されたかどうかを確認する。
2. V サービス及び P 社専用 W サービスの URL を Web ブラウザのブックマークに登録する。

図 2　初期設定後の追加作業

〔インターネットバンキング変更の検討〕

経理係の G さんから情報システム係に，“現在利用している Y 銀行のインターネットバンキング（以下，インターネットバンキングを IB，Y 銀行のインターネットバンキングを Y-IB という）から Z 銀行の IB（以下，Z 銀行の IB を Z-IB という）への変更を検討しているが，情報セキュリティの観点で，Z-IB を利用しても問題ないか教えてほしい”という相談があった。

現在，経理係では，振込みを，操作担当者と操作確認者の 2 名で行っており，Z-IB への変更後も同様に 2 名で行うことを計画している。

IB では取引を認証するための専用のハードウェアトークンとして，数字が入力できるトークン（以下，数字入力トークンという）とカメラ付きトークンの 2 種類のトークンがあり，Y-IB では数字入力トークンを，Z-IB ではカメラ付きトークンを使用している。IB におけるトークンの種別と認証方法の概要を表 4 に示す。

表 4　IB におけるトークンの種別と認証方法の概要（抜粋）

トークンの種別	認証方法の概要
数字入力トークン	（省略）
カメラ付きトークン	IB は，ログイン後の操作で，Web 画面に入力された取引内容を基に 2 次元コードを生成して Web 画面に表示する。操作担当者がカメラ付きトークンで 2 次元コードを読み取ると，カメラ付きトークンは，2 次元コードを基に認証番号を生成し，取引内容及び認証番号をカメラ付きトークンのディスプレイに表示する。操作担当者は，認証番号を Web 画面に入力する。

IB では，振込先の金融機関名，店名，口座種別，口座番号（以下，金融機関名，店名，口座種別，口座番号を口座情報という）の改ざんによって，攻撃者の用意した口座（以下，攻撃者口座という）に振り込んでしまう被害が発生している。T 主任は F さんに，このような被害に遭うリスクを Y-IB と Z-IB それぞれで検討し，どちらの IB の方がリスクが低いかを比較するよう指示した。

〔攻撃者口座に振り込んでしまうリスクの検討〕

P社において想定される振込先の口座情報の改ざん手口には，IBにアクセスする社有PCに感染させたマルウェアによる方法などがある。

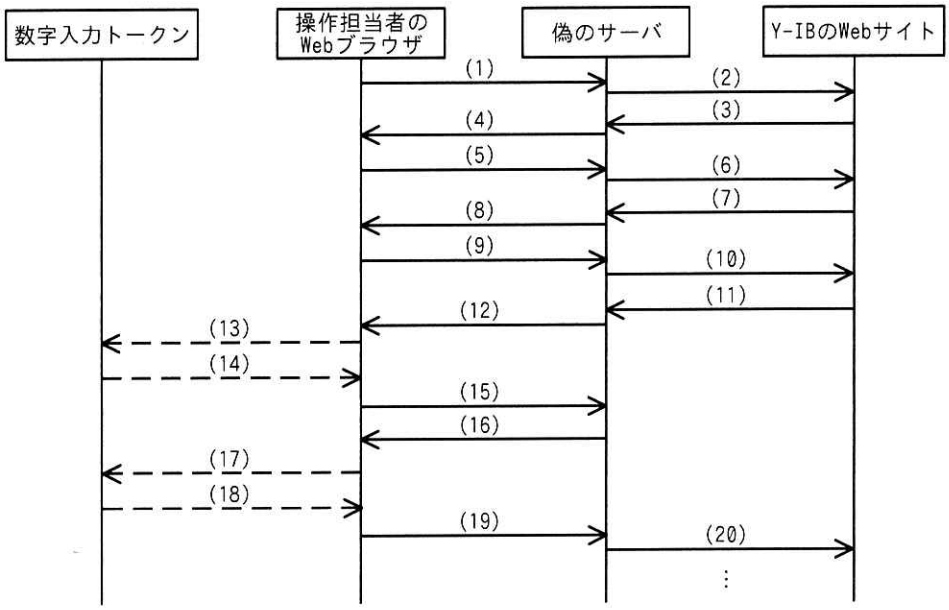
Fさんは，まず，Y-IBについてリスクを検討した。Y-IBでの振込みの流れを図3に示す。

1. 操作担当者が，Web画面で，振込先の金融機関名及び店名を選択する。
2. 操作担当者が“次へ”ボタンをクリックした後，Web画面で，振込先の口座種別及び口座番号を入力する。
3. 操作担当者が“次へ”ボタンをクリックした後，Web画面に振込先の口座名義人が表示される。振込先の金融機関又は操作した時刻によっては表示されないことがある。
4. 操作担当者が，Web画面で，振込金額を入力する。
5. 操作担当者が“次へ”ボタンをクリックした後，数字入力トークンに振込先の口座番号を入力する。
6. 数字入力トークンは，口座番号と時刻情報を基に認証番号を生成し，表示する。操作担当者が，Web画面で，認証番号を入力する。
7. 操作担当者が“次へ”ボタンをクリックした後，Web画面に振込元の口座情報，振込先の口座情報及び振込金額が表示される。
8. 操作担当者が，Web画面で“振込”ボタンをクリックすると，振込みが実行される。

注記　全ての操作において操作確認者は表示内容と入力内容を確認し，操作担当者と操作確認者の両方が合意したら次に進む。

図3　Y-IBでの振込みの流れ

Fさんは，図3を基に，操作担当者が仮に偽のサーバにアクセスした場合に攻撃者口座に振り込まれてしまうまでにやり取りされる情報を考えた。やり取りの流れを図4に，図4でやり取りされる情報を表5に示す。

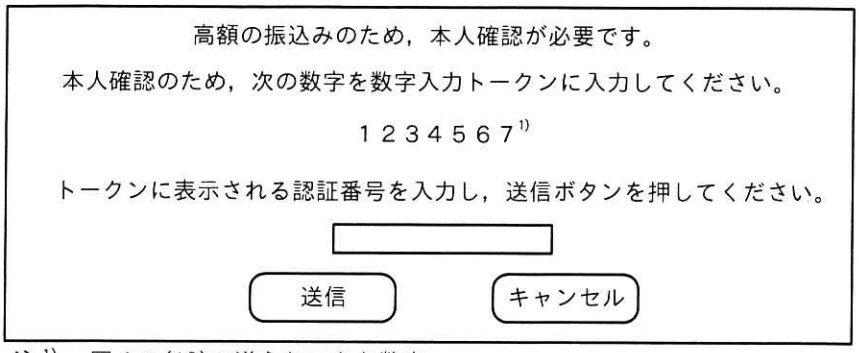


注記１　番号は流れの順序を示す。
注記２　破線はトークン操作を伴うやり取りを示す。

図４　やり取りの流れ

表５　図４でやり取りされる情報（抜粋）

図４の番号	やり取りされる情報
(2)	攻撃者口座の金融機関名及び店名
(6)	攻撃者口座の口座種別及び口座番号
(7)	攻撃者口座の口座名義人
(8)	(7)の各文字を空白に置き換えた文字列
(10)	攻撃者による書換え後の振込金額
(13)	d
(14)	認証番号
(16)	図５のポップアップ画面
(17)	e
(18)	認証番号



注[1)]　図４の(16)で送られてきた数字

図５　ポップアップ画面

図４の(16)～(19)は図３にない流れなので，操作担当者及び操作確認者が図３の流れを理解していれば，違和感を覚える可能性が高い。しかし，図３の流れを理解していなければ，気付くことなくだまされてしまうリスクも排除できない。

次に，Z-IB についてリスクを検討した。Z-IB の場合，振込先の口座情報を改ざんされたとしても，改ざん後の口座情報などの取引内容がカメラ付きトークンのディスプレイに表示されるので，口座情報が改ざんされたことに気付きやすい。

F さんは，これらの検討結果を踏まえ，攻撃者口座に振り込んでしまうリスクは Z-IB の方が低いと T 主任に報告した。T 主任は報告の内容に加えて他の機能も比較し，P 社での利用において Z-IB のセキュリティ対策に問題がないことを確認した。T 主任は G さんに，Y-IB より Z-IB の方が被害に遭うリスクが低く，利用しても問題がないと回答し，経理係では Y-IB から Z-IB に変更することにした。

〔リモートワークの検討〕

各部から育児，看護及び介護を理由とした，自宅でのリモートワーク導入の要望が挙がったことから，H 部長は，経理係の IB の利用及び情報システム係の情報システムの管理はリモートワークの対象外にする前提で，全従業員のリモートワークに必要なインフラを検討するよう T 主任に指示した。また，リモートワーク実施に当たって必要となる情報セキュリティ対策を併せて検討するように指示した。

T 主任と F さんは，最初に，リモートワークに必要なインフラを検討することにした。まず，R 社のモバイルルータ（以下，R-MR という）及び R-MR を用いるインターネット接続サービス（以下，R サービスという）について調査した。その結果，R サ

ービスではインターネットに接続したときに割り当てられるグローバル IP アドレスに，固定グローバル IP アドレスを割り当てることはできないことが分かった。次に，HTTPS を用いた VPN サービスである K 社セキュリティサービス（以下，K サービスという）を調査した。K サービスの利用方法は図 6 のとおりである。

1. 専用のソフト（以下，K ソフトという）を用いて接続する。
2. 認証には，V サービスの認証基盤サービスを IdP とする SAML を利用できる。
3. K サービス接続時に，接続元 PC の OS のバージョン，OS の脆弱性修正プログラム適用状況，マルウェア定義ファイルのバージョン（以下，三つを併せて PC 情報という）をチェックし，接続の可否を判定できる。アカウント名，PC のシリアル番号，PC 情報及び接続可否はログに記録される。接続を許可する PC 情報の条件は契約企業の管理者アカウントで設定できる。
4. K サービス経由でのインターネットアクセス時の送信元 IP アドレスとして，契約者専用の K サービス用固定グローバル IP アドレスを指定することができる。
5. インターネットアクセス時の URL フィルタリングサービスがある。HTTPS 通信の場合，K サービスと接続元 PC との間の HTTPS 通信，K サービスとインターネットのアクセス先との間の HTTPS 通信のそれぞれを終端し，K サービスで URL フィルタリングを行う。
6. URL フィルタリングサービスの除外リストに FQDN を登録すると，そのサイト宛ての HTTPS 通信は，K サービスでは HTTPS 通信の終端を行わない。
7. 契約企業の管理者アカウントでログの検索及び参照ができる。
8. 契約企業向けに用意された設定画面（以下，K サービス設定サイトという）へのアクセスを許可する接続元 IP アドレスを設定することができる。
9. K ソフトは，利用者が，PC の Web ブラウザから K サービス設定サイトに HTTPS でアクセスしてダウンロードし，インストールする。インストール時には，契約企業を識別する ID を設定する。

図 6　K サービスの利用方法

次に，T 主任と F さんは，リモートワーク用の新規社有 PC 導入時の追加の初期設定手順及び P 社におけるリモートワークでの K サービスの利用方針を検討し，検討結果をそれぞれ図 7，図 8 にまとめた。

1. 利用者が認証基盤サービスにアカウントをもっていない場合，情報システム係が認証基盤サービスでアカウントの作成を行う。
2. 情報システム係は，あらかじめダウンロードしておいた最新の脆弱性修正プログラムを社有 PC に適用する。
3. 項番 1 でアカウントが作成された場合，利用者は社有スマホに認証アプリをインストールする。利用者は自身のアカウントを使い，P 社内から社有 PC を使って MFA 設定画面にログインし，社有スマホの認証アプリを登録する。
4. 利用者は P 社内から社有 PC を使って K サービス設定サイトにアクセスし，K ソフトのダウンロード及びインストールを行う。
5. 利用者は K サービス経由で，図 2 を行う。

図 7　リモートワーク用の新規社有 PC 導入時の追加の初期設定手順（抜粋）

1. リモートワーク時には，K サービスを利用する。
2. K サービスの管理者は T 主任と F さんとする。
3. 認証に V サービスの MFA を利用する。
4. 図 6 の項番 3 については，表 1 の項番 1(2)を満たしていない PC からの接続を拒否するように設定する。
5. 図 6 の項番 4 を利用する。
6. 図 6 の項番 5 を利用する。
7. 図 6 の項番 6 については，URL フィルタリングサービスの除外リストに，基本サイトの FQDN，取引先サービスの FQDN を登録する。
8. 図 6 の項番 8 については，①K サービス設定サイトへのアクセスは P 社内だけからできるよう制限する。

図 8　P 社におけるリモートワークでの K サービスの利用方針

T 主任と F さんは検討を進め，K サービスを用いれば，リモートワーク用の社有 PC が P 社内の LAN に接続されている場合でも HTTPS 通信の URL フィルタリングサービスが適用できると考えた。そのため，リモートワーク時に限らず，P 社出勤時も経理係の IB の利用及び情報システム係の情報システムの管理を除き，社有 PC での K サービスの利用を必須にする方針とした。

F さんと T 主任は，まとめた内容を H 部長に報告し，了承を得た。

〔段階的な利用計画〕

T 主任と F さんは，R サービス及び K サービスを，T 主任と F さんが情報システムの管理以外の業務に利用する先行利用と，全従業員で利用する全体利用の 2 段階で行うことにした。

F さんは，図 8 以外に必要となる変更について，次の案を T 主任に報告した。

(1)　W 社に設定変更を依頼する。

(2)　M-FW のファイアウォール機能では社内からの HTTP 通信を禁止とし，HTTPS 通信の宛先は K サービスだけを許可する。

(3)　各取引先サービスについて，次の依頼を取引先に行う。

依頼：［　　f　　］。

T 主任は，(2)について，問題を指摘し，許可する宛先の追加を指示した。F さんは，②追加する宛先を T 主任に報告し，了承を得た。

T 主任は，これまでの検討結果を H 部長に報告し，先行利用実施の許可を得た。

〔先行利用の実施とOS移行の施策〕

先行利用では，利用中に社有スマホが故障し，認証ができないという問題が発生した。そこで，H部長とも相談し，社有スマホの故障時でもKサービスが利用できるように，MFA設定画面で次の二つを行った。

・管理者のアカウントで，認証方式を表2の認証方式3に変更する。

・先行利用の利用者アカウントについては，［ g ］。

Tさんは，1か月間，Kサービスを社内から利用し，基本サイトの利用などに問題がないことを確認した。

次に，Tさんは，社有PCをRサービスに接続し，Kサービスを利用することにした。1か月間利用し，同様に問題がないことを確認した。

Tさんは，現状，社有PCのOSの移行が滞っていることから，③情報システム係がKサービスを活用して移行を促進させる施策を考えた。

T主任は，先行利用の振返り及びOS移行の施策をH部長に報告した。H部長は，Kサービスがリモートワーク及び情報セキュリティの強化に有効であると判断し，リモートワークの導入を進めていくことにした。

設問1　〔情報システムの現状〕について答えよ。

(1)　表2中の［ a ］に入れる適切な字句を，英字10字以内で答えよ。

(2)　表2中の［ b ］，［ c ］に入れる適切な字句を，それぞれ英字5字以内で答えよ。

設問2　表5中の［ d ］，［ e ］に入れる適切な字句を解答群の中からそれぞれ選び，記号で答えよ。なお，解答は重複して選んでもよい。

解答群

ア　攻撃者口座の口座番号

イ　攻撃者による書換え前の口座番号

設問3　図8中の下線①について，設定内容を具体的に答えよ。

設問4　〔段階的な利用計画〕について答えよ。

(1)　本文中の［ f ］に入れる依頼の内容を具体的に答えよ。

(2) 本文中の下線②について，追加する宛先を答えよ。

設問5 〔先行利用の実施とOS移行の施策〕について答えよ。

(1) 本文中の［ g ］に入れる設定内容を具体的に答えよ。

(2) 本文中の下線③について，施策を具体的に答えよ。

問4　製造業におけるセキュリティ管理に関する次の記述を読んで，設問に答えよ。

L 社は，従業員 100 名の，主に家電製品の部品を製造する企業である。精密加工技術に定評があり，他社では製造が難しい部品も製造している。L 社の売上げのうち 90%は大手家電製品製造企業である J 社への売上げである。昨年度，L 社は J 社の資本参加を受け入れ，J 社の子会社になった。

今年度，L 社は，J 社から，経済産業省及び IPA が策定した“サイバーセキュリティ経営ガイドライン Ver 3.0”（以下，経営ガイドラインという）に基づき，対策を整備することを求められた。

要求を受けた L 社は，サイバーセキュリティの専門企業である N 社のコンサルティングを受けることを決め，コンサルタントで情報処理安全確保支援士（登録セキスペ）である C 氏が担当になった。L 社では最高情報セキュリティ責任者（CISO）である E 取締役を中心にして，整備を開始した。

〔L 社の状況〕

L 社の組織図を図 1 に，L 社と J 社の関係など，L 社の状況を図 2 に示す。

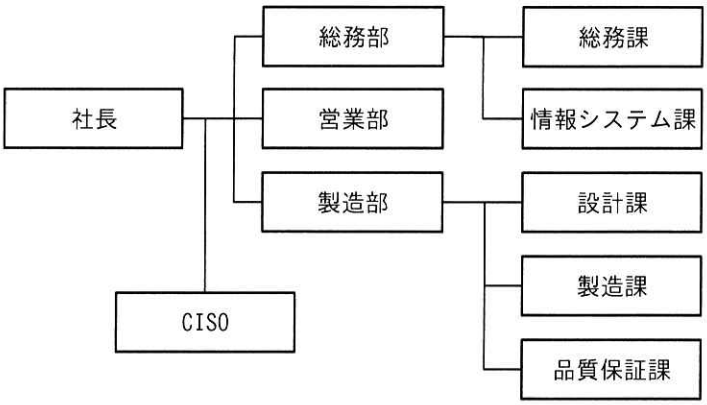
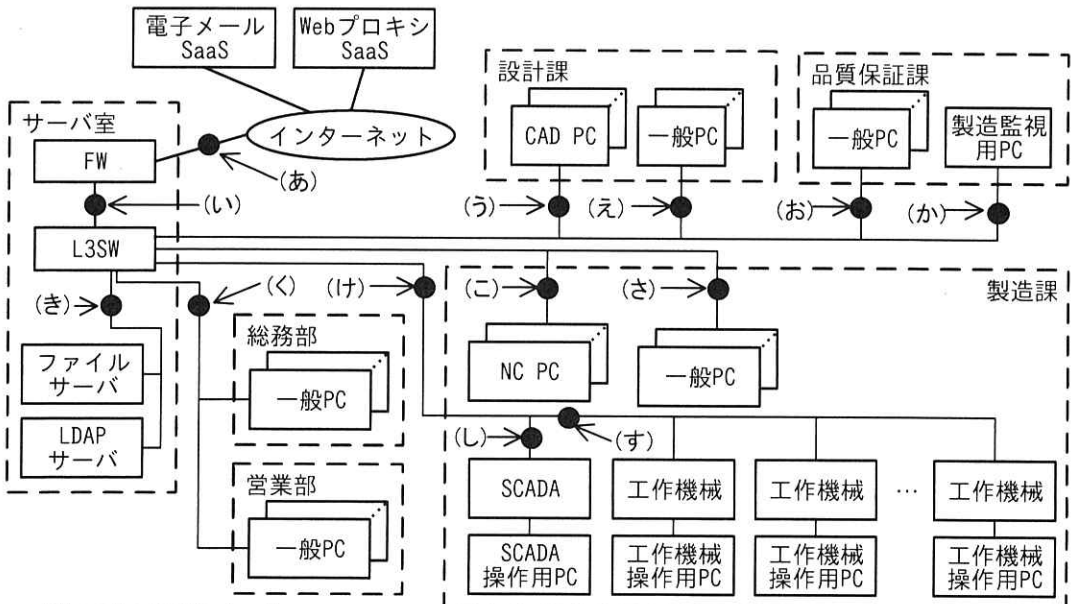


図 1　L 社の組織図

・J社とは取引基本契約を結んでいる。その契約には，次の内容が含まれている。
  - J社が秘密情報として提供した情報についての秘密保持の義務
  - 秘密保持の状況についてのJ社の監査を受ける義務
  - L社の責による秘密情報の漏えい時のJ社への損害賠償責任
  - 納期遅延，品質不良などの発生時のJ社への損害賠償責任
・部品製造に必要な設計情報ファイルなどの設計資料は，受注時にJ社から秘密情報として提供されている。
・L社が使用している工作機械は，コンピュータによる数値制御の機械である。
・全ての工作機械が停止してしまった場合でも，停止時間が2時間以内であれば出荷への大きな影響は避けられる。

図2　L社の状況

C氏は，E取締役に対してL社内のネットワークの説明を求めたが，L社にはネットワーク図がなかった。L社では，急ぎ，ネットワークの調査を行い，図3に示すL社のネットワーク図並びに表1に示すL社で使用しているSaaS及び機器の説明をまとめた。



FW：ファイアウォール
L3SW：レイヤー3スイッチ
SCADA：監視制御システム
注記　レイヤー2スイッチは，省略している。

図3　L社のネットワーク図

表1　L社で使用しているSaaS及び機器の説明（抜粋）

名称	説明
電子メールSaaS	電子メールの送受信を行う。オプションとして，表2に示すマルウェア対策機能を利用できるが，契約していない。
ファイルサーバ	設計情報ファイル，設計図ファイルなどを保存する。設計情報ファイルの保存領域，設計図ファイルの保存領域がある。領域ごとに権限を付与できる。
LDAPサーバ	ファイルサーバにアクセスするときの利用者認証を行う。
一般PC	一般事務に使用する。パターンマッチング型のマルウェア対策ソフトを導入している。
CAD PC	設計図ファイルの作成に使用する。パターンマッチング型のマルウェア対策ソフトを導入している。
NC PC	NCプログラム[1)]の作成に使用する。パターンマッチング型のマルウェア対策ソフトを導入している。
SCADA	工作機械の監視及び制御を行う。PCで使用しているOSと同じ開発元が開発したサーバ用OSを使用している。工作機械の稼働状況を製造監視用PCに送信する。パターンマッチング型のマルウェア対策ソフトを導入している。なお，故障時の予備機を1台保管している。予備機にはOSを含め何もインストールしていない。
SCADA操作用PC	SCADAの専用ポートに接続され，SCADAを直接操作する。なお，故障時の予備機としてPCを1台保管している。予備機にはOSを含め何もインストールしていない。
工作機械	SCADAからの指示，又は工作機械操作用PCの操作に従い，材料の加工を行う。
工作機械操作用PC	工作機械の専用ポートに接続されている。

注記　全PCとも同じOSを使用する。

注[1)] 工作機械の動作を指令するプログラム

表2　電子メールSaaSのマルウェア対策機能

機能	メリット	デメリット
パターンマッチング型のマルウェア対策機能	・検査時間が短い。	・［a］マルウェアは検知できない。 ・［b］された添付ファイル内のマルウェアは検知できない。
サンドボックス型のマルウェア対策機能	・［a］マルウェアでも検知が期待できる。	・検査に時間が掛かる。 ・［b］された添付ファイル内のマルウェアは検知できない。

C 氏が E 取締役に対して部品の製造の流れの説明を求めたところ，E 取締役は，試作時の製造の流れとして図 4 を，量産時の製造の流れとして図 5 を示した。

1. 営業部員が，J 社から試作の注文書と設計情報ファイルを電子メールで受け取る。設計情報ファイルは，部品の三面図[1)]である。
2. 営業部員は，設計情報ファイルをファイルサーバ内の設計情報ファイルの保存領域に保存する。保存した後，正常に読み込めるか確認する。その後，受注処理が完了したら，製造部に試作の指示を出す。
3. 設計課員が，CAD PC で，設計情報ファイルを参照し，設計図ファイルを作成する。設計図ファイルは，ファイルサーバ内の設計図ファイルの保存領域に保存する。
4. 製造課員が，NC PC で，設計図ファイルを参照して試作用 NC プログラムを作成し，次の手順で試作品を製造する。
   (1) 製造課員は，NC PC に USB メモリを接続して，その USB メモリに試作用 NC プログラムをコピーする。
   (2) 製造課員は，SCADA 操作用 PC に，(1)の USB メモリを接続して，試作用 NC プログラムを SCADA 内の試作用 NC プログラム領域に保存する。
   (3) 製造課員は，試作品を製造するように，SCADA を操作する。操作は，SCADA 操作用 PC で行う。
   (4) SCADA は，SCADA 内の試作用 NC プログラムを工作機械に投入した後，工作機械に工作開始を指示する。
   (5) 工作機械は，SCADA からの指示に従い，工作を行う。
5. 製造課員が，工作機械から完成した試作品を取り出す。その後，設計課員，製造課員及び品質保証課員それぞれが，試作品が J 社の設計情報ファイル及び L 社の品質基準に適合しているか確認する。不具合があれば，製造課員が試作用 NC プログラムを修正して，再度試作を行う。最終的に適合していると確認できた試作用 NC プログラムを量産用 NC プログラムとする。
6. 製造課員が，量産用 NC プログラムを，項番 4 の(1)，(2)と同様の手順で SCADA 内の量産用 NC プログラム領域に保存する。

注 1) 対象物を三方向から見た形状を記した図面であり，正面図，平面図，側面図から成る。

図 4　試作時の製造の流れ

1. 営業部員が，生産個数，納期を含めた量産の注文書を，電子メールで受け取る。受注処理が完了したら，製造課に製造指示を出す。
2. 製造課員は，製造指示を受けた部品を製造するように，SCADA を操作する。操作は，SCADA 操作用 PC で行う。
3. SCADA は，当該部品の量産用 NC プログラムを工作機械に投入した後，工作機械に工作開始を指示する。
4. 工作機械は，SCADA からの指示に従い，工作を行う。
5. 工作が全て完了したら，工作機械は操作員呼出しを行うとともに，SCADA に工作の完了を通知する。
6. 製造課員が，工作機械から完成した部品を取り出す。その後，品質保証課による検査を受け，梱包などを行い，出荷する。

図 5　量産時の製造の流れ

C 氏は，E 取締役に対してファイルサーバの権限の設定状況について説明を求めた。表 3 は，その時に提示された設計情報ファイルの保存領域での権限の設定状況である。

表 3　設計情報ファイルの保存領域での権限の設定状況

所属組織	読込権限	書込権限	権限変更権限
総務部総務課	○	×	×
総務部情報システム課	○	○	○
営業部	○	○	×
製造部設計課	○	○	○
製造部製造課	○	○	×
製造部品質保証課	○	×	×

注記　○は権限があることを，×は権限がないことを示す。

〔経営ガイドライン〕

図 6 は，経営ガイドラインに示された“サイバーセキュリティ経営の重要 10 項目”である。C 氏は，この指示 1～10 に沿って L 社に対策の助言を始めた。

指示 1　サイバーセキュリティリスクの認識，組織全体での対応方針の策定
指示 2　サイバーセキュリティリスク管理体制の構築
指示 3　サイバーセキュリティ対策のための資源（予算，人材等）確保
指示 4　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示 5　サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示 6　PDCA サイクルによるサイバーセキュリティ対策の継続的改善
指示 7　インシデント発生時の緊急対応体制の整備
指示 8　インシデントによる被害に備えた事業継続・復旧体制の整備
指示 9　ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
指示 10　サイバーセキュリティに関する情報の収集，共有及び開示の促進

図 6　サイバーセキュリティ経営の重要 10 項目

〔指示 4 に関する助言〕

経営ガイドラインにおける指示 4 の説明は，図 7 のとおりである。

●事業に用いるデジタル環境，サービス及び情報を特定させ，それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から，自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。
●サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダへの委託を含めたリスク対応計画を策定させ，対応後の残留リスクを識別させる。

図 7　経営ガイドラインにおける指示 4 の説明

C 氏は，経営ガイドラインの指示 4 では，サイバー攻撃に関してリスクアセスメントを行い，対応計画を策定することを求めていると説明した。C 氏は，リスクの識別と対応計画の策定を図 8 の手順で進めるように助言した。

1. L 社が管理する情報資産のうち，守るべきものを特定する。
2. 守るべき情報資産について，保存場所や取扱状況を把握する。
3. 守るべき情報資産に影響を与えるリスクを洗い出し，レベル分けを行う。
4. 洗い出したリスクについて，対応する方法を決定し，対応計画を策定する。リスクに対応する方法は，低減，［ c ］，［ d ］，［ e ］の四つに分類される。

図 8　リスクの識別と対応計画の策定の手順（概要）

次は，その時の C 氏と E 取締役の会話である。

C 氏　　：例えば，J 社から受け取った設計情報ファイルに影響を与えるリスクについて，図 8 の項番 3 と 4 は実行できそうでしょうか。

E 取締役：はい。例えば，LAN に接続された PC がマルウェアに感染して情報の漏えいが起きるリスクがありますが，マルウェア対策ソフトを導入していますので，追加の対策は不要だと考えています。

C 氏　　：マルウェアによっては，パターンマッチング型のマルウェア対策ソフトでは検知できないおそれがあります。そう考えると，追加の対策は必要でしょう。リスクのレベル分けについては，別の機会に説明します。

E 取締役：分かりました。

C 氏　　：項番 4 について例を挙げると，設計情報ファイルを扱う業務が図 4 だけなら，①最小権限の原則に沿って表 3 の権限の設定を見直すことによって，PC がマルウェアに感染したときの設計情報ファイルに影響を与えるリスクを低減することができます。

E 取締役：分かりました。

〔指示 5 に関する助言〕

経営ガイドラインにおける指示 5 の説明は，図 9 のとおりである。

●サイバーセキュリティリスクに対応するための保護対策として，防御・検知・分析の各機能を実現する仕組みを構築させる。
●構築した仕組みについて，事業環境やリスクの変化に対応するための見直しを実施させる。

図9　経営ガイドラインにおける指示5の説明

C氏は，経営ガイドラインの指示5では，指示4で識別したリスクに対応するための保護対策として，効果的な仕組みの導入と見直しを求めていると説明した。C氏は，リスクに対応するための具体的な保護対策を考えるため，図8で洗い出したリスクが顕在化する具体的な攻撃シナリオと，そのシナリオから情報やシステムを保護する対策を並べた表を作るよう助言した。C氏の助言を受けながらL社が作成した表が表4である。

表4　攻撃シナリオと対策

項番	攻撃シナリオ	保護する対策
1	営業部員が，営業部の一般PCに私有のUSBメモリを接続し，そのUSBメモリに設計情報ファイルをコピーして持ち出し，J社の競合他社に売却する。	図3中の営業部の一般PCのOSの設定を変更し，USBメモリを使用できなくする。
2	現行のFWに未修正の脆弱性があり，攻撃者がその脆弱性を悪用しインターネットから直接L社のネットワークに接続する。次に，利用者IDとパスワードを推測してファイルサーバに不正アクセスし，全てのファイルを削除する。	図3中の(あ)の箇所に，現行のFWとは異なるベンダーのFWを導入する。 （省略）
3	電子メールに添付されたマルウェアによって，社内の一般PCにマルウェアの感染が広がった後，SCADAに感染が広がり，NCプログラムが使用できなくなる。	図3中の電子メールSaaSで，表2の両方のマルウェア対策機能を契約する。 図3中の一般PC及びSCADAに，パターンマッチング型以外のマルウェア対策ソフトを導入する。 ［ f ］を導入する。
4	購入したUSBメモリがマルウェアに感染していて，そのUSBメモリからSCADA操作用PCがマルウェアに感染し，マルウェアがSCADAを不正に操作した結果，SCADAが停止してしまう。	図3中のSCADA操作用PCに，マルウェア対策ソフトを導入する。 ［ g ］を導入する。
（省略）		

注記　一つのシナリオに対して複数の併用すべき対策を挙げたものもある。

〔指示 8 に関する助言〕

経営ガイドラインにおける指示 8 の説明は図 10 のとおりである。

●インシデントにより業務停止等に至った場合，企業経営への影響を考慮していつまでに復旧すべきかを特定し，復旧に向けた手順書策定や，復旧対応体制の整備をさせる。 ●制御系も含めた BCP との連携等，組織全体として有効かつ整合のとれた復旧目標計画を定めさせる。

図 10　経営ガイドラインにおける指示 8 の説明（抜粋）

C 氏は，経営ガイドラインの指示 8 では，業務停止に至るインシデントを想定して，復旧計画及びその体制を整えることを求めていると説明した。次は，その時の C 氏と E 取締役の会話である。

C 氏　　：何らかの理由で工作機械が停止してしまった場合の復旧対応体制は整備していますか。

E 取締役：今まで 2 時間を超える停止は起こっていなかったので，整備していません。

C 氏　　：最大許容停止時間 2 時間以内を実現するには，まず製造が停止する被害に至るシナリオ（以下，被害のシナリオという）を想定します。次に，被害のシナリオが実際に起こった場合に 2 時間以内で製造を再開するために必要となるソフトウェアやハードウェアなど（以下，必要な仕組みという）及び必要な手順をまとめます。例として，表 5 に SCADA の偶発的な故障を発端とした被害のシナリオ，必要な仕組み及び必要な手順を挙げました。

表 5　被害のシナリオ，必要な仕組み及び必要な手順の例

被害のシナリオ	必要な仕組み	必要な手順
SCADA が故障して，工作機械に NC プログラムを投入できなくなる。	SCADA のホットスタンバイ機	ホットスタンバイ機に切り替える手順

E 取締役：分かりました。まとめてみます。

C 氏　　：必要な仕組み及び必要な手順が整備できた後に，演習を行う必要もあります。

この後，L 社では C 氏の助言を受けながら，外部からのサイバー攻撃を発端とした被害のシナリオ，必要な仕組み及び必要な手順について表 6 にまとめた。

表 6　外部からのサイバー攻撃を発端とした被害のシナリオ，必要な仕組み及び必要な手順

被害のシナリオ	必要な仕組み	必要な手順
表 4 の項番 3	（省略）	（省略）
表 4 の項番 4	（省略）	（省略）
一般 PC，CAD PC 又は NC PC がマルウェアに感染し，SCADA に感染が広がり，工作ができなくなる。	PC を復旧するための，業務アプリケーションプログラム（以下，アプリケーションプログラムをアプリという）を含むリカバリメディア	PC を一斉に復旧する手順
	予備機を用いて SCADA を復旧するための，SCADA アプリを含むリカバリメディア	SCADA を復旧する手順
	h	i
j	k	l
（省略）		

注記　一つのシナリオに対して複数の併用すべき対策を挙げたものもある。

C 氏は，その他の指示についても対策を助言し，L 社は助言に従って対策を実施した。その後，L 社は，対策の整備状況を報告書にまとめて J 社に報告した。

設問 1　表 2 中の a，b に入れる適切な字句を，それぞれ 5 字以内で答えよ。

設問 2　〔指示 4 に関する助言〕について答えよ。

(1)　図 8 中の c ～ e に入れる適切な字句を答えよ。

(2)　本文中の下線①について，見直し後の権限の設定を答えよ。

設問 3　表 4 中の f，g に入れる適切な字句を，対策とその導入箇所を含めて答えよ。いずれも，できるだけ効果が高いものを答えるものとし，効果が同程度であれば，業務への影響が少ないものを答えるものとする。なお，導入箇所がネットワーク上の場合は，導入箇所については，図 3 の(あ)～(す)から選んで含めよ。

設問４　〔指示８に関する助言〕について答えよ。

(1)　表６中の［　h　］，［　i　］に入れる適切な字句を答えよ。

(2)　表６中の［　j　］～［　l　］に入れる適切な字句を答えよ。［　j　］には，できるだけ起こる可能性が高いものを，攻撃の発端を含めて答えよ。［　k　］には，できるだけ効果の高いものを答えよ。

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	13:10 ～ 14:50

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。