問１　協力会社とのファイルの受渡しに関する次の記述を読んで，設問1～5に答えよ。

U社は，従業員10,000名の半導体製造業であり，国内に工場を置いている。U社では，幾つかの工程を国内の40社の協力会社に委託しており，生産計画や設計書類のファイルを協力会社との間で受け渡す必要がある。ファイルの受渡し件数は，協力会社によって異なるが，1日当たり1件から10件である。U社では，生産管理課が協力会社とのファイルの受渡しを担当している。ファイルの受渡しには，Webベースのファイル交換システム（以下，Dシステムという）を使用している。Dシステムは，HTTPサーバ及びU社が開発したWebアプリケーションプログラム（以下，Uアプリという）から成る。Dシステムでは受発注に関するファイルは取り扱っていない。

図1は，Dシステムに関係する機器の全体構成である。

図1　Dシステムに関係する機器の全体構成

U社の生産管理課及び協力会社に設置したファイル受渡し用PCからDシステムまでのアクセスは，HTTPSで行われている。U社ネットワーク内からDシステムにアクセスできる端末は，FWの設定によって，生産管理課に設置したファイル受渡し用PCだけに制限している。

Dシステムのアカウントは，協力会社の拠点ごとに一つ，U社が発行している。Dシステムの利用者認証は，利用者IDとパスワードによって行われている。

〔セキュリティインシデントの発生〕

ある日，D システムのトップページが改ざんされるというセキュリティインシデントが発生した。調査したところ，HTTP サーバの既知の脆弱性を悪用した攻撃によって改ざんされたと分かり，脆弱性修正プログラムの適用などをしてから復旧した。

セキュリティインシデントの調査の過程で，HTTP サーバのアクセスログから，協力会社 P 社に発行したアカウントを用いて海外の IP アドレスからアクセスした履歴が見つかった。このアクセスは，D システムの利用規約や法令に違反しているおそれがあるので，P 社に問い合わせたところ，P 社の従業員の 1 人が海外出張先からアクセスしていたことが分かった。

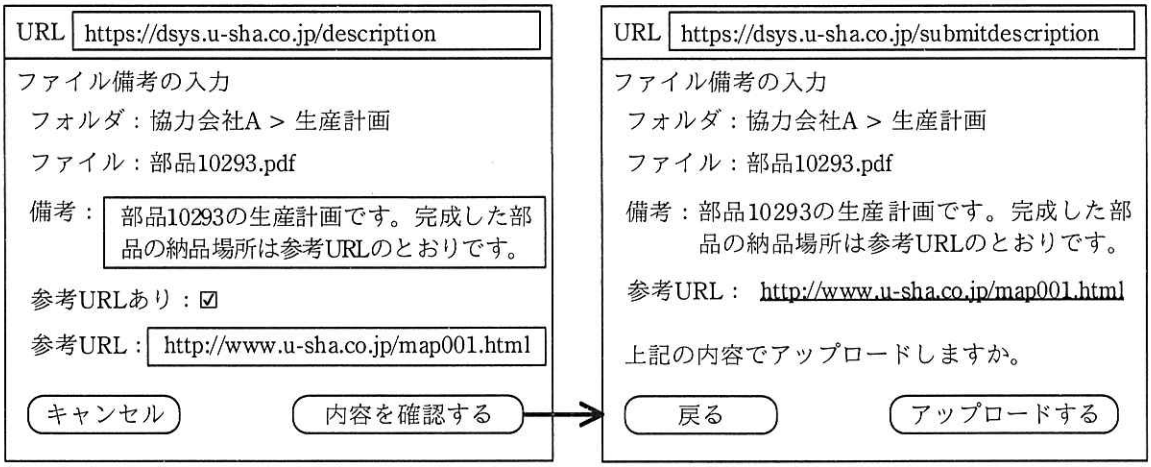
D システムの利用規約では，ファイル受渡し用 PC には，各協力会社の社内への設置，並びに盗難対策，マルウェア対策及びファイルの不正持出し対策を求めている。また，D システムには，ファイル受渡し用 PC からだけアクセスすることを求めている。しかし，U 社ではいずれの遵守状況も確認していなかった。

こういった利用規約違反への対策として，海外からのアクセスを FW で禁止した。さらに，協力会社以外からのアクセスを検知するために，SIEM（Security Information and Event Management）を導入した。

〔D システムの脆弱性診断〕

U 社は，ほかにも D システムに対策が必要な脆弱性がないかどうかを確認するために，脆弱性診断をセキュリティ専門会社である N 社に依頼した。

診断の結果，クロスサイトスクリプティング（以下，XSS という）脆弱性などが発見された。XSS 脆弱性が発見された箇所を，図 2 に示す。



画面A　備考などの入力画面　　画面B　入力後に遷移する確認画面

注記 1　矢印は画面 A の入力欄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。
注記 2　画面 B の下線は，リンクであることを示している。

図 2　XSS 脆弱性が発見された箇所

N 社の，XSS 脆弱性についての報告を図 3 に示す。

(1) XSS 脆弱性の診断は，URL を Web ブラウザのアドレスバーに入力し，HTTP レスポンス及び表示される画面の内容を確認することによって行った。
(2) まず，図 2 の画面 A と画面 B の診断のために，診断用 URL1 と診断用 URL2 の二つを入力した。診断用 URL1 を図 4，診断用 URL1 を入力した時に得られたサーバからの HTTP レスポンスのボディ部を図 5，診断用 URL2 を図 6，診断用 URL2 を入力した時に得られたサーバからの HTTP レスポンスのボディ部を図 7 に示す。
(3) 図 5 から，description パラメタの値を画面 B の備考に出力する際には，エスケープ処理が正しく行われており，XSS 脆弱性は認められない。
(4) 診断用 URL2 を入力した時に表示された画面 B 上で，参考 URL のリンクをクリックすると，“XSS!” という内容のダイアログボックスが表示された。
(5) 上記(4)と，図 7 から，refURL パラメタの値を画面 B の参考 URL のリンクとして出力する際の処理に問題があり，XSS 脆弱性が存在すると認められる。
(6) 上記(5)で示した脆弱性の原因は，refURL パラメタの出力部において，プログラミングに関する次の二つの誤りのうちのどちらかによるものと想定される。
　- XSS を防ぐための処理を一切していない。
　- XSS を防ぐための基本的な処理はしているが，HTML タグの属性値の出力時に必要な処理が行われていない。
(7) 次に，いずれの誤りなのかを調べるために，図 8 に示す診断用 URL3 を入力した。その時に得られたサーバからの HTTP レスポンスのボディ部が図 9 である。

図 3　XSS 脆弱性の報告（抜粋）

```
https://dsys.u-sha.co.jp/submitdescription?fileID=001023&description=<script>alert('XSS!')</script>&checkbox=on&refURL=http%3A%2F%2Fwww.u-sha.co.jp/
```

図 4　診断用 URL1

```
（省略）
備考：[ a ] script [ b ] alert('XSS!') [ a ] /script [ b ] <br>
（省略）
参考 URL：<a href="http://www.u-sha.co.jp/">http://www.u-sha.co.jp/</a>
（省略）
```

図 5　診断用 URL1 を入力した時の HTTP レスポンスのボディ部

```
https://dsys.u-sha.co.jp/submitdescription?fileID=001023&description=test2&checkbox=on
&refURL=[ c ]
```

図 6　診断用 URL2

```
（省略）
備考：test2<br>
（省略）
参考 URL：<a href="[ c ]">[ c ]</a>
（省略）
```

図 7　診断用 URL2 を入力した時の HTTP レスポンスのボディ部

```
https://dsys.u-sha.co.jp/submitdescription?fileID=001023&description=test3&checkbox=on
&refURL="%20onmouseover=alert('XSS!')%20foo="
```

図 8　診断用 URL3

```
（省略）
備考：test3<br>
（省略）
参考 URL：<a href="&quot; onmouseover=alert('XSS!') foo=&quot;">&quot;
onmouseover=alert('XSS!') foo=&quot;</a>
（省略）
```

図 9　診断用 URL3 を入力した時の HTTP レスポンスのボディ部

〔D システムの脆弱性対策〕

XSS 脆弱性の報告を受けた U 社は，N 社の支援を受けて，D システムの XSS 脆弱性対策を進めることにした。支援を担当した情報処理安全確保支援士（登録セキスペ）である R 氏は，二つの対策を提案した。

一つ目の対策は，①図 3 で特定された XSS 脆弱性を解消するための U アプリの改修である。

二つ目の対策は，“Content-Security-Policy: script-src 'self';” というヘッダフィールドを，HTTP レスポンスのヘッダに追加することによって，Web ブラウザに対して②指定したスクリプトファイルの実行だけを許可するというものである。この対策は，一つ目の対策に比べて短期間で実施可能であるが，D システムが用いている正規のスクリプトが意図したとおりに動作するように，③実行が制限されてしまうスクリプトの有無を確認し，もしあれば，当該箇所の呼出し方法を変更する必要がある。

一部の古い Web ブラウザは Content-Security-Policy に対応していないので，万全の対策のためには，二つの対策を両方実施することが必要である。

U 社は，R 氏の提案どおり，Content-Security-Policy を速やかに追加するとともに，U アプリの改修計画の策定を開始した。

〔D システムの SaaS への移行の検討〕

U 社の情報システム部の Y さんが U アプリの改修を計画していたところ，将来にわたり U 社で U アプリのメンテナンスを続けるよりも SaaS に移行する方が機能面でもセキュリティ対策の面でもよいのではないかという意見が出た。

そこで，Y さんは，U アプリのメンテナンス継続と SaaS への移行のメリットとデメリットを比較した。比較の結果，表 1 に概要を示す G 社提供の SaaS（以下，G サービスという）に移行する方が，U アプリのメンテナンスを継続するよりもメリットが多そうなので，更に詳細に検討することにした。

表1　Gサービスの概要

項目	内容
基本機能	・利用者は，Web ブラウザでアクセスする。 ・G サービス上のストレージにファイルをアップロードしたり，ローカルのストレージにダウンロードしたりできる。 ・アップロードしたファイルは，複数階層にわたるフォルダで管理される。利用者は，アクセス権に従ってフォルダを作成することができる。
アクセス権	・ファイル及びフォルダに対して，利用者ごとにアクセス権を設定できる。
契約に伴う制限	・契約で定められた容量が割り当てられる。 ・ほかの契約者に割り当てられた領域には，アクセスできない。 ・契約では発行できるアカウント数の上限が定められている。

Yさんは，Gサービスへの移行について，Dシステムの利用規約の継続を前提として，次の項目を検討することにした。

項目1：必要なセキュリティ対策のGサービスでの実現可否

項目2：SIEMとの連携

〔項目1の検討〕

Yさんは，項目1について検討した。表2は，その検討結果である。

表2　項目1の検討結果

必要なセキュリティ対策	Gサービスでの実現可否
協力会社以外からのアクセス禁止	G サービスで，送信元 IP アドレスの制限を行うことができないので否
Web アプリケーションプログラムの脆弱性への対応	G社が実施するので可
サーバ OS 及び HTTP サーバへの脆弱性修正プログラムの適用	G社が実施するので可
ファイルを G サービス上のストレージに保存するときの暗号化	Gサービスの機能として，自動的に暗号化され，暗号鍵はG社が管理するので可
ファイルの完全削除	ファイルを削除しても，Gサービス上のストレージに情報が残る可能性があるので否
災害時の業務継続	ファイルや管理情報が，日本国内とF国の両方のデータセンタに保存されており，片方が災害に遭ってもデータの消失とサービスの停止を防ぐことができるので可

次は，検討結果に関するYさんとU社のCSIRTリーダであるTさんの会話である。

Y さん：表2のとおり，セキュリティ対策の大部分はGサービスで実現できますが，Gサービスが信頼できるかどうかの見極めが必要です。

T さん：そのとおりだね。例えば，クラウドサービスのための［ d ］の実践の規範である ISO/IEC 27017 に基づく認証や，D システムとは直接関係がないが，パブリッククラウドにおける［ e ］の実践の規範である ISO/IEC 27018 に基づく認証を取得しているサービスであれば信頼してよいのではないかな。

Y さん：G サービスは，ISO/IEC 27017 に基づく認証を取得しているので，信頼できそうですね。

T さん：そうだね。ところで，F 国では安全保障上の要請があれば，F 国内に保存されているデータを，F 国政府に強制的に提出させる国内法が存在する。④Gサービスを経由して協力会社との間で受け渡すファイルの内容を保護するという観点で，どのような措置が当社として取り得るか，考えてほしい。

Y さん：分かりました。

〔項目2の検討〕

現行のDシステムでは，協力会社以外からのアクセスを検知するために SIEM を利用しているが，G サービスでは SIEM の機能は提供していない。Y さんが調査した結果，G サービスに移行した場合でも，G サービスの API を利用すれば，表3に示すログを U 社の SIEM へ取り込めることが分かった。

表3　提供しているログ

対象	実行された操作
アカウント	ログイン，ログアウト，作成，削除，権限変更
フォルダ	作成，削除，名称変更，アクセス権変更
ファイル	ダウンロード，アップロード，削除，名称変更，アクセス権変更

ログには，操作対象，実行された操作とともに，日付，時刻，実行した利用者 ID，アクセス元 IP アドレス，及び結果（成功又は失敗）が記録される。

続いて，Y さんは，G サービスが提供している，利用者 ID とパスワードによる認証を利用した場合に，SIEM を利用してログから不正アクセスが検知できるかどうか

を検討した。表4は，Yさんが考えた，ログから不正アクセスを検知する方法である。

表4　ログから不正アクセスを検知する方法（抜粋）

項番	不正アクセスの方法	検知の方法
1	利用者 ID を固定して，パスワードを総当たりする。	一定時間当たりの［　f　］の回数がしきい値を超えたら，不正アクセスとして検知する。
2	少数のパスワードについて，利用者 ID を総当たりする。	一定時間当たりの同一 IP アドレスからの異なる利用者 ID によるログイン失敗の回数がしきい値を超えたら，不正アクセスとして検知する。

表4を確認したTさんは，いずれの不正アクセスもゆっくりと実行された場合には見逃すことがあることと，項番2については，⑤ほかの場合にも見逃すことがあることを指摘した。さらに，不正アクセスを防ぐには，多要素認証を採用する方がよいことと，多要素認証は，G サービス単独では実現できないが，IDaaS との連携で実現できることを説明した。

〔IDaaS との連携による多要素認証の実現方式の検討〕

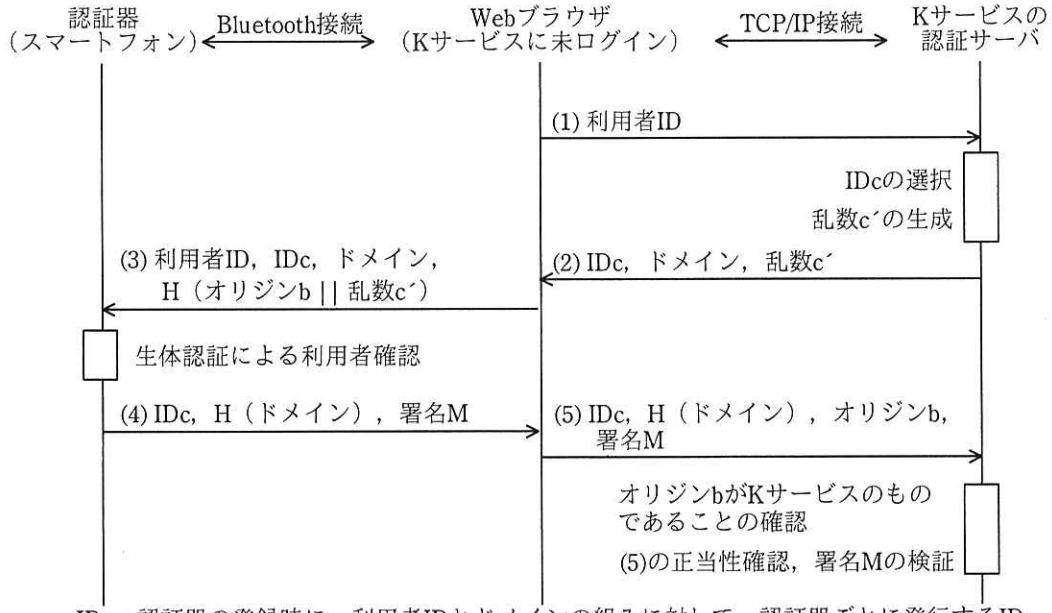
Y さんは，IDaaS との連携による多要素認証の実現方式の検討を開始した。幾つかの IDaaS を検討した結果，国内の互いに地理的に離れた複数のデータセンタで運用されている K サービスとの連携による実現が最適であると考えた。K サービスでは，様々な認証方式を選択できるが，Y さんは，G サービスを利用した新たなファイル交換システム（以下，E システムという）には，FIDO 認証が最もふさわしいと考え，FIDO 認証器として何を選択するべきか，検討を開始した。まず，K サービスで利用できる FIDO 認証器の仕組みについて調査し，表5にまとめた。

表 5　FIDO 認証器の仕組み

認証器	Web ブラウザとの通信方法	認証器使用時の利用者確認（User Verification）	複数利用者による認証器の共用	組合せ[1)]
スマートフォン	Bluetooth 経由	スマートフォンに組み込まれた生体認証装置による生体認証	できない	限定されない
USB 接続外部認証器	USB ポート経由	なし	できない	限定されない
OS 内蔵の生体認証機能	OS 内部処理	OS に内蔵された生体認証機能による生体認証	OS の利用者 ID 間で可能	限定される

注[1)]　K サービスにアクセスする PC と，認証器の組合せ

認証器としてスマートフォンを利用した場合の利用者認証の流れは図 10 のとおりであった。



IDc：認証器の登録時に，利用者IDとドメインの組みに対して，認証器ごとに発行するID
H（A）：Aのハッシュ値
A || B：AとBを連結
オリジンb：Webブラウザがアクセスしているwebサイトのオリジン
署名M：H（ドメイン），H（オリジンb || 乱数c´）に対するディジタル署名

図 10　利用者認証の流れ

Y さんは，図 10 中の(3)～(5)のメッセージの生成にオリジン b が使われていることについて T さんにその目的を尋ねた。T さんは，攻撃者が，［　g　］するための

特別なサーバをインターネット上に用意し，何らかの方法で被害者をそのサーバに誘導し，認証情報を不正に入手して悪用するという攻撃を防御するためだと答えた。

続いて Y さんは，E システムにおいて，それぞれの認証器を使用した場合を想定し，認証器の取扱いを表6に，運用上のリスクと対策を表7にまとめた。

表6　認証器の取扱い

認証器	K サービスにおける取扱い	E システムにおける認証器の所有者	E システムにおける認証器の配布方法
スマートフォン	供給せず，要件を提示している。	各協力会社又は利用者個人	協力会社によって異なる。
USB 接続外部認証器	専用機器を契約者だけに販売している。	U 社の一括購入となるので，U 社	U 社から必要個数を各協力会社に配布する。
OS 内蔵の生体認証機能	供給せず，要件を提示している。	各協力会社	ファイル受渡し用 PC が認証器を兼ねるので，認証器の別途配布は不要である。

表7　運用上のリスクと対策（抜粋）

認証器	認証器の紛失・盗難時のリスクと対策	退職時のリスクと対策[1]
スマートフォン	認証器の使用時に［ h ］が必要なので，不正利用される可能性は低い。	退職者による不正なアクセスを防ぐために，個人所有のスマートフォンを利用していた場合も想定して，退職時又は退職後直ちに，［ i ］では，［ j ］する必要がある。
USB 接続外部認証器	第三者による不正利用を防ぐために，直ちに［ k ］する必要がある。	（省略）
OS 内蔵の生体認証機能	認証器の使用時に［ h ］が必要なので，不正利用される可能性は低い。	休眠アカウントを悪用した不正アクセスを防ぐために，ファイル受渡し用 PC にログインするためのアカウントを忘れずに削除する必要がある。

注[1]　E システムの利用者だった従業員が退職した場合のリスクと対策

Yさんは，各認証器を比較し，次のようにまとめた。

・Kサービスのアカウントに対して認証器を登録する際は，いずれの認証器でも，不正がないように確認する必要があり，登録について大きな差はない。

・USB接続外部認証器は，紛失・盗難に備えた体制を整えるのが難しいので，採用しない。

・スマートフォン及びOS内蔵の生体認証機能は，認証器として大きな差はないが，⑥Dシステムで要求されていたセキュリティ要件を技術的に実現できるので，OS内蔵の生体認証機能の方が望ましい。

上記からYさんは認証器としてOS内蔵の生体認証機能を採用することにした。

その後，Yさんは検討を続け，DシステムをEシステムに移行する案をまとめた。U社では，その案を承認し，Eシステムへの移行を開始した。

設問1　〔Dシステムの脆弱性診断〕について，(1)，(2)に答えよ。

(1)　図5中の［ a ］，［ b ］に入れる適切な文字列を，それぞれ4字で答えよ。

(2)　図6中及び図7中の［ c ］に入れる適切な文字列を，解答群の中から選び，記号で答えよ。

解答群

ア　onmouseover=alert('XSS!')

イ　"><script>alert('XSS!')</script>

ウ　http:<script>alert('XSS!')</script>

エ　javascript:alert('XSS!')

設問2　〔Dシステムの脆弱性対策〕について，(1)～(3)に答えよ。

(1)　本文中の下線①について，改修方法を45字以内で具体的に述べよ。

(2)　本文中の下線②について，実行が許可されるのはどのようなスクリプトファイルか。40字以内で述べよ。

(3)　本文中の下線③について，実行が制限されてしまうのはどのようなスクリ

プトか。30 字以内で述べよ。また，変更後の呼出し方法を 50 字以内で具体的に述べよ。

設問３　〔項目１の検討〕について，(1)，(2)に答えよ。

(1)　本文中の［ d ］，［ e ］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　個人情報保護　　イ　システム監査

ウ　情報セキュリティ管理策　　エ　審査及び認証

(2)　本文中の下線④について，取り得る措置を 40 字以内で述べよ。

設問４　〔項目２の検討〕について，(1)，(2)に答えよ。

(1)　表４中の［ f ］に入れる適切な内容を 20 字以内で答えよ。

(2)　本文中の下線⑤について，ほかの場合とはどのような場合か。40 字以内で述べよ。

設問５　〔IDaaS との連携による多要素認証の実現方式の検討〕について，(1)～(3)に答えよ。

(1)　本文中の［ g ］に入れる適切な内容を，20 字以内で具体的に答えよ。

(2)　表７中の［ h ］～［ k ］に入れる，適切な内容を，それぞれ 10 字以内で答えよ。

(3)　本文中の下線⑥のように考えた理由は何か。50 字以内で述べよ。