問１　セキュリティ対策の評価に関する次の記述を読んで，設問 1～4 に答えよ。

R 団体はある科学技術分野のノウハウを有する，職員数 300 名の一般社団法人である。特殊な用途に用いる精密機器のプロトタイプ製作，民間企業や教育機関への技術情報の提供，安全基準の助言などを行っている。R 団体とステークホルダとの関係を図 1 に，ステークホルダの概要を表 1 に示す。

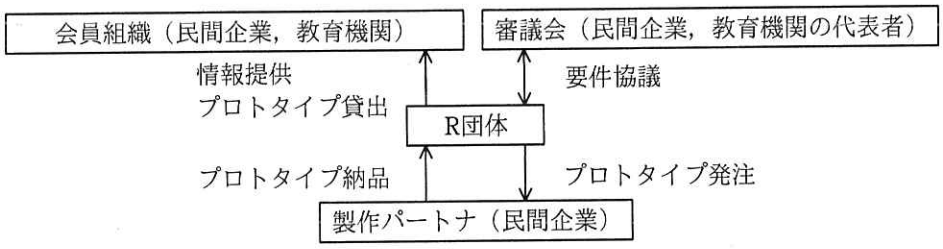

図 1　R 団体とステークホルダとの関係

表 1　ステークホルダの概要

名称	概要
会員組織	R 団体に入会を申請し，R 団体が入会を認めた組織。会員組織は，自組織の活動を有利に進めるために，R 団体が提供する情報や貸し出すプロトタイプを活用する。
審議会	一部の会員組織の代表者で構成される会議体。R 団体に製作を要請するプロトタイプの要件を取りまとめる。R 団体が要求仕様書や図面を作成するに当たって，R 団体と打合せを行う。打合せは不定期に R 団体の会議室で行われ，議事録などは主に電子メール（以下，メールという）で共有される。
製作パートナ	要求仕様書と図面を基に，プロトタイプを製作する業者。原則として，プロトタイプごとに公募され，入札で選ばれる。R 団体と製作パートナとの契約後の情報のやり取りは，R 団体が運用するポータルサイト（以下，R ポータルという）で行う。

R 団体の各部署の業務内容を表 2 に示す。

表２　各部署の業務内容（抜粋）

部署名	業務名	業務内容
システム企画課	システム企画	R 団体の情報システムの要件をまとめ，設計や構築を開発業者に依頼する。
	セキュリティ管理	R 団体全体のセキュリティ維持に責任をもち，情報システムのセキュリティの見直しを行う。
システム運用課	R ポータルのサーバ管理	システム運用課員が運用管理に利用する PC（以下，運用管理 PC という）から SSH で Web アプリケーションサーバ（以下，WebAP サーバという）やデータベースサーバ（以下，DB サーバという）にアクセスし，設定情報変更などを行う。
設計第１課	プロトタイプ製作	審議会と打合せを行い，要求仕様書や図面を作成する。製作パートナと情報共有する場合，PC で作成した図面などのファイルを，R ポータルの Web インタフェースを用いて，アップロードする。
人事総務課	人事サーバ管理	サーバセグメントに設置されている人事サーバのデータを更新する。

プロトタイプ製作業務において扱う情報は全て機密性が高く，その中でも図面は特に機密性が高い。

R 団体では，一般業務用の PC が職員に１台ずつ貸与されており，Web 閲覧，メール送受信，図面作成などに利用されている。各 PC には固定 IP アドレスが割り当てられている。PC にログインする際には各職員の利用者 ID を入力する。R 団体のネットワーク構成を図２に示す。

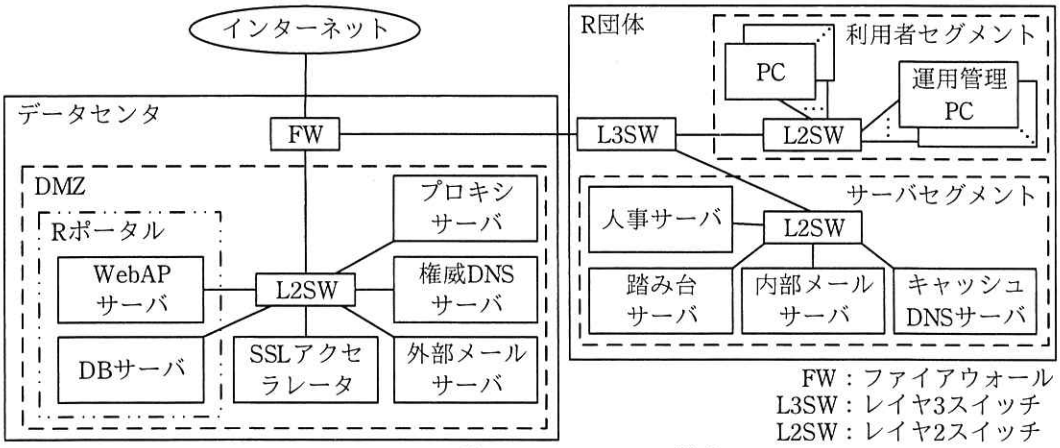

図２　R 団体のネットワーク構成

R ポータルは，利用者の認証機能，利用者ごとに権限を定義できるアクセス制御機能，ファイルをアップロード及びダウンロードできる文書共有機能，問合せ内容や回答の履歴を記録する掲示板機能を備えている。R ポータルの利用者 ID は，職員，会員組織，及び製作パートナに発行される。

また，R ポータルは，フロントエンドの WebAP サーバと，会員組織情報，要求仕様書や図面が保存されるバックエンドの DB サーバで構成され，WebAP サーバと DB サーバは ODBC（Open Database Connectivity）を用いて特定のポート間で通信している。R 団体のセキュリティ対策基準にのっとり，DB サーバには，システム運用課員によるログインと，WebAP サーバからの接続だけが許可されている。利用者セグメントから DB サーバへのアクセスは，FW によって運用管理 PC の IP アドレスからのアクセスだけが許可されている。

人事サーバ管理での人事データの更新には二つの方法がある。通常の更新は，人事サーバの Web インタフェースを使用して PC 上で行う。期初などの大量の人事異動が発生するタイミングでは，PC からリモートデスクトップ機能を使い，一度，踏み台サーバの利用者 ID（以下，管理 ID という）を用いて踏み台サーバにログイン後，さらに，踏み台サーバからリモートデスクトップ機能を使い，共通の利用者 ID とパスワード（以下，共通管理者アカウントという）で人事サーバにログインして，一括で更新している。管理 ID は職員ごとに異なっている。R 団体では，踏み台サーバを除き，サーバセグメントと DMZ に置くサーバでは，運用負荷軽減の観点から，共通管理者アカウントが設定されている。

サーバセグメント内のサーバでは，表 3 のアクセスだけを許可している。

表3　サーバへのアクセス許可

項番	アクセス元	アクセス先	アクセス制御方法	サービス
1	人事総務課の一部の職員のPC	踏み台サーバ	管理 ID とパスワードによる認証	リモートデスクトップ
2	運用管理 PC	踏み台サーバ	管理 ID とパスワードによる認証	リモートデスクトップ
3	踏み台サーバ	サーバセグメントの全てのサーバ	サーバの共通管理者アカウントによる認証	リモートデスクトップを含むメンテナンス用のサービス
4	利用者セグメントの全てのPC	サーバセグメントの全てのサーバ	IP アドレスによるフィルタリング，又は職員の利用者 ID とパスワードによる認証	職員に許可されている必要最小限のサービス

踏み台サーバには操作記録機能があり，ログインした利用者のデスクトップ画面が数秒間隔で画像データとして記録され，実行したコマンドやキーボード入力がテキストで記録される。全てのサーバがアクセスログを取得しており，どの利用者 ID によっていつログイン，ログアウトしたかの記録が残る。踏み台サーバの利用者管理はシステム運用課が担当している。

FW のフィルタリングルールを表4に示す。

表4　FWのフィルタリングルール

項番	送信元	宛先	サービス	動作
1	インターネット	SSLアクセラレータ	HTTP over TLS	許可
2	インターネット	外部メールサーバ	SMTP	許可
3	インターネット	権威DNSサーバ	DNS	許可
4	プロキシサーバ	インターネット	HTTP, HTTP over TLS	許可
5	外部メールサーバ	インターネット	SMTP	許可
6	外部メールサーバ	内部メールサーバ	SMTP	許可
7	権威DNSサーバ	インターネット	DNS	許可
8	運用管理PC	WebAPサーバ	SSH	許可
9	運用管理PC	DBサーバ	SSH	許可
10	運用管理PC	プロキシサーバ	SSH	許可
11	運用管理PC	権威DNSサーバ	SSH	許可
12	運用管理PC	外部メールサーバ	SSH	許可
13	利用者セグメント	プロキシサーバ	HTTP, HTTP over TLS	許可
⋮	⋮	⋮	⋮	⋮
30	全て	全て	全て	拒否

注記1　FW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　項番の小さいルールから順にマッチングし，最初に合致したルールが適用される。
注記3　項番14～29には，送信元がDMZの機器であり，かつ，宛先がサーバセグメントの機器であるルールは存在しない。

〔セキュリティ対策の評価〕

今年に入り，関連業界を狙ったサイバー攻撃が急増しているという話を聞き，R団体の理事がセキュリティコンサルタント（以下，コンサルタントという）に相談したところ，セキュリティ対策の評価を勧められた。そこで，図面及び会員組織情報と，それらが保存されているDBサーバについて，セキュリティ対策が適切か，コンサルタントによる評価を受けることにした。

さらに，R団体の理事は，かねてから付き合いのあるベンダに相談し，情報処理安全確保支援士（登録セキスペ）のM氏に，R団体のシステム企画課に主任として出向してきてもらい，同じシステム企画課のNさんとともに，コンサルタントの評価結果への対応を検討してもらうことにした。評価では，検査ツールを用いたRポータルの脆弱(ぜい)性検査や，職員へのインタビューを通しての秘密情報の取扱状況確認と，セキュリティ対策基準の妥当性確認などが行われた。

2か月後，コンサルタントは，評価結果を理事に報告した後，図3に示す評価結果

の詳細を，M 主任と N さんに説明した。

検出事項 1：R ポータルの脆弱性検査を実施したところ，図 4 に示す 2 件のクロスサイトスクリプティング（以下，XSS という）脆弱性が存在する。（省略） 検出事項 2：踏み台サーバを除く全てのサーバの管理者用アカウントに，共通管理者アカウントが使用されている。（省略） 検出事項 3：DB サーバは，利用者セグメントからのアクセスを運用管理 PC からだけに限定している点は良いが，DMZ に設置されている点が課題である。DB サーバは，DMZ よりも安全性の高いセグメントに設置することが望まれる。（省略） 検出事項 4：製作パートナに貸与する図面の機密性の担保が，包括的な基本契約の中の守秘義務条項だけであり，製作パートナが実施すべきセキュリティ対策の具体的内容が定められていない。（省略） （省略）

図 3　評価結果の詳細（抜粋）

脆弱性 1：図面を検索するページ（以下，検索ページという）に反射型 XSS が存在する。（省略） 脆弱性 2：検索ページで使用されるスクリプトに DOM-based XSS が存在する。攻撃者が“#”から始まるフラグメント識別子に攻撃コードを記述できる。

図 4　2 件の XSS 脆弱性

理事から対応計画を策定するように指示があり，M 主任と N さんは，それぞれの検出事項について，一つ一つ対応方針を検討することにした。

〔検出事項 1 の対応方針の検討〕

次は，XSS 脆弱性についての N さんと M 主任の会話である。

N さん：脆弱性 1 は，検索ページの一部の GET パラメタで起こるようです。今回の脆弱性検査では，脆弱性 1 の検知には，攻撃コードとして，スクリプトに相当する文字列を含めたリクエストをサーバに送信したときに，その文字列がレスポンス中にスクリプトとして出力されるかどうかで判断する方法（以下，検知方法 1 という）を用います。一般的には WAF を導入すれば，攻撃者が脆弱性 1 の有無を分析しようと攻撃試行すると，検知できます。

M 主任：そのとおりだね。R 団体では，WAF は導入していないが，もし導入していて，かつ，攻撃試行があったとしたら，攻撃試行を検知できていたかもし

れないな。

Nさん：では，脆弱性2は，検知方法1やWAFで検知できますか。

Nさんの質問に対して，M主任は次の二つを説明した。

・①検知方法1では脆弱性2を検知できない。

・WAFでも脆弱性2を検知できない。②Rポータルへのアクセスを繰り返すことなく，脆弱性2の有無を分析する方法がある。

次は，XSS脆弱性への対処についてのNさんとM主任の会話である。

Nさん：脆弱性1及び脆弱性2について，早急に開発業者に脆弱性の修正を依頼します。

M主任：Rポータルはセッション管理をCookieで実現しているので，XSS攻撃によってCookieを窃取されないようにする必要もある。③Rポータルの動作に影響が出ないことを確認した上で，Cookieの発行時にHttpOnly属性を付与するように修正した方がいい。

〔検出事項2の対応方針の検討〕

共通管理者アカウントを用いてサーバにログインするプログラムも複数存在することから，共通管理者アカウントは，容易に変更できない。一方，④共通管理者アカウントが正しく利用されていることが確認できる証跡は取得している。共通管理者アカウントの利用は，時間を掛けて共通管理者アカウントをやめ，個別のアカウントにする対策を検討することにした。

〔検出事項3の対応方針の検討〕

M主任は，DBサーバをDMZとは別のセグメントに移動する案を検討するようにNさんに指示した。Nさんは，二つの案を検討した。

案1は，DMZ内に新たにL3SWを設置して，DBサーバ専用のセグメントを設け，L3SWでDBサーバへの通信を業務上必要なものだけに限定する案である。

案2は，DBサーバをサーバセグメントに移動し，表5に示すルールを追加するな

ど，FWのフィルタリングルールを変更するとともに，図2のL3SWによって，利用者セグメントからのアクセスを禁止する案である。

表5　追加するFWのフィルタリングルール

項番	送信元	宛先	サービス	動作
14	a	b	c	許可

次は，二つの案についてのNさんとM主任との会話である。

Nさん：新たにL3SWを導入する必要もないですし，案1よりも案2が良いと思います。

M主任：案2は，FWのフィルタリングルール変更の他にもいろいろと考慮すべき点があるね。例えば，⑤DBサーバに関してR団体のセキュリティ対策基準に違反するおそれがある。そのため，案2を採用する場合は，検出事項 d の対策と併せて実施する必要がある。

M主任とNさんは，社内関係者の意見を集約し，現行システムへの影響などから案1を理事に提案することにした。

〔検出事項4の対応方針の検討〕

R団体は，ISMS適合性評価制度の認証を取得していることを公募要件とした上で，製作パートナが順守すべきルールを明確にした。そのルールを図5に示す。

・R団体の図面とプロトタイプについて，次の施策を管理策の中に含めること
　施策1：図面の管理責任者を定めること
　施策2：図面の取扱いやプロトタイプの製作は，入退室が管理されたエリアで行うこと
　施策3：図面を複製した場合は，複製物に対しても原本と同等の管理を行うこと
（省略）
・R団体からの貸与品は，契約終了時に，管理責任者が確実に破棄し，証跡を提出すること
（省略）

図5　製作パートナが順守すべきルール

さらに，M主任は，製作パートナが図5に示すルールを逸脱するような，不正な

方法で図面を取り扱うことを技術的対策によって防止しようと考えた。M 主任は技術的対策の候補を DRM（Digital Rights Management）方式とコンテナ方式の二つに絞り込んだ。

M 主任が検討した DRM 方式は，DRM に対応した図面編集用のアプリケーションソフトウェア（以下，図面アプリという）を用いて，図面にセキュリティ情報を埋め込んだ上で，図面を暗号化する方式である。暗号化した図面（以下，S 図面という）は，DRM に対応した図面アプリだけで開くことができる。市場に流通している図面アプリのうち，一部のアプリだけが DRM に対応している。この DRM 方式は，図面へのアクセスを主にアプリケーションソフトウェアのレイヤで制御する。

一方，M 主任が検討したコンテナ方式では，共有ファイルサーバ（以下，コンテナサーバという）上に図面を置く。コンテナサーバ上の図面は，PC 上でコンテナ方式専用ソフトウェア（以下，CC という）を起動すると編集可能になるが，同時にローカルドライブなど他のドライブや外部記憶媒体へのアクセスが禁止され，コンテナサーバ内から持ち出せなくなる。図面は，市場に流通している図面アプリの多くを使って開くことができる。このコンテナ方式は，図面へのアクセスを主にファイルシステムのレイヤで制御する。

DRM 方式の利用イメージを図 6 に，コンテナ方式の利用イメージを図 7 に示す。

- R 団体は，DRM 対応の図面アプリを用いて S 図面を作成し，S 図面を R ポータルにアップロードする。
- 製作パートナが S 図面をダウンロードして，PC 上の DRM 対応の図面アプリで S 図面を開くと，PC と DRM サーバとの間で通信が行われ，認証ダイアログが表示される。DRM サーバは，R 団体の DMZ 上に設置され，利用者の認証機能や，利用者の図面へのアクセスを制御する機能をもっている。認証ダイアログに，あらかじめ R 団体から与えられた S 図面用の利用者 ID，パスワードを入力すると，S 図面が正常に開く。
- R 団体は，DRM サーバの設定によって，S 図面ごとに，アクセス可能な利用者 ID，及びアクセス可能な利用者 ID ごとの，閲覧期限，印刷可否，編集可否を設定できる。

図 6　DRM 方式の利用イメージ

・R 団体は，DMZ にコンテナサーバを設置し，そのサーバ内のフォルダに図面を保存する。
・コンテナサーバには，CC のインストーラ（以下，CCI という）を生成する機能がある。プロトタイプ製作の契約ごとに，R 団体は，必要な数の CCI を製作パートナにメディアで渡す。製作パートナに渡す CCI には，CC ごとの識別情報が組み込まれている。
・製作パートナの PC で CCI を実行すると，PC に CC がインストールされる。CC は PC のプロセスとして常駐し，普段は PC の動作に影響を与えないが，機密モードログイン機能が起動されると認証ダイアログを表示する。認証ダイアログに，あらかじめ R 団体から利用者の人数分だけ与えられた CC 用の利用者 ID，パスワードを入力すると，PC が機密モードになる。機密モード時は，コンテナサーバのフォルダが専用のドライブ（以下，コンテナドライブという）として PC からアクセス可能になり，図面を，汎用の図面アプリで閲覧，編集，保存できる。
機密モードでは，PC に次の制限が掛かる。
(1) R 団体が定めたアプリケーションソフトウェアだけが起動できる。
(2) PC はコンテナサーバだけにアクセスできる。それ以外のインターネット，ネットワークにはアクセスできない。
(3) PC はコンテナドライブ以外，つまり PC の他のドライブや外部記憶媒体にはアクセスできない。そのため，PC 利用者が編集した図面を保存できるのは，コンテナドライブ上だけである。
機密モードからログアウトすると，コンテナドライブは切断され，機密モード時に編集した図面にはアクセスできなくなる。また，クリップボードや一時ファイルなどの一時情報は，全て削除される。
・CC が，インストール後，最初にコンテナドライブにアクセスする際，CC の識別情報と PC の端末情報の組がコンテナサーバに登録される。仮に製作パートナが，同一の CC を複数台の PC にインストールしても，そのうち最初にコンテナドライブにアクセスした 1 台だけがコンテナドライブにアクセスできる。
・仮想デスクトップ環境には CC をインストールすることはできない。

図 7　コンテナ方式の利用イメージ

次は，DRM 方式とコンテナ方式についての M 主任と N さんの会話である。

M 主任：まず製作パートナに事前に確認する必要がある事項について考えてみよう。コンテナ方式では，製作パートナとの間で，DRM 方式と比べてより多くの事項を確認しておく必要があるね。

N さん：第一に，製作パートナが使用している図面アプリなど，機密モードで起動できるアプリケーションソフトウェアを確認する必要があります。第二に，［　e　］を確認する必要があります。

M 主任：分かった。次に，肝心の図面の機密性の担保の面はどうだろうか。

N さん：いずれの方式とも，製作パートナの PC で表示した図面をカメラで撮影したり，手で紙に写したりされることは防げませんが，製作パートナの不正

による図面の流出防止に一定の効果はあると考えます。

M 主任：どちらの方式がより効果があるか，掘り下げてみよう。仮に N さんが製作パートナの従業員で，海外の第三者（以下，協力者という）に有効期限内の S 図面又は図面を渡すという不正行為を行おうとした場合，どのようにするのか，それぞれの方式で考えてみよう。

N さん：DRM 方式の場合，受け取った S 図面を，まずはメールで協力者に送付します。その後，利用者 ID とパスワードを電話などで伝えます。

M 主任：確かに持ち出せるな。では，コンテナ方式ではどうかな。

N さん：基本的には DRM 方式と同じですが，コンテナ方式の場合は，まずは [f] します。その後，利用者 ID とパスワードを電話で協力者に伝えます。

M 主任：コンテナ方式の方が，不正行為はより困難だといえるね。いずれの方式でも，このような不正行為への技術的対策としては，FW での対策が効果的だな。例えば，DRM 方式であれば，FW で [g] ことができる。

M 主任は両方式の比較結果をまとめ，理事に報告した。図面の流出防止の効果が決め手となり，R 団体は，最終的にはコンテナ方式を採用することにした。

M 主任は，評価結果への対応方針をまとめ，対応計画を策定した。対応計画は R 団体の理事会で承認され，M 主任は対応計画を実行に移すことになった。

設問 1　検出事項 1 について，(1)～(3)に答えよ。

(1) 本文中の下線①について，サーバからのレスポンスの内容を見て脆弱性を判断するツールを用いた場合，脆弱性 2 を検知できないのはなぜか。その理由を 35 字以内で具体的に述べよ。

(2) 本文中の下線②について，脆弱性の原理を踏まえ，攻撃者が分析する方法を 40 字以内で述べよ。

(3) 本文中の下線③について，R ポータルがどのような実装方法を用いている場合に動作に影響があるか。45 字以内で述べよ。

設問 2　本文中の下線④について，サーバセグメント内のサーバで共通管理者アカウ

ントを用いる R 団体では，どのような機能を使ってどのような証跡を取得しているか。本文中の字句を用いて，70 字以内で具体的に述べよ。

設問３　検出事項３について，(1)～(3)に答えよ。

(1)　表 5 中の［ a ］～［ c ］に入れる適切な字句を答えよ。また，表 4 のルールのうち不要となるものを項番で答えよ。

(2)　本文中の下線⑤について，誰がどのようなアクセス経路で何を行うと，セキュリティ対策基準違反になるか。違反になる行為を本文の内容を基に，55 字以内で具体的に述べよ。

(3)　本文中の［ d ］に入れる，適切な検出事項の番号を答えよ。

設問４　検出事項４について，(1)～(3)に答えよ。

(1)　本文中の［ e ］に入れる，製作パートナに確認する必要がある事項を 20 字以内で具体的に述べよ。

(2)　本文中の［ f ］に入れる，コンテナ方式における不正行為の手口を 30 字以内で述べよ。

(3)　本文中の［ g ］に入れる，適切な技術的対策を，45 字以内で述べよ。