SC

平成30年度　春期
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〕

選択欄	
1問選択	問1
	(問2)

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　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。

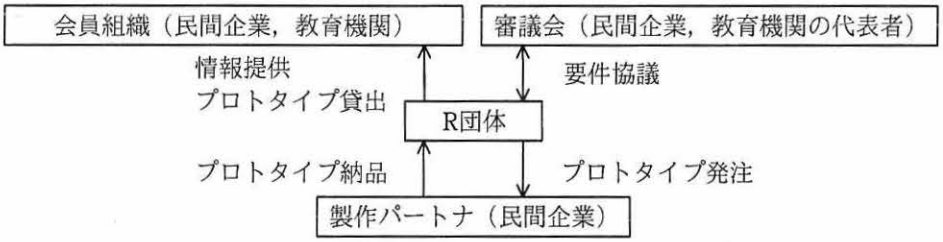


図1　R団体とステークホルダとの関係

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。

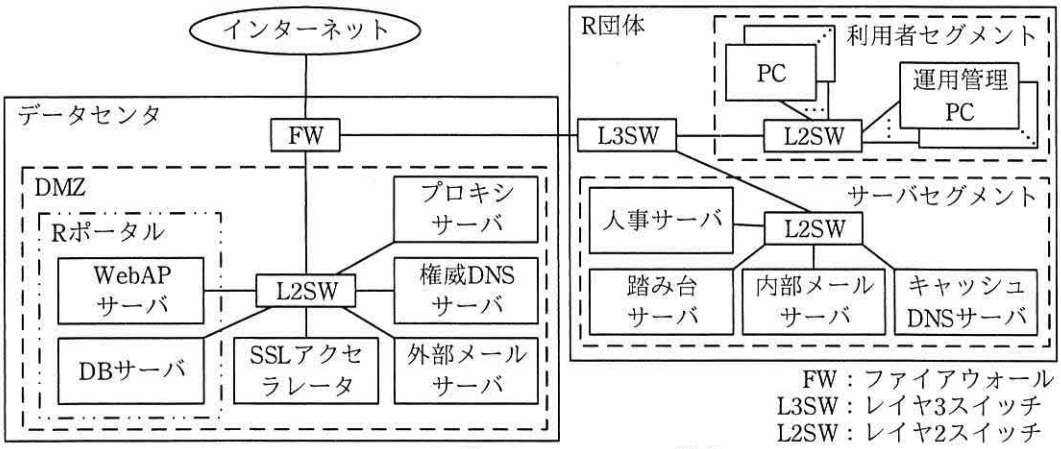


図 2　R 団体のネットワーク構成

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。

問2　Webサイトのセキュリティに関する次の記述を読んで，設問1～6に答えよ。

A社は，従業員数1,200名のマスメディア関連会社である。A社では，提供するサービスごとにWebサイトを用意し，インターネット上に公開している。Webサイトには，情報提供サイトやショッピングサイトなど様々なものがある。Webサイトでは，Webアプリケーションソフトウェア（以下，Webアプリという）が動作し，その設計，実装，テスト（以下，この3工程を開発という）及び運用は，Webサイトごとに情報システム子会社B社又は外部の業者に委託されている。多くのWebサイトでは，キャンペーンなどのたびに，開発とリリースを繰り返している。

〔現状のセキュリティ施策〕

A社では，脆弱(ぜい)性を作り込まないようにするために，Webサイトのライフサイクルの五つの工程（要件定義，設計，実装，テスト，運用）に関するセキュリティガイドライン（以下，Webセキュリティガイドという）を整備している。現行のWebセキュリティガイド第1版を図1に示す。

```
（省略）
工程3．実装
  Webアプリの実装時に，次の脆弱性について対策すること
  1．クロスサイトスクリプティング（以下，XSSという）
  2．SQLインジェクション
（省略）
工程4．テスト
  リリース前にWebアプリの脆弱性診断（以下，診断という）を実施すること
（省略）
```

図1　Webセキュリティガイド第1版

Webセキュリティガイドは，開発及び運用を委託している外部の業者にも順守を義務付けている。

〔Webサイトの運用について〕

A社のカスタマサポートサービス提供用のWebサイトXは，A社のデータセンタXに設置されている。Webサイト Xは，B社に開発と運用を委託している。データ

センタ X と B 社本社のシステム構成を図 2 に示す。

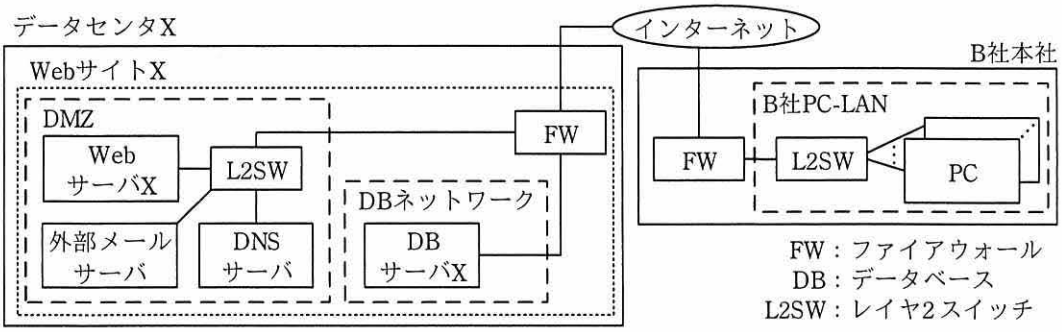


図 2　データセンタ X と B 社本社のシステム構成

Web サーバ X 上では，Web アプリ X が稼働している。Web アプリ X は，Web アプリケーションフレームワーク（以下，WF という）の一つである WF-K を使用して開発されている。

Web サイト X とシステム構成が全く同じ Web サイト Y を，別のデータセンタ Y に災害対策用として設置している。Web サイト X 稼働時には Web サイト Y は，インターネットに公開しておらず，ホットスタンバイの状態で運用している。

Web サイト X と Web サイト Y のソフトウェアの脆弱性修正プログラム（以下，パッチという）は，3 か月ごとの定期メンテナンス日に B 社運用チームの C さんが適用している。C さんは，新しいパッチが公開されているかを定期メンテナンス日の前に確認し，もしあれば，まず Web サイト Y にパッチを適用している。Web サイト Y での稼働に問題がなければ，Web サイト X にもパッチを適用している。コンテンツも，まず Web サイト Y を更新し，問題がなければ，Web サイト X を更新している。パッチ適用とコンテンツ更新は，B 社 PC-LAN 上の C さんの PC から行っている。

なお，B 社では，全従業員に PC が 1 台ずつ貸与されており，その PC で Web サイトを閲覧して情報を収集したり，電子メール（以下，メールという）を送受信したりしている。

〔セキュリティインシデントの発生〕

ある日，Web サイト X の利用者から，Web サイト X のダウンロードページでファイルをダウンロードしたところ，マルウェア対策ソフトが警告を表示したという連

絡があった。C さんがダウンロードページを確認したところ，あるダウンロードファイルへのリンクが外部の URL に改ざんされていた。C さんは運用チームのリーダである D さんに報告し，Web サイト Y に切り替えるべきかを相談した。D さんは，切り替えると Web サイト Y も改ざんされてしまうことを懸念して，Web サイト Y には切り替えないよう C さんに伝えた。代わりに，DNS サーバの設定を変更して，メンテナンス中であることを表示するサーバに切り替えるよう C さんに指示した。D さんは，すぐに A 社に連絡し，ファイルへのリンクが改ざんされたと伝えた。その後，A 社の Web サイト X 及び Web サイト Y の担当部署の E さんがセキュリティ専門業者に連絡して，今後の対応について相談することになった。

〔セキュリティ専門業者による調査〕

セキュリティ専門業者の情報処理安全確保支援士（登録セキスペ）である F 氏が，被害の状況を調査した。調査内容と調査結果を表 1 に示す。

表 1　F 氏の調査内容と調査結果

No.	調査内容	調査結果
1	外部の URL に改ざんされているリンクが他にもあるかを Web サーバ X の全ページについて調査	他に外部の URL に改ざんされているものはなかった。
2	外部からの改ざんに悪用される既知の脆弱性が Web サイト X にあるかを調査	WF-K に脆弱性 K が存在する。そのため，特定の文字列を含む HTTP リクエストを送信すると，Web アプリの実行ユーザ権限で任意のファイルの読出しと書込みができる可能性がある（以下，この攻撃手法を攻撃手法 K という）。 なお，脆弱性 K については，WF-K のパッチが提供されている。
3	Web サーバ X のアクセスログに攻撃手法 K の痕跡があるかを調査	ダウンロードページの更新日に当たる 3 日前のアクセスログを確認したところ，Web サイト X への外部からのアクセスがあったが，攻撃手法 K の痕跡は見付けられなかった。ただし，攻撃手法 K に使われる文字列が Web サーバ X の標準設定では①アクセスログに残らないので，脆弱性 K が原因である可能性は否定できない。
4	DB サーバ X とその DB が改ざんされているかを調査	DB サーバ X のコマンド履歴と DB サーバ X の DB の操作ログを確認したところ，改ざんされた痕跡は見付けられなかった。
5	Web サイト Y が改ざんされているかを調査	アクセスログを確認したところ，外部からのアクセスはなく，改ざんされた痕跡も見付けられなかった。

F 氏は，D さんと E さんに調査結果を伝えた。次は，その時の F 氏，D さん，E さんの会話である。

F 氏　：脆弱性 K は，改ざんの 3 週間前に公表されたものです。

D さん：そうですか。その脆弱性は，認識していませんでした。すぐに確認して，パッチを適用します。仮に，認識していたとしてもパッチ適用は定期メンテナンス日，つまり，来週の月曜日にしていたと思うので，やはり改ざんされていましたね。

F 氏　：ダウンロードページのリンク以外に外部の URL に改ざんされているページはありませんでした。しかし，スクリプトを埋め込まれるなど，他の形でページが改ざんされている可能性もあるので確認が必要です。

D さん：分かりました。ページの改ざんは，実際にはどのように確認すればよいでしょうか。

F 氏　：Web サイト X の全ファイルを［　a　］して確認すると漏れがなく，効率も良いでしょう。

D さん：なるほど。分かりました。

F 氏　：調査結果は以上です。

E さん：ありがとうございました。攻撃手法 K によって実際に Web サーバ X を改ざんできるかどうかを知りたいので，調査してもらえないでしょうか。また，他に脆弱性がないかについても調査をお願いします。

F 氏　：分かりました。

F 氏が，まず，Web サイト X に対して，攻撃手法 K による攻撃を実施したところ，実際に Web サーバ X を改ざんできることが確認できた。

次に，他に脆弱性がないか，Web サイト Y に対して B 社 PC-LAN から OS 及びミドルウェア（以下，プラットフォームという）の診断並びに Web アプリ X の診断を実施した。

プラットフォームの診断では，メンテナンスで使っている SSH サービスに対して辞書攻撃が容易に成功することが確認された。F 氏が C さんにセキュリティ上の問題がないか確認したところ，“SSH サービスは B 社 PC-LAN からだけアクセスできる

ように設定しているので問題はないと考えている”とのことであった。F 氏によると B 社 PC-LAN 内に攻撃者が侵入できると，Web サイト Y に不正にログインできる。そこで，F 氏は，②SSH の認証方式をパスワード認証方式以外に設定するよう D さんにアドバイスした。また，この設定をしたとしても，メンテナンスに自分の PC を利用するのはセキュリティ上の問題があるので，新たにメンテナンス専用 PC を準備し，それを B 社運用チームだけが利用できるようにすることをアドバイスした。

次に，Web アプリ X を診断したところ，XSS の脆弱性が 5 件検出された。

F 氏の調査結果を基に，D さんは，脆弱性 K に対するパッチ適用，SSH サービスの設定変更，メンテナンス専用 PC の準備，XSS が検出されたプログラムの修正及び Web サイト X の復旧を行うよう C さんに指示した。C さんは 1 週間で対応を完了し，Web サイト X が再稼働した。

〔全社の Web サイトのセキュリティ強化〕

セキュリティインシデントの発生及び F 氏の調査結果を受けて，A 社の情報システム担当役員である G 取締役は，全社の Web サイトのセキュリティを強化するよう，A 社情報システム部長を通じて同部の H 課長に指示した。H 課長は，WF，プラットフォーム及び Web アプリの脆弱性について調査を開始し，対策を検討することにした。

WF 及びプラットフォームの脆弱性については，Web サイトの改ざんなどの被害につながるので，全社の Web サイトについて脆弱性への対応状況を調査した。その結果，対応漏れがある Web サイトが 5 サイト見つかった。漏れがあった理由を各 Web サイト担当者にヒアリングしたところ，脆弱性が発表されていることを知らなかったとのことであった。

そこで，今後は情報システム部が一括して脆弱性情報を収集し，各 Web サイト担当者にその情報を提供することにした。それに先立って，効率的な情報収集ができるよう，各 Web サイト担当者には，［　b　］を報告させた。また，Web サイトの更改などに伴って［　b　］に変更がある場合は，その都度報告させることにした。

パッチ適用は従来どおり各 Web サイト担当者に任せることにしたが，脆弱性情報を提供するだけでは，パッチ適用の遅れによって被害が出ることも考えられるので，パッチ適用期限を Web セキュリティガイドに追加することにした。

Web アプリの脆弱性については，まず，今回検出された XSS を作り込んだ原因について，B 社にヒアリングした。その結果，Web セキュリティガイドの記載が抽象的なので，誤った実装をしてしまったことが分かった。そこで，全ての担当者が正しい実装方法を理解できるように，Web セキュリティガイドを改訂して具体的な実装方法を追加することにした。改訂後の Web セキュリティガイド第 2 版を図 3 に示す。

（省略）
工程 3. 実装
Web アプリの実装時に，次の脆弱性について対策すること
1. XSS
・Web ページに出力する全ての要素に対して，エスケープ処理を施すこと
（省略）
2. SQL インジェクション
・SQL 文の組立ては全てプレースホルダで実装すること
（省略）
工程 5. 運用
・Web サイトのメンテナンス用にメンテナンス専用 PC を準備すること。メンテナンス専用 PC は，Web サイト担当者だけが利用できるようにすること
・運用している Web サイトに脆弱性が発見された場合は，次の基準で対応すること
- リスクが高の場合は，9 日以内に対応すること
- リスクが中の場合は，1 か月以内に対応すること
- リスクが低の場合は，3 か月以内に対応すること
（省略）

注記　第 1 版から追加された部分を破線の下線で示す。

図 3　Web セキュリティガイド第 2 版

また，Web アプリの診断の実施状況について各 Web サイト担当者にヒアリングしたところ，“Web サイトの開発スケジュールが短くて，診断をセキュリティ専門業者に依頼するとリリースに間に合わないので，診断できずにリリースすることがある”とのことであった。そこで，H 課長は情報システム部が中心となって，いつでもすぐに診断を実施できるように，A 社内に Web アプリを診断できる体制を作ることを G 取締役に提案し，採用された。

〔自社による診断の実施検討〕

的確な診断を実施できる体制を作るには，A 社内で診断する項目（以下，A 社診断

項目という）を定め，その項目の診断手順に診断員が習熟する必要があり，H 課長は，診断手順の作成と習熟には，1 年は掛かると考えた。それを少しでも短くするために，診断経験があり，登録セキスペでもある部下の Q さんと一緒に A 社診断項目と診断手順を検討した。

検討の結果，外部で公開されていた診断項目を参考にして，Web アプリに関する A 社診断項目を図 4 のとおり定めた。

・XSS
・SQL インジェクション
・OS コマンドインジェクション
・［ c ］トラバーサル
・［ d ］リクエストフォージェリ
・セッション管理の不備 1)
・アクセス制御の不備や認可制御の欠落
・［ e ］ヘッダインジェクション
・メールヘッダインジェクション
・クリック［ f ］

注 1) セッション ID が推測可能，セッション ID を URL 内に格納，HTTP over TLS 通信で利用する Cookie に Secure 属性がない，ログイン成功後にセッションを継続利用の 4 項目

図 4 A 社診断項目

診断方法には，自動診断ツールによる診断と手動による診断がある。A 社では自動診断ツールとして，自動診断ツール J を使う予定である。自動診断ツールによる診断は効率的だが，ツールによっては診断できない項目もある。そこで，2 人は両方の診断方法を組み合わせることにした。それを踏まえて作成した診断手順書第 1 版を図 5 に示す。

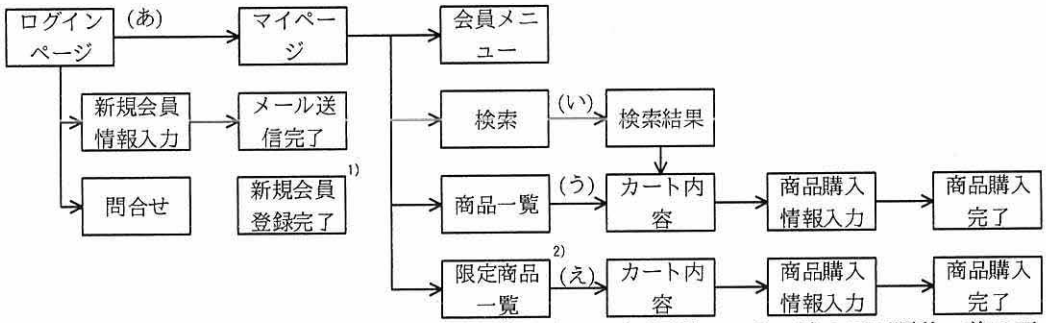
1. 診断準備
（省略）
2. 自動診断ツールJによる診断
（省略）
3. 手動による診断
・診断項目
- [d] リクエストフォージェリ
-セッションIDが推測可能
-セッションIDをURL内に格納
-アクセス制御の不備や認可制御の欠落
・診断方法
ローカルプロキシを用いて通信ログを取得しながら診断する。必要に応じて，リクエスト中のパラメタの値を変更して，リクエストを送る。
（省略）

図5　診断手順書第1版

その後，A社の情報システム部のメンバ3名が，Qさんのトレーニングを受け，診断チームを結成した。しかし，トレーニングを受けただけでは，最初から精度の高い診断結果を安定して出せないかもしれない。そこで，当初はセキュリティ専門業者が診断を実施する際に同時に診断を実施することとし，両者の診断結果を比較・検証して，経験を積むことにした。

〔Webサイト Z に対する診断の実施〕

A社のある部署が，新規に構築したショッピング用の Web サイト Z をリリースするに当たり，セキュリティ専門業者に診断を依頼した。その際に，診断チームのメンバの L さんにも診断を担当させることにした。Web サイト Z の開発は，外部の業者の P 社に委託しており，委託時に Web セキュリティガイドの最新版を渡している。Web サイト Z の画面遷移図を図6に，画面遷移の仕様を表2に示す。



注記 1　ログインページ画面以外からマイページ画面への画面遷移，エラー時の画面遷移，前の画面に戻るための画面遷移などは省略している。

注記 2　全ての画面を同一ドメイン（www.z-site.com）で提供している。

注 1)　メール送信完了画面への遷移時に会員に送付されるメールに記載された URL に利用者がアクセスすると表示される。

2)　有料会員の場合だけ表示する。

図 6　Web サイト Z の画面遷移図（抜粋）

表2　Web サイト Z の画面遷移の仕様（抜粋）

画面遷移	PC での操作例，URL 及び POST データ	操作の結果
(あ)	操作例：利用者 ID（例：user0001）とパスワード（例：9a8b7c6d）を入力し，“ログイン”ボタンをクリックする。 URL：https://www.z-site.com/login POST データ：user_id=user0001&passwd=9a8b7c6d	・利用者認証が成功した場合，新しいセッション ID（JSESSIONID）とセッションオブジェクトを取得し，マイページ画面を表示する。それ以外の場合，セッション ID とセッションオブジェクトは取得せず，エラー内容を記載したログインページ画面に戻る。 ・セッション ID は Cookie に格納する。 ・user_id の値が有料会員の利用者 ID の場合には，マイページ画面に限定商品一覧へのリンクを追加する。
(い)	操作例：検索画面でキーワード（例：New）を選び，“検索”ボタンをクリックする。 URL：https://www.z-site.com/kensaku POST データ：keyword=New	・keyword の値を DB から検索し，該当する商品を次画面に表示する。 ・該当する商品数が n 件の場合，画面上部に“該当商品数：n 件”と表示する。 ・該当する商品がない場合は 0 件と表示する。また，キーワードが指定されていない場合は全件を表示する。
(う)	操作例：商品一覧画面で商品を選び，“選択”ボタンをクリックする。 URL：https://www.z-site.com/kounyu POST データ：code=0001344	・code の値で DB を検索し，該当する商品をカートに入れ，次画面に表示する。また，code の値をセッションオブジェクトに格納する。該当する商品が存在しない場合はエラーを表示する。
(え)	操作例：有料会員の場合だけ表示される限定商品一覧画面で商品を選び，“選択”ボタンをクリックする。 URL：https://www.z-site.com/kounyu POST データ：code=1000021	・code の値で DB を検索し，該当する商品をカートに入れ，次画面に表示する。また，code の値をセッションオブジェクトに格納する。該当する商品が存在しない場合はエラーを表示する。

L さんは，Web サイト Z に対して診断を実施し，結果をとりまとめた。L さんは，L さんの診断結果と，セキュリティ専門業者の診断結果とを比較した。すると，両者ともに検出したものが 1 件，セキュリティ専門業者だけが検出したものが 3 件あった。Web サイト Z の診断結果を表 3 に示す。

表3　Webサイト Z の診断結果

項番	脆弱性の名称	検出箇所	L さんの診断方法・結果	セキュリティ専門業者の診断方法・結果
(ア)	SQL インジェクション	検索画面からの遷移	診断方法：表 4 に示す自動診断ツール J の入出力結果を基に判定 診断結果：検出	診断方法：(省略) 診断結果：検出
(イ)	XSS	配達希望日を入力するためのカレンダ機能	診断方法：自動診断ツール J を利用 診断結果：未検出	診断方法：図 8 の URL をアドレスバーに入力して診断 診断結果：検出
(ウ)	アクセス制御の不備や認可制御の欠落	商品一覧画面からの遷移	診断方法：(省略) 診断結果：未検出	診断方法：表 5 の方法で確認 診断結果：検出
(エ)	[d] リクエストフォージェリ	商品購入情報入力画面からの遷移	診断方法：(省略) 診断結果：未検出	診断方法：(省略) 診断結果：検出

表4　自動診断ツール J の入出力結果（抜粋）

No.	対象画面	keyword の値	ステータスコード	画面に表示された該当商品数
1	検索画面	bag' and '1'='1	200	該当商品数：[g] 件
2	検索画面	bag' and '1'='2	200	該当商品数：[h] 件
3	検索画面	bag	200	該当商品数：30 件

注記　診断時に DB には商品が 100 件登録されていた。

(イ)の脆弱性については，商品購入情報入力画面から，配達希望日を入力するために起動するカレンダ機能で検出された。カレンダ機能を図 7 に示す。

・次に示す URL にアクセスするためのポップアップウィンドウが開き，カレンダが表示される。
　https://www.z-site.com/calendar?inputfieldid=haitatsukiboubi
・カレンダ上で利用者が任意の日付を選択する。
・その日付が商品購入情報入力画面の配達希望日に設定される。

図7　カレンダ機能

セキュリティ専門業者が脆弱性を確認するためにカレンダを開き，そのカレンダが表示されているポップアップウィンドウのアドレスバーに入力した URL を図 8 に，警告ダイアログに“NG”を表示させたレスポンスの該当箇所を図 9 に示す。

```
https://www.z-site.com/calendar?inputfieldid=[ i ]
```

図 8　脆弱性を確認するためにアドレスバーに入力した URL

```
<script type="text/javascript">
  var returnobj = window.opener.document.getElementById('[ i ]');
  （省略）
  returnobj.value = selected_date;
  （省略）
</script>
```

図 9　警告ダイアログに“NG”を表示させたレスポンスの該当箇所

なお，(イ)の脆弱性は，Web サイト Z とは異なるドメインのサイトから，図 8 の URL にアクセスさせられるような攻撃を受けた場合でも，現在普及している Web ブラウザの多くでは，スクリプトの実行時にエラーが発生し，攻撃が失敗する。しかし，Web ブラウザの種類やバージョンによっては被害が発生するおそれがあるので，セキュリティ専門業者は修正することを提言した。

(ウ)の脆弱性は，有料会員だけが購入できることになっている限定商品を一般会員が購入できてしまうというものであった。セキュリティ専門業者が確認した方法を表 5 に示す。

表 5　(ウ)の脆弱性をセキュリティ専門業者が確認した方法

No.	操作の内容	操作の結果
1	一般会員アカウントでログインして，商品一覧画面の URL にアクセスする。	商品一覧画面が表示される。
2	商品一覧画面で[j]。	カートに限定商品が入った状態となる。
3	商品購入処理を行う。	限定商品を購入できる。

表 3 の診断結果から，Q さんは脆弱性を作り込まないよう Web セキュリティガイドに項目を追加した。さらに，XSS の脆弱性をよく作り込むパターン，アクセス制御の不備や認可制御の欠落及び[d]リクエストフォージェリについて，診断手順書を改訂して，診断手順を追加した。改訂された診断手順書第 2 版を図 10 に示す。

1. 診断準備
（省略）
・アクセス制御の不備や認可制御の欠落を確認する場合には，事前に［ k ］アカウントを用意し，［ l ］を確認する。
2. 自動診断ツールJによる診断
（省略）
3. 手動による診断
・診断項目と確認手順
-XSS
（省略）
-［ d ］リクエストフォージェリ
処理を実行するページで，次のいずれかを満たす場合に脆弱性ありと判定する。
・トークンなどのパラメタが存在しない。
・トークンなどを削除しても処理が実行される。
・トークン文字列の推測が可能である。
・別の利用者のトークンが使用できる。

処理が実行されたかどうかは，画面に表示されるメッセージなどから判断する。
-セッションIDが推測可能
-セッションIDをURL内に格納
-アクセス制御の不備や認可制御の欠落
［ k ］アカウントそれぞれについて，パラメタの値を変更するなどして，許可されていない操作ができる場合に脆弱性ありと判定する。
・診断方法
ローカルプロキシを用いて通信ログを取得しながら診断する。必要に応じて，リクエスト中のパラメタの値を変更して，リクエストを送る。
（省略）

注記　第1版から追加された部分を破線の下線で示す。

図10　診断手順書第2版

Webサイト Z で検出された脆弱性は，リリース前に修正するよう A 社の Web サイト Z の担当者から P 社に伝えた。Q さんが，脆弱性が作り込まれた原因を P 社に確認したところ，いずれも確認不足であるとのことであった。

〔改善案の検討〕

Q さんは，各工程でのレビューポイントを Web セキュリティガイドに記載することを H 課長に提案した。改訂された Web セキュリティガイド第3版を図11に示す。

注意事項：各工程の最後にレビューを行い，作業の妥当性を確認すること
工程 1．要件定義
（省略）
レビューポイント：A 社のセキュリティポリシ及び想定される脅威に対して，必要なセキュリティ要件が盛り込まれていること
工程 2．設計
（省略）
レビューポイント：セキュリティ要件が機能又は運用によって満足されていること
工程 3．実装
（省略）
レビューポイント：Web セキュリティガイドに基づき，実装されていること
工程 4．テスト
（省略）
レビューポイント：セキュリティ機能及びセキュリティに関する運用が設計どおりになっているかがテストされていること，適切な診断が実施されていること，並びに検出された脆弱性が修正されていること
工程 5．運用
（省略）

注記　第 2 版から追加された部分を破線の下線で示す。

図 11　Web セキュリティガイド第 3 版

しかし，今回のように開発を外部の業者に委託する場合，図 11 に従って開発されていることを確認するには工夫が必要である。そこで，H 課長は，③外部に開発を委託する契約の検収条件に追加すべき記載内容を検討した。

H 課長は，その後も Web セキュリティガイドの改善を続けた。迅速なパッチ適用の効果もあり，A 社では，今のところ Web サイトへの攻撃による被害は起きていない。

設問 1　〔セキュリティ専門業者による調査〕について，(1)～(3)に答えよ。

(1) 表 1 中の下線①について，アクセスログに残らないのは，どのような攻撃の場合か。35 字以内で述べよ。

(2) 本文中の［　a　］に入れる適切な確認方法を，表 1 の結果を考慮し，20 字以内で具体的に述べよ。

(3) 本文中の下線②について，設定すべき認証方式の名称を，10 字以内で答えよ。

設問2　本文中の［　b　］に入れる適切な報告内容を，50字以内で具体的に述べよ。

設問3　図4中の［　c　］，本文中，図4中，図5中，表3中及び図10中の［　d　］，図4中の［　e　］，図4中の［　f　］に入れる適切な字句を，それぞれ10字以内で答えよ。

設問4　〔Webサイト Z に対する診断の実施〕について，(1)～(4)に答えよ。

(1)　表4中の［　g　］，［　h　］に入れる適切な数値を答えよ。

(2)　図8中及び図9中の［　i　］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　"><script>alert('NG');</script>　　イ　');alert('NG

ウ　'alert('NG');　　エ　<script>alert('NG');</script>

(3)　表5中の［　j　］に入れる適切な操作内容を，表2中の画面遷移を指定して40字以内で述べよ。

(4)　図10中の［　k　］に入れる適切な字句を，表5の方法を踏まえて，15字以内で答えよ。また，図10中の［　l　］に入れる適切な字句を，表5の方法を踏まえて，20字以内で具体的に述べよ。

設問5　本文中の下線③について，検収条件に追加すべき記載内容は何か。40字以内で具体的に述べよ。

設問6　診断で見つかった個々の脆弱性は Web セキュリティガイドを改善するためにどのように利用できるか。40字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，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。