SC

令和７年度　春期
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）

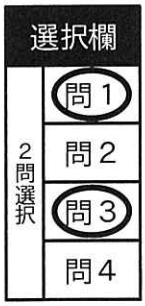
注意事項

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　サプライチェーンのリスク対策に関する次の記述を読んで，設問に答えよ。

L 社は，金融業向けにシステムを開発している従業員 1,000 名の企業である。L 社のシステム開発プロジェクトでは，プラットフォーム G というソフトウェア開発プラットフォームを利用している。プラットフォーム G の機能には，ソースコード及び開発ドキュメントのバージョンを管理する機能，CI/CD パイプラインの管理機能，開発対象の SBOM 作成機能がある。CI/CD パイプラインの管理機能を利用してテストやリリースの自動実行が可能である。開発対象の SBOM 作成機能はプラットフォーム G 上のリポジトリサーバ内のソースコード及びライブラリをシステム構成要素として一覧化する。開発対象の SBOM 作成機能は現状では特に利用していない。また，L 社が採用している SAST ツール（以下，ツール F という）は，プラットフォーム G 上のリポジトリサーバや開発者の端末にインストールして利用するツールであり，コンパイルエラーが解消されたソースコードに対してだけ正常な検査が可能である。プラットフォーム G の CI/CD パイプラインの管理機能で，ツール F でのチェックを自動的に行うようなワークフローを構成することができる。

近年，業務委託先でのセキュリティ侵害に起因する情報セキュリティインシデントが大きく報道されるなど外部環境が変化し，L 社経営陣もサプライチェーンリスク対策の強化を考えるようになった。経営陣の指示で，情報セキュリティ担当の B さんは，サプライチェーンリスク対策を強化したセキュリティガイドライン（以下，ガイドラインという）を作成し，全てのシステム開発プロジェクト及び運用サービスを点検することになった。B さんは，L 社が契約しているセキュリティ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）の D 氏にガイドラインの作成について相談することにした。

〔ガイドラインの作成〕

次は，ガイドラインの作成についての B さんと D 氏の会話である。

B さん：ガイドラインはどのような構成がよいでしょうか。

D 氏　：システムライフサイクルの工程に合わせるのがよいでしょう。L 社のシステム開発業務を踏まえて，調達，開発，リリース・デプロイ，運用の工程に分類し，さらに全ての工程で共通するような項目も抜き出して記載しましょう。

Bさんは，ガイドライン案を表1のように作成した。

表1　ガイドライン案（抜粋）

工程	項番	対策
共通	1	システムに関連する情報資産を，業務委託先と共同で利用するものも含めて一覧化し，管理すること。一覧化すべき情報資産は，次のとおりである。 ・サーバ ・ネットワーク機器 ・ソースコード ・リポジトリ内のライブラリ
	2	各工程で利用するシステムのアカウントは，業務委託先を含めて必要な利用者にだけ発行すること。その際，責任追跡性を確保するためにアカウントの利用者を特定できるようにすること
	3	一覧化した情報資産ごとに，パッチ適用状況など最新の構成情報を把握すること
調達	4	業務委託先の企業を，再委託先まで含めて一覧として管理すること
	5	業務委託先でのセキュリティ管理に関する要件を，業務委託先との契約に含めること
開発	6	ソフトウェア開発プラットフォームなどの開発環境は，アクセス制御を行い，必要な利用者だけがアクセスできるようにすること
	7	開発環境にアクセスしたアカウントを特定できるようにアクセスログを記録すること
	8	開発したソフトウェアのソースコードは，人手によるレビュー及びSASTツールによるチェックを行うこと
	9	システムの仕様，機能を精査し，不要な機能やセキュリティ上の欠陥がないことを設計書から確認すること
リリース・デプロイ	10	開発したソフトウェアのSBOMを作成すること
	11	リリースしたソフトウェアは，リリースバージョンを管理すること
運用	12	システムの稼働環境において，稼働状況を監視すること
	13	システムの稼働環境において，要件に応じたアクセス制御を実施すること
	14	システムの運用端末がある部屋は，要件に応じた入退室管理を実施すること
	15	インシデント対応手順書を作成すること

次は，ガイドライン案についてのBさんとD氏の会話である。

Bさん：①セキュリティ・バイ・デザインの考え方を一部取り入れました。その他，留意すべき点などはありますか。

D氏　：項番5には，②業務委託先が再委託を行う場合に備えて，L社と業務委託先との間の契約書に明記すべき事項を具体的に示しておくとよいでしょう。

B さんが修正したガイドライン案を経営陣に報告したところ，過去に外部ベンダーでのセキュリティ侵害に起因してL社でインシデントが何度か発生したことがあったので，それらのインシデントに対するガイドライン案の有効性を評価するように指示があった。

〔過去のインシデントの確認〕

B さんは，過去のインシデントに対するガイドライン案の有効性を評価することにした。次は，1件目のインシデントについてのD氏とBさんの会話である。

D氏　：はじめに，インシデントの内容を確認しておきましょう。

Bさん：L社が開発し，運用していたシステム（以下，システムQという）では，古いWebブラウザをサポートするためのJavaScript（以下，スクリプトPという）を利用していました。スクリプトPは，当時広く使われていたT社製のものです。スクリプトPは，T社が運営するサーバ（以下，サーバTという）に配置され，システムQにアクセスしたWebブラウザがスクリプトPを都度読み込むようにシステムQは構成されていました。ある日，サーバTが乗っ取られてしまい，スクリプトPが改ざんされたことによって，システムQへの利用者のアクセスが悪意のあるWebサイトにリダイレクトされてしまいました。

D氏　：発見の経緯を教えてください。

Bさん：システムQの利用者からの問合せで気付き，対策を実施しました。当時の情報セキュリティ担当は，サーバTが侵害されたというニュースは知っていましたが，システムQへのアクセスが影響を受けることを把握していませんでした。

D氏　：他社の発表によると，③スクリプトPを利用していたシステムでもスクリプトPの配置方法が違えば，影響を受けなかったようですね。

Bさん：はい。違う配置方法にするという対策もありました。しかし，Web ブラウザ開発元での古いWebブラウザの公式サポートが終了していたことから，当社の対策としては，④システムQのソースコードに変更を加えて，古いWebブラウザのサポートを終了しました。

D氏　：1件目のインシデントについてはおおむね理解できました。

Bさん：案の項番10が，1件目のインシデントを未然に防ぐために有効ではありませんか。

D氏　：いいえ，開発対象のSBOM作成機能でSBOMを作成していたとしても，スクリプトPはSBOMに含まれないので，インシデントは防げなかったでしょう。

Bさんは，⑤SBOM以外の手段で，システムが利用している外部のスクリプトを把握できるよう，案の項目を一つ修正した。D氏とともに，そのほかの過去のインシデントについても案を評価したところ，案は有効であると確認できたので，経営陣に報告して承認を得た。

〔ガイドラインを用いた点検の実施〕

ガイドラインを用いて，現在進行中の全てのシステム開発プロジェクト及び運用サービスを点検することになった。最初の点検対象は，システムSの開発プロジェクト及び運用サービスである。Bさんがプロジェクト計画書，運用計画書などからまとめたシステムSの開発プロジェクト及び運用サービスの概要を図1に，開発環境の構成図を図2に示す。

1. システムSは，L社が3年前からS銀行向けに提供しているインターネットバンキングシステムである。運用と追加機能の開発をL社が請け負っている。
2. セキュリティ監視を情報セキュリティ会社のN社に委託している。開発は，L社従業員，L社に派遣された派遣エンジニア及び他の業務委託先の従業員が行っている。なお，運用ツールなど一部のソフトウェアはN社が開発することがある。
3. L社がシステムSを運用するためにS銀行内にセキュアルームが用意されている。セキュアルームへの入室にS銀行が貸与するカードでの認証を必須とする入退室装置が導入され，S銀行の管理者及びL社の運用担当者しか入室できないようになっている。
4. 派遣元及び業務委託先との間では，L社のセキュリティポリシーの順守とプロジェクトでのセキュリティルールの順守について契約書で定めている。N社との業務委託契約には，N社内のセキュリティ管理についての実施事項及びN社が再委託を行わないことを明記している。N社での委託契約の順守状況を定期的な監査によって確認する。
5. 開発時に，要件定義段階での脅威モデリング及び設計段階での設計書の確認を行い，不要な機能やセキュリティ上の欠陥がないことを確認する。
6. プラットフォームGに設計書を格納する。開発したソフトウェアのSBOMは作成しない。
7. 開発したソフトウェアのソースコードは，開発リーダーがレビューして承認する。開発したソフトウェアをリリースする際は，開発リーダーがリリースバージョンを更新する。

図1　システムSの開発プロジェクト及び運用サービスの概要

8. 資産管理台帳にサーバ及びネットワーク機器の一覧を担当者が入力する。
9. システムSに組み込むOSSライブラリは，開発者が取得する。OSSライブラリは資産管理台帳に入力しない。
10. 開発は，L社内及びオフショア拠点で行い，次のLANに接続した端末で実施する。
・L社内に用意した従業員LAN
・L社内に用意したパートナーLAN
・オフショア拠点にある業務委託先のLAN
また，テストなどのためにシステムSの開発系サーバがあるLAN（以下，開発LANという）にアクセスする際には一旦，踏み台サーバにログインする。踏み台サーバには，L社，業務委託先など会社ごとに発行した共用アカウントでログインするが，ログインごとに，利用記録簿に記載する。開発LAN上のサーバには製品仕様上，アクセスログが取れないものもある。
11. インシデント発生時にL社のシステムSの担当者に連絡するための業務フローがインシデント対応手順書に定められており，システムSの担当者がインシデントのハンドリングを行う。
12. ツールFが開発者の端末とプラットフォームGにインストールされている。

図1　システムSの開発プロジェクト及び運用サービスの概要（続き）

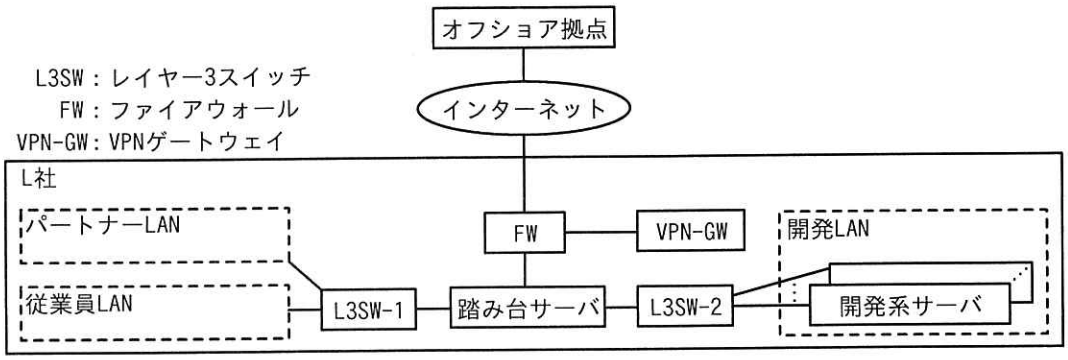


図2　システムSの開発環境の構成図（抜粋）

Bさんは，システムSの担当者へのヒアリング前に論点を整理しておこうと考え，表1の各項番について，図1に基づき，対策状況を確認した。結果は表2のとおりである。

表2　システムSの事前確認結果（抜粋）

工程	表1の項番	確認した図1の項番	確認結果又は問題点
共通	1	8，9	OSSライブラリを台帳管理していない。
	2	ア	a
調達	5	イ	問題なし。
開発	9	ウ	b
リリース・デプロイ	10	6	開発したソフトウェアについてSBOMを作成していない。
運用	15	エ	c

Bさんは，システムSの担当者であるCさんにヒアリングを行った。

〔SBOMについての確認〕

次は，表1の項番10についてのCさんとBさんの会話である。

Cさん：システムSのソフトウェア構成は設計書で把握できると考えていますが，SBOMの作成も必要でしょうか。

Bさん：SBOMを利用すると，⑥将来，脆弱性管理がしやすくなります。プラットフォームGで作成することができます。

Cさん：なるほど。それでは，SBOMの作成を検討します。

〔開発工程のセキュリティ対策についての確認〕

Bさんは，表1の項番7，8について確認した。次は，そのときのBさんとCさんの会話である。

Bさん：表1の項番7の対策は実施できていますか。

Cさん：オフショア拠点から開発LANへのアクセスについてはVPN-GWでアクセスログを取得できているものの，社内からのアクセスについては取得できていません。

Bさん：アクセスログは図2中の［　d　］で取得するのがよいでしょう。

Cさん：分かりました。

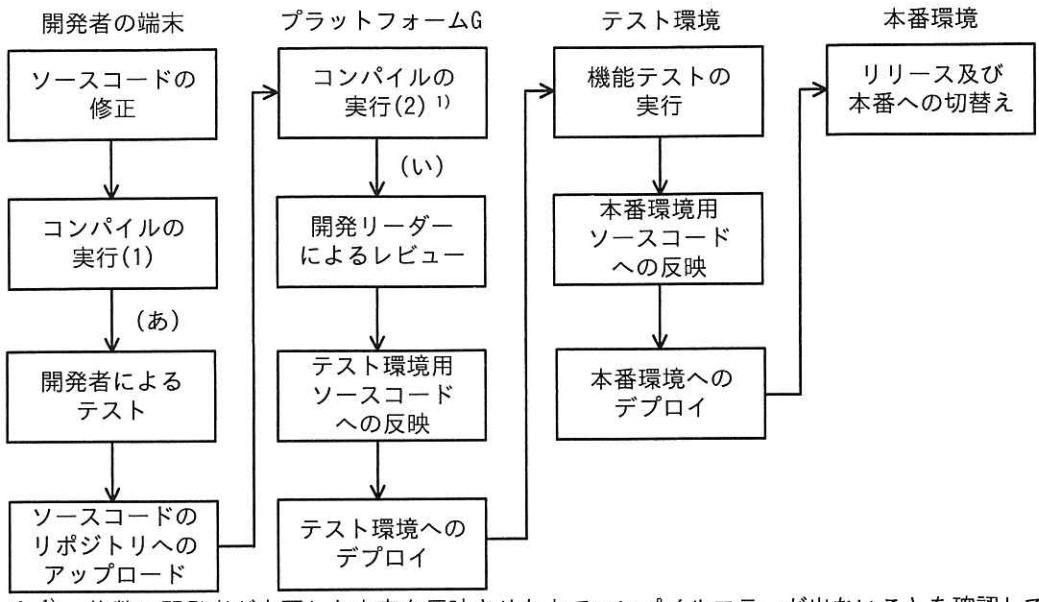
Bさん：表1の項番8の対策はどのようにしていますか。

Cさん：現在はソースコードの変更内容を開発リーダーがレビューしています。

Bさん：開発リーダーによるレビューに加えて，ツールFでチェックするのがよいでしょう。

Cさん：開発フローのどこでツールFを実行するのがよいでしょうか。

Bさん：ツールFの特性を踏まえると，図3のシステムSの開発フロー中の(あ)又は(い)で実行するのがよいと考えられます。⑦それぞれ利点が異なります。



注 1) 複数の開発者が変更した内容を反映させた上でコンパイルエラーが出ないことを確認している。

図3 システムSの開発フロー

ガイドラインを用いた点検の後，L 社のサプライチェーンリスク対策は強化された。

設問1 〔ガイドラインの作成〕について答えよ。

(1) 本文中の下線①について，どのような考え方か答えよ。

(2) 本文中の下線②について，明記すべき事項を，50 字以内で答えよ。

設問2 〔過去のインシデントの確認〕について答えよ。

(1) 本文中の下線③について，影響を受けない配置方法を答えよ。

(2) 本文中の下線④について，加えた変更を，具体的に答えよ。

(3) 本文中の下線⑤について，修正した項番と修正内容を答えよ。

設問3 〔ガイドラインを用いた点検の実施〕について答えよ。

(1) 表2中の［ア］～［エ］に入れる適切な項番を答えよ。

(2) 表2中の［a］～［c］に入れる適切な字句を答えよ。

設問4 本文中の下線⑥について，脆弱性管理がしやすくなる理由を，具体的に答えよ。

設問５　〔開発工程のセキュリティ対策についての確認〕について答えよ。

(1)　本文中の［　d　］に入れる適切な字句を，図２中の名称で答えよ。

(2)　本文中の下線⑦について，(あ)，(い)で実行する利点を，それぞれ 40 字以内で答えよ。

問２　脆弱性管理に関する次の記述を読んで，設問に答えよ。

M 社は，従業員 3,000 名の情報サービス業を営む企業である。ソフトウェアの開発・販売を行っており，自社ホームページのほか，販売したソフトウェアのサポート用 Web サイトなど複数の Web サイト（以下，Web サイトをサイトという）を保有している。M 社では，メンテナンスのために管理者が自宅や外出先からサイトにリモートアクセスする。セキュリティに関する問合せ窓口は，情報システム部が担当している。

M 社が保有するサイトのうち，重要なサイト（以下，重要サイトという）は，プラットフォームに対する脆弱性診断（以下，PF 診断という）及び Web アプリケーションプログラムに対する脆弱性診断（以下，Web アプリ診断といい，PF 診断と Web アプリ診断を併せて両診断という）を初回リリース前に実施するルールになっている。初回リリース後の両診断の実施については任意である。重要サイトの指定は，扱う情報の重要性，停止による影響などを勘案し，各サイトの所管部門が判断している。重要サイト以外のサイトに対する両診断の実施は任意である。

両診断は，情報システム部の選定した専門ベンダーP 社に依頼して実施，又は情報システム部の選定した脆弱性診断ツール（以下，診断ツールという）を用いて各サイト担当者が実施する。ただし，緊急の場合，情報システム部が実施することもある。P 社の Web アプリ診断は，脆弱性が実際に悪用できることを確認した上で報告してくれるので，評判がよい。

脆弱性は Critical，High，Medium，Low，None の 5 段階の深刻度レベルに分類される。P 社に依頼して診断を行う場合は，P 社から深刻度レベルの報告を受ける。深刻度レベルは，情報システム部が選定した診断ツールの場合は CVSS 基本値によって分類される。P 社の診断では，P 社が独自の知見で CVSS 基本値を基に値を変え，分類している。M 社では，深刻度レベルが High 以上の場合は速やかな修正を必須とし，それ以外は所管部門が対応要否を判断する。

〔脆弱性の報告〕

ある日，M 社のキャンペーンサイト X（以下，サイト X という）のキャンペーンページに SQL インジェクションの脆弱性が存在しているという指摘が問合せ窓口に報告

された。報告内容についてサイト担当者に確認したところ，脆弱性が存在する可能性があるとの回答であった。サイトXは重要サイトに指定されていなかった。サイトXの仕様を図1に示す。

・Webサーバ，Webアプリケーションサーバ及びデータベース（以下，DBという）サーバから成る。
・キャンペーン情報をDBサーバに格納している。
・顧客情報は保有していない。
・キャンペーンページのURLのクエリパラメータにコンテンツ番号が含まれている。
URL例：https://site-x.m-sha.co.jp/info?article=20250101
・コンテンツ番号がDBサーバ上に存在しない場合，又はSQLが構文エラーになる場合は，“コンテンツがありません”というメッセージを返す。
・Webアプリケーションプログラムにおいて，クエリパラメータarticleの値はSQLでの検索では数値型として扱われる。

図1　サイトXの仕様（抜粋）

情報システム部のEさんとJ課長は，報告の内容を確認するために，情報システム部が診断ツールを実行する旨をサイトXの担当者に伝えた。

Webアプリ診断用の診断ツールを該当ページに対して実行したところ，深刻度レベルがHighのSQLインジェクションの脆弱性が検出された。SQLインジェクションの脆弱性検出時のクエリパラメータ及び応答を表1に示す。

表1　クエリパラメータ及び応答（概要）

クエリパラメータ	応答
article=20250401	2025年4月1日のキャンペーンのコンテンツが返される。
article=20250401’	a
article=20250401’%20and%20’a’=’a	b
article=20250401’%20and%20’a’=’b	c
article=20250401%20and%201=0	d
article=20250401%20and%201=1	e

Eさんは，速やかにサイト担当者に連絡し，インターネットからサイトXにアクセスできないようネットワーク構成を変更した上で，該当するプログラムを修正するよう依頼した。これに対してサイトXの担当者は，“重要情報の漏えいなどの問題が

発生することはない。DB には重要情報もない。サイト X にアクセスできないようにする必要はない。”と主張した。それに対して E さんは，“本脆弱性はブラインド SQL インジェクションの脆弱性に該当する。そのため，表 1 と同様の手法を用いることによって，DB のテーブル名が特定できることになる。”と説明した。E さんは，DB のテーブル名を使うと攻撃者が次にどのような攻撃を行えるかを説明し，対応する必要性を説いた。これを受け，迅速に対応が行われた。

〔脆弱性が存在していた状況の確認と一斉診断の実施〕

対応完了後，情報システム部では，公開サイトは全て重要サイトに指定するようにルールを変更することにした。同時に，M 社が保有する全ての公開サイトに対する一斉の両診断（以下，一斉診断という）を実施することにし，その診断を P 社に依頼した。診断対象サイトの情報を表 2 に示す。

表 2　診断対象サイトの情報

サイト名	サイト特性	社外利用者向けアカウントの作成方法	1 日当たりのアクセス数	顧客情報有無	停止による影響
サイト A	EC サイト	利用者が作成	10,000	有	大
サイト B	業務サイト	管理者が発行	3,000	有	中
サイト C	情報提供サイト	なし	10,000	無	小
⋮	⋮	⋮	⋮	⋮	⋮
サイト Z	（省略）	（省略）	（省略）	（省略）	（省略）

診断の結果，深刻度レベル High 以上の脆弱性が検出されたサイトが数サイトあり，Medium 以下の脆弱性が数十件検出されたサイトも多数あった。

サイトによっては，初回リリース時の両診断以降にアップデートや設定変更をしていないにもかかわらず，初回リリース時の両診断結果と今回の一斉診断結果が異なっている場合もあった。P 社の診断は，決められた手順に従って行い，診断結果は技術レビューを行うので，診断員による差異はほぼないと，E さんは P 社から聞いていた。また，初回リリース時の両診断では，サイトに不具合はなかったと報告を受けている。E さんが，改めて P 社に確認すると，診断結果が異なっていた要因は，［ f ］や［ g ］だった。これらのことから，E さんは初回リリース後も定期的な両診断が必要であると結論づけた。

〔PF 診断で検出された脆弱性〕

PF 診断で検出された脆弱性を表 3 に示す。

表 3　PF 診断で検出された脆弱性（抜粋）

サイト名	脆弱性 ID	脆弱性	深刻度レベル	CVSSv3 基本値	補足
サイト A	PA-1	SSL/TLS サーバの暗号強度が弱く，推奨されていない鍵交換をサポート	Medium	5.9	—
サイト B	PB-1	OpenSSH でリモートから認証なしに任意のコード実行が可能	High	8.1	CVE 番号：CVE-20XX-XXXXX
	PB-2	管理者用の Web のログイン画面に認証試行が何回でも可能	Medium	5.3	—
	PB-3	SSL/TLS サーバの暗号強度が弱く，推奨されていない鍵交換をサポート	Medium	5.9	—
サイト C	PC-1	SSH 接続の安全性を低下させることが可能	Medium	5.9	CVE 番号：CVE-20YY-YYYYY
サイト D	PD-1	（省略）	High	7.2	—
	PD-2	（省略）	Critical	9.8	—
サイト E	PE-1	（省略）	Medium	6.5	—

脆弱性 PA-1 と PB-3 について，CRYPTREC が作成し，IPA が発行している“TLS 暗号設定ガイドライン Ver. 3.1.0”の“4. 推奨セキュリティ型の要求設定”には，表 4 に示す鍵交換におけるビットセキュリティの基準を満たすよう記載されていた。そのため，サイト A 及びサイト B は基準を満たす設定に変更することにした。

表 4　鍵交換におけるビットセキュリティの基準

鍵交換プロトコル	基準
ECDHE	h ビットセキュリティ以上を満たす i
DHE	j ビットセキュリティ以上を満たす k

脆弱性 PB-1 は，管理者がメンテナンス用にリモートアクセスで使っている OpenSSH において検出された。OpenSSH では，ログインが一定時間内に成功しないと，認証試行のタイムアウト処理が実行される。脆弱性 PB-1 は，あるセキュリティベンダーの報告によると，認証試行のタイムアウト処理が同時に多数実行されると起き得る問

題であり，認証試行の接続時間（LoginGraceTime）の設定が 120 秒の場合，その間に 100 件試行されると，OpenSSH のログに “Timeout before authentication” という認証タイムアウトのメッセージが多数出力され，3～4 時間で悪用に成功する可能性があるとのことだった。もしも，脆弱性を修正したバージョンの OpenSSH に更新できない場合には，次のいずれかを行う。

・トレードオフはあるものの，認証試行にタイムアウトを設けないようにサーバの設定を変更する。

・①サイト担当者が攻撃を早期に検知する方法を採用することによって被害を抑制する。

サイト B では，OpenSSH の更新を行った。

脆弱性 PB-2 は，送信元 IP アドレス制限が対策の一つだが現実的な運用が難しい。代わりの対策として，ログイン画面のアカウントロックがあるが，採用する場合はロック解除の運用方法や実装について検討が必要である。サイト B では，②アクセス元の PC を認証する対策を採用した。

〔Web アプリ診断で検出された脆弱性〕

Web アプリ診断で検出された脆弱性を表 5 に示す。

表 5　Web アプリ診断で検出された脆弱性（抜粋）

サイト名	脆弱性 ID	脆弱性	深刻度レベル	CVSSv3 基本値	補足
サイト A	WA-1	本来閲覧できない画面を閲覧可能	Medium	4.3	購入機能で，商品の詳細を閲覧するリクエストに含まれるパラメータ item の 5 桁の数字を変更することによって一般会員が本来閲覧できない商品の説明画面を閲覧できた。評価指標を次に示す。 CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
サイト B	WB-1	本来閲覧できない画面を閲覧可能	Medium	5.3	管理者用アカウントでログインし，発注確認機能の URL[1)]を確認後，一般利用者アカウントでログインし直し，Web ブラウザのアドレスバーに当該 URL を入力することによって，管理者用の画面を閲覧できた。この画面では，他人の発注情報が全て閲覧できた。評価指標を次に示す。 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N

注 1)　https://site-b.m-sha.co.jp/administrator0001/order_history

表5　Webアプリ診断で検出された脆弱性（抜粋）（続き）

サイト名	脆弱性ID	脆弱性	深刻度レベル	CVSSv3基本値	補足
サイトC	WC-1	OSコマンドインジェクション	Critical	9.8	問合せフォームが直接シェルに入力値を渡す作りになっていて，任意のOSコマンドが実行できた。ただし，管理者権限が必要な操作はできなかった。

脆弱性WA-1とWB-1は，HTTPリクエストの内容を一部変更することによって本来閲覧できない画面を閲覧できるという点では同じであるが，評価指標の値が異なる。評価指標のうち，③Attack Complexity（AC）の値はそれぞれLとHであった。

脆弱性WC-1について，④管理者権限が必要な操作ができなかったのは，サイトCの仕様どおりであった。サイトCの仕様を図2に示す。

1. Webサーバ及びWebアプリケーションサーバから成る。
2. DBサーバとの連携はしていない。
3. Webアプリケーションプログラムは，一般利用者権限の専用アカウントでプロセスを実行している。
4. 問合せフォームに入力された値をメールコマンドで管理者宛てに送る。
5. 問合せ内容がログに保存され，その中にメールアドレスなどの個人情報をもつ。
6. ログには特定のアカウントだけがアクセスできる。

図2　サイトCの仕様（抜粋）

〔脆弱性評価方法の検討〕

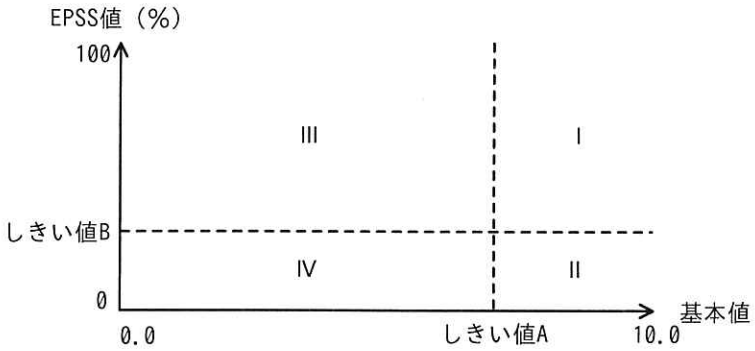
一斉診断が一段落したところで，情報システム部は脆弱性管理についての課題を議論した。対応の要否判断が不適切であったサイトや対応が遅すぎたサイトがあったので，J課長は，Eさんに新たな脆弱性評価方法を検討するよう指示した。

はじめにEさんが調査したところ，IPAのホームページに“脆弱性対応におけるリスク評価手法のまとめ”というレポートが公開されていたので，これを参考にすることにした。Eさんは，検討内容をJ課長に報告した。次は，その際のEさんとJ課長の会話である。

Eさん：レポートでは，対応要の脆弱性を簡易的な1次評価で選び，さらに，2次評価で優先度を評価する手法が提案されています。

J課長 ：1次評価は具体的にはどのような評価をするのか。

Eさん ：1次評価では，基本値とExploit Prediction Scoring System（EPSS）値を用います。EPSS値の代わりにCVSSv3の現状値を用いる方法もありますが，⑤現状値とEPSS値を比べると，現状値は手間が掛かり，EPSS値は手間が掛からないとされています。1次評価では図3のように脆弱性を領域図で4領域に分類します。



注記　EPSS値がしきい値Bの場合は，領域III又はIと，基本値がしきい値Aの場合は，領域I又はIIと考える。

図3　1次評価の領域図

J課長 ：しきい値はどうするのか。

Eさん ：しきい値Aは7.0に，しきい値Bは1%に設定しようと考えています。領域IVは対応不要とし，領域I～IIIを2次評価の対象にします。

J課長 ：なるほど。では，そのしきい値に設定してみて，対応すべき脆弱性に漏れが出るなどの問題があれば，しきい値を見直すことにしよう。

Eさん ：はい。分かりました。

J課長 ：あとはEPSS値を用いた脆弱性評価について，しきい値の見直し以外にも，［　l　］を継続的に行うことで被害を防ぐ助けになるだろう。

Eさん ：分かりました。

J課長 ：ところで，Webアプリ診断では，見つかった脆弱性のEPSS値が報告されないことが普通だが，どのように評価するのか。

Eさん ：⑥P社のWebアプリ診断であれば，見つかった脆弱性のEPSS値は，しきい値Bよりも高いとみなすのが妥当であると考えられます。Webアプリ診断で検

出される脆弱性を，全て領域Ⅰか Ⅲとみなそうと考えています。

J 課長 ：その方法が安全だな。次に，2 次評価はどうするのか。

E さん ：2 次評価は，環境値と先に評価した領域とを組み合わせた方法にしようと考えています。

J 課長 ：環境値を全て算出するのだな。

E さん ：環境値の算出においては，現状評価基準の各評価指標を，“Not Defined”と設定することができます。環境評価基準での各評価指標の値の判断は各サイト担当者に依頼します。そして，表 6 に示す対応優先度表によって S～C の最終的な対応優先度を決定します。

表 6　対応優先度表

領域	CVSSv3 環境値			
	0～3.9	4.0～6.9	7.0～8.9	9.0～10.0
Ⅰ，Ⅲ	C	B	A	S
Ⅱ	C	C	B	A

S：即時対応　　A：対応優先度高　　B：対応優先度中　　C：対応優先度低

J 課長 ：分かった。一斉診断の結果で幾つか評価して確認してほしい。

E さん ：分かりました。

〔対応優先度評価の実施〕

E さんが 2 次評価を幾つか行った結果を表 7 及び表 8 に示す。

表 7　PF 診断で検出された脆弱性に対する評価結果（抜粋）

脆弱性 ID	PB-1	PC-1	PD-1	PD-2	PE-1
EPSS 値（%）	39	96.54	0.0	2.6	8.7
CVSSv3 環境値	8.1	7.7	5.7	8.0	6.5
対応優先度	m	n	o	p	q

表 8　Web アプリ診断で検出された脆弱性に対する評価結果（抜粋）

脆弱性 ID	WA-1	WB-1	WC-1
EPSS 値（%）	対象外	対象外	対象外
CVSSv3 環境値	5.0	7.1	9.8
対応優先度	r	s	t

この運用によって，脆弱性対応の優先度評価がサイト担当者によらず適切かつ迅速にできるようになった。

設問1　表1中の［ a ］～［ e ］に入れる応答を，解答群の中から選び，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　“コンテンツがありません”というメッセージが返される。

イ　2025年4月1日のキャンペーンのコンテンツが返される。

ウ　サーバから応答が返されない。

エ　内部サーバエラーが返される。

設問2　本文中の［ f ］，［ g ］に入れる適切な字句を，それぞれ 20 字以内で答えよ。

設問3　〔PF診断で検出された脆弱性〕について答えよ。

(1)　表4中の［ h ］～［ k ］に入れる適切な字句の組合せを，解答群の中から選び，記号で答えよ。

解答群

記号	h	i	j	k
ア	112	曲線	128	鍵長
イ	112	直線	128	署名
ウ	128	曲線	112	鍵長
エ	128	直線	112	署名

(2)　本文中の下線①について，検知する方法を，具体的に答えよ。

(3)　本文中の下線②について，採用した対策を，20字以内で具体的に答えよ。

設問4　〔Webアプリ診断で検出された脆弱性〕について答えよ。

(1)　本文中の下線③について，脆弱性WA-1のACがLと評価された評価根拠と脆弱性WB-1のACがHと評価された評価根拠を，それぞれ具体的に答えよ。

(2)　本文中の下線④について，該当するサイトCの仕様を，図2中の項番から選び，答えよ。

設問５　〔脆弱性評価方法の検討〕について答えよ。

(1)　本文中の下線⑤について，現状値は手間が掛かる理由と EPSS 値は手間が掛からない理由を，それぞれ 40 字以内で答えよ。

(2)　本文中の［　l　］に入れる適切な字句を，15 字以内で答えよ。

(3)　本文中の下線⑥について，妥当である理由を，30 字以内で答えよ。

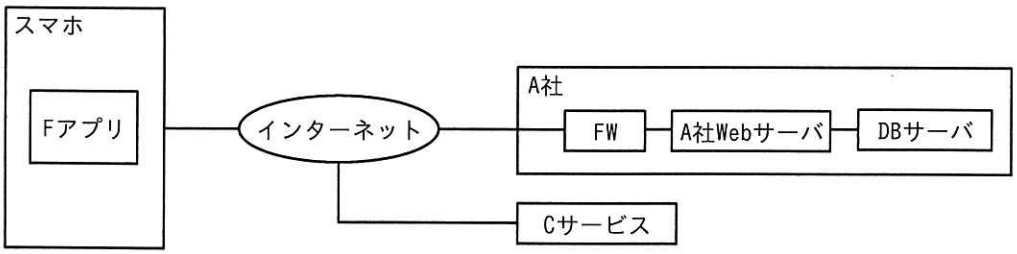
設問６　表７中及び表８中の［　m　］～［　t　］に入れる対応優先度を答えよ。

問３　スマートフォン用アプリケーションプログラムの開発に関する次の記述を読んで，設問に答えよ。

A 社は，撮影機器の販売や写真のプリントサービスを全国に 200 店舗で展開する従業員 2,000 名の企業である。実店舗の運営に加え，インターネットを介して撮影機器の販売を行う EC サイト事業を有している。このたび，会員がスマートフォン（以下，スマホという）用アプリケーションプログラム（以下，スマホ用アプリケーションプログラムをスマホアプリという）を通じて，写真入りのカレンダーなどのグッズ（以下，フォトグッズという）を注文できるサービス（以下，E サービスという）を新規に開始することになった。E サービス用スマホアプリ（以下，F アプリという）は国内で流通する主要なスマホ OS である OS-α と OS-β の過去 5 年以内に正式リリースされたバージョンをサポートする。

〔E サービスの説明〕

E サービスは，F アプリとサーバサイドのシステム群で構成される。F アプリは，インターネットを介して E サービス用 Web サーバ（以下，A 社 Web サーバといい，FQDN は www.a-sha.co.jp とする）及び大手クラウドサービスプロバイダ C 社のクラウドストレージサービス（以下，C サービスという）との間で HTTPS を使用して通信する。フォトグッズの作成に使う写真は，F アプリから C サービスにアップロードする。E サービスのネットワーク構成を図 1 に，機能概要を図 2 に，F アプリの画面構成を図 3 に，フォトグッズの注文処理の流れを図 4 に，C サービスの仕様を図 5 に示す。



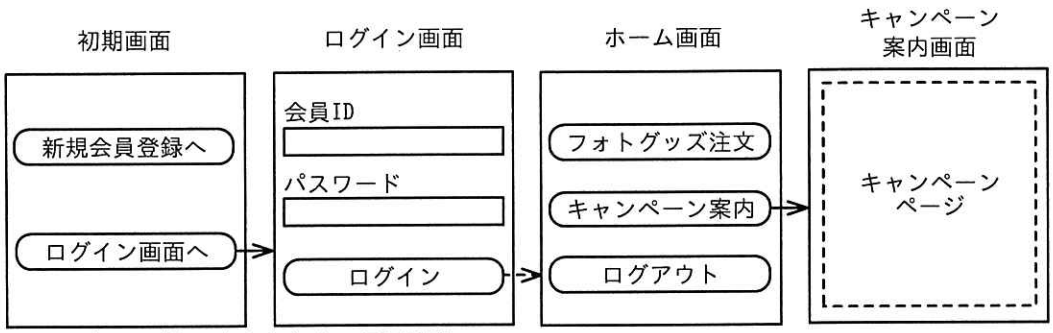
FW：ファイアウォール　　DBサーバ：データベースサーバ

図 1　E サービスのネットワーク構成（概要）

1. 新規会員登録機能
   E サービスを利用するための新規会員登録を行う。
2. ログイン機能
   会員 ID とパスワードでログインする。ログインした会員には，認証トークン [1] が払い出され，ログアウトするまでの間，F アプリに保存される。認証トークンは，A 社 Web サーバ上で会員のセッションを識別するために使用する推測困難な値である。
3. フォトグッズ注文機能
   F アプリ上でフォトグッズを注文する。ログイン済み会員だけが利用できる。
   なお，フォトグッズは，指定した A 社の実店舗で受け取ることができる。
4. キャンペーン案内機能
   キャンペーンの Web ページ（以下，キャンペーンページという）を表示する。ログイン済み会員だけが利用できる。
   なお，キャンペーンに応募することによって，フォトグッズの割引などに利用可能なクーポンを入手できる。会員には，電子メール（以下，メールという）などを通じて，期間限定のキャンペーンを案内する。キャンペーンの内容は，2 週間ごとに更新される。

注 [1] 認証トークンは，ログイン後に F アプリが A 社 Web サーバに HTTP リクエストを送信する際，Authorization ヘッダーに指定される。

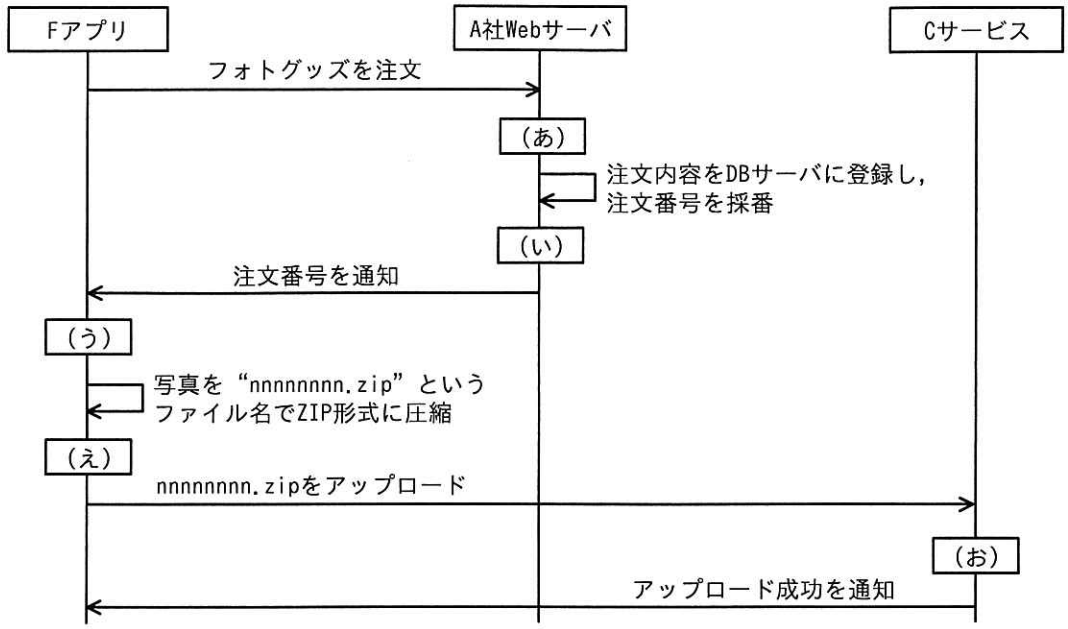
図 2　E サービスの機能概要（抜粋）



→：ボタンが押下されたときの画面遷移
-→：適切な値を入力してボタンが押下されたときの画面遷移

注記　キャンペーンページは HTML 形式で作成し，A 社 Web サーバにアップロードしておく。

図 3　F アプリの画面構成（抜粋）



注記　“nnnnnnnn”は注文番号であり，00000001から始まる十進数の連番である。

図4　フォトグッズの注文処理の流れ

1. サービスの概要

(1) Cサービスはマルチテナントのストレージサービスである。テナントの管理権限をもつ利用者（以下，管理者という）が作成したストレージに対し，テナントの作成したシステム（以下，利用システムという）からファイルのアップロードやダウンロード（以下，アップロード，ダウンロードを併せてファイル操作という）を行う。

(2) 管理者は，ストレージの作成時に任意のストレージ名を設定する。ストレージを作成すると，Cサービスからアクセスキーが発行される。アクセスキーはストレージごとに異なる40字の英数字である。

(3) 利用システムは，ストレージ上のファイルをURLのパスで指定する。例えば，ストレージ“●●●”上のファイル“▲▲▲”をファイル操作する際は，“/●●●/▲▲▲”を指定する。ファイルのアップロードにはHTTPのPUTメソッドを，ファイルのダウンロードにはGETメソッドを用いる。

(4) 利用システムは，次の方式a又は方式bでファイル操作を行う。

2. 方式a

(1) 説明

アクセスキーをHTTPリクエストのAuthorizationヘッダーに指定する方式である。利用システムは，Cサービスから発行されたアクセスキーを用いることによって，アクセスキーに対応するストレージに格納された全てのファイルに対するファイル操作が可能となる。

Authorizationヘッダーに正しいアクセスキーが指定されていない場合，ファイル操作は拒否される。

図5　Cサービスの仕様（抜粋）

(2) 使用例

アクセスキー“○○○”を指定して，ストレージ“abc”上のファイル“xyz”をダウンロードする際に送信するHTTPリクエストの例を次に示す。

リクエストライン　：GET /abc/xyz HTTP/1.1

ヘッダーフィールド：Host: storage.c-sha.jp

Authorization: Bearer ○○○

3. 方式b

(1) 説明

有効期限（Expires）と署名値（Signature）をクエリパラメータとして付加したURL（以下，署名付きURLという）を用いて，特定のファイルに対するファイル操作を一時的に可能とする方式である。ここで，Expiresパラメータに指定する有効期限はUNIXタイムスタンプ形式である。署名値の生成は次のように行う。

（i）GET又はPUTから始まり，パス中の“/●●●/▲▲▲?Expires=【有効期限】”で終わる文字列を署名対象文字列とする。

（ii）アクセスキーを秘密鍵とする。

（iii）署名対象文字列と秘密鍵からHMAC-SHA256値を求める。

（iv）（iii）で求めた値をbase64urlエンコードする。

利用システムは，署名付きURLを生成し，ファイル操作を許可する利用者に伝える。伝えられた利用者は，署名付きURLを指定してHTTPリクエストを送ることによって，ファイル操作ができる。有効期限が切れた場合やサーバ側で署名値の検証が失敗した場合は，ファイル操作が拒否される。

(2) 使用例

ストレージ“abc”上のファイル“xyz”をダウンロードする場合で，かつ，署名値が“△△△”の場合のHTTPリクエストの例を次に示す。xyzは，日本時間の2025年5月30日0時0分0秒，つまりUNIXタイムスタンプで1748530800までの間，ダウンロードが許可されている。

リクエストライン　：GET /abc/xyz?Expires=1748530800&Signature=△△△ HTTP/1.1

ヘッダーフィールド：Host: storage.c-sha.jp

図5　Cサービスの仕様（抜粋）（続き）

Eサービスで使うCサービスのストレージ名は，e-serviceである。Fアプリでは，方式aを利用する。アクセスキーは，鍵長256ビットの共通鍵とAES-CBCアルゴリズムで暗号化し，Fアプリ内にリソースとして保存する。Cサービスのストレージ名並びにAES-CBCの共通鍵及び初期ベクトルは，Fアプリのコード中に定数として定義する。

〔キャンペーン案内機能の実装方法〕

Fアプリでのキャンペーンページの表示には，WebViewという仕組みを用いる。WebViewは，スマホOSの提供する仕組みであり，スマホアプリの画面の一部にWebペ

ージを表示させることができる。キャンペーンページのHTMLは，WebViewを用いて，Fアプリの画面上に表示させる。

会員に送るキャンペーン案内のメール本文中には，F アプリでキャンペーンページを表示するための URL（以下，F-URL という）を含める。会員がメールアプリから F-URL を開くと，F アプリが起動し，WebView 上にキャンペーンページが表示される。キャンペーンページからキャンペーンに応募する際の会員のセッションの識別には，F アプリに保存されている認証トークンを用いる。OS-αでは，キャンペーンページが表示された後に，WebView の機能によってキャンペーンページ上の ECMAScript コードが F アプリの getToken 関数を呼び出す。これによって，認証トークンが F アプリからキャンペーンページに引き渡される。OS-βでは別の方式で同様の機能を実現する。キャンペーンページ上の ECMAScript コードを図 6 に示す。

```
const token = f_app.getToken();
```

図 6　キャンペーンページ上の ECMAScript コード

キャンペーンページ以外から getToken 関数を悪用されないように，getToken 関数の内部では，図 7 のように呼出し元の Web ページの URL を確認する。

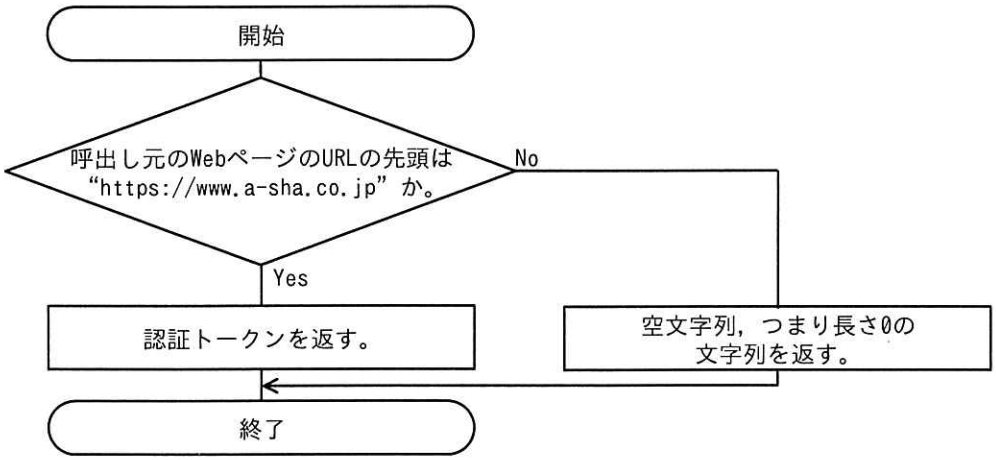


図 7　getToken 関数の処理の流れ

F-URL の例を図 8 に示す。

```
f-app://campaign?url=https://www.a-sha.co.jp/campaign/□□□
```

注記1　“f-app”はカスタムURLスキームである。
注記2　“□□□”はキャンペーンページのURLのパスである。

図8　F-URLの例

〔Fアプリの脆弱性診断結果〕

A社は，セキュリティ専門会社のD社に依頼してFアプリの脆弱性診断を実施した。その結果，表1に示す脆弱性が検出された。

表1　脆弱性診断結果（抜粋）

脆弱性	脆弱性の概要	解説
1	サーバ証明書の検証不備がある。	Fアプリは，HTTPSでサーバと接続する際，サーバ証明書の検証エラーがあっても無視し，通信を続行する。そのため，HTTPS通信の内容が盗聴されたり，改ざんされたりするおそれがある。盗聴されると，①盗聴した内容からアクセスキーとストレージ名を攻撃者が取得するおそれがある。 （省略）
2	Cサービスのアクセスキーの保護に不備がある。	②攻撃者がFアプリから平文のアクセスキーとストレージ名を取得できる。そのアクセスキーを用いて，③攻撃者がEサービスの全利用者の写真を不正にダウンロードするおそれがある。 （省略）
3	F-URLの処理にアクセス制御の不備がある。	F-URLのurlクエリパラメータに，④細工したURLが指定されることによって，攻撃者のWebサイトにアクセスしてしまうおそれがある。また，攻撃者が会員の認証トークンを取得するおそれがある。 （省略）

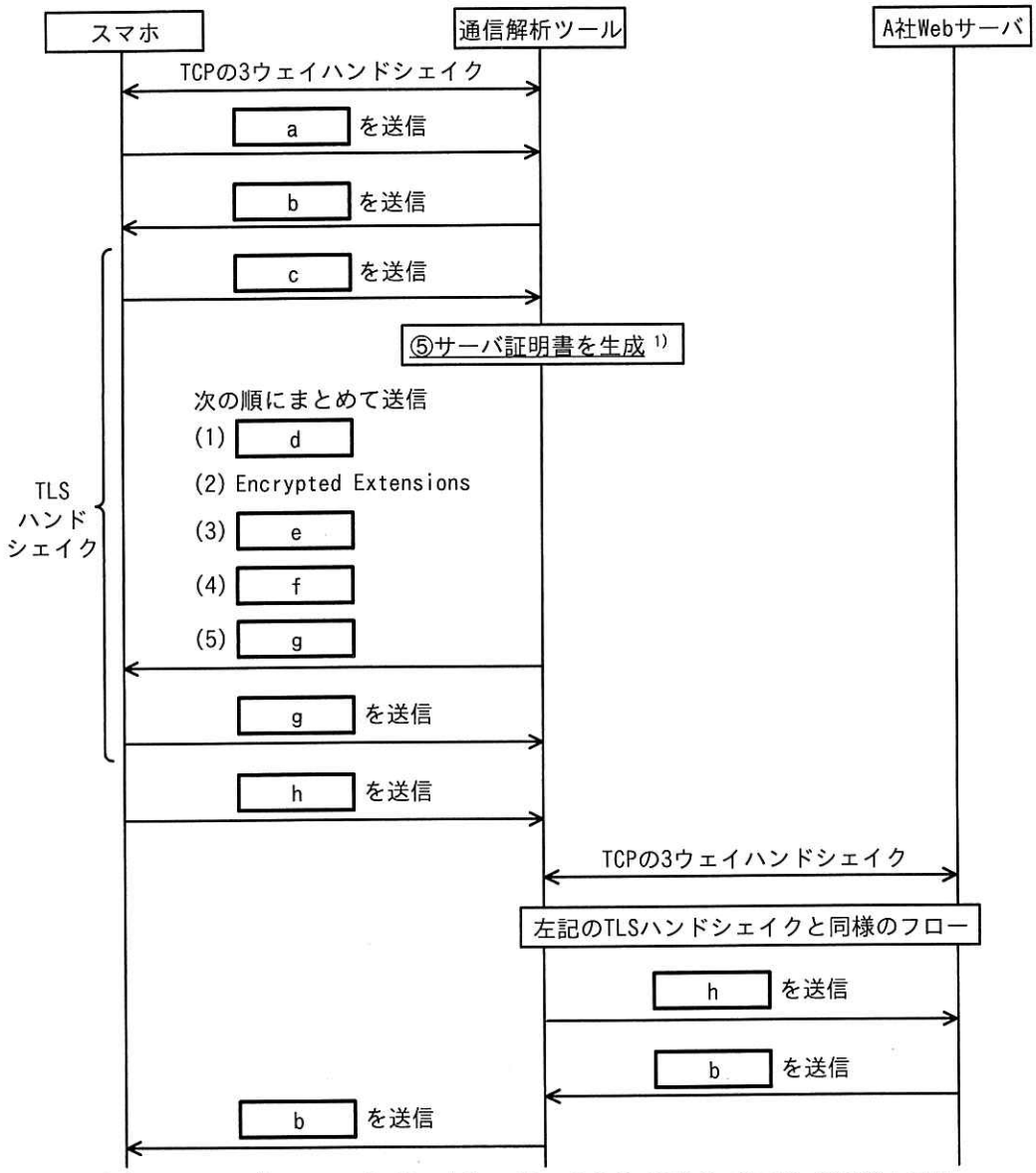
〔脆弱性1〕

Fアプリの開発チームに所属するUさんは，D社のSさんが開催する診断結果報告会に参加した。

Uさんは，脆弱性1が作り込まれた経緯を説明した。Uさんによると，FアプリとA社Webサーバとの間の通信内容に異常がないかどうかを調査するために，開発用PCで通信解析ツールを利用した。この通信解析ツールはプロキシサーバとして動作する。このツールを利用すると，Fアプリでは，サーバ証明書の検証エラーが発生し，FアプリとA社Webサーバとの間の通信が中断されてしまった。そこで，インターネット上のある記事でエラーが発生しても通信を続行する方法が紹介されていたのを

参考にして，F アプリのコードを変更したということであった。

この通信解析ツールを利用し，“https://www.a-sha.co.jp/campaign/□□□”にアクセスした際のレイヤー4～7 の通信フローの例を図 9 に示す。



注記　通信解析ツールのプライベート IP アドレスは，○○○.○○○.○○○.○○○とする。
注 1)　通信解析ツールは，自身のプライベート認証局機能を用いる。

図 9　通信解析ツールを利用した際の通信フローの例（抜粋）

U さんは，通信解析ツールを利用してテストを行う際も通信を正常に続行させる方

法をチーム内で話し合った。その結果，今後，開発用のスマホに⑥必要な設定を行うことにした。加えて，OS-αではテストを行う際だけその設定を有効化するように，Fアプリの中にも設定を追加した。

〔脆弱性2〕

脆弱性2への対応について，Sさんからは方式bを利用し，その際に署名付きURLの生成を図4中の［　i　］の時点で行ってはどうかとの提案があった。Uさんは Sさんの提案を了承した。

〔脆弱性3〕

次は，脆弱性3についてのUさんとSさんの会話である。

Uさん：対策として，図7の処理を修正します。

Sさん：図7の処理を修正すれば，認証トークンを盗まれるリスクは回避できます。しかし，Web ブラウザと比べると，⑦フィッシングサイトにアクセスしてしまっても気付くことができないというFアプリの仕様上の問題点が残ります。フィッシングサイトに気付くことができるようにするための機能か，そもそもフィッシングサイトにアクセスできないようにする機能が必要です。

Uさん：はい。図7の処理の修正に加えて，⑧フィッシングサイトにアクセスできないようにする機能を実装します。

A社は，検出された脆弱性を修正し，Eサービスの提供を開始した。

設問1　〔Fアプリの脆弱性診断結果〕について答えよ。

(1)　表1中の下線①について，アクセスキーを取得する方法を，具体的に答えよ。

(2)　表1中の下線②について，アクセスキーを取得する方法を，具体的に答えよ。

(3)　表1中の下線③について，ダウンロードする方法を，具体的に答えよ。

(4) 表 1 中の下線④について，攻撃者の Web サイトにアクセスさせることができるように細工した URL の例を，攻撃者が取得したドメイン名を k-sha.co.jp とした場合で答えよ。

設問２ 〔脆弱性 1〕について答えよ。

(1) 図 9 中の下線⑤について，サーバ証明書の Subject Alternative Name の値を，具体的に答えよ。

(2) 図 9 中の［ a ］～［ h ］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 Certificate

イ Certificate Verify

ウ Client Hello

エ CONNECT ○○○.○○○.○○○.○○○:443 HTTP/1.1

オ CONNECT www.a-sha.co.jp:443 HTTP/1.1

カ Finished

キ GET /campaign/□□□ HTTP/1.1

ク HTTP ステータスコード 101 (Switching Protocols)

ケ HTTP ステータスコード 200 (OK)

コ Server Hello

(3) 本文中の下線⑥について，設定の内容を，具体的に答えよ。

設問３ 本文中の［ i ］に入れる記号を，図 4 中の(あ)～(お)から選び，答えよ。

設問４ 〔脆弱性 3〕について答えよ。

(1) 本文中の下線⑦について，問題点を，20 字以内で答えよ。

(2) 本文中の下線⑧について，実装する機能を，具体的に答えよ。

問4　IT資産管理及び脆弱性管理に関する次の記述を読んで，設問に答えよ。

V社は，従業員3,000名の製造業である。東京に本社，大阪，名古屋，福岡に支社がある。V社は，J事業部，K事業部，情報システム部（以下，情シ部という），総務部，経理部などから成る。

V社の社内システム及びネットワークの運用並びに情報セキュリティ管理は，情シ部のB部長とS主任を含む8名の部員が担当している。V社のネットワーク構成を図1に示す。

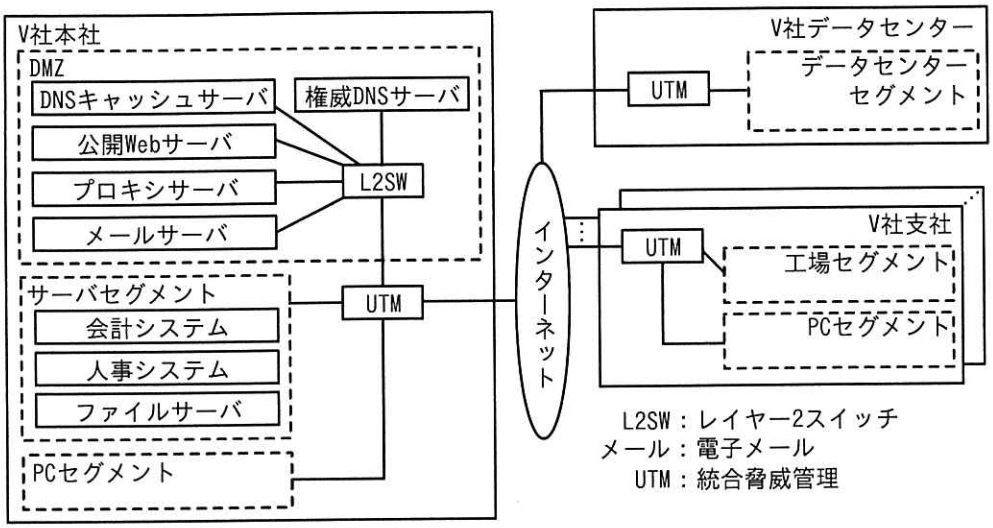


図1　V社のネットワーク構成

公開Webサーバでは，V社製品のキャンペーンなどを紹介している。V社本社と各支社及びV社データセンターの間はUTMのVPN機能を使用して通信を行っている。各支社には，UTMを除いてインターネットからアクセス可能なIT機器はない。

V社のIT資産管理，ドメイン名及びIPアドレスの管理，導入ソフトウェア（以下，ソフトウェアをSWという）の管理並びに脆弱性管理の現状を表1に示す。

表1　V社のIT資産管理，ドメイン名及びIPアドレスの管理，導入SWの管理並びに脆弱性管理の現状

項目	状況
IT資産管理	1. IT資産管理台帳に対して，IT資産の登録，更新及び削除を行う。 2. IT資産管理台帳は，全社で共有されている。 3. インターネットからアクセス可能な全てのIT資産を公開IT資産と定義する。 4. IT資産管理台帳の管理項目には，資産ID，資産名称，取得金額，管理部門名，管理者名，公開IT資産かどうかの区分，及びその他特記事項を含める。また，公開IT資産の場合はグローバルIPアドレス（以下，GIPという）[1]及びドメイン名も含める。 5. IT資産管理台帳への登録は次のように行っている。 (1) 情シ部が購入するIT資産は，情シ部がIT資産管理台帳に登録する。 (2) 事業部がV社データセンター又はV社DMZにサーバを設置する場合は，情シ部に設置申請し，承認を得た後に設置する。情シ部は承認後IT資産管理台帳に登録する。 (3) 事業部が他社データセンター，クラウドサービス又はレンタルサービスを契約して，サーバなどを利用する場合については，IT資産管理台帳に登録していない。 6. IT資産は，年1回の棚卸しで管理部門が現物確認する。その際に，管理部門がIT資産管理台帳を更新する。IT資産の廃棄は管理部門が実施し，その際に，管理部門がIT資産管理台帳を更新する。
ドメイン名及びIPアドレスの管理	1. V社データセンター及びV社本社で使用するIPアドレス及びドメイン名の管理は，次のように行っている。 (1) 情シ部が，“v-sha.co.jp”というドメイン名（以下，V社のドメイン名という）をレジストラのW社から取得し，V社データセンター，V社DMZなどにある公開IT資産に使用している。ドメイン名の使用料は情シ部が支払っている。JPRSが管理しているドメイン名の登録者情報の組織名にV社を，担当者情報の部署名に情シ部を，担当者名にS主任を登録している。 (2) GIPは，ISPのR社から割り当てられている。GIPの使用料は，情シ部が回線使用料と併せてR社に支払っている。JPNICの登録者情報の組織名にV社を，担当者情報の部署名に情シ部を，担当者名にS主任を登録している。 (3) 事業部がV社データセンター又はV社DMZにサーバなどを設置する場合は，情シ部にIPアドレス使用申請を行う。 (4) 事業部がV社のドメイン名を使用する場合は，情シ部にドメイン使用申請を行う。この際，情シ部は，必要なDNSレコードを登録している。 2. 事業部が他社データセンター，クラウドサービス又はレンタルサービスを契約し，新たなドメイン名を登録してサーバを利用する場合は，次のように行っている。 (1) GIPは，各サービス会社から割り当てられたものを使用している。 (2) ドメイン名は，各事業部が取得している。なお，使用するドメイン名は全て，トップレベルドメインが“.jp”のドメインを使用している。

表1　V社のIT資産管理，ドメイン名及びIPアドレスの管理，導入SWの管理並びに脆弱性管理の現状（続き）

項目	状況
導入SWの管理	1. PCに導入するSWは，IT資産管理ツール（以下，AMツールという）で管理しており，IT資産管理台帳には登録せず，PCの“資産ID”をAMツールに入力して管理している。 2. ビジネス上，重要なサーバに導入するSWは，AMツールで管理している。ビジネス上，重要ではないサーバに導入するSWは，主なものをIT資産管理台帳の“その他特記事項”に記入している。
脆弱性管理	1. サーバに導入したSWの脆弱性情報は，情シ部が脆弱性のニュースを毎日見て確認している。 2. 情シ部が，脆弱性のニュースで話題になった脆弱性情報全てを全部門に連絡している。 3. 連絡を受けた各部門が取捨選択し，必要に応じて対応している。

注[1)]　インターネットから当該IT資産にアクセスするときのGIPである。

最近，次のようなサイバー攻撃のニュースが報道された。

(1)　CVE-20XX-XXXXXというWebサーバでの通信の暗号化に関する脆弱性が公表され，それを悪用した攻撃で，ある広告代理店に大きな被害が発生した。

(2)　著名な会社が1年前，CDN事業者のサービスを利用してWebサーバを立ち上げ，1か月間商品のキャンペーンを行った。このWebサーバには，その会社のサブドメインを使用した。キャンペーン後すぐに，CDNサービスを解約したが，今になって，そのサブドメインが海外の会社の広告サイトとして使われていることが発覚した。

(3)　競合他社で，不要になったにもかかわらず公開されたままとなっていたWebサーバが改ざんされ，フィッシングに悪用されていることが発覚した。

これらを受けて，V社の経営層は，V社でも対策が必要だと考え，対策の検討と実施を情シ部に指示した。(2)については，V社でも，CDN事業者のサービスを利用してWebサーバを立ち上げてキャンペーンを行った後，CDNサービスを解約した経緯があったので，緊急に確認した。その結果，問題があることが分かり，①図1中のサーバの設定を変更した。この事態も踏まえて，公開IT資産管理及び脆弱性管理を見直すことにした。

〔公開IT資産管理及び脆弱性管理の目標の設定〕

情シ部のB部長とS主任は，まず，公開IT資産管理の現状を分析し，公開IT資産

管理及び脆弱性管理の主な目標を表2にまとめた。

表2　公開IT資産管理及び脆弱性管理の主な目標（抜粋）

目標	内容
K-1	IT資産管理台帳に公開IT資産を漏れなく登録する。具体的には，次のようなケースの登録漏れをなくす。 (1)　事業部がクラウドサービスを契約して利用している公開IT資産 （省略）
K-2	情シ部が，サーバの導入SWを一元管理する。
K-3	重要な脆弱性を事業部が修正したかどうかを情シ部が確認できるようにする。
K-4	利用が終了した公開IT資産について，必要な措置を漏れなく行う。

〔目標K-1の実現〕

まず，目標K-1について検討を行い，各事業部への未登録の公開IT資産の調査依頼を図2にまとめた。

次の未登録の公開IT資産を調査し，その一覧を回答すること
・クラウドサービスを契約して利用している公開IT資産
・［　a　］公開IT資産
・［　b　］公開IT資産

図2　事業部への調査依頼

次は，目標K-1の実現に関するB部長とS主任の会話である。

B部長：事業部への調査依頼だけでは漏れが出そうだ。情シ部としても調査すべきだが，どのような方法があるのか。

S主任：自分でインターネットをスキャンする方法（以下，オンアクセス型という）と，既に外部に構築されているデータベースを検索する方法（以下，検索エンジン型という）があります。

B部長：どちらの方がよいだろうか。

S主任：オンアクセス型では他社の環境に負荷を与える可能性があります。また，スキャンするには時間が掛かります。今回は検索エンジン型を使用したいと思います。

B部長：分かった。検索エンジン型だと，具体的には，どのような方法があり，どのような情報が収集できるのかな。

S主任：まず，IP アドレスの割当て，ドメイン名の登録などに関する情報をレジストラ又はレジストリに問い合わせることができます。そのための標準プロトコルとして，［ c ］が用意されており，RFC 3912 で定義されています。次に，Web ブラウザから利用できるサービスには，無償のものとして，ドメインの検索サービス（以下，X サービスという）と，GIP の検索サービス（以下，Y サービスという）があります。その他，一部有償になりますが，Z サービスというサービスなどがあります。X サービスで検索可能な情報を表 3 に，Y サービスで検索可能な情報を表 4 に，Z サービスで検索可能な情報を表 5 に示します。

表 3　X サービスで検索可能な情報（抜粋）

検索キーワード	検索可能な情報
組織名 [1]	登録されているドメイン名
ドメイン名	組織名，ドメイン名の担当者識別番号 [2]，ドメイン名を管理するネームサーバ名 [3]，登録年月日，接続年月日，最終更新日時など
ネームサーバ名	ネームサーバの IP アドレス，登録年月日，最終更新日時など
ドメイン名の担当者識別番号 [2]	ドメイン名の担当者名，メールアドレス，ドメイン名の部署名，電話番号など

注 [1]　検索キーワードとして入力した文字列が“組織名”とマッチした検索結果が全て得られる。
注 [2]　一部の“.jp”ドメインの場合だけ検索可能である。
注 [3]　セカンダリ DNS などが設置されている場合は，複数得られる。

表 4　Y サービスで検索可能な情報（抜粋）

検索キーワード	検索可能な情報
GIP	組織名，GIP の担当者識別番号，ネームサーバ名，割当て年月日，返却年月日，最終更新日時など
GIP の担当者識別番号	GIP の担当者名，メールアドレス，GIP の部署名，電話番号など

表 5　Z サービスで検索可能な情報（抜粋）

検索キーワード	検索可能な情報
ドメイン名，GIP，又は組織名	GIP，GIP 割当て元の事業者名，FQDN，位置情報（国名，都市名，緯度・経度），ポート番号，OS，応答メッセージ情報 [1]

注記 1　検索キーワードとして入力した文字列が，“ドメイン名”とマッチした検索結果が全て得られる。
注記 2　検索キーワードとして入力した文字列が，“GIP”とマッチした検索結果が全て得られる。
注記 3　検索キーワードとして入力した文字列が，“ドメイン名を取得した組織名”又は“GIP を取得した組織名”とマッチした検索結果が全て得られる。
注 [1]　製品名やバージョン情報，デフォルトパスワードの使用などである。

B 部長 ：当社が管理すべき公開 IT 資産をできるだけ多くリストアップしてほしい。

S 主任：事業部から提出されるリストと突合せができるように，当社が取得した GIP，ドメイン名，GIP の組織名，部署名及び担当者名，ドメイン名の組織名，部署名及び担当者名並びに FQDN を抽出してまとめたリスト（以下，F リストという）を作成してみます。F リストの作成手順を図 3 に示します。

手順 1：［あ］サービスを用い，検索キーワードとして［d］を入力して，検索し，検索結果として［e］及び［f］を得る。

手順 2-1：手順 1 の結果を基に，［い］サービスを用い，検索キーワードとして［g］を指定して，検索し，検索結果として［g］の組織名及び［g］の［h］を得る。

手順 2-2：手順 2-1 の結果を基に，［い］サービスを用い，検索キーワードとして［g］の［h］を指定して，検索し，検索結果として［g］の部署名及び［g］の担当者名を得る。

手順 3-1：手順 1 の結果を基に，［う］サービスを用い，検索キーワードとして［f］を指定して，検索し，検索結果として［f］の組織名及び［f］の［h］を得る。

手順 3-2：手順 3-1 の結果を基に，［う］サービスを用い，検索キーワードとして［f］の［h］を指定して，検索し，検索結果として［f］の部署名及び［f］の担当者名を得る。

手順 4：得られた検索結果から F リストをまとめる。

注記 1　手順 2-1～3-2 は，手順 1 で得られた検索結果のうち，“.jp” ドメインのものについて，それぞれ行う。

注記 2　手順 4 では，F リストの作成に必要な検索結果だけを選択する。

図 3　F リストの作成手順

〔V 社の管理すべき IT 資産の確認と管理の強化〕

事業部の提出した未登録の公開 IT 資産一覧と S 主任の調査結果を突合したところ，幾つか F リストだけにあるもの（以下，調査漏れという）が見つかった。次は，B 部長と S 主任の会話である。

B 部長 ：どのような調査漏れが見つかったのか。

S 主任 ：調査漏れのリストは表 6 のとおりです。事業部からの説明では，古いケース

で調査しきれなかったとのことでした。

表6　調査漏れのリスト（抜粋）

結果項番	GIP	GIP の部署名	ドメイン名の組織名	FQDN
結果 1	（省略）	V 社 G 事業部	V 社	sub1.v-sha-g.jp
結果 2	（省略）	V 社 H 部	P 協議会	（省略）

S 主任 ：表 6 の結果 1 については，SSH では接続できませんでしたが，公開サービスは Web だけが稼働しているようだということが，X，Y，Z サービス以外の②調査から分かりました。しかし，G 事業部はもはや存在しません。調べたところ，K 事業部が業務継承部門です。また，利用 OS や SW もバージョンが古く，多くの脆弱性が内在しているようだということが，③別の調査から分かりました。

攻撃を受けて被害が発生しないようにするために，④表 6 の結果 1 の公開 IT 資産を継続利用する場合としない場合のそれぞれの場合に K 事業部が行うべき具体的な対応方法を伝えます。

〔脆弱性管理の改善〕

次に，目標 K-2 及び目標 K-3 に対する実現方法を検討した。目標 K-2 については，S 主任が必要なルールを決めた。次は，目標 K-3 の実現方法についての B 部長と S 主任の会話である。

B 部長 ：目標 K-2 が実現できたとしても，次々発表される脆弱性に対して，対策の優先度などはどのように判断すればよいのか。

S 主任 ：脆弱性についての⑤CVSS の深刻度と⑥KEV カタログへの掲載の有無に基づいて判断するのがよいです。対策の優先度などの判断ルールを作成します。

B 部長 ：分かった。そのルールも踏まえ，目標 K-3 を実現するために，⑦表 1 の脆弱性管理の改善策を考えてほしい。

S 主任 ：分かりました。

さらに，目標 K-4 について，公開 IT 資産の利用終了時に行うべき措置を S 主任がまとめた。

経営層に対応策を説明し，了承を得た。その後，B 部長と S 主任が作成したルールに従って，V 社の公開 IT 資産管理及び脆弱性管理の運用が開始された。

設問 1　本文中の下線①について，設定を変更したサーバを，図 1 中から一つ選び，サーバ名を答えよ。また，その設定の変更内容を，30 字以内で具体的に答えよ。

設問 2　〔目標 K-1 の実現〕について答えよ。

(1)　図 2 中の［ a ］，［ b ］に入れる適切な内容を，それぞれ 30 字以内で答えよ。

(2)　本文中の［ c ］に入れる適切な字句を，英字 10 字以内で答えよ。

(3)　図 3 中の［ あ ］～［ う ］に入れる適切な文字を，X，Y，Z から選び，答えよ。

(4)　図 3 中の［ d ］～［ h ］に入れる適切な内容を，次の解答群の中から選び，記号で答えよ。

解答群

ア　FQDN	イ　GIP	ウ　GIP 割振り元の事業者名
エ　OS	オ　V 社	カ　位置情報
キ　担当者識別番号	ク　ドメイン名	ケ　ポート番号
コ　メールアドレス		

設問 3　〔V 社の管理すべき IT 資産の確認と管理の強化〕について答えよ。

(1)　本文中の下線②について，調査方法を，40 字以内で具体的に答えよ。

(2)　本文中の下線③について，調査方法を，40 字以内で具体的に答えよ。

(3)　本文中の下線④について，二つの場合における主な対応方法を，それぞれ 35 字以内で具体的に答えよ。

設問 4　〔脆弱性管理の改善〕について答えよ。

(1)　本文中の下線⑤について，CVSS の最新のバージョン番号を，4 字以内で答えよ。

(2) 本文中の下線⑥について，KEV カタログのフルスペルを，解答群の中から選び，記号で答えよ。

解答群

ア Key Exploited Vulnerabilities catalog

イ Key Exposure Vulnerabilities catalog

ウ Known Exploited Vulnerabilities catalog

エ Known Exposure Vulnerabilities catalog

(3) 本文中の下線⑥について，KEV カタログに掲載される脆弱性はどのようなものか。掲載される条件のうち主なものを，20 字以内で答えよ。

(4) 本文中の下線⑦について，表 1 の脆弱性管理の項番 1，2 の改善策を，項番 1 の改善策は 60 字以内で，項番 2 の改善策は 40 字以内でそれぞれ具体的に答えよ。

〔 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	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。