

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。

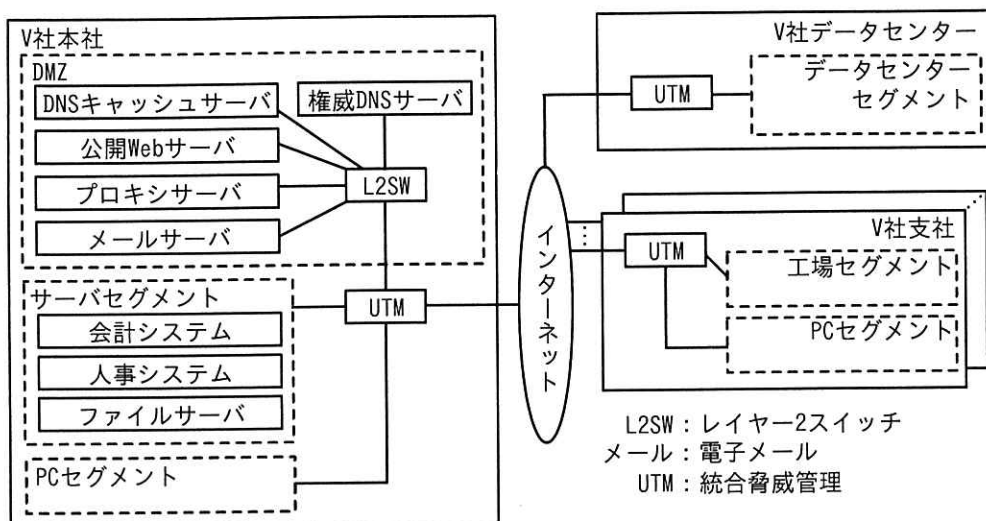


図1 V社のネットワーク構成

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時の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。

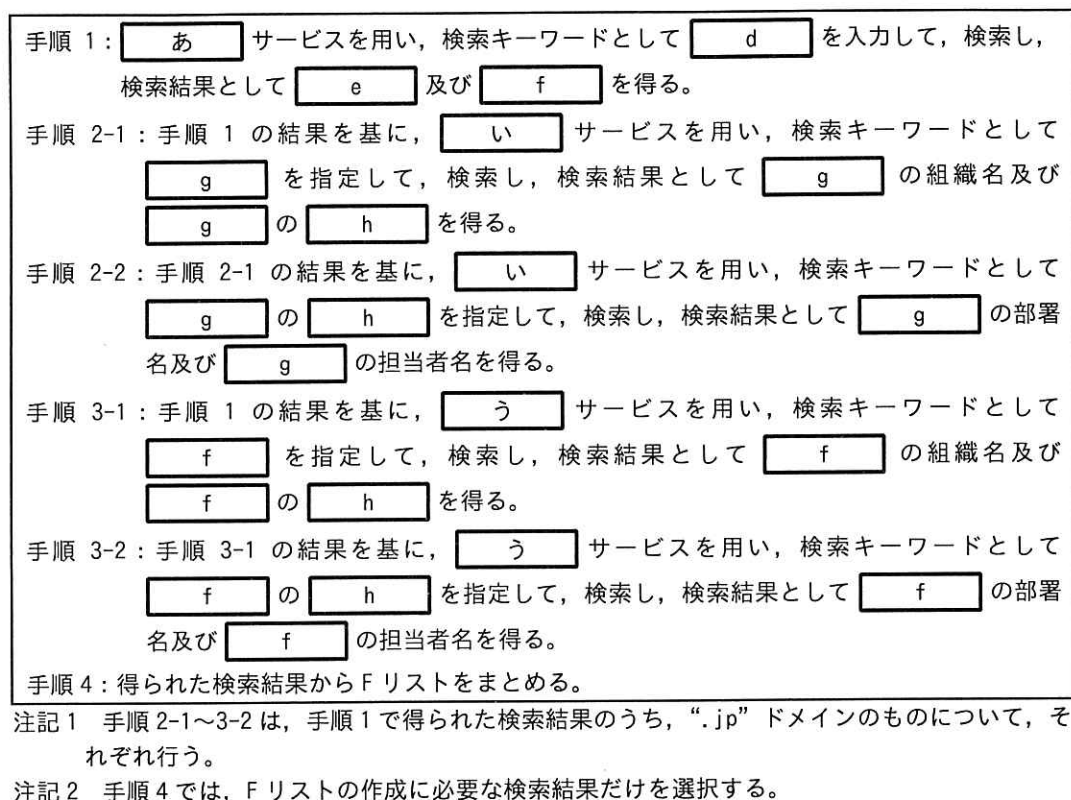


図 3 F リストの作成手順

〔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のが、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のが、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 , 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 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 ~ 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 ~ 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。