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〕

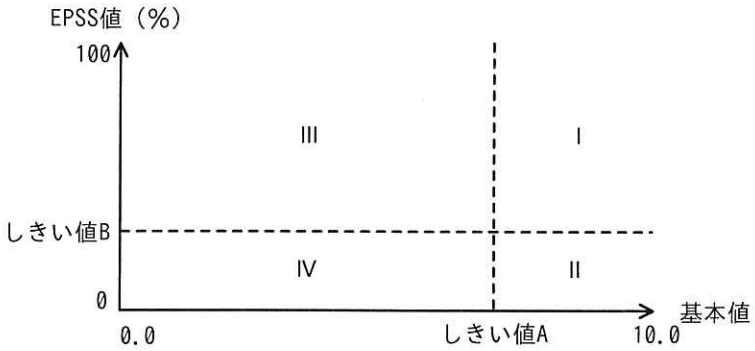
一斉診断が一段落したところで，情報システム部は脆弱性管理についての課題を議論した。対応の要否判断が不適切であったサイトや対応が遅すぎたサイトがあったので，J課長は，Eさんに新たな脆弱性評価方法を検討するよう指示した。

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。