問2　脆弱性対策に関する次の記述を読んで，設問1～5に答えよ。

A社は，従業員数3,000名の製造会社である。A社の組織構成は図1のとおりであり，全社を統括する経営管理本部，及び製品の製造・販売を行う三つの製品本部がある。三つの製品本部は，それぞれ取り扱う製品分野が異なっている。経営管理本部には，データセンタ部（以下，センタ部という），総務部などがある。

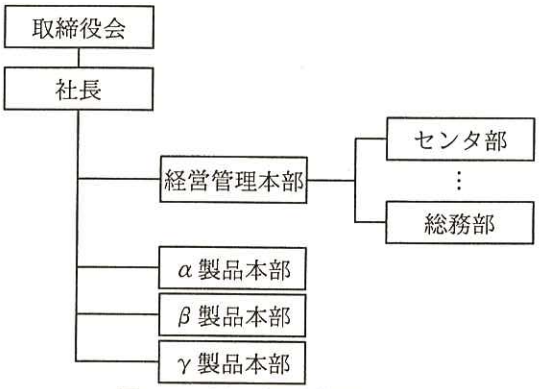
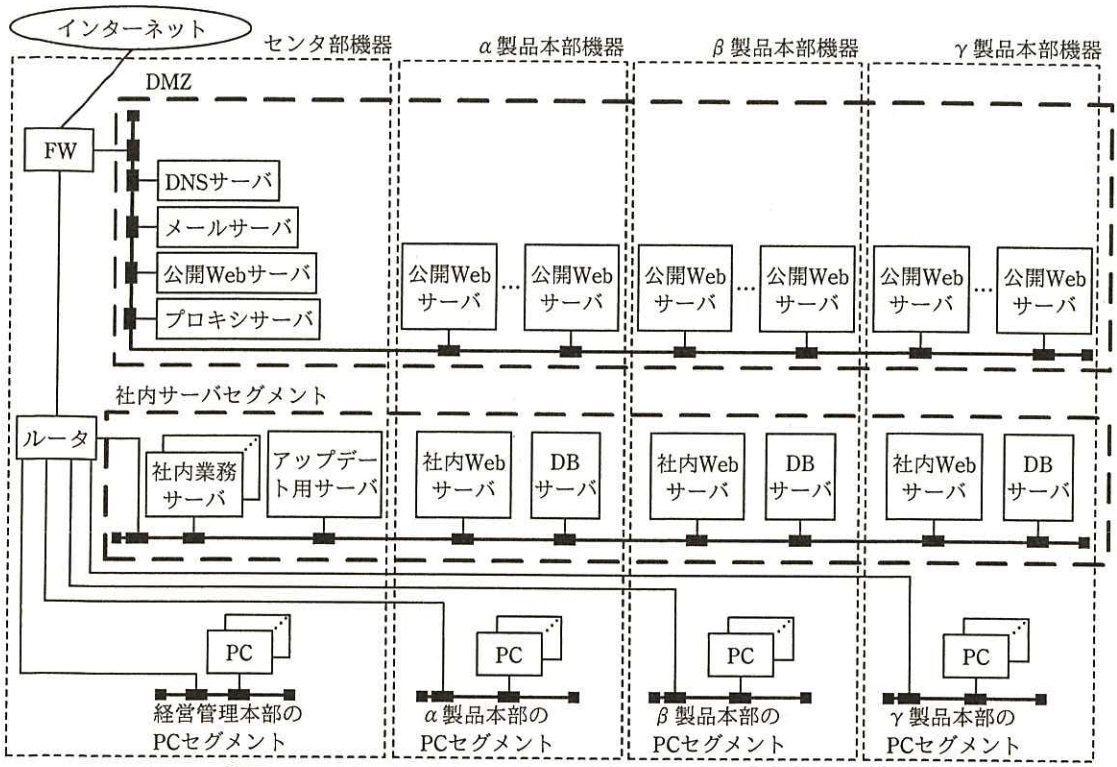


図1　A社の組織構成

〔A社の情報システムの構成〕

経営管理本部では，センタ部に所属する20名の運用担当者が，A社内で共同利用される機器群（以下，センタ部機器という）を運用している。各製品本部では，情報システム担当チームが，各製品本部が独自に導入している機器群（以下，製品本部機器という）を運用している。

A社の情報システムの構成は，図2のとおりである。



FW：ファイアウォール
DBサーバ：データベースサーバ
公開Webサーバ：会社情報提供用Webサーバ，広報用Webサーバ，一般消費者向けインターネット通販用Webサーバなどの社外に公開しているWebサーバ，及び社外の取引先と情報共有するためのWebサーバ
社内Webサーバ：社内での情報共有に利用する，社外に公開していないWebサーバ
社内業務サーバ：人事管理などの業務に利用するサーバ

図2　A社の情報システムの構成

各製品本部には，5～10台の公開Webサーバがある。

センタ部機器のアップデート用サーバは，社内で利用しているソフトウェアパッケージのセキュリティパッチ（以下，パッチという）を含む修正プログラムをインターネットからダウンロードし，格納している。

社内サーバセグメントと各PCセグメント上の機器からは，プロキシサーバを経由したインターネット上のWebサイトへのアクセスが許可されており，アップデート用サーバとPCにはプロキシサーバを経由するような設定がされている。一方，社内サーバセグメントと各PCセグメント上の機器からのプロキシサーバを経由しないインターネットへのアクセスは，FWによって禁止されている。アップデート用サーバからのアクセス先は，特定のベンダのサイトに限定されている。

〔脆弱性対策の立案〕

最近，国内外でソフトウェアの重大な脆弱性が数多く報告されており，それらの悪用によって，製造業の複数の企業でも被害が起きている。そのため，センタ部では，A社の情報システムについて，脆弱性対策を強化する必要があると考え，脆弱性対策方針案を作成し，取締役会に提案した。脆弱性対策方針案を図3に示す。

脆弱性対策を行うチーム（以下，Vチームという）を組織する。
Vチームは，脆弱性対策に関する次の業務を担当する。
1. 機器の特定及び重要度の決定
   脆弱性対策の対象となる機器を特定し，その重要度を決定する。
2. 脆弱性に関する情報（以下，脆弱性情報という）の収集と選別
   脆弱性情報を収集し，その中からA社の機器に影響する情報を選別する。
3. 脆弱性対策適用の判断
   A社の機器に影響する脆弱性情報について，機器の重要度レベルと脆弱性の影響度（以下，脆弱性レベルという）を勘案し，脆弱性対策適用の緊急度を判断する。
4. 脆弱性対策の実施
   脆弱性情報を各情報システム担当者に通知し，脆弱性対策適用を指示する。
5. 適用状況の確認
   脆弱性対策を各情報システム担当者が適切に適用できたかどうかを確認する。

図3　脆弱性対策方針案

取締役会は，この脆弱性対策方針案を了承し，センタ部が中心となってVチームを製品本部横断的に組織することを決定した。Vチームの責任者には，センタ部のP部長が任命された。P部長は，部下のQ主任をチームリーダに任命した。他にセンタ部の3名と各製品本部の情報システム担当チームから2名ずつの計9名（以下，Vチーム員という）から成るVチームを発足させた。Q主任の役割は，情報システムの脆弱性対策の立案，Vチーム員への指示，及び脆弱性対策の実施状況のP部長への報告である。

Q主任は，任命を受けてVチーム員を招集し，図3の業務を具体化するための協議をした。その中で，脆弱性対策適用の緊急度を機器ごとに判断するための基準（以下，脆弱性対策基準という）を作成した。脆弱性レベルの判断基準には，脆弱性情報に記載された共通脆弱性評価システム（CVSS）の基本値を利用することにした。Vチームが作成した脆弱性対策基準を図4に示す。

機器の特定及び重要度の決定には，総務部が半年ごとに固定資産の棚卸を実施して記載内容を更新している，固定資産管理台帳を利用することにした。この台帳に

は，個人情報又はその他の秘密情報（以下，重要情報という）の扱いの有無と，社外に対して公開しているか非公開としているかの区分が記載されている。各機器に搭載された OS，サーバソフトウェアやミドルウェアなどのソフトウェアの名称とバージョンは記載されていない。

1. 機器の重要度レベルの定義
機器ごとの重要度レベルを，次表によって高・低の 2 段階に分ける。

	重要情報を扱っている	重要情報を扱っていない
社外からアクセスできる	重要度レベル高	重要度レベル低
社外からアクセスできない	重要度レベル低	重要度レベル低

2. 脆弱性レベルの定義
脆弱性情報ごとに脆弱性レベルを，高・低の 2 段階に分ける。
・CVSS 基本値が 7.0 以上の脆弱性を脆弱性レベル高とする。
・それ以外は，脆弱性レベル低とする。

3. リスクレベルの定義
機器と脆弱性情報の組合せごとのリスクレベルを，次表によってリスクが低い順に 1・2・3 の 3 段階に分ける。

	重要度レベル高	重要度レベル低
脆弱性レベル高	リスクレベル 3	リスクレベル 2
脆弱性レベル低	リスクレベル 2	リスクレベル 1

4. 脆弱性対策適用の緊急度判断基準
リスクレベルに基づき，脆弱性対策適用の緊急度を判断する。
・リスクレベル 3 の場合は，直ちに脆弱性対策を実施する。
・リスクレベル 2 の場合は，次回のシステム保守時に脆弱性対策を実施する。
・リスクレベル 1 の場合は，今後の追加情報に注意して経過を見守る。
脆弱性対策については，脆弱性情報にパッチや回避策の記載がある場合には，その適用方法を検討する。脆弱性情報に脆弱性対策の記載がない場合には，何らかの対策を検討する。

図 4　脆弱性対策基準

〔脆弱性の公表と対応〕

脆弱性対策基準の運用を開始して間もなく，ある Web アプリケーションのソフトウェアパッケージ（以下，ソフトウェア M という）のバージョン Z に SQL インジェクションの脆弱性（以下，X 脆弱性という）があり，パッチが提供されているという情報が公表された。CVSS 基本値は 6.5 であった。Q 主任は，A 社の機器にソフトウェア M が導入されているかどうかが分からなかった。そこで，V チーム員に次の対応を指示した。

・固定資産管理台帳に記載がある機器について，ソフトウェア M を導入しているか

どうかを調査すること

・導入している機器について，X 脆弱性に対する脆弱性対策適用の緊急度を判断すること

V チーム員は，ソフトウェア M を導入しているかどうかの確認に手間取り，1 週間後に Q 主任に調査結果を報告した。ソフトウェア M を導入した機器はないとの調査結果だったので，Q 主任は，X 脆弱性への対応を終了し，P 部長に報告した。ところがその 2 週間後，α製品本部の V チーム員から，①社外の取引先と重要情報を共有するための公開 Web サーバにソフトウェア M のバージョン Z が導入されていることが分かり，対応したとの報告が入った。

当初の調査に見落としがあったことを問題視し，Q 主任は，α製品本部の V チーム員に見落としの原因を調べさせた。原因は，当該機器が先月導入されたばかりで，固定資産管理台帳に記載がなかったことにあった。Q 主任は，V チーム員に対して，固定資産の棚卸以降に導入された機器がないかの確認を指示した。他に見落とした機器はなかったことが分かり，Q 主任は P 部長に報告した。

報告を受けた P 部長は，当初の調査のような見落としの再発防止策を検討するよう Q 主任に指示した。Q 主任は，まず，固定資産管理台帳を基に，機器の新たな管理台帳（以下，新台帳という）を V チームで作成することにした。②新台帳にはバージョンを含むソフトウェアの情報も記載することにした。また，機器の新規導入や構成変更の際には，新台帳を速やかに修正する手順にした。Q 主任は，これらの改善策について P 部長に報告し，承認を得て実施した。

〔新たな脆弱性の公表と対応〕

改善策を実施して 1 か月後，UNIX / Linux で利用される shell の一つである bash に重大な脆弱性（以下，Y 脆弱性という）が存在するという脆弱性情報が公表された。CVSS 基本値は 10.0 であった。Y 脆弱性の概要は次のとおりである。

Y 脆弱性が存在する bash では，環境変数の値が“() {”という文字列で始まる場合，関数として解釈され，実行することができる。例えば，図 5 のように，export コマンドを使って環境変数として TEST1 を設定し，bash で呼び出すと“echo test”が実行される。

```
export TEST1='() { echo test; }'
bash -c TEST1
```

図5　bashにおける環境変数の設定とその利用の例

Y脆弱性は，例えば，図6のように環境変数としてTEST2を設定すると，bashを起動しただけで，TEST2を呼び出さなくても，bashが起動されて環境変数を引き継ぐ際，区切り文字“;”の後に書かれたコマンドを実行してしまうというものである。図6の例では，catコマンドが実行されてしまい，ファイル/etc/passwdが表示される。

```
export TEST2='() { echo test; }; /usr/bin/cat /etc/passwd'
bash
```

図6　Y脆弱性の確認例

Webサーバにおいても，③ある条件を満たす場合には，このY脆弱性を悪用される。図7は，CGIを利用した，あるWebアプリケーションプログラム（以下，Webアプリ Bという）が呼び出される際のフローである。

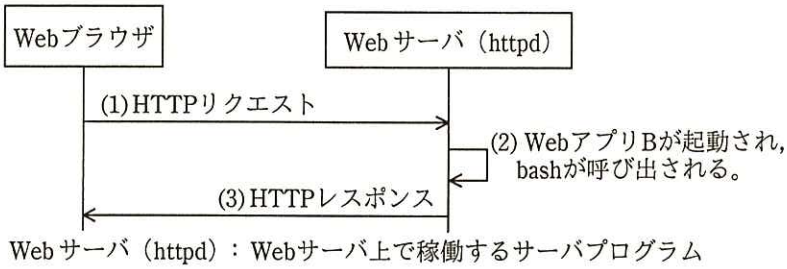


図7　Webアプリ Bに対するアクセスのフロー

典型的なWebサーバでは，Webサーバ（httpd）が［　a　］ヘッダの④フィールド値を環境変数として設定してからWebアプリ Bを起動するので，攻撃者は，Y脆弱性を悪用してWebサーバで任意のコードを実行することができる。例えば，図6の例と同様の場合であれば，catコマンドが実行され，このとき，catコマンドの実行時の権限によっては，攻撃者にどのようなファイルでも参照されてしまう。

Q主任は，直ちにY脆弱性への対応を開始した。新台帳を基に，Y脆弱性が影響する機器があるかをVチーム員が確認したところ，公開Webサーバのうち，重要度レベル高のサーバ8台と重要度レベル低のサーバ5台が該当していることが分かった。

Y 脆弱性が悪用されると公開 Web サーバが改ざんされるおそれもあり，事態を重く受け止めた Q 主任は，重要度レベル高のサーバだけでなく，該当する重要度レベル低のサーバ 5 台に対しても直ちに脆弱性対策を適用するよう V チーム員に指示した。

〔WAF による脆弱性対策〕

Y 脆弱性への対応指示に対して，β製品本部の V チーム員からは，β製品本部機器は，パッチの適用作業に 1 か月が必要なので，代替策を検討する必要があるとの報告を受けた。V チームでは，シグネチャによる［ b ］という手法で攻撃を検知できる Web アプリケーションファイアウォール（WAF）が代替策になるかどうか，セキュリティベンダの G 氏に相談することにした。

G 氏によれば，WAF による対応は，サーバへのパッチ適用に比べて，⑤対策を実施するまでの期間が短いといわれており，Y 脆弱性への対応も既に可能になっているとのことであった。そこで，Q 主任は，WAF の導入について，導入形態が異なる表 1 のような 2 案を作成した。

表 1　WAF の導入案

案	導入形態	概要
案 1	オンプレミス型	・WAF は，センタ部機器として購入し，A 社内に設置する。 ・設定とログ解析は，セキュリティ専門業者に委託する。 ・通信量の上限は，導入機器の性能によって制限される。
案 2	クラウド型	・WAF は，サービス事業者に設置されたものを利用する。 ・設定とログ解析は，サービス事業者が実施する。 ・図 2 中の機器のうち，［ c ］サーバにおいて，サービス事業者の指示どおりに次のように設定する。 －［ d ］レコードにおいて，公開 Web サーバの別名としてサービス事業者に指定された FQDN を記述する。 －（省略） ・通信量の上限は，サービス利用契約を随時変更し，切り替えることができる。

β製品本部の Y 脆弱性がある公開 Web サーバには，新製品の発表時などに，購入希望者からのアクセスが通常時の 100 倍程度まで一時的に増大するものがあり，かつ，次の新製品発表が 3 週間後に予定されている。このため，Q 主任は，案 2 を選び，⑥クラウド型の WAF を 1 週間後に導入し，β製品本部での Y 脆弱性に対する代替策

とする案をP部長に提案した。P部長は，この提案を承認し，センタ部に作業を指示した。

〔Y脆弱性への追加対応〕

WAF導入後，β製品本部でのサーバへのパッチ適用前のある日，Y脆弱性について，社外から直接はアクセスできない機器も社外から攻撃を受ける可能性があるという追加情報（以下，Y追加情報という）が公表された。A社の情報システムの構成では，FWによって社外から社内Webサーバへのアクセスを防いでいる。しかし，Y追加情報によれば，図8に示すような，社外から社内Webサーバに対するY脆弱性を悪用した攻撃が考えられるという。

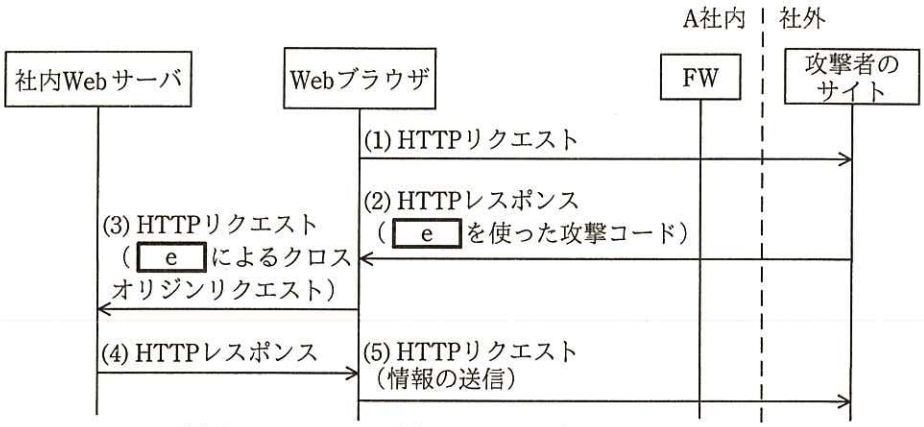


図8　社内Webサーバに対するY脆弱性を悪用した攻撃

次の条件1～3が全て成立すると，この攻撃は，成功する可能性がある。

条件1　攻撃者が［　f　］を知ることができ，その情報を図8の(2)の攻撃コードに組み込むことができること

条件2　社内Webサーバにおいて，CGIを利用したWebアプリケーションプログラムが，bashを呼び出すこと

条件3　図8の(4)のHTTPレスポンスにヘッダとして［　g　］が付加されていること

A 社内の Web ブラウザが攻撃者のサイトにアクセスしてしまうと，［ e ］を使った攻撃コードがダウンロードされ，実行される。攻撃コードが実行されたとしても，条件 3 が成立していない場合，現在 A 社で利用を許可している Web ブラウザでは，［ h ］ポリシによって，攻撃コードが社内 Web サーバからの HTTP レスポンスを読み取ることはできない。しかし，条件 3 が成立している場合，攻撃コードが社内 Web サーバからの HTTP レスポンスを読み取ることができ，その内容を攻撃者のサイトへ送信することで，社内 Web サーバに対する攻撃が成功する。

A 社では，社内 Web サーバは，クロスオリジンリクエストに対する図 8 中の(4)の HTTP レスポンスに，ヘッダとして［ g ］を付加していないことが調査の結果分かった。このため，Q 主任は，社内 Web サーバ上のデータが操作される可能性はあるものの，Web ブラウザ経由で情報が攻撃者のサイトに送信される可能性は低いと判断した。

Q 主任は，Y 追加情報による対策の変更は必要ないことを P 部長に報告した。P 部長は，念のため社外のセキュリティ専門業者の F 氏にレビューを依頼するよう Q 主任に指示した。

Q 主任から説明を受け，F 氏は，攻撃者が A 社のプロキシサーバを利用するために必要な情報を知ることができた場合には，図 8 中の(4)，(5)とは別の手法を用いることで，社内 Web サーバの情報が攻撃者のサイトに送信されるおそれがあると指摘した。そして，F 氏は，⑦どのような機能をもつ OS コマンドが社内 Web サーバで利用できる場合に，それが可能かを説明した。Q 主任は，直ちに対策する必要があると P 部長に報告した。P 部長は，対策を追加するとともに，Y 脆弱性への対応を振り返ると，脆弱性レベル高の脆弱性については，重要度レベル低の機器であっても，直ちに脆弱性対策を実施すべき場合があるとして，Q 主任に脆弱性対策基準の見直しを指示した。

〔脆弱性対策基準の見直し〕

Q 主任は，重要情報を扱ってはいないが社外からアクセスできる機器，及び社外からアクセスできないが重要情報を扱っている機器も，場合によっては直ちに脆弱性に対応する必要があると考えた。ただし，情報システム担当者の作業負荷の観点から，図 4 において対策が不要となる機器については，引き続き，対策を行わずに済

むようにしたい。そこで，脆弱性対策基準の中の“4. 脆弱性対策適用の緊急度判断基準”の修正案（図9）を作成した。

4. 脆弱性対策適用の緊急度判断基準
リスクレベルに基づき，脆弱性対策適用の緊急度を判断する。
・リスクレベル3の場合は，直ちに脆弱性対策を実施する。
・リスクレベル2の場合は，次回のシステム保守時に脆弱性対策を実施する。ただし，Vチームが機器ごとに緊急度を評価し，その結果，緊急度が高いと判断された場合は，リスクレベル3と同じく，直ちに脆弱性対策を実施する。
・リスクレベル1の場合は，今後の追加情報に注意して経過を見守る。
脆弱性対策については，脆弱性情報にパッチや回避策の記載がある場合には，その適用方法を検討する。脆弱性情報に脆弱性対策の記載がない場合には，何らかの対策を検討する。

図9　脆弱性対策基準の修正案

この修正案について，F氏は，⑧Vチームによる評価が必要な場合の数を減らすことができると指摘した。Q主任による修正案（図9）の代わりとして，F氏は，次の2点を提案した。

・重要度レベルの定義を修正する。
・リスクレベルの定義を修正する。

Q主任は，この提案を基に，脆弱性対策基準の別の修正案を作成した。修正箇所を図10に示す。

1. 機器の重要度レベルの定義
機器ごとの重要度レベルを，次表によって高・中・低の3段階に分ける。

	重要情報を扱っている	重要情報を扱っていない
社外からアクセスできる	重要度レベル高	重要度レベル［ i ］
社外からアクセスできない	重要度レベル中	重要度レベル低

3. リスクレベルの定義
機器と脆弱性情報の組合せごとのリスクレベルを，次表によってリスクが低い順に1・2・3の3段階に分ける。

	重要度レベル高	重要度レベル中	重要度レベル低
脆弱性レベル高	リスクレベル3	リスクレベル2又は3[1)]	リスクレベル2
脆弱性レベル低	リスクレベル2	リスクレベル1	リスクレベル1

注 1)　Vチームが機器ごとにリスクを評価し，その結果，［ j ］というリスク又は［ k ］というリスクが高いと判断された場合は，リスクレベル3とする。

図10　脆弱性対策基準の修正箇所

Q 主任は，脆弱性対策基準の修正箇所を P 部長に説明し，承認を得た。承認された脆弱性対策基準は，即時，V チーム内に周知された。その後，WAF の導入を含む対応作業も完了し，Y 脆弱性対応が終結した。

設問1　〔脆弱性の公表と対応〕について，(1)，(2)に答えよ。

(1) 本文中の下線①について，公開 Web サーバに対する X 脆弱性の適切なリスクレベルを，図 4 の脆弱性対策基準に基づき判断し，解答群の中から選び，記号で答えよ。

解答群

ア　該当しない　　イ　リスクレベル 1

ウ　リスクレベル 2　　エ　リスクレベル 3

(2) 本文中の下線②について，記載する目的は何か。45 字以内で述べよ。

設問2　〔新たな脆弱性の公表と対応〕について，(1)～(4)に答えよ。

(1) 本文中の下線③について，必要な条件を解答群の中から選び，記号で答えよ。

解答群

ア　HTTP の通信が TLS で暗号化されていないこと

イ　HTTP の通信が TLS で暗号化されていること

ウ　Web サーバに Y 脆弱性がある bash が導入されていること

エ　Web ブラウザが Cookie を受け入れないように設定されていること

オ　Web ブラウザが Cookie を受け入れるように設定されていること

(2) 図 7 について，Web サーバ（httpd）に対して Y 脆弱性を悪用され，図 6 の例と同様に cat コマンドが実行されたとき，どのような権限で，cat コマンドが実行されるか。解答群の中から選び，記号で答えよ。

解答群

ア　bash の所有者の権限

イ　cat コマンドの所有者の権限

ウ　Web アプリ B の実行時の権限

エ　Web ブラウザの実行時の権限

(3) 本文中の［　a　］に入れる適切な字句を，10 字以内で答えよ。

(4) 本文中の下線④について，図 7 中の Web サーバ（httpd）に対して Y 脆弱性を悪用された場合，ファイル /etc/passwd を不正に参照されるときにフィールド値として指定される文字列を答えよ。ここで，cat コマンドはディレクトリ /usr/bin 下にあるものとする。

設問３　〔WAF による脆弱性対策〕について，(1)～(4)に答えよ。

(1) 本文中の［ b ］に入れる WAF の攻撃検知手法を，15 字以内で答えよ。

(2) 本文中の下線⑤について，期間が短い理由を検証作業の観点から 40 字以内で述べよ。

(3) 表 1 中の［ c ］，［ d ］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 bash　イ CNAME　ウ DNS　エ HINFO

オ MX　カ 公開 Web　キ 社内 Web　ク メール

(4) 本文中の下線⑥について，Q 主任がオンプレミス型ではなくクラウド型を選ぶ根拠となったクラウド型の利点を，50 字以内で述べよ。

設問４　〔Y 脆弱性への追加対応〕について，(1)～(3)に答えよ。

(1) 本文中の［ f ］に入れる適切な字句を，20 字以内で答えよ。

(2) 図 8 中及び本文中の［ e ］，［ g ］及び［ 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 Access-Control-Allow-Origin　イ Canvas

ウ HSTS　エ X-Forwarded-For

オ XMLHttpRequest（XHR）　カ 情報セキュリティ

キ 同一生成元　ク プライベートブラウジング

(3) 本文中の下線⑦について，どのような機能がこれに該当するか。30 字以内で具体的に述べよ。

設問5　〔脆弱性対策基準の見直し〕について，(1)～(3)に答えよ。

(1)　図10中の［　i　］に入れる適切な字句を答えよ。

(2)　本文中の下線⑧について，図9の案ではリスクレベルの評価を行わなければならないが，図10では行わなくて済むのはどのような場合か。解答群の中から全て選び，記号で答えよ。

解答群

記号	重要情報の扱い	社外からのアクセス	脆弱性レベル
ア	扱っていない	できない	高
イ	扱っていない	できない	低
ウ	扱っていない	できる	高
エ	扱っていない	できる	低
オ	扱っている	できない	高
カ	扱っている	できない	低
キ	扱っている	できる	高
ク	扱っている	できる	低

(3)　図10中の［　j　］，［　k　］に入れる適切な字句をそれぞれ15字以内で答えよ。