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。

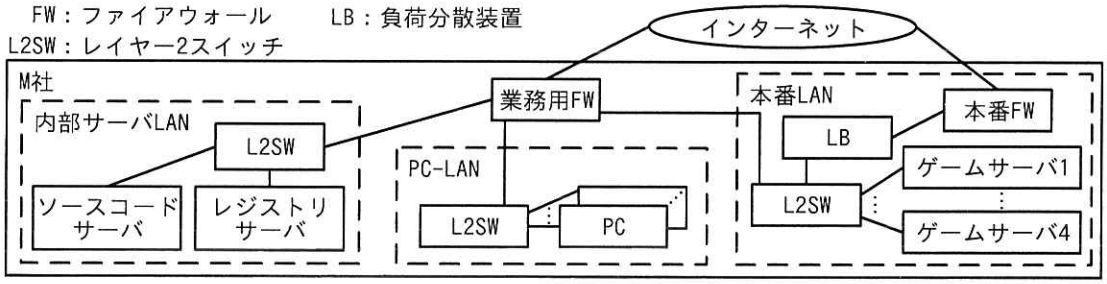

図 1　M 社のネットワーク構成（抜粋）

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