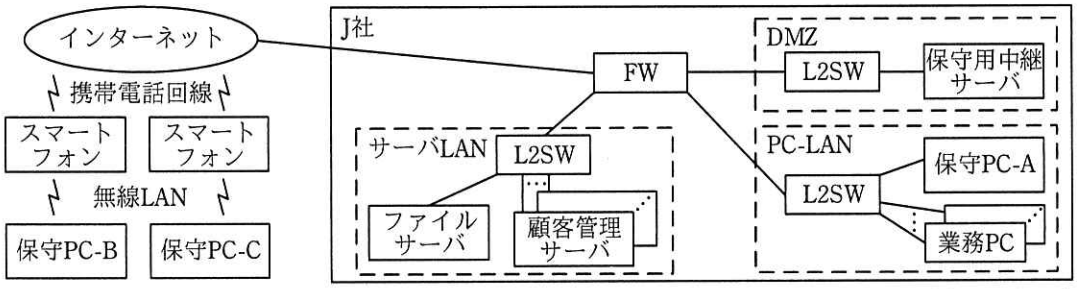
問1　セキュリティインシデントに関する次の記述を読んで，設問1～3に答えよ。

J社は，従業員1,000名の小売業である。J社では，顧客情報を顧客管理サーバで管理している。J社のネットワーク構成を図1に示す。



FW：ステートフルパケットインスペクション型ファイアウォール　　L2SW：レイヤ2スイッチ
保守PC：顧客管理サーバの保守作業に使うPC
注記1　保守PC-A及びサーバLAN上のサーバには，固定のプライベートIPアドレスを割り当てている。
注記2　DMZ上のサーバには，固定のグローバルIPアドレスを割り当てている。

図1　J社ネットワーク構成（抜粋）

〔顧客管理サーバの保守方法〕

顧客管理サーバの保守作業は，図2に示す保守方法に従って行われる。

顧客管理サーバの保守はM社に委託している。M社の保守員2名（以下，保守員1，保守員2という）が，通常は保守PC-Aから，必要に応じて保守PC-B又は保守PC-Cから保守を行っている。

保守PC-A

・未使用時はロッカーに保管している。

保守PC-B，保守PC-C

・M社が保守員ごとに貸与する。

接続経路と接続方法

・保守PCのいずれかから保守用中継サーバにSSH接続し，さらに，保守用中継サーバから顧客管理サーバにSSH接続する。

・保守PC-B及び保守PC-Cは，M社が貸与するスマートフォンでテザリングし，インターネットに接続する。固定のグローバルIPアドレスは付与されない。

保守用中継サーバに初めてSSH接続する際の接続先確認方法

1. 保守員が保守PC-B又は保守PC-CをJ社に持参する。
2. 保守PC-B又は保守PC-Cをスマートフォンでテザリングし，インターネット経由で保守用中継サーバにSSH接続する。
3. 接続したサーバのフィンガプリントが表示されるので，保守員はJ社のシステム管理者が紙に印刷しておいた保守用中継サーバのフィンガプリントと一致することを確認する。
4. 一致する場合は，次の確認メッセージに対して“yes”を選択する。
   “Are you sure you want to continue connecting (yes/no)?”
5. 当該接続先確認の手順が正常に完了すると，次回以降は確認メッセージが表示されなくなる。もし，SSH接続する際に警告メッセージが表示され，接続が切断された場合，保守用中継サーバのフィンガプリントが変わったか，[a] という状況が想定されるので，J社に確認する。

識別・認証・認可方法

a. 保守用中継サーバ

・保守員の着任時に，利用者IDとして，保守員1にはop1，保守員2にはop2を割り当てる。

・①当該利用者IDには，一般利用者の権限を与える。

・パスワード認証を行う。パスワードは保守員自身が設定する。

・保守員の離任時，パスワードをJ社のシステム管理者が変更する。

b. 顧客管理サーバ

・保守員の着任時に，保守用中継サーバの利用者IDと同じ名称のop1，op2を割り当てる。

・当該利用者IDには，特権利用者の権限を与える。

・パスワード認証を行う。パスワードはJ社のシステム管理者が設定し，安全な方法で保守員に伝える。

・保守員の離任時，パスワードをJ社のシステム管理者が変更する。

ログ

・SSH認証について，成功と失敗が接続先のサーバ上にSSH認証ログとして記録される。

・保守用中継サーバでのコマンド実行及びその結果，並びに顧客管理サーバでのコマンド実行及びその結果が，保守用中継サーバ上に操作ログとして記録される。

・SSH認証ログ及び操作ログへのアクセスには特権利用者の権限が必要であり，それらのログの確認はJ社のシステム管理者が実施する。

備考

・保守員は，保守作業に当たってJ社への事前申請及び事後の作業報告が必要である。

図2　顧客管理サーバの保守方法

FWのフィルタリングルールを表1に示す。

表1　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	ログの記録
1	PC-LAN	インターネット	HTTP，HTTPS	許可	する
2	PC-LAN	サーバLAN	HTTP，HTTPS，SMB	許可	する
3	b	保守用中継サーバ	SSH	許可	する
4	c	保守用中継サーバ	SSH	拒否[1]	する
5	保守用中継サーバ	顧客管理サーバ[2]	SSH	許可	する
6	DMZ	インターネット	全て	拒否	する
⋮	⋮	⋮	⋮	⋮	⋮
15	全て	全て	全て	拒否	しない

注記1　項番が小さいルールから順に，最初に合致したルールが適用される。
注記2　項番7～14には，保守用中継サーバ，DMZ，SSHに関するルールはない。
注[1]　保守PC-B又は保守PC-Cからの保守作業の際は，事前申請に記載された作業時間帯だけ，J社のシステム管理者が“許可”に変更する。
[2]　複数台の顧客管理サーバそれぞれのIPアドレスが指定されている。

〔セキュリティインシデントの発生と対応〕

6月16日に，J社のシステム管理者であるFさんが，FWのフィルタリングルールに基づいて記録されたログ（以下，FWログという）から不審なログを発見した。調査したところ，暗号資産を採掘するプログラム（以下，プログラムHという）が保守用中継サーバで動作しており，②定期的にインターネット上のサーバに通信を試みていたことが分かった。そこで，外部の情報処理安全確保支援士（登録セキスペ）のS氏の助言の下，影響範囲及び原因の調査並びに対策方法の検討をすることにした。S氏からは，保守作業関連書類，FWログ，SSH認証ログ及び操作ログの調査並びに保守員へのヒアリングをするように助言があった。

翌日，Fさんは，S氏に図3に示す保守作業関連書類及び各種ログの調査結果並びに図4に示すヒアリング結果を報告した。

事前申請及びFWの設定変更
・保守員2から，顧客管理サーバの保守を，保守PC-Cを使って6月14日7時から9時30分に行うという事前申請が出されていた。事前申請に従って，J社のシステム管理者はFWの設定を変更した。
FWログの調査結果
・申請された保守作業時間帯に，二つのグローバルIPアドレスから保守用中継サーバにSSH接続されていた。
操作ログの調査結果
・6月14日8時に，op1がプログラムHを設置した。
・6月14日7時20分から9時10分の間に，op2による顧客管理サーバの保守作業の操作が行われた。操作内容は事前申請のとおりだった。
保守用中継サーバ上のSSH認証ログの調査結果
・op1は6月14日7時30分から認証の失敗が84回続き，7時40分に認証に成功していた。
・op2は6月14日7時20分に認証に成功していた。
保守作業報告
・保守員2から，6月14日7時20分から9時10分の保守作業について報告されていた。

図3　保守作業関連書類及び各種ログの調査結果

6月14日の保守作業に関するヒアリング結果
・保守員1からは，保守作業は実施していないと回答があった。
・保守員2からは，保守PC-Cを使い事前申請どおりに作業を行い，ほかの作業はしていないと回答があった。事前申請，操作ログ及び事後の作業報告と矛盾する回答はなかった。
そのほかの調査結果
・op1に設定されているパスワードが，推測の容易な文字列であることが分かった。

図4　保守員へのヒアリング結果

S氏は，この報告から，第三者がop1のパスワードを推測してインターネット経由で不正アクセスした可能性が高いと判断し，被害範囲の特定のために各種ログを追加調査するように助言した。Fさんによる追加調査の結果，FWログ，SSH認証ログ及び操作ログからは，保守用中継サーバにプログラムHを設置した記録は見つかったが，保守用中継サーバから顧客管理サーバを含む他機器へのアクセスの記録は見つからなかった。FさんとS氏は，これらの調査結果から，影響範囲は保守用中継サーバだけにとどまり，情報漏えいの被害もなかったと結論付けた。

〔セキュリティインシデントの再発防止〕

S氏から，今回のセキュリティインシデントの再発防止について，幾つか提言があった。

一つ目の提言は，サーバに対する認証の強化である。保守用中継サーバ及び顧客管理サーバへの SSH 接続の認証方式を，パスワード認証から公開鍵認証に変更するというものである。F さんは，図 5 に示す公開鍵認証の初期登録手順を作成した。

保守用中継サーバへの SSH 接続に用いる公開鍵認証の初期登録手順
・公開鍵認証に使う鍵ペアは，各保守員が保守 PC ごとに作成し，管理する。
・③鍵ペアの秘密鍵には，十分な強度のパスフレーズを設定する。
・公開鍵は，J 社のシステム管理者が保守用中継サーバに登録する。
・SSH サーバの設定では，公開鍵認証を有効にするとともに，［ d ］を無効にする。

図 5　公開鍵認証の初期登録手順（抜粋）

次は，図 5 に関する S 氏と F さんの会話である。

S 氏　：万一，保守用中継サーバが不正アクセスされた場合を想定して，顧客管理サーバへの SSH 接続に必要な［ e ］を利用されないように，保守用中継サーバに保存しない運用にしましょう。SSH Agent Forwarding と呼ばれる機能を使うと，保守作業の SSH 接続に必要な［ e ］の全てを保守 PC にだけ保存する運用にできます。

F さん：承知しました。

二つ目の提言は，SSH の接続元の制限である。FW で接続元を制限することができれば，万一，SSH サーバソフトウェアで認証バイパスなどの脆弱（ぜい）性が発見されて悪用された場合にも有効な対策となる。

そこで，F さんは，保守 PC-B 及び保守 PC-C を，VPN 装置を介して又は直接，M 社内のネットワークに接続させた後に，インターネット経由で保守用中継サーバにアクセスさせることを考えた。このとき，［ f ］ことができれば，保守用中継サーバへのアクセスを表 1 の項番 4 のルールを変更することによって制限できる。そこで，これらへの対応を M 社に打診した。

そのほかの再発防止策についても，F さんは S 氏の提言について検討を重ね，保守用中継サーバ及び顧客管理サーバに関するセキュリティを強化した。

設問1　〔顧客管理サーバの保守方法〕について，(1)～(3)に答えよ。

(1)　図2中の［　a　］に入れる適切な字句を20字以内で答えよ。

(2)　図2中の下線①の設定にした目的を，“操作ログ”という字句を用いて25字以内で述べよ。

(3)　表1中の［　b　］，［　c　］に入れる適切な字句を，図1中の字句を用いて答えよ。

設問2　〔セキュリティインシデントの発生と対応〕について，(1)，(2)に答えよ。

(1)　本文中の下線②の通信は，表1のどのルールによってFWログに記録されるか。表1中の項番で答えよ。

(2)　今回のセキュリティインシデントにおいて，第三者が保守用中継サーバにSSH 接続可能だった期間は何月何日の何時何分から何月何日の何時何分までか。期間を答えよ。

設問3　〔セキュリティインシデントの再発防止〕について，(1)～(4)に答えよ。

(1)　図5中の下線③について，パスフレーズを設定する目的を30字以内で具体的に述べよ。

(2)　図5中の［　d　］に入れる適切な字句を10字以内で答えよ。

(3)　本文中の［　e　］に入れる適切な字句を5字以内で答えよ。

(4)　本文中の［　f　］に入れる適切な字句を20字以内で答えよ。