問1　組込み機器を利用したシステムのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

C社は，製造事業者向けの機械及び制御用コンピュータを製作・販売している従業員数1,200名の会社である。保守サービスの事業拡大を目的として，顧客の工場に設置されたC社製品の稼働状況を遠隔で監視するシステム（以下，工場遠隔監視システムという）を開発することになった。

工場遠隔監視システムは，機械に取り付けられているセンサの情報を制御用コンピュータ経由でリアルタイムにクラウドサービス上の監視サーバへ送信し，それをC社保守員が遠隔で監視する。センサ情報には，異常や故障を知らせる“障害情報”及び部品交換時期の目安となる使用回数などの“統計情報”が含まれる。

携帯電話網を通じてインターネットにアクセスするために，C社は自社が保有する組込み機器の開発技術を生かしてLinuxで動作するLTE（Long Term Evolution）対応ルータ（以下，LTEルータという）を開発することにした。制御用コンピュータは，LTEルータを使用することによって，機械から収集したセンサの情報をクラウドサービス上の監視サーバに送信できるようになる。監視サーバでは，通信プログラムが制御用コンピュータからセンサの情報を受信して，データベースに格納する。格納したデータは，保守員が使用する監視端末に表示される。また，顧客はWebブラウザで監視サーバにアクセスし，稼働状況を確認できる。監視端末からLTEルータの設定変更ができるように，LTEルータではSSHサービスを稼働させる。

〔試験環境の構築〕

開発担当のE君は，工場遠隔監視システムの試験環境（以下，試験環境という）を構築した。試験環境の構成を図1に示す。

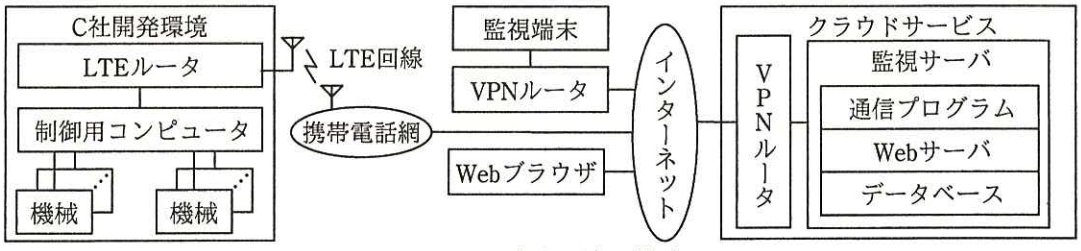

図1　試験環境の構成

インターネットを流れる通信は，Web ブラウザから監視サーバへの通信を除き，全て IPsec を使って暗号化する。IPsec では，通信モードに［ a ］モードを使用し，ルータ間の通信を全て暗号化する。鍵交換には，IKEv2 を使用し，認証方式には，事前共有鍵方式を選択する。片側のルータの IP アドレスが動的に変わる環境においては，IKEv1 の場合，［ b ］モードを使用する必要があるが，IKEv2 の場合は標準で対応している。

〔試験環境における情報セキュリティインシデントの発生〕

試験を開始してから 7 日後，E 君が監視端末から LTE ルータに SSH でログインしたところ，見覚えのない IP アドレスからログインされていることに気付いた。E 君は，不正アクセスを受けている可能性があることをプロジェクト責任者の W 主任に報告し，調査を開始した。

LTE ルータにおいて，netstat コマンドを実行したところ，表 1 に示すとおり，試験環境と無関係のグローバル IP アドレスとの接続が複数あること，及び［ c ］を送信元として SSH サービスにログインされていることが分かった。

表 1　netstat コマンドの実行結果（抜粋）

プロトコル	ローカルアドレス	外部アドレス	状態	プロセス ID
TCP	0.0.0.0:22	0.0.0.0:*	LISTEN	1543
UDP	0.0.0.0:53	0.0.0.0:*	LISTEN	1145
UDP	0.0.0.0:123	0.0.0.0:*	LISTEN	1380
UDP	0.0.0.0:500	0.0.0.0:*	LISTEN	1417
TCP	192.168.10.1:22	192.168.20.123:54433	ESTABLISHED	1545
TCP	z1.z2.z3.z4:22	x1.x2.x3.x4:32489	ESTABLISHED	1547
TCP	z1.z2.z3.z4:45532	y1.y2.y3.y4:25	ESTABLISHED	1689
TCP	z1.z2.z3.z4:45533	y1.y2.y3.y4:25	SYN_SENT	1689

注記　x1.x2.x3.x4，y1.y2.y3.y4 及び z1.z2.z3.z4 は，グローバル IP アドレスである。

更に調査したところ，攻撃者が SSH のポートフォワード機能を使って，［ d ］を宛先として SMTP で電子メールを転送していることが分かった。LTE ルータのログには，SSH サービスがパスワードの辞書攻撃を受けた痕跡が残っていた。

E 君は，IPsec を経由しなくても，インターネットから LTE ルータの SSH サービスにアクセスできる状態になっていることに気付いた。不正にログインされないた

めの暫定対策として，①SSH のログイン認証をパスワード強度に依存しない方式に設定変更した。

〔セキュリティ対策の検討〕

情報セキュリティインシデントの発生を受けて，C 社は，LTE ルータのセキュリティ対策について，セキュリティ専門業者 N 社の S 氏に相談した。

次は，セキュリティ対策に関する E 君と S 氏との会話である。

E 君 ：SSH サービスについて暫定対策を行いましたが，工場遠隔監視システムのリリースに向けてどのような対策を行う必要がありますか。

S 氏 ：LTE ルータでは，監視端末を利用した場合にだけ，SSH サービスにアクセスできる仕様にすべきです。

E 君 ：そのようにします。具体的には，どのように実現すればよいでしょうか。

S 氏 ：TCP Wrapper を使って，［ e ］することで実現できます。

E 君 ：SSH サービスに関して，他に気を付ける点はありますか。

S 氏 ：市販の幾つかの組込み機器について，②SSH のホスト鍵が同一モデルで全て同じになっているという脆弱性（ぜい）が，セキュリティ機関から注意喚起されています。C 社でも，SSH のホスト鍵は，機器 1 台ごとに異なるものを使用するように設定してください。

E 君 ：出荷する前に，いろいろとセキュリティ設定を行う必要があるのですね。

S 氏 ：さらに，新たな脆弱性が発見された場合の対応として，LTE ルータのファームウェアを更新する仕組みを実装しておく必要があります。

E 君 ：インターネット又は外部記憶媒体経由で，ファームウェアの更新用イメージファイル（以下，イメージファイルという）を LTE ルータに読み込んで保存し，コマンドを使って更新するという機能を実装したいと考えています。どのようなことに注意が必要ですか。

S 氏 ：ファームウェアの更新機能において，イメージファイルが③改ざんされていないか検証できるようにする必要があります。

E 君 ：イメージファイルを暗号化しておく必要はありますか。

S 氏 ：イメージファイルの解析ツールを使うことで，パスワードなどの重要な情報

がファームウェアにハードコードされているという脆弱性が見つかった事例が報告されており，解析されないように暗号化することも対策の一つです。④しかし，イメージファイルを暗号化しても，攻撃者が復号のための鍵を入手して，イメージファイルを復号するという可能性を排除できません。解析されても問題がないように設計することが重要です。

E君　：セキュリティに関する仕様を明確化し，基本仕様書に反映します。また，顧客に引き渡す前に，チェックリストを基にセキュリティに関する設定項目についてレビューするようにしたいと思います。

E君は，LTEルータのセキュリティ対策を実施し，W主任の承認を得ることができた。E君は，工場遠隔監視システムのリリースに向けて作業を開始した。

設問1　本文中の［　a　］，［　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　アグレッシブ　　イ　アドホック　　ウ　トランスポート

エ　トンネル　　オ　パッシブ　　カ　ブロック

設問2　〔試験環境における情報セキュリティインシデントの発生〕について，(1)，(2)に答えよ。

(1)　本文中の［　c　］，［　d　］に入れるIPアドレスを答えよ。

(2)　本文中の下線①について，実施したSSHの設定変更を30字以内で述べよ。

設問3　〔セキュリティ対策の検討〕について，(1)～(4)に答えよ。

(1)　本文中の［　e　］に入れる適切な設定内容を30字以内で述べよ。

(2)　本文中の下線②の脆弱性を悪用する攻撃手法にはどのようなものが考えられるか。20字以内で述べよ。

(3)　本文中の下線③について，どのようにして実現するか。イメージファイルの作成時と更新時に行うディジタル署名に関連した処理を，使用する鍵の種類を明示した上で，それぞれ35字以内で述べよ。

(4)　本文中の下線④について，攻撃者はどのような方法で復号のための鍵を入手するか。35字以内で具体的に述べよ。