SC

平成30年度　秋期
情報処理安全確保支援士試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

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2
選択方法	1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。2問とも○印で囲んだ場合は，はじめの1問について採点します。

〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	○問2

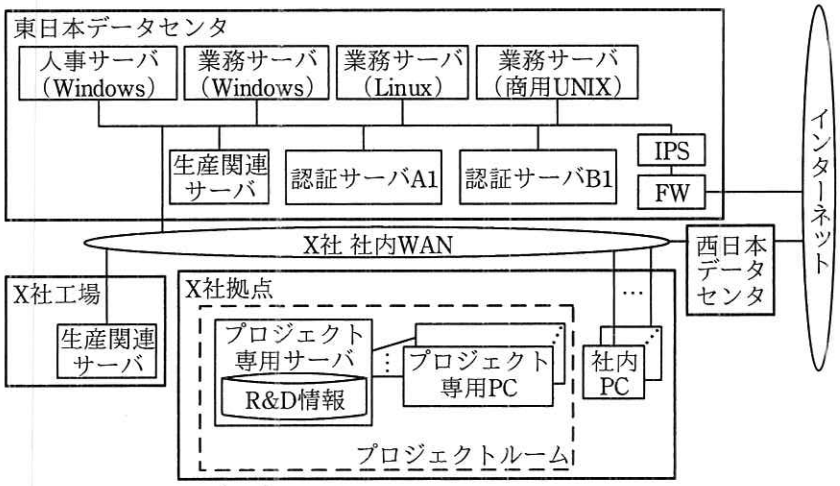
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

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　クラウド環境におけるセキュリティ対策に関する次の記述を読んで，設問 1～5 に答えよ。

X 社は，日本，米国，欧州に事業を展開している従業員数 80,000 名の製造会社であり，重要インフラ設備を製造している。日本国内の従業員数は 40,000 名である。

X 社のシステムは，サーバ，ネットワーク機器及び PC で構成されている。X 社の日本国内のネットワークの論理構成を，図 1 に示す。



FW :ファイアウォール
人事サーバ :X社の人事管理を行うサーバ
業務サーバ :X社の様々な業務のためのサーバ。部門ごとの業務システムや，国又は地域ごとのメールシステムなどが稼働
認証サーバA1 :Windows用の認証サーバ
認証サーバB1 :Linux及び商用UNIX上で稼働するWebアプリケーションにアクセスする際の利用者認証に用いるリバースプロキシ型の認証サーバ
R&D情報 :基礎研究，並びに開発中の重要インフラ設備の設計及び生産技術に関する情報
プロジェクト専用サーバ :R&D情報を取り扱うプロジェクトで利用するサーバ
プロジェクト専用PC :プロジェクト専用サーバを利用するためのWindows PC
社内PC :プロジェクト専用サーバ以外の一般業務のためのWindows PC
生産関連サーバ :重要インフラ設備を製造する工場の設備管理，生産管理，製造に必要な物品の物流管理を行うシステムのサーバ

図 1　X 社の日本国内のネットワークの論理構成

従業員が社内 PC，並びに Windows の業務サーバ及び人事サーバにログオンする際は，認証サーバ A1 による利用者認証が行われる。従業員が Web ブラウザを用いて Linux 及び商用 UNIX の業務サーバにログオンする際は，認証サーバ B1 による利用

者認証が行われる。認証サーバ A1 は，人事サーバと連携しており，人事サーバの従業員の情報を日次で反映している。認証サーバ B1 は，認証サーバ A1 の LDAP サービスを利用している。

X 社のシステムには，X 社の情報セキュリティ標準，X 社が事業を展開している各国及び各地域において特定の製品とそれら製品の技術情報を他国又は他地域に持ち出すことを制限した輸出管理規制，並びに①各国及び各地域の個人情報保護に関する法規制の三つに準拠すること（以下，三つに準拠することを基本要件という）が求められる。基本要件の具体的内容は次のとおりである。

・R&D 情報は，物理的な入退室管理が行われているプロジェクトルーム内に配置されたプロジェクト専用サーバに保管する。
・プロジェクト専用サーバには，プロジェクトルーム内のプロジェクト専用 PC からだけアクセスさせる。
・生産関連サーバは，X 社の工場及びデータセンタに配置する。
・生産関連サーバは，重要インフラ設備の製造の事業継続のために，バックアップを他の工場又はデータセンタに配置する。
・各国及び各地域の輸出管理規制への準拠のために，同じ重要インフラ設備を製造する工場及び生産関連サーバは同一の国又は地域内の 2 か所以上に配置する。日本国内では，システムを東日本地区のシステムと西日本地区のシステムに分け，東日本データセンタと西日本データセンタにそれぞれサーバを配置する。
・X 社のシステムの機器には，プライベート IP アドレスを割り当てる。
・社外ネットワークと X 社社内ネットワークを接続する際は，次のようにする。
  (1) X 社が管理する FW と IPS を介して接続する。
  (2) FW で，業務上必要な通信だけを許可する。
  (3) IPS とセキュリティベンダの監視サービスを併用して，攻撃が疑われる通信を検知・遮断する。

X 社は，米国におけるビジネスの強化，IT を活用した新しいビジネスの開発，並びにシステム部門の役割をシステム運用からビジネス企画及びシステム企画へシフトするために，各国及び各地域のシステムをクラウド環境に移行することにした。X 社の経営層は，クラウド環境への移行に関して次の方針を示し，X 社システム部門に

具体的な検討を指示した。

方針１　メールシステムをクラウドベンダ M 社の SaaS Q に，業務システムのうち二つのシステムをクラウドベンダ S 社の SaaS S に，それぞれ 1 年以内に移行する。各国及び各地域とも同じ方針で移行するが，SaaS の契約はそれぞれの国又は地域で行う。

方針２　他のシステムは，クラウドベンダ H 社が提供する IaaS C の仮想マシン上に 5 年間で段階的に移行する。ただし，移行できないもの又は移行すると基本要件を満たせなくなるものは移行しない。また，IaaS C の仮想マシン上に移行したサーバの OS 及びミドルウェアの運用管理には SI ベンダ J 社の運用サービスを利用する。

IaaS C の主なサービス仕様の内容は次のとおりである。

・データセンタは，日本国内 1 か所，海外 60 か所に配置され，それらが高速の閉域網で相互に接続されている。データセンタ間の通信は課金されない。
・オプションサービスとして災害対策のサービスが提供されている。日本国内のデータセンタが被災した場合はシンガポールのデータセンタでサービスが継続される。
・ネットワーク及び仮想サーバは，H 社の情報セキュリティ標準に基づいてセキュリティ管理が行われており，顧客企業には監査法人によるセキュリティ管理の監査報告書が開示される。
・あらかじめ予約されているプライベート IP アドレスがあり，利用者はそれらを使うことができない。

〔クラウド環境への移行に関する検討〕

X 社システム部門は，次の条件のいずれかに該当するシステム及びサーバは，IaaS C に移行できない又は移行すると基本要件を満たせなくなるとして，現状のまま X 社の工場，データセンタ又は拠点に配置し，X 社システム部門がシステム運用業務を担当することにした。

条件１　IaaS C が提供する仮想サーバでは稼働しない OS を用いているサーバ

条件２　プロジェクト専用サーバ

条件3　X社が取り扱う個人情報を管理するシステム

条件4　生産関連サーバ

また，X社システム部門は，IaaS C と X 社社内ネットワークとの接続においては，X社が管理するFW及びIPSを介して接続することにし，さらにIaaS Cのサービス仕様上の制約から起こる問題を回避するために，FW の NAT 機能を用いて一部のアドレスを変換することにした。

〔ID管理及び利用者認証の検討〕

X社システム部門は，X社のデータセンタ，工場及び拠点のシステム環境（以下，オンプレミス環境という）にIaaS C，SaaS Q及びSaaS Sを加えた環境（以下，ハイブリッドクラウド環境という）における ID 管理及び利用者認証を次のように設計した。

- IaaS C に配置する Windows の業務サーバに従業員がアクセスする際に利用者認証を行う認証サーバとして，認証サーバ A1 と同じ製品を用いた認証サーバ A2 を IaaS C の環境に新たに配置する。
- 認証サーバA2にはIaaS Cに配置するWindowsの業務サーバのコンピュータ情報及びそれらを運用管理するJ社の運用管理要員の利用者情報を登録し，認証サーバA1とSAML 2.0プロトコルで通信する。
- 認証サーバB1をバージョンアップし，新バージョンで提供されたSPNEGOプロトコルによって，認証サーバB1が認証サーバA1と通信し，認証サーバA1が発行するトークンを用いて利用者認証を行うようにする。
- SaaS Q及びSaaS Sは，認証サーバB1とSAML 2.0プロトコルで通信し，認証サーバB1が発行するトークンを用いて利用者認証を行う。

X社システム部門は，認証サーバ B1 の配置について，次の二つの案を比較検討した。

案1　現行の構成のまま，オンプレミス環境に認証サーバB1を配置する。

案2　認証サーバB1をIaaS Cに移行する。

X社システム部門は，それぞれの案において，利用者認証後の通信経路を比較した。

その結果，移行の初期段階においては案1とし，社内PCと，オンプレミス環境及びIaaS C環境それぞれの業務サーバとの間の通信データ量を定期的に測定し，案2に変更する時期を見極めることにした。案1における日本国内のハイブリッドクラウド環境の論理構成を図2に示す。

なお，X社の各国及び各地域のデータセンタは，VPNを介してIaaS Cのデータセンタにアクセスする。

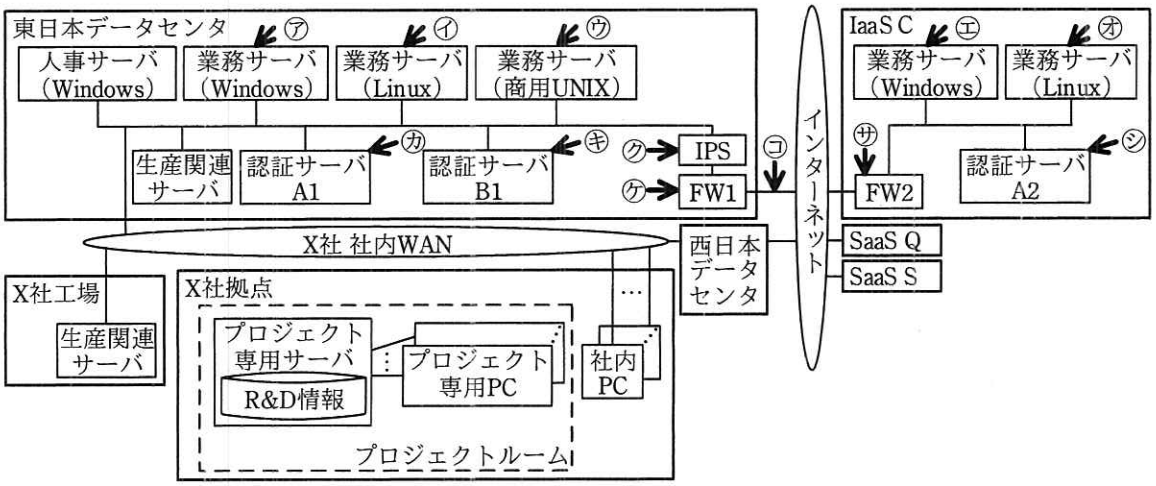


図2　案1における日本国内のハイブリッドクラウド環境の論理構成

〔エンドポイント管理の検討〕

X社は，独自の情報セキュリティ標準を定めているが，NIST サイバーセキュリティフレームワークとして知られている“重要インフラのサイバーセキュリティを向上させるためのフレームワーク”（以下，NIST CSF という）を基に改定することにした。NIST CSF においては，組織のサイバーセキュリティリスク管理策が NIST CSF で定義されている特性をどの程度達成できているかを示す段階として，②フレームワークインプリメンテーションティア（以下，ティアという）1からティア4までの段階を定義しており，ティア4が最も高い段階である。

現状の情報セキュリティ標準とNIST CSFを比較した結果，X社システム部門は，情報セキュリティ標準を，次のように改定することにした。

改定1　構成管理システムへの登録

X社内の各サーバ及び各ネットワーク機器について，管理責任者，機種名及びシ

リアル番号，OS 及びファームウェアを含むソフトウェアの製品名及びバージョンなどを登録する構成管理システムを整備する。X 社が使用するクラウドサービスについては，システム名，システム管理責任者，クラウドサービスの名称，X 社側で管理する必要があるソフトウェアの製品名及びバージョンなどを構成管理システムに登録する。PC についても，使用者，管理責任者，機種名，シリアル番号，OS を含むソフトウェアの製品名及びバージョンなどを構成管理システムに登録する。

改定２　サーバ及び PC のセキュリティチェックの実施

脆弱性修正プログラム（以下，パッチという）の適用状況及びセキュリティ設定パラメタの設定値を定期的にチェックする。必要なパッチが未適用であったり，セキュリティ設定パラメタの設定値が X 社の標準値ではない場合，サーバ，ネットワーク機器及びシステムの管理責任者，又は PC の管理責任者，並びにその所属長に通知し，1 週間以内の是正を求める。X 社の標準値は，NIST が公開している National Checklist Program Repository にあるチェックリストを参考にして決定する。

改定３　脆弱性管理の実施

サーバ，ネットワーク機器及び PC において，使用している OS 及びファームウェアを含むソフトウェアの脆弱性情報，及びクラウドサービスにおいて X 社側で管理する必要があるソフトウェアの脆弱性情報が新たに公開された場合は，その重要度を評価し，重要度に応じた期限内にパッチを適用するよう，サーバ，ネットワーク機器及びシステムの管理責任者，又は PC の管理責任者，並びにその所属長に通知する。

なお，上記の改定は，クラウド環境への移行に関する検討結果には影響しない。

X 社システム部門は，三つの改定に伴って必要になる運用について，J 社に運用サービスの提案を求めた。J 社からは，サーバ及び PC で使用するソフトウェア（以下，標準ソフトウェアという）の一覧を運用サービス契約時に取り決めた上で，次の運用サービスを提供できるという回答があった。

運用サービス１　標準ソフトウェアに関する脆弱性情報を日次で収集する。

運用サービス２　エンドポイント管理用ソフトウェアである製品 D を導入し，運用サービス１で収集した情報を用いてプロジェクト専用 PC 及びプロジェクト専用サーバを除く全てのサーバ及び PC 内の標準ソフトウ

エアのパッチ適用状況及びセキュリティ設定を日次で監視する。

製品Dの仕様は次のとおりである。

・サーバ又はPCに導入されるエージェントソフトウェアと，各エージェントソフトウェアが通信するサーバソフトウェアとで構成される。

・エージェントソフトウェアが，サーバ又はPCにおけるパッチの適用状況及びセキュリティ設定パラメタの設定値を収集し，サーバソフトウェアに送信する。

・サーバソフトウェアが提供する管理画面において，必要なパッチ，並びに必要なパッチが適用されていないサーバ及びPCの一覧を表示することができる。同様に，セキュリティ設定パラメタの設定値が指定した値と異なるサーバ及びPCの一覧を表示することができる。

・必要なパッチが適用されていないサーバ及びPCの一覧から，1台以上のサーバ又はPC並びにパッチを選択し，1回の操作で，選択したサーバ又はPCに必要なパッチを適用することができる。

・セキュリティ設定パラメタの設定値が指定した値と異なるサーバ及びPCの一覧から，1台以上のサーバ又はPCを選択し，1回の操作で，選択したサーバ又はPCのセキュリティ設定パラメタの設定値を指定した値に変更することができる。

〔モバイル環境の検討〕

X社システム部門は，従業員が出張先や自宅からでも社内にいるのと同様に業務ができるよう，モバイルPCとスマートフォン（以下，二つを併せてモバイル端末という）を従業員に貸与し，インターネット経由で社内システムやクラウド環境にWebのインタフェースを介してアクセスできるモバイル環境を検討した。モバイル環境においては，モバイル端末からの情報漏えい，モバイル端末のマルウェア感染などのリスクが懸念されることから，次の対策を実施することにした。

対策1　スマートフォンにモバイル機器管理ソフトウェアである製品Fのエージェントソフトウェアを導入し，スマートフォンのパッチ適用状況及びセキュリティ設定を監視し，パッチ適用及びX社の情報セキュリティ標準が定めるセキュリティ設定を強制する。

対策2　VPNサーバ及びVPNクライアントを導入し，モバイル端末にクライアント証明書を組み込む。従業員がモバイル端末からインターネット経由で社内

システム及びクラウド環境にアクセスする際，VPN サーバでクライアント証明書を用いた端末認証が行われる。モバイル端末が，X 社のデータセンタに接続した後，認証サーバ B1 による利用者認証が行われ，トークンが発行される。トークンが発行された後，従業員は，IaaS C，SaaS Q 及び SaaS S にアクセスできる。

認証サーバ B1 による利用者認証においては，認証サーバ B1 が提供するリスクベース認証の機能が利用され，パッチ適用状況やセキュリティ設定に問題のあるモバイル端末からのアクセスを拒否する。

X 社システム部門は，モバイル環境の導入に伴い，負荷の観点から再度認証サーバ B1 の配置を見直すことにし，次の三つの案を比較検討した。

案 A　現行の構成のまま，オンプレミス環境に認証サーバ B1 を配置する。

案 B　認証サーバ B1 を IaaS C に移行する。

案 C　新たに IaaS C に認証サーバ B1 と同じ製品を用いた認証サーバ B2 を配置し，従業員が IaaS C に配置された Linux の業務サーバ上で稼働する Web アプリケーションにアクセスする際の利用者認証に用いる。認証サーバ B2 は，オンプレミス環境の認証サーバ B1 と SAML 2.0 プロトコルによる通信を行う。この場合，認証サーバ B1 が IdP，認証サーバ B2 が SP になる。

X 社システム部門は，三つの案を，社内 PC 及びモバイル端末から業務サーバへの利用者認証後のアクセスにおける通信経路上の構成要素ごとの負荷の観点から比較し，案 C を選択した。

X 社が設計した，モバイル環境を含む日本国内のハイブリッドクラウド環境の論理構成を図 3 に示す。

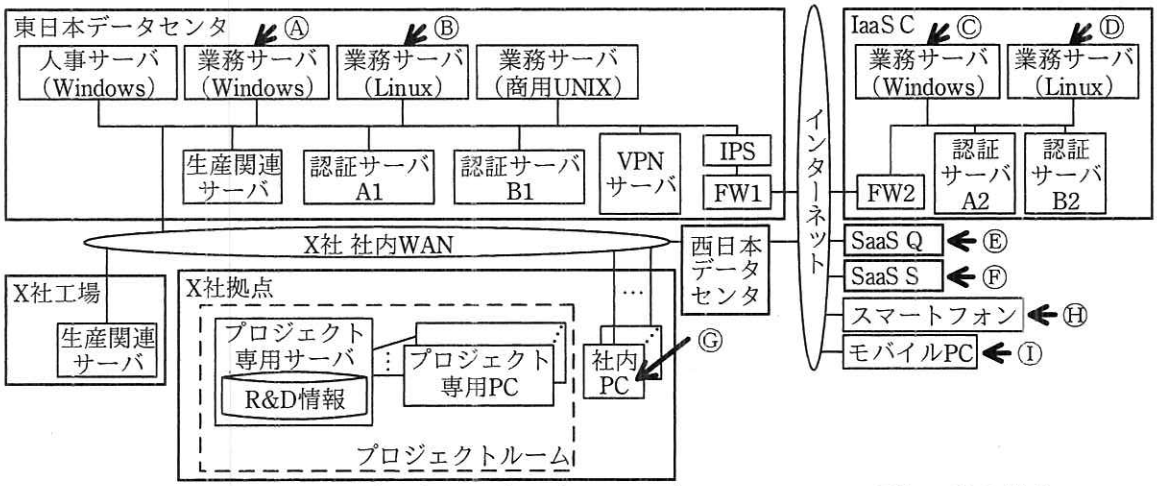


図 3　モバイル環境を含む日本国内のハイブリッドクラウド環境の論理構成

図 3 において，従業員がスマートフォンから SaaS Q にアクセスする際の通信シーケンスを図 4 に示す。

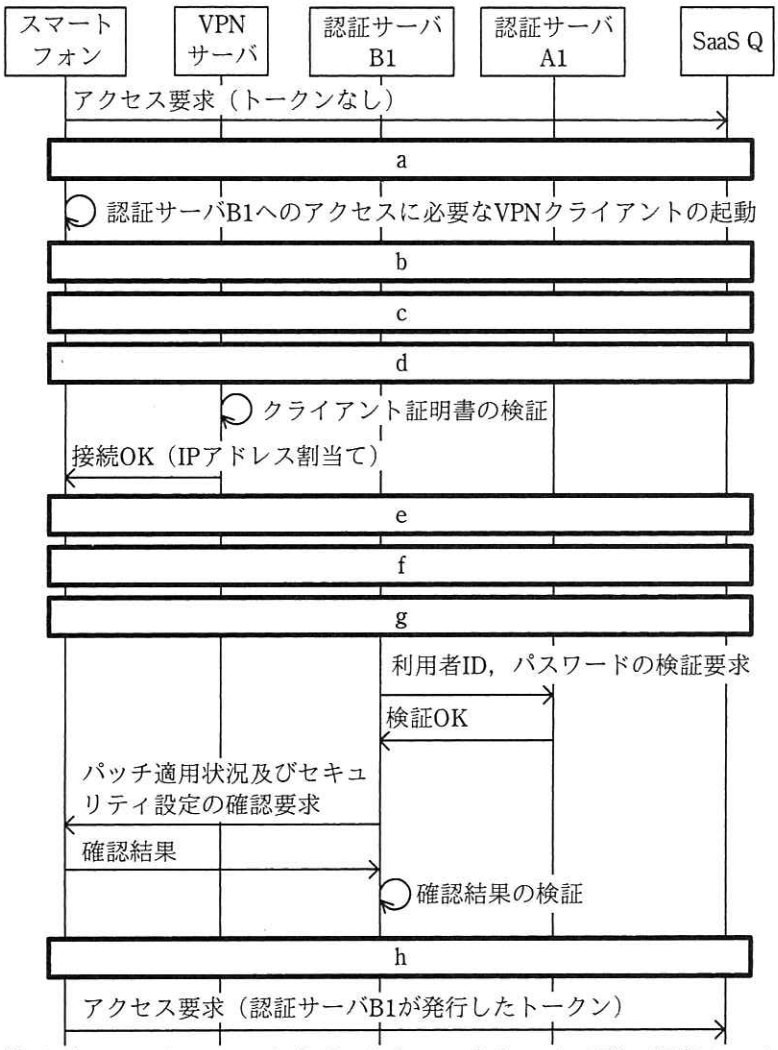


図4　従業員がスマートフォンから SaaS Q にアクセスする際の通信シーケンス

X 社システム部門は，モバイル端末からの利用を想定したハイブリッドクラウド環境の設計，及び SaaS S に移行する二つの業務システムについて経営層の承認を得て，システムのクラウド環境への移行とモバイル環境の導入を開始した。

設問1　本文中の下線①について，2018年5月25日に適用が開始された欧州連合の規則の略称を英字4字で答えよ。

設問2　〔クラウド環境への移行に関する検討〕について，(1)～(3)に答えよ。

(1)　条件2について，プロジェクト専用サーバをクラウド環境に移行した場合に満たせなくなる基本要件の具体的内容を，60字以内で述べよ。

(2)　条件4について，生産関連サーバをクラウド環境に移行し，かつIaaS Cの本文中に示したサービスを全て利用した場合に満たせなくなる基本要件の具体的内容を三つ挙げ，それぞれ50字以内で述べよ。また，挙げた三つのうちの一つの理由となるIaaS Cのサービス仕様の内容を，50字以内で述べよ。

(3)　X社社内ネットワークとIaaS Cとの接続において，FWのNAT機能を用いることにしたのはどのような問題を回避するためだと考えられるか。IaaS Cのサービス仕様の制約から起こる問題を70字以内で述べよ。

設問3　〔ID管理及び利用者認証の検討〕について，(1)，(2)に答えよ。

(1)　各認証サーバ及び各SaaSをSAML 2.0プロトコルやSPNEGOプロトコルで通信させることによって，X社の従業員にはどのような利便性が提供されるか。30字以内で述べよ。

(2)　案2を選択した場合，案1と比べて，利用者認証後の通信経路上の構成要素の負荷が高くなるのは，社内PCからどの業務サーバへの通信か。全て選び，図2中の記号㋐～㋓で答えよ。また，負荷が高くなる構成要素を全て選び，同じく図2中の記号㋐～㋓で答えよ。

設問4　〔エンドポイント管理の検討〕について，(1)～(3)に答えよ。

(1)　本文中の下線②について，ティア1からティア3に該当するものを，解答群の中から選び，それぞれ記号で答えよ。

解答群

ア　繰返し適用可能である（Repeatable）

イ　部分的である（Partial）

ウ　リスク情報を活用している（Risk Informed）

(2)　運用サービス1及び2が提供される場合，標準ソフトウェア以外のソフトウェアがサーバ又はPCに導入されていたとすると，セキュリティ管理上どのような不都合が生じるか。40字以内で述べよ。

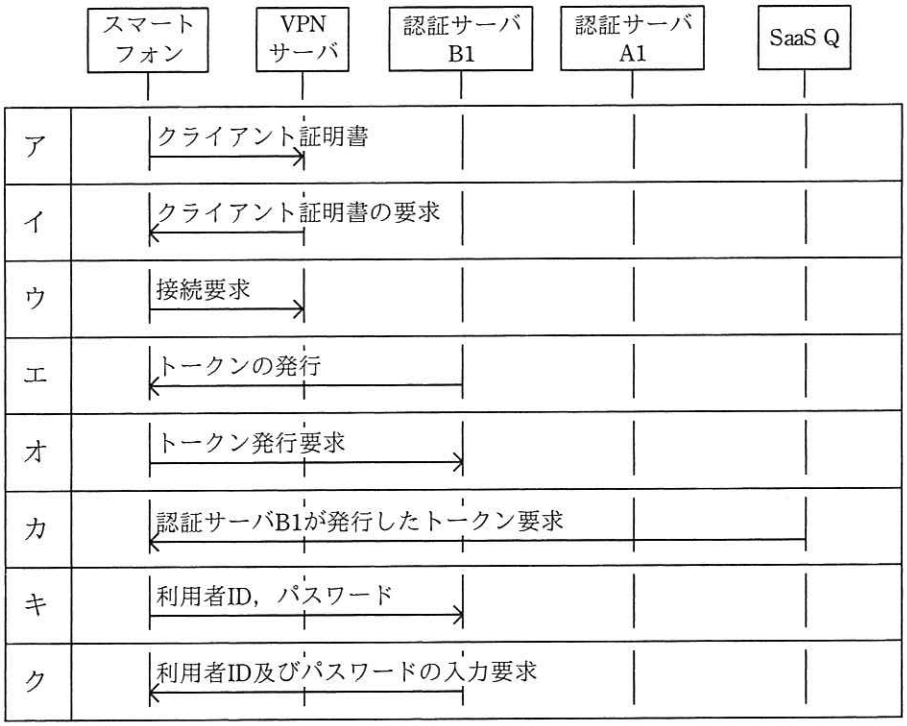
(3) 情報セキュリティ標準を基に手作業及び目視でセキュリティ設定パラメタの設定値をチェックする方法と比べて，製品 D による方法は，どのような利点があるか。二つ挙げ，それぞれ 15 字以内で答えよ。

設問5 〔モバイル環境の検討〕について，(1)，(2) に答えよ。

(1) 案 A 及び B における利用者認証後の通信経路のうち，案 C に比べて通信経路上の構成要素の負荷が高くなるのは，どのクライアントからどの業務サーバへの通信か。案 A については 2 組み，案 B については 3 組み挙げ，それぞれ図 3 中の記号Ⓐ～①で答えよ。

(2) 図 4 中の [a] ～ [h] に入れる適切な通信メッセージを，解答群の中から選び，記号で答えよ。

解答群



問2　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 1～5 に答えよ。

A 社は，玩具を製造販売する従業員数 1,500 名の企業である。A 社の組織図を図 1 に示す。

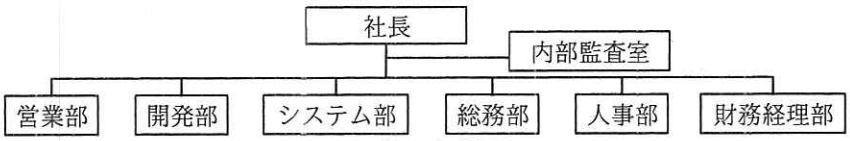
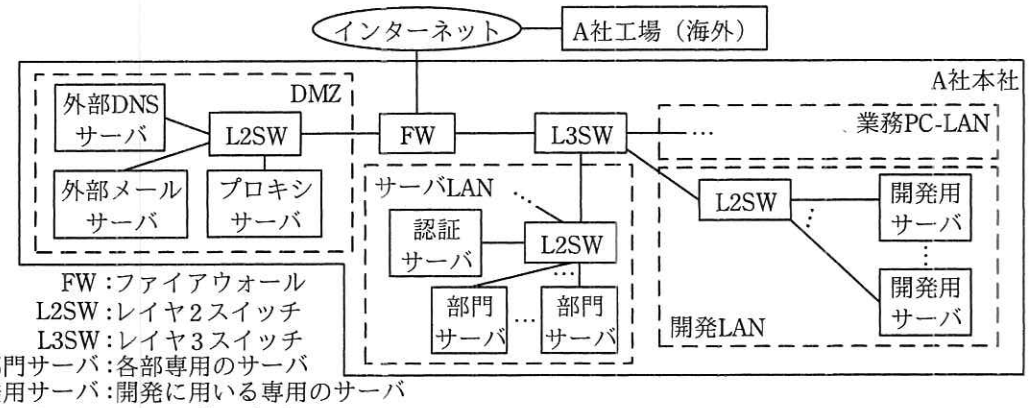


図 1　A 社の組織図

A 社は，情報セキュリティ基本方針を定めており，これに従い，情報セキュリティ委員会を設けている。情報セキュリティ委員会は，A 社の情報セキュリティについて意思決定する。情報セキュリティ委員会の委員長は社長，委員は各部の部長であり，事務局は総務部が担当する。情報セキュリティ委員会は，下部組織として，セキュリティインシデント（以下，インシデントという）に対応する非常時対応チームをもつ。非常時対応チームには，各部の代表者が参加する。ただし，非常時対応チームが取り扱うべきインシデントの範囲や，具体的な活動内容は明文化されていない。これまでのところ，非常時対応チームの活動実績は極めて少ない。

〔ネットワーク構成〕

A 社は，国内に本社を置き，海外に工場をもつ。A 社のネットワーク構成を図 2 に示す。



注記 1　個別の PC の記載は省略している。
注記 2　開発業務に用いる PC は開発 LAN に接続し，ほかの PC は業務 PC-LAN に接続している。

図 2　A 社のネットワーク構成（概要）

A 社本社のネットワークに接続する機器には，サーバ，ネットワーク機器及び PC がある。各部は，必要に応じて部門サーバをサーバ LAN に設置し，業務に利用している。各部の部門サーバは，各部が管理している。開発部は，開発部の部門サーバに加えて，開発用サーバを設置し，管理している。部門サーバと開発用サーバ以外のサーバ，全てのネットワーク機器及び全ての PC は，システム部が管理している。各部でシステム管理者を任命し，そのシステム管理者が適切に機器を管理するというのが A 社の機器管理方針である。

DMZ に設置されたサーバにはグローバル IP アドレスが付与され，インターネットとの間で通信できる。DMZ 以外に設置された機器には固定のプライベート IP アドレスが付与され，インターネットとの間の直接の通信は FW によって禁止されている。ただし，業務 PC-LAN に接続された PC は，プロキシサーバを介してインターネットにアクセスできる。プロキシサーバは直近 60 日分のログを保存している。開発 LAN から DMZ への通信は，FW によって禁止されている。

〔情報漏えいの発生〕

2018 年 9 月 11 日，A 社において，インシデント（以下，本インシデントをインシデント P という）が発覚した。この日，A 社の商品問合せ窓口に，A 社の発売前の新製品 α の操作説明書（以下，漏えい文書 X という）がインターネットの掲示板 U に投稿されている旨の通報が寄せられた。開発部の担当者が確認したところ，投稿されていたのは間違いなく A 社のもので，開発過程で作成された文書であることが分かった。

情報セキュリティ委員会は，インシデント P への対応方法を議論した。同委員会は，次の理由から，非常時対応チームではなく，当該文書を所管する開発部がインシデント P に対応することを決定した。

・個人情報及び重要な秘密情報の漏えいは見つかっておらず，緊急度及び重要度は低い。
・社内での調査活動について，非常時対応チームの権限及び調査手順が明確に定められておらず，調整が必要である。
・非常時対応チームのメンバの多くは，本来の業務のため，対応する時間の確保が難しい。

開発部は，急きょ，インシデント P に対応するためのチーム（以下，開発部対応チームという）を立ち上げ，対応を開始した。同チームの調査結果と措置状況を図 3 に示す。

(1) 開発部対応チームの調査活動の目的
・インシデント P の原因を調べて，必要な措置を講じること
(2) 調査の範囲
・検討の結果，次の機器を主な調査対象とした。
開発用サーバ及び開発部の部門サーバ
(3) 調査によって判明したこと
・漏えい文書 X は，開発部の部門サーバに保管されていた文書 Y と内容が同じだった。文書 Y は，8 月 29 日前後に作成された。
・文書 Y が保管されていた部門サーバは，開発部のメンバなら誰でもアクセスでき，文書を閲覧及び複製できる状態だった。文書 Y へのアクセスのログは取得されていなかった。
・開発部の商品企画第 2 チームは，委託先事業者である V 社と共同で新製品 α の操作説明書を執筆しており，V 社とのデータ交換に利用した USB メモリ（以下，USB メモリ R という）を紛失していた。USB メモリ R に文書 Y が格納されていた可能性があることから，USB メモリ R が情報漏えいの経路と考えられる。
(4) 調査で分からなかったこと
・文書 Y を流出させた者
・文書 Y 以外のデータの漏えいの有無，及びそのほかの被害の範囲
(5) 措置
・掲示板事業者に対する漏えい文書 X の公開中止の要請（状況：要請済み）
・USB メモリの管理方法の見直し（状況：システム部が近々見直す予定）
・本件の通報者へのお礼と対処した旨の報告（状況：担当部署を調整中）
(6) 開発部対応チームの活動時に認識された課題
次のように，会社としてのインシデント対応能力が不足している。
a. インシデント対応についての各部の責任や役割が曖昧で協力を得にくい場面があった。
b. インシデント対応についての作業手順が明確になっておらず，手探りの作業となった。このため，掲示板事業者への要請といった措置の着手が遅れた。
c. インシデント対応の経験をもつ者又はスキルをもつ者がおらず，非効率な作業になった。
d. ログが少なく調査が難航した。開発部はログ取得を定めた規程をもたず，開発部が管理する機器のうちログを取得していたものは少数だった。また，取得していたログの種類や保存期間にはばらつきがあった。

図 3　開発部対応チームの調査結果と措置状況（概要）

開発部対応チームの調査結果と措置状況は情報セキュリティ委員会に報告された。報告を受けて，委員会では，図 3 中の(5)に挙げられた一連の措置の完了をもってインシデント P への対応を終了することが了承された。また，インシデント対応能力の向上を目指すことを決め，システム部の G 部長に対応を指示した。

〔早期に取り組むべき事項のとりまとめ〕

G 部長は，情報セキュリティ委員会の承認の下，情報セキュリティに関わるコンサルティングサービスを提供する E 社に支援を依頼した。

E 社のコンサルタントである F 氏は，A 社がインシデント対応能力の向上のために早期に取り組むべき事項を図 4 のとおりまとめ，G 部長に報告した。

1. インシデント対応ポリシの策定
インシデント対応のための基本的な方針として，インシデント対応ポリシを定める。
インシデント対応ポリシに記載する項目の例として，NIST の文書 SP 800-61 Rev. 2 に挙げられているものを図 5 に示す。
2. インシデント対応のための体制整備
インシデントに迅速に対応することを目的に，インシデント対応チームを整備する。インシデント対応チームは，次の役割を担う。
・インシデントが発生した時点での対応活動
・インシデント対応に関係する他のサービスの提供
インシデント対応チームが提供するサービスの例として，NIST SP 800-61 Rev. 2 は，［ a ］，脆弱性や脅威についてのアドバイザリの配信，［ b ］，及び社内外での情報共有の推進を挙げている。
インシデント対応チームの母体として，非常時対応チームを活用することもできる。
3. 取得するログの見直し
（省略）

図 4　A 社が早期に取り組むべき事項（概要）

・［ c ］の責任表明
・本ポリシの目的と目標
・本ポリシの適用範囲
・［ d ］と関連用語の定義
・組織構造，並びに役割，責任及び権限レベルの定義
・［ d ］についての［ e ］又は深刻度評価
・パフォーマンス測定
・報告と連絡の様式

図 5　インシデント対応ポリシに記載する項目の例

〔インシデント対応能力の向上への取組み〕

G 部長は，図 4 の事項の具体化を，F 氏の支援を受けながら進めることにした。

インシデント対応ポリシの適用範囲は全社とした。非常時対応チームは，A 社におけるインシデント対応のための組織横断チーム（以下，A-CSIRT という）として，再編成することにした。インシデント対応ポリシでは，A-CSIRT 及び各部の役割，

責任及び権限レベルを規定した。A-CSIRT は，従来の非常時対応チーム同様，各部の代表者で構成することにした。ただし，インシデントへの迅速な対応を可能にするため，各部で人選を見直し，更にシステム部所属のメンバを増やした。A-CSIRT のリーダは G 部長が務めることにした。メンバのスキルを高めるため，定期的に勉強会を開催し，外部の研修などにも積極的に参加してもらう方針を立てた。

ログについては，ログの管理に関する規程（以下，ログ管理ポリシという）を作成することにした。ログ管理ポリシの適用対象は，社内の全ての機器であり，システム部が管理する機器，部門サーバ及び開発用サーバも含まれる。ログ管理ポリシでは図 3 中の(6) d に挙げられたログに関わる課題を解決できるように，次の要件を定める。

要件 1　取得するログについての要件

・［ f ］について

・［ g ］について

要件 2　取得したログについての要件

・［ h ］について

・バックアップの作成について

・アクセス制御について

要件 3　各機器の時計を同期するとともに，各機器が出力するログに記録する時刻情報の［ i ］を［ j ］するという要件

情報セキュリティ委員会は，各部に対して，それぞれが管理する機器について，早急に，ログ管理ポリシに従った運用を開始するよう指示した。また，システム管理者に対して，①管理する機器について，通常時のネットワークトラフィック量や日，週，月，年の中でのその推移などの情報（以下，通常時プロファイルという）の把握に努めるよう指示した。

〔マルウェアについての通知〕

マルウェアを配布していたサイト（以下，サイト M という）に A 社の機器のうち 1 台がアクセスし，遠隔操作の機能をもつ，“new3.exe”というファイル名のマルウェア K をダウンロードした可能性がある旨の通知が，10 月 10 日に，ある民間組織か

ら A 社に対してあった。伝えられたサイト M の IP アドレスは A 社管理外のものであり，サイト M のログに残っていたアクセス元の IP アドレスは A 社のプロキシサーバのものだった。この通知は A-CSIRT に伝えられ，インシデント対応ポリシに照らして判断した結果，A-CSIRT が，インシデント（以下，本インシデントをインシデント Q という）として直ちに対応を開始することになった。

A-CSIRT のメンバであるシステム部の C さんが，外部のインシデント対応研修に参加して得た知識を基に手順を手探りしながらも調査したところ，次のことが分かった。

・9 月 4 日 14 時 30 分頃，②業務 PC-LAN に接続されている PC である PC-A がサイト M にアクセスし，“new3.exe” をダウンロードした。

・PC-A の利用者は開発部の D さんである。

・プロキシサーバのログに，上記のダウンロードの直後，③PC-A が特定のサイトにアクセスし，その後頻繁に同じサイトにアクセスを繰り返す様子が記録されていた。プロキシサーバのログのうち，送信元が PC-A であるものを図 6 に示す。

```
 1: [04/Sep/2018:14:23:34 +0900] "GET http://xxxx/ HTTP/1.1" 200 57028 "-" "▲▲"
 2: [04/Sep/2018:14:28:42 +0900] "GET http://zzzz/2018/ne/bunrei.html HTTP/1.1" 200 14252
  "http://zzzz/2018/ne/topics.html" "▲▲"
 3: [04/Sep/2018:14:29:22 +0900] "GET http://xxxx/news/2018_3325.html HTTP/1.1" 200 22177
  "http://xxxx/" "▲▲"
 4: [04/Sep/2018:14:31:15 +0900] "GET http://yyyy/dl/samplebun.zip HTTP/1.1" 200 89331
  "http://zzzz/2018/ne/bunrei.html" "▲▲"
 5: [04/Sep/2018:14:31:23 +0900] "GET http://xxxx/news/2018_3353.html HTTP/1.1" 200 24555
  "http://xxxx/" "▲▲"
 6: [04/Sep/2018:14:34:20 +0900] "GET http://IPm/ HTTP/1.1" 200 563 "-" "▽▽"
 7: [04/Sep/2018:14:35:31 +0900] "GET http://IPm/dl/new3.exe HTTP/1.1" 200 143623 "-" "▽▽"
 8: [04/Sep/2018:14:37:06 +0900] "GET http://IPn/news.php HTTP/1.1" 200 5429 "-" "▽▽"
 9: [04/Sep/2018:14:37:32 +0900] "POST http://IPn/login/pro.php HTTP/1.1" 200 646 "-" "▽▽"
10: [04/Sep/2018:14:37:32 +0900] "POST http://IPn/login/pro.php HTTP/1.1" 200 35621 "-" "▽▽"
11: [04/Sep/2018:14:37:37 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
12: [04/Sep/2018:14:37:47 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
13: [04/Sep/2018:14:37:52 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
14: [04/Sep/2018:14:37:58 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
15: [04/Sep/2018:14:38:04 +0900] "GET http://IPn/login/pro.php HTTP/1.1" 200 563 "-" "▽▽"
16: [04/Sep/2018:14:38:09 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
17: [04/Sep/2018:14:38:14 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
18: [04/Sep/2018:14:38:19 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
```

図 6　プロキシサーバのログのうち，送信元が PC-A であるもの

```
（省略）
19: [05/Sep/2018:16:43:51 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
20: [05/Sep/2018:16:43:56 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
21: [05/Sep/2018:16:44:01 +0900] "POST http://IPn/login/pro.php HTTP/1.1" 200 35614 "-" "▽▽"
22: [05/Sep/2018:16:44:05 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
（省略）
23: [06/Sep/2018:20:12:33 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
24: [06/Sep/2018:20:12:39 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
25: [06/Sep/2018:20:12:44 +0900] "GET http://IPn/admin/g.php HTTP/1.1" 200 563 "-" "▽▽"
26: [06/Sep/2018:20:12:48 +0900] "POST http://IPn/news.php HTTP/1.1" 200 451 "-" "▽▽"
（省略）
27: [08/Sep/2018:03:39:04 +0900] "GET http://IPn/login/pro.php HTTP/1.1" 200 563 "-" "▽▽"
28: [08/Sep/2018:03:39:04 +0900] "POST http://IPn/admin/g.php HTTP/1.1" 200 35618 "-" "▽▽"
29: [08/Sep/2018:03:39:08 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
30: [08/Sep/2018:03:39:12 +0900] "GET http://IPn/news.php HTTP/1.1" 200 563 "-" "▽▽"
```

注記1　インシデントQとの関係が疑われるエントリを示す。

注記2　プロキシサーバが取得したログのうち，日時，リクエストのメソッド，リクエストのURL，リクエストのプロトコルとバージョン，要求元PCに送信したレスポンスのHTTPステータスコード，要求元PCに送信したレスポンスメッセージのサイズ，リクエストのRefererヘッダの値，及びリクエストのUser-Agentヘッダの値を示す。

注記3　図中のxxxx，yyyy，zzzzは，それぞれ，A社以外の特定のFQDNを示す。

注記4　図中のIPmはサイトMのIPアドレス，IPnはIPmとは異なる特定のIPアドレスを示す。

注記5　図中の▲▲及び▽▽は，それぞれ，特定のユーザエージェントを表す文字列を示す。

図6　プロキシサーバのログのうち，送信元がPC-Aであるもの（続き）

Cさんは，直ちに④PC-Aをネットワークから切断して回収した。また，ここまでに分かったことを基に，［　k　］を調査して，マルウェアKがほかの機器にも感染している可能性を簡易的に確認した。

その後，Cさんは，試行錯誤しながら更に詳しく調査を進め，図7に示す調査結果を得た。

Dさんは業務で複数の機器を利用している。そのうち，PC-A及び開発用のPC-BがインシデントQに関係していることが強く疑われる。

(1) PC-Aについて

・PC-Aは，Windows PCであり，業務PC-LANに接続されている。IPアドレスは192.168.70.131である。

・Dさんのユーザフォルダ内で“new3.exe”が見つかった。当該ファイルのプロパティ情報における作成日時は9月4日14時35分であった。

・Dさんのユーザフォルダ内で，アイコンを文書ファイルのアイコンに偽装した実行形式のファイルWが見つかった。

　ファイルWの情報：

　　ファイル名“samplebun.docx␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣␣.exe”

　　プロパティ情報における作成日時　8月20日16時31分

・“new3.exe”及びファイルWをマルウェア対策ソフトベンダであるY社に提供してファイル解析を依頼し，表1の情報を得た。

(2) PC-Bについて

・PC-Bは，Linux PCであり，開発LANに接続されている。IPアドレスは192.168.75.245である。Dさんは，PC-Bを主にPC-Aからリモートログインして利用している。

・9月5日10時35分から45分までに，PC-Aから，⑤Dさんの利用者IDでのログイン試行が複数あり，一部は失敗し，一部は成功していた。PC-B上でのlast及びlastbコマンドの実行結果を，図8と図9にそれぞれ示す。lastはログイン履歴を，lastbはログイン失敗の履歴を出力するコマンドである。図中の“d0325”は，Dさんの利用者IDである。

・PC-Bのディレクトリ“/tmp/20xx/”に次のファイルが置かれていた。

　・新製品αの設計資料

　・文書Yを含む新製品αの操作説明書の草稿

　・そのほかのファイル

　・上記のファイルを格納したアーカイブファイル（以下，ファイルAという）

　ファイルAの所有者はDさんであり，作成日時は9月7日4時15分であった。規則では，設計資料及び操作説明書のファイルはそのアーカイブファイルも含めてサーバ上にだけ保管することになっている。

(3) Dさんへのヒアリングによって得た情報

・Dさんは，サイトMにアクセスした記憶はない。

・Dさんは，9月4日午後にPC-AのWebブラウザを用いてインターネットで挨拶文例を検索し，見つけたZIP形式のファイル“samplebun.zip”をダウンロードした。Dさんは，このファイルを展開した上で，中にあったファイルWをダブルクリックし参考にした。

・Dさんは，出張のため9月5日から7日までオフィスに来ておらず，PC-Aを利用していない。この間，PC-AとPC-Bの電源は入ったままで，PC-Bはリモートログインできる状態だった。

・Dさんは，利用している機器について，それぞれの利用者IDとパスワードをファイルに記録し，PC-Aに保管していた。

・Dさんは，PC-Bの“/tmp/20xx/”ディレクトリ及びその下に置かれていたファイルについて，心当たりがない。

注記　ファイル名の“␣”は空白文字を示す。

図7　調査結果（抜粋）

表1　ファイルについての情報

ファイル	説明
new3.exe	遠隔操作の機能をもつマルウェアKである。実行されると，IPnのサイトにアクセスして，そのレスポンスに従って動作する。また，指定されたファイルを，HTTPのPOSTメソッドを用いてIPnのサイトに送信する機能をもつ。
ファイルW	ダウンローダの機能をもつマルウェアLである。サイトMからプログラムをダウンロードし，実行する。また，これらの処理と並行して文書作成ソフトを起動し，特定の文書を表示する。

```
d0325    pts/0      192.168.70.131   Fri Sep  7 01:33 - 09:40 (08:06)
d0325    pts/0      192.168.70.131   Wed Sep  5 10:45 - 22:13 (11:27)
d0325    pts/0      192.168.70.131   Wed Sep  5 10:41 - 10:43 (00:01)
d0325    pts/0      192.168.70.131   Tue Sep  4 11:20 - 13:45 (02:24)
d0325    pts/0      192.168.70.131   Mon Sep  3 09:35 - 20:23 (10:47)
```

注記　lastコマンドの実行結果のうち，9月1日から7日までの期間における利用者ID“d0325”に関わる全ての行を抽出した。

図8　lastコマンドの実行結果

```
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:44 - 10:44 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:44 - 10:44 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:43 - 10:43 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:40 - 10:40 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:37 - 10:37 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:37 - 10:37 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:37 - 10:37 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:36 - 10:36 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:36 - 10:36 (00:00)
d0325    ssh:notty  192.168.70.131   Wed Sep  5 10:35 - 10:35 (00:00)
d0325    ssh:notty  192.168.70.131   Mon Sep  3 09:34 - 09:34 (00:00)
```

注記　lastbコマンドの実行結果のうち，9月1日から7日までの期間における利用者ID“d0325”に関わる全ての行を抽出した。

図9　lastbコマンドの実行結果

次は，これまでの調査結果についての，Cさんと G部長との会話である。

Cさん：PC-A が攻撃者によって遠隔操作されたことは間違いないと思います。また，PC-B は，少なくとも，Dさんがオフィスに来ていなかった9月5日に攻撃者に遠隔操作されていたようです。

G部長：PC-B で見つかったファイルAについては，どのように考えればよいか。

C さん：ファイル A は，情報を社外に送信するために攻撃者が作成したと考えればよいと思います。しかし，PC-B はインターネットにアクセスできないので，情報は社外に送信されなかったと思われます。

G 部長：そうだろうか。例えば，ほかの機器を経由して送信された可能性はないのか。

C さん：ほかの機器もいろいろと調査しましたが，ファイル A と同じ名前のファイルは見つかりませんでした。

G 部長：ファイル名が同じとは限らない。ファイルが既に削除されている可能性もある。そういった可能性も考えて調査を続けてほしい。

C さんは，D さんが利用している機器について，フォレンジックツールを用いて，ファイル A のファイルサイズと［ l ］をキーにしてファイルを検索した。その結果，PC-A において，9 月 8 日 3 時 35 分に，ファイル名は異なっていたものの，ファイル A と同じ内容のファイルが作成されていたことが分かった。また，プロキシサーバのログから，⑥当該ファイルが社外に送信された可能性があることが分かった。

加えて，C さんがインターネット検索をしたところ，ファイル A に格納されていた複数のファイルが，掲示板 U に，インシデント P のときと同じ投稿者によって投稿されていたことが分かった。これらのファイルのうち幾つかは，USB メモリ R に格納されたことはないと考えられるものだった。

〔インシデント Q のタイムラインと措置〕

G 部長は，調査結果の確認及び対応措置の検討について F 氏の支援を受けるよう C さんに指示した。F 氏の支援を受けて C さんが作成したインシデント Q のタイムラインを表 2 に示す。

表2　インシデントQのタイムライン

No.	日時	事象
1	ア	Dさんは，PC-AのWebブラウザで社外のサイトにアクセスし，ファイルWを格納したZIP形式のファイルをダウンロード
2	9/4 14:XX	Dさんは，No.1でダウンロードしたファイルをPC-A上で展開してファイルWを取り出した上で，これをダブルクリックし，m を実行
3	9/4 14:35	m は，n にアクセスし，“new3.exe”をダウンロード
4	9/4 14:XX	m は，o を実行
5	イ	o は，IPnのサイトとの頻繁な通信を開始 攻撃者による p が始まったと推測
6	9/5 10:35	攻撃者はPC-Bへのログインの試行を開始
7	ウ	攻撃者はPC-Bへのログインに初成功
8	～9/7 4:15	攻撃者は，漏えいが疑われるファイルのコピーと q を，r のローカルディスクに作成
9	9/8 3:35	攻撃者は，q と同じ内容のファイルを s のローカルディスクに作成
10	不明	No.9で作成されたファイルがIPnのサイトに送信された可能性

注記　XXは，正確な時刻が不明であることを示す。

また，F氏による追加調査の結果，社内の文書Zが，9月22日までの間に，攻撃者によって社外に送信されていたことが確認された。文書Zは，それまでに漏えいしたものとは別の新製品βの設計書である。

Cさんは，F氏の支援を受け，インシデントの封じ込め，根絶及び復旧のための措置を検討した。マルウェアLとマルウェアKについては，Y社から，これらを検知するためのマルウェア定義ファイルの提供を受け，全てのサーバ及びPCに適用することにした。Cさんは，そのほか必要と思われる措置をまとめて，G部長に提案した。G部長は，Cさんの提案を承認し，承認された措置が実施された。

〔インシデント対応のレビュー〕

インシデントQの対応が一段落した後，インシデント対応ポリシに従い，インシデントQの対応についてレビューが開催された。レビューにおいて，最初にG部長から，インシデントPとインシデントQは一連の攻撃だと推定されるという報告があった。次にインシデントQの対応が報告された。インシデントQの対応は，イン

シデント P の対応に比べて大幅に改善されたとの評価を受け，インシデント対応能力が向上してきていると判断された。最後に，⑦インシデント対応能力について未対応の課題を解決するための措置がまとめられ，順次実施されていくことになった。

設問1　〔早期に取り組むべき事項のとりまとめ〕について，(1)，(2)に答えよ。

(1)　図 4 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　ISO/IEC 15408 の PP の作成　　イ　教育と意識向上

ウ　情報セキュリティポリシの管理　　エ　侵入検知

オ　内部統制基準の作成　　カ　ネットワーク機器の保守

(2)　図 5 中の［ c ］～［ e ］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　CVSS v3 基本値　　イ　SIEM　　ウ　インシデント

エ　受付窓口　　オ　個人情報　　カ　情報公開

キ　情報システム部門　　ク　ポリシ　　ケ　マネジメント層

コ　優先順位付け　　サ　ログと証跡

設問2　〔インシデント対応能力の向上への取組み〕について，(1)～(3)に答えよ。

(1)　本文中の［ f ］～［ h ］に入れる適切な字句を，それぞれ 12 字以内で答えよ。

(2)　本文中の［ i ］，［ j ］に入れる適切な字句を，それぞれ 8 字以内で答えよ。

(3)　本文中の下線①について，取得した通常時プロファイルの利用方法を 35 字以内で具体的に述べよ。

設問3　〔マルウェアについての通知〕について，(1)～(7)に答えよ。

(1)　本文中の下線②について，サイト M にアクセスした PC を特定した方法を，60 字以内で具体的に述べよ。

(2)　本文中の下線③について，このアクセスによってマルウェアが何を行っていたと考えられるか。HTTP リクエストと HTTP レスポンスによってマルウ

エアが行っていた活動を，HTTP リクエストによる活動は 30 字以内で，HTTP レスポンスによる活動は 20 字以内でそれぞれ具体的に述べよ。

(3) 本文中の下線④について，調査の観点から見たときの問題は何か。40 字以内で具体的に述べよ。また，この問題を軽減するために本文中の下線④を実行する前に行うべき措置を，30 字以内で具体的に述べよ。

(4) 本文中の［ k ］に入れる適切な調査内容を，40 字以内で具体的に述べよ。

(5) 図 7 中の下線⑤について，D さんの利用者 ID を用いた PC-B へのログインに最初に成功するまでに，攻撃者が何回ログインに失敗したことが記録されているか。記録されている失敗の回数を答えよ。

(6) 本文中の［ l ］に入れる適切な字句を，8 字以内で答えよ。

(7) 本文中の下線⑥について，ファイルの社外への送信の可能性を示す記録を図 6 中から選び，行番号で答えよ。また，プロキシサーバ又は FW が取得できる情報のうち，当該記録と併せて見ることによってファイル送信の有無を判断するのに役立つ情報を 35 字以内で答えよ。ただし，送信元の IP アドレス及び図 6 中に示された情報は対象外とする。

設問 4 〔インシデント Q のタイムラインと措置〕について，(1)，(2) に答えよ。

(1) 表 2 中の［ ア ］～［ ウ ］に入れる適切な日時を答えよ。

(2) 表 2 中の［ m ］～［ s ］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 “samplebun.zip”	イ C さん	ウ D さん
エ IPn のサイト	オ PC-A	カ PC-B
キ SQL インジェクション	ク WHOIS サービス	ケ 遠隔操作
コ サイト M	サ 総当たり攻撃	シ ファイル A
ス フィッシング	セ プロキシサーバ	ソ マルウェア K
タ マルウェア L		

設問 5 本文中の下線⑦について，図 3 中の(6)に示された課題 a ～ d の中から，この時点で未対応の課題を選び，記号で答えよ。また，その課題を解決するための措置を，25 字以内で具体的に述べよ。

〔 メ モ 用 紙 〕

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	15:10 ～ 16:20

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。

午