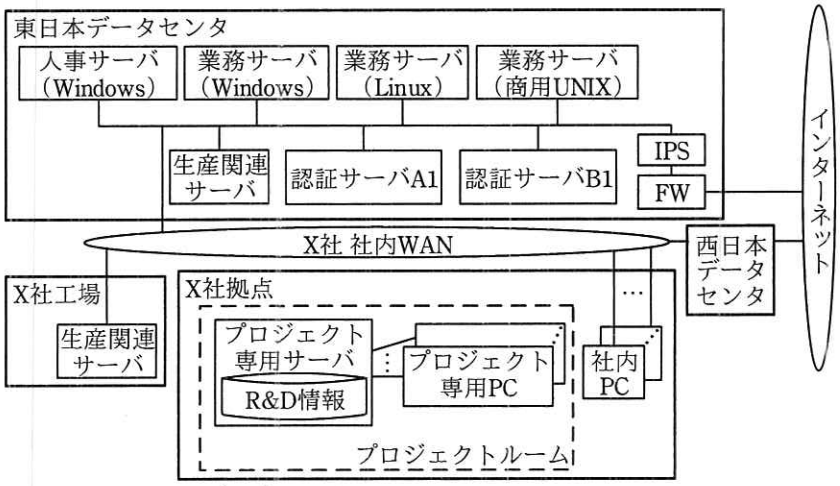
問1　クラウド環境におけるセキュリティ対策に関する次の記述を読んで，設問 1～5 に答えよ。

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。

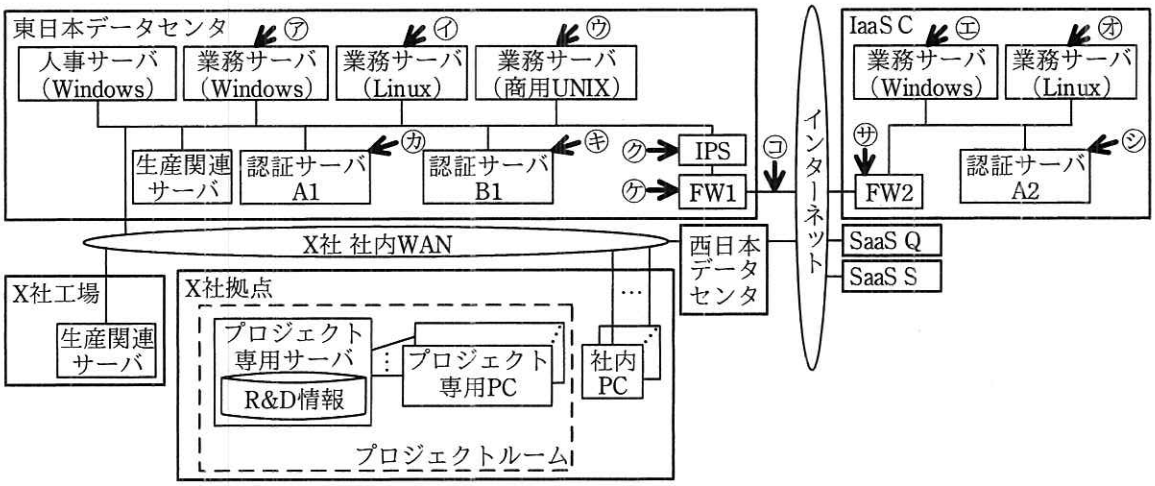


図2　案1における日本国内のハイブリッドクラウド環境の論理構成

〔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

ェ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。

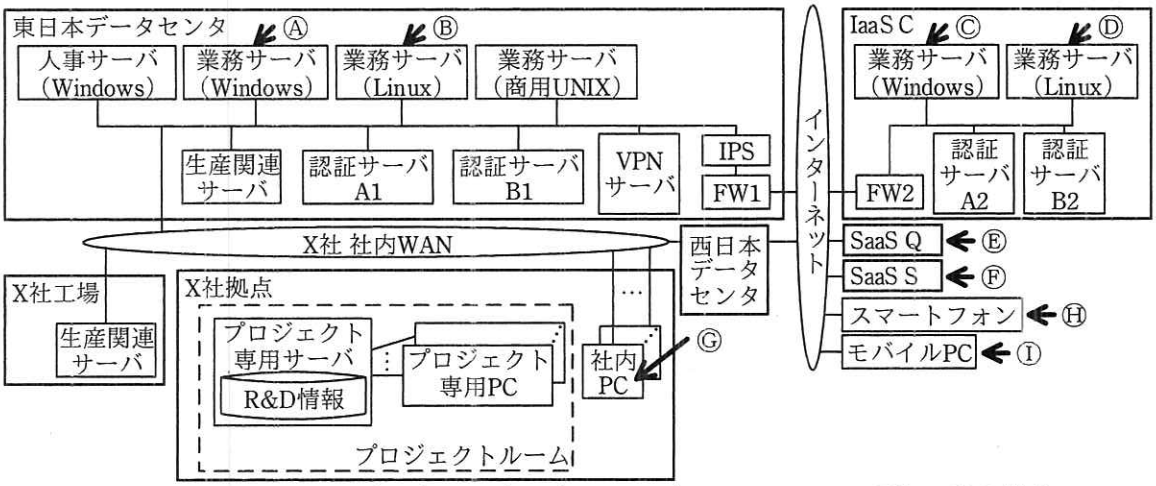


図 3　モバイル環境を含む日本国内のハイブリッドクラウド環境の論理構成

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。

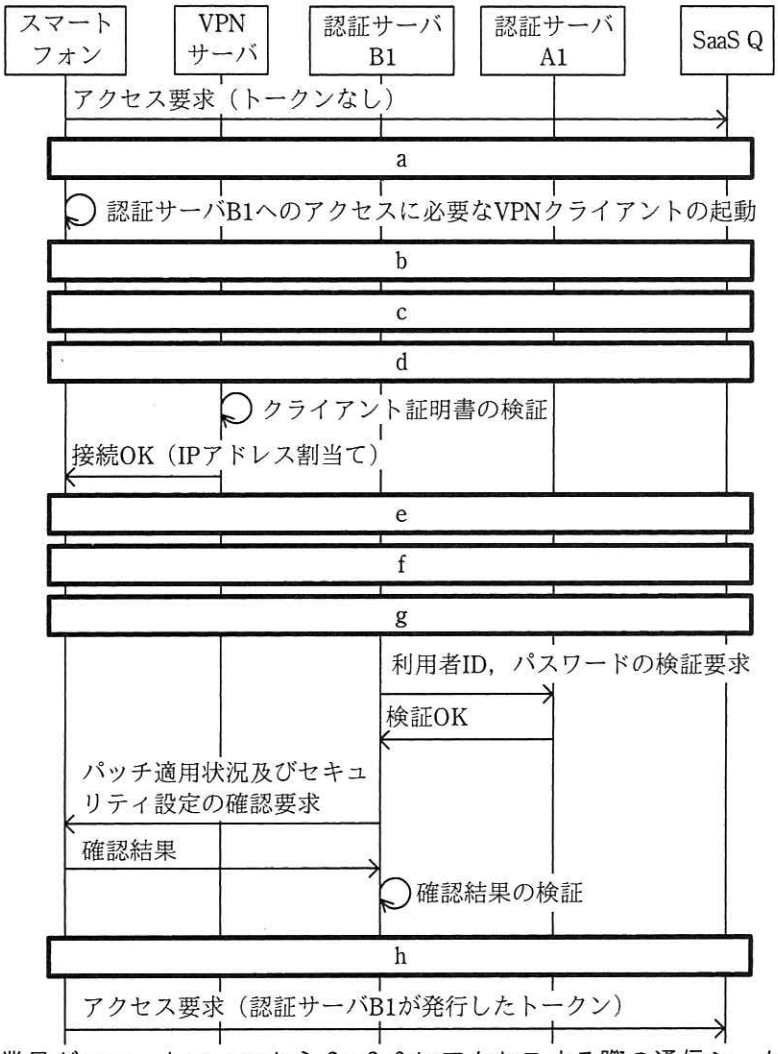


図4　従業員がスマートフォンから SaaS Q にアクセスする際の通信シーケンス

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～㋚で答えよ。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～㋚で答えよ。

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Ⓐ～Ⓘ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