問3　スマートデバイスの業務利用における情報セキュリティ対策に関する次の記述を読んで，設問1，2に答えよ。

J社は，従業員数150名の消費者向け化粧品販売会社である。J社は，自社で構築したECサイトを通して商品を販売している。J社には営業企画部，情報システム部，人事総務部，ロジスティック部などがある。

J社では，情報セキュリティ委員会（以下，委員会という）を毎月末に開催しており，最高情報セキュリティ責任者（CISO）が委員長を，各部の部長が委員を務めている。各部の部長は，自部署の情報セキュリティ責任者を兼ねている。また各部には，情報セキュリティの推進者として，情報セキュリティリーダを配置している。委員会では，情報セキュリティ関連規程の整備，情報セキュリティ対策の強化などが検討される。CISOは，委員会に提案する規程，マニュアル，対策などは提案前に十分に検証するように提案者に指示している。

J社は，取引先訪問中など，いつでも，どこでも仕事ができる制度（以下，モバイルワークという）を，主に営業企画部の従業員を対象に，1年前から導入している。営業企画部のモバイルワークは，営業企画部の情報セキュリティリーダであるR課長が中心となって管理することになっており，情報システム部のG主任がモバイルワークのシステム運用担当者（以下，運用担当者という）として支援している。

現在，モバイルワークを利用する従業員（以下，モバイルワーカという）は20名おり，モバイルワークについて改善点や問題点などを発見した場合は，R課長に連絡することになっている。J社はモバイルワーク用に許可した機器（以下，モバイル端末という）としてノートPCを一人1台貸与している。

モバイルワーク利用規程を図1に，モバイルワークで使用が認められているソフトウェア及びその用途を表1に示す。

・モバイルワークの利用を希望する従業員は，モバイル端末利用申請書に必要事項（所属部門，従業員 ID，従業員氏名，申請理由，モバイルワーク利用期間）を記入し，所属部門長の承認を得た後，情報システム部に提出すること
・モバイルワーカは，モバイル端末のセキュリティ設定のうち，情報システム部が指定したものを変更しないこと
・モバイルワーカは，モバイル端末で社外から内部ネットワーク及びインターネットにアクセスする場合，会社が用意した VPN 経由で VPN サーバに接続し，自らの利用者アカウントを用いてログインすること
・モバイルワーカは，業務データをモバイル端末に保存したままにせずに，内部ネットワークのファイルサーバに保存すること
・モバイルワーカは，取引先とのファイル共有に会社が用意したファイル共有サービスだけを使用すること
・モバイルワーカは，モバイル端末を紛失した場合，速やかに運用担当者に連絡すること
・運用担当者は，モバイルワーク利用期間が終了したモバイル端末を速やかに初期化すること

図 1　モバイルワーク利用規程（抜粋）

表 1　モバイルワークで使用が認められているソフトウェア及びその用途

ソフトウェア	提供元	用途
電子メールソフト	B 社	・社内及び社外の関係者との業務連絡
オフィスソフト	B 社	・データの集計や分析，報告書などの資料作成
Web ブラウザ	B 社	・業務での Web サイトへのアクセス及び会社が用意したファイル共有サービスの利用

J 社では，取引先や社外の関係者とのファイル共有のために B 社のファイル共有サービスを用意している。B 社のファイル共有サービスは法人向けのクラウドサービスである。モバイルワーカが社外からインターネットにアクセスする場合は，必ず J 社の DMZ 上の VPN サーバからプロキシサーバを経由してアクセスする。プロキシサーバには利用者認証機能はあるが，その機能は現在使用していない。一方，J 社からインターネット上の Web サイト及びファイル共有サービスへのアクセスは，ホワイトリスト方式によって制御している。B 社のファイル共有サービスには，アクセス元に対する IP アドレス制限機能が実装されているが，その機能は現在使用していない。

営業企画部は，モバイルワーカを対象にモバイルワークに関する満足度調査を実施した。調査では，ノート PC は大きく重いのでスマートフォンやタブレット（以下，スマートデバイスという）に替えてほしいという要望が多かった。また，他社では個人所有のスマートデバイスを業務で活用することによって業務の生産性が向上したという事例があるので，併せて検討してほしいという要望もあった。

〔情報セキュリティ上のリスクと対策〕

営業企画部の情報セキュリティ責任者である K 部長は，スマートデバイスを人数を限定して試験的に利用させることにし，スマートデバイスの利用案を G 主任と検討して，報告するよう R 課長に指示した。

利用案の検討に当たり，G 主任は，スマートデバイスの一般的な機能を図 2 のとおりまとめた。G 主任は R 課長に，モバイルワークで使用する表 1 のソフトウェアはスマートデバイス用のアプリケーションソフトウェア（以下，アプリという）としても B 社から提供されている（以下，B 社から提供されているアプリを B 社アプリという）と伝えた。

a) ネットワーク接続
・無線 LAN 又は携帯電話網を利用できる。
b) アプリの利用
・アプリを配布するマーケット [1]（以下，アプリストアという）からアプリを選んでスマートデバイスに導入できる。
c) 記憶媒体へのデータ保存
・内蔵されている記憶媒体（以下，内部記憶媒体という）にアプリや写真などのデータを保存できる。
・機種によっては，データをマイクロ SD カードなどの外部記憶媒体にも保存できる。
d) SIM カードの使い分け
・機種によっては，携帯電話事業者の SIM カードを使い分けることができる。

注 [1] マーケットは，スマートデバイスの OS ベンダなどが運用している。それらの中には，アプリの安全性審査を行っていないところがある。

図 2　スマートデバイスの一般的な機能（抜粋）

R 課長がスマートデバイスの利用案をまとめ，K 部長に報告したところ，モバイルワークにスマートデバイスを利用した場合の情報セキュリティ上のリスクと対策についても検討し，報告するよう指示を受けた。

早速，R 課長と G 主任は，リスクと対策案を表 2 のとおりまとめ，さらに R 課長は G 主任に，表 2 の対策を実現する方法を調査するよう依頼した。

表2　モバイルワークにスマートデバイスを利用した場合のリスクと対策案（抜粋）

リスク	対策案（J社で実施中の対策を含む）
モバイルワーカ以外によるスマートデバイスの不正利用及び内部ネットワークへの侵入	・スマートデバイスのロック[1)]を解除するためのパスワードを設定・変更 ・［　a　］
スマートデバイスの紛失・盗難による情報漏えい及び消失	・紛失・盗難時に，スマートデバイスを遠隔操作で運用担当者がロック ・紛失・盗難時に，スマートデバイスの内部記憶媒体及びスマートデバイスに装着している外部記憶媒体の全領域を遠隔操作で運用担当者が初期化 ・［　b　］
通信内容の盗聴及び改ざん	（省略）
スマートデバイスのマルウェア感染	・OS及びアプリの最新版を利用 ・マルウェア対策用のアプリを導入 ・J社が指定したWebサイトにだけアクセス ・J社が指定したアプリだけを使用 ・［　c　］
知識不足による誤操作	・［　d1　］ ・［　d2　］
①利用者による OS の改造（Jailbreak，root 化など）	・OSの改造の禁止をモバイルワーク利用規程に追加

注記　リスクに対して複数の対策案が示されている場合は，全て行うことを意味する。

注[1)]　スマートデバイスのロックとは，パスワードなどによって認証されないとスマートデバイスの操作ができないようにする機能のことである。

〔対策の実現に向けた調査〕

G主任が調査したところ，表2の対策を実現する上で利用可能な機能をもつクラウドサービスが複数のベンダから提供されていた。G主任はその中でも，市場シェアが高いE社のクラウドサービスMM1及びMM2を対策の候補とし，それぞれが提供している機能を図3のとおりまとめ，R課長に報告した。

1. MM1 の機能
1-1 自動で実行される機能
・端末データ（電話番号，国際移動体装置識別番号 [1]，機種名，位置情報，OS 名及びバージョン，並びに導入済みの全てのアプリの名称及びバージョン）の収集
・スマートデバイスの内部記憶媒体及びスマートデバイスに装着されている外部記憶媒体の全領域の暗号化
・OS 改造の検知
1-2 管理画面 [2] 上で手動で実行できる機能
・スマートデバイスのロック
・スマートデバイスのロックを解除するためのパスワード設定・変更
・アクセスできる Web サイト及び導入できるアプリの制限
・スマートデバイスの内部記憶媒体及びスマートデバイスに装着されている外部記憶媒体の全領域の初期化
・スマートデバイスへのアプリの配布
・端末データの閲覧
2. MM2 の機能
2-1 自動で実行される機能
・アプリによって生成される業務データを保存するフォルダ（以下，業務フォルダという）の作成
・内部記憶媒体のうち，業務フォルダが使用する領域の暗号化
・業務フォルダ内のデータの，スマートデバイス内の業務フォルダ以外の領域への移動禁止，複製禁止
・端末データ（電話番号，国際移動体装置識別番号，機種名，OS 名及びバージョン，並びに業務フォルダ内のアプリの名称及びバージョン）の収集
・OS 改造の検知
2-2 管理画面上で手動で実行できる機能
・業務フォルダにアクセスするためのパスワード設定の強制
・業務フォルダへのアプリの配布
・業務フォルダ内の初期化
・端末データの閲覧

注記　図中の機能は，アプリストアで提供されている E 社のエージェントアプリをスマートデバイスに導入している場合にだけ有効である。

注 [1]　国際移動体装置識別番号とは，スマートデバイスなどの情報端末ごとに割り当てられた固有の識別番号のことである。

注 [2]　管理画面とは，運用担当者がアクセスできるクラウドサービス上の Web 画面のことである。MM2 も同様である。

図 3　MM1 及び MM2 の機能（抜粋）

MM1 と MM2 の機能を比較すると，MM1 は［ e1 ］を保護対象にすることによって情報漏えいを防ぐ。MM2 は［ e2 ］を保護対象にすることによって情報漏えいを防ぐ。

R 課長は，MM1 又は MM2 を個人所有のスマートデバイスで使用する場合，幾つかの課題があることに気付いた。そこで，R 課長は G 主任の協力を得て，課題とその解決案を表 3 のとおりまとめた。

表 3　課題とその解決案

項番	課題	解決案
1	MM1 が収集した端末データを運用担当者が閲覧した場合，モバイルワーカから J 社にプライバシ侵害のクレームがある。	・委員会がモバイルワークの利用を希望する従業員に対して，運用担当者による端末データの閲覧範囲について，［ f ］。 （省略）
2	スマートデバイスの紛失・盗難時に，運用担当者が MM1 の機能を実行すると機能によっては次のいずれかが起きる。 ・［ g ］。 ・［ h ］。	（省略）
3	許可されていない個人所有のスマートデバイスが使用される。	・②モバイル端末利用申請書の一部を修正する。
4	J 社が購入した B 社アプリのライセンスが，許可されていない個人所有のスマートデバイスで使用される。	・③B 社アプリを J 社が許可した個人所有のスマートデバイスにだけ配布するという運用手順を定める。

R 課長は，G 主任と一緒に検討した案をまとめ，K 部長に報告した。

後日，検討した案は委員会で説明され，モバイルワークでのスマートデバイスの人数を限定した試験的な利用が承認された。試験的な利用はモバイルワーカに好評であり，情報セキュリティインシデントも起きていないことから，モバイルワークでのスマートデバイスの全社利用へと発展した。

設問1　〔情報セキュリティ上のリスクと対策〕について，(1)～(3)に答えよ。

(1)　表2中の［　a　］～［　c　］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

aに関する解答群

ア　B社のファイル共有サービスのIPアドレス制限機能を有効化

イ　VPNサーバへの接続時に利用者を認証

ウ　プロキシサーバでの利用者認証を有効化

エ　プロキシサーバのアクセス管理をブラックリスト方式に変更

bに関する解答群

ア　J社の内部ネットワークのファイルサーバに業務データを保存

イ　スマートデバイス内にフォルダを作成し，そこに業務データをバックアップ

ウ　スマートデバイスに常に装着されている外部記憶媒体に業務データをバックアップ

エ　モバイルワーカが個人で契約しているファイル共有サービスに業務データをバックアップ

cに関する解答群

ア　J社が指定したアプリストアだけを利用

イ　J社が指定した携帯電話事業者の無線LANサービスだけを利用

ウ　J社が指定した時間帯だけにアプリストアを利用

エ　J社が指定したプログラム言語だけでアプリを開発

(2) 表 2 中の［ d1 ］，［ d2 ］に入れる，次の (i) ～ (v) の組合せはどれか。d に関する解答群のうち，最も適切なものを選べ。

(i) 営業企画部は，参照先としてスマートデバイス及び B 社アプリの設定方法が掲載されているインターネット上の SNS やブログなどの URL を利用マニュアルに記載

(ii) 営業企画部は，実際に手順の検証を行い，スマートデバイス及び B 社アプリの利用マニュアルを作成

(iii) 営業企画部は，モバイルワーカが自分専用の利用マニュアルを独自に作成できるようにインターネット上の SNS やブログへのアクセスを許可

(iv) 営業企画部は，モバイルワーカがスマートデバイス及び B 社アプリの利用マニュアルに不備を発見した場合，直ちにモバイルワーカが修正することを推奨

(v) 営業企画部は，モバイルワーカにスマートデバイス及び B 社アプリの正しい設定，利用手順，注意事項などについて定期的に教育を実施

d に関する解答群

	d1	d2
ア	(i)	(iii)
イ	(i)	(iv)
ウ	(ii)	(iv)
エ	(ii)	(v)
オ	(iii)	(iv)
カ	(iv)	(v)

(3) 表 2 中の下線 ① が原因で起こり得る事象はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア OS の脆弱性を悪用されて，バックドアを仕掛けられる。

イ 公衆無線 LAN の電波と携帯電話回線の電波が干渉したときに，通話とインターネット通信ができなくなる。

ウ スマートデバイスの利用者が出荷時のセキュリティ設定を解除できるようになる。

エ 不正なショートメッセージサービスがスマートデバイスに送られたとき，架空の未払料金を請求されて支払うことになる。

オ 不正な電子メールがスマートデバイスに送られたときに，フィッシングサイトに誘導されて，個人情報が漏えいする。

設問2　〔対策の実現に向けた調査〕について，(1) ～ (4) に答えよ。

(1)　本文中の［ e1 ］，［ e2 ］に入れる，次の (i) ～ (v) の組合せはどれか。e に関する解答群のうち，最も適切なものを選べ。

(i)　エージェントアプリ

(ii)　公衆無線 LAN 及び携帯電話回線

(iii)　スマートデバイスに保存されている全てのデータ

(iv)　スマートデバイスの業務フォルダ内に保存されているデータ

(v)　スマートデバイスの操作ログ

e に関する解答群

	e1	e2
ア	(i)	(ii)
イ	(iii)	(iv)
ウ	(iii)	(v)
エ	(iv)	(iii)
オ	(iv)	(v)
カ	(v)	(iii)
キ	(v)	(iv)

(2) 表 3 項番 1 に示したクレームを避けるために，端末データの閲覧に先立ち実施しておくべき措置として，表 3 中の［ f ］に入れる字句はどれか。解答群のうち，最も適切なものを選べ。

f に関する解答群

ア　モバイルワーク利用前に口頭で説明する

イ　モバイルワーク利用前に書面で同意を得る

ウ　モバイルワーク利用前に説明し，その日時を記録する

エ　モバイルワーク利用前に電子メールで通知し，開封通知を保存する

(3) 表 3 中の［ g ］，［ h ］に入れる適切な字句を，解答群の中から選べ。

g，h に関する解答群

ア　業務データと私的データの両方のデータが消える

イ　業務データと私的データは残り，B 社アプリは消える

ウ　スマートデバイスがロックされるので，自動で初期化される

エ　スマートデバイスのロックを解除するためのパスワードが変更されるので，スマートデバイスを発見した場合，モバイルワーカ本人はロックを解除できず，利用することができない

(4) 表 3 中の下線 ② 及び下線 ③ について，修正内容と運用手順を，次の (i) ～ (v) の中から一つずつ挙げた組合せはどれか。解答群のうち，最も適切なものを選べ。

［モバイル端末利用申請書の修正内容］

(i) モバイルワークで使用する可能性がある全ての個人所有のスマートデバイスの機種名及び OS 名を記入できるように修正する。

(ii) モバイルワークで使用する個人所有のスマートデバイスの電話番号及び機種名を記入できるように修正する。

(iii) モバイルワークで使用する個人所有のスマートデバイスの電話番号及び国際移動体装置識別番号を記入できるように修正する。

［運用手順］

(iv) MM1 又は MM2 の管理画面上で，端末データが全項目とも収集されていることを複数の運用担当者が一緒に目視で確認した後，B 社アプリを MM1 又は MM2 を利用して配布する。

(v) MM1 又は MM2 の管理画面上の端末データと，モバイル端末利用申請書を運用担当者が目視で突合し，一致した場合にだけ B 社アプリを MM1 又は MM2 を利用して配布する。

解答群

ア (i), (iv)　　イ (i), (v)　　ウ (ii), (iv)

エ (ii), (v)　　オ (iii), (iv)　　カ (iii), (v)