問2　スマートフォンを利用したリモートアクセス環境に関する次の記述を読んで，設問1～3に答えよ。

D 社は，従業員数 5,000 名の情報システム会社である。D 社は，東京に本社とデータセンタをもち，全国 8 か所に支店をもっている。D 社従業員の多くは，他社との共同プロジェクトに参画する技術者，顧客訪問をする営業員などであり，主に社外で業務を行っている。

D 社では，このような業務形態を踏まえて，従業員が社外でも効率よく業務を行えるよう，全従業員にモバイル PC を 1 台ずつ貸与している。

従業員は，インターネット接続環境があれば，モバイル PC を VPN 経由で社内ネットワークに接続し，社内にいるときと同じように，メールサーバ及び社内 Web サーバにアクセスできる（以下，社外からのメールサーバ及び社内 Web サーバへのアクセスをリモートアクセスという）。モバイル PC とリモートアクセス環境は，業務を行うのに十分なものである。

モバイル PC を VPN 経由で社内ネットワークに接続する際は，まず，VPN サーバに登録された利用者 ID とパスワード（以下，VPN 認証情報という）による利用者認証が行われる。さらに，モバイル PC からメールサーバにアクセスする際は，メールサーバに登録された利用者 ID とパスワード（以下，メールサーバ認証情報という）による利用者認証が行われる。社内 Web サーバにアクセスする際は，利用者認証は行われない。メールサーバ認証情報と VPN 認証情報は異なるものを使用し，また，電子メール（以下，メールという）を他のメールアドレスに自動転送することがないよう，従業員がメールボックスの設定を変更できないようにしている。

モバイル PC に業務データを保存することは認められているが，情報漏えい対策としてハードディスク全体の暗号化が行われている。業務データを暗号化している場合でも，D 社の管理及び規程が及ばないサービス又はシステム，例えば，クラウドコンピューティングサービス（以下，クラウドサービスという）によって提供されるサービス，オンラインストレージサービス，ファイル共有システムなどを利用して保管することは禁止されている。また，業務上必要な場合を除き，利用者がメールを社外のメールアドレスに転送することは禁止されている。

〔スマートフォンを利用したリモートアクセス環境の構築〕

D 社は，従業員の利便性を更に向上させるために，移動中でもメールで社内及び顧

客への連絡が行えるよう，モバイル PC に加えて個人所有のスマートフォンからリモートアクセスできる環境を構築することにした。ただし，社内 Web サーバには機密情報が保管されているので，スマートフォンから社内 Web サーバへのアクセスは認めないことにした。

情報システム部の X 部長は，D 社におけるスマートフォンからのリモートアクセス環境について，希望した従業員だけに利用させる前提で実現方法を検討し，情報セキュリティスペシャリストの Z 主任のレビューを受けるよう，情報システム部の Y 氏に指示した。

Y 氏は，従業員の多くが所有している，スマートフォン A，B の仕様を調査した。Y 氏が整理した，スマートフォン A，B の環境を表 1 に，機能を表 2 に，それぞれ示す。

表 1　スマートフォン A，B の環境（抜粋）

種別 / 環境	スマートフォン A	スマートフォン B
OS	・スマートフォンベンダ H 社が提供している。内部仕様は非公開である。	・IT 企業 T 社が提供しているオープンソースソフトウェアをスマートフォンメーカ各社が搭載している。
アプリケーションインタフェース	・仕様が公開されている。	
アプリケーションの提供形態	・アプリケーション開発ベンダが H 社とアプリケーション提供の契約を締結すると，H 社からアプリケーション開発ベンダのディジタル証明書が発行される。ディジタル署名が付与されたアプリケーションは，H 社の安全性審査を受けることができる。 ・H 社の安全性審査に合格したアプリケーションは，インターネット上の H 社ストアから提供される。 ・スマートフォンの利用者が H 社ストアからアプリケーションを導入する際，アプリケーションのディジタル署名が検証される。ディジタル署名の検証に失敗した場合はエラーとなり，アプリケーションを導入できない。	・アプリケーションは，インターネット上の T 社ストア及び携帯電話事業者の Web サイトから提供されている。また，独自に開発したアプリケーションを公開している Web サイトもある。 ・アプリケーションの安全性審査及び導入時のディジタル署名の検証は行われない。 ・導入するアプリケーションの選択は，利用者に任されている。
OS 及びアプリケーションの更新方法	・OS 又はアプリケーションの更新があった場合は，通知メッセージが表示され，更新ボタンに触れると更新される。	・OS 又はアプリケーションの更新があった場合は，通知メッセージが表示され，更新ボタンに触れると更新が行われる。 ・OS 及び各アプリケーションに自動更新を設定できる。自動更新が設定されている場合は，通知メッセージが表示されることなく更新される。

表２　スマートフォンＡ，Ｂの機能（抜粋）

種別 機能	スマートフォンＡ	スマートフォンＢ
デバイス 保護機能	・デバイスパスワードが設定されている場合，電源を入れるとスマートフォンがロック状態になる。ロック解除には，デバイスパスワードの入力が必要である。 ・一定時間，スマートフォンを操作しなかった場合，スマートフォンを自動ロックさせる設定ができる。	
ネットワーク 接続機能	・無線 LAN を利用して，インターネットにアクセスできる。 ・VPN クライアント機能をもち，L2TP over IPsec 又は PPTP で VPN に接続できる。	
電話帳機能	・氏名，電話番号，メールアドレス，住所，画像データ，URL を登録したり検索したりすることができる。 ・電話の発着信履歴から電話番号を登録したり，登録済みの電話番号に電話を掛けたりすることができる。 ・受信したメールのメールアドレスを登録したり，メールクライアントからメールを送信する際に，登録されたメールアドレスを呼び出したりすることができる。	
メール クライアント	・メールクライアントが導入されており，POP3 によるメール受信及び SMTP によるメール送信ができる。メール受信においては POP3 over TLS を，メール送信においては SMTP over TLS を，それぞれ使用できる。 ・添付ファイル付き受信メールを閲覧するとファイル名が表示され，ファイル名を選択すると添付ファイルがメールサーバからスマートフォンにダウンロードされる。	
ブラウザ	・ブラウザが導入されており，Web サイトを閲覧できる。 ・Web サイトからファイルをダウンロードして，スマートフォンに保存できる。	
メディアプレーヤ及びドキュメントビューア	・メディアプレーヤ及びドキュメントビューアが導入されており，音声及び動画の再生並びに画像及び文書ファイルの表示ができる。	
外部記憶媒体の利用	・利用できない。	・マイクロ SDHC カードが利用できる。
PC との接続及びファイルコピー機能	・専用ケーブル又は無線 LAN を利用して，専用ソフトウェアが導入済みの PC と接続し，PC から音声，動画，画像及び文書ファイルをコピーしたり，スマートフォン上のデータのバックアップを PC 上に保管したりすることができる。	・USB ケーブルを利用して PC と接続し，スマートフォンの内蔵ストレージ及びスマートフォンのマイクロ SDHC カードを PC の外部記憶媒体として利用できる。
クラウドサービスの利用	・アプリケーションを導入・設定することなく，H 社が提供するクラウドサービスに接続し，スマートフォンに保存されている電話帳，メール，音声，動画，画像及び文書ファイルを，利用者が意識することなく，クラウドサービスのサーバに定期的にコピーする自動同期機能を利用できる。 ・一部の機種は，デフォルトの状態で自動同期機能が有効になっている。	・アプリケーションを導入・設定することでクラウドサービスに接続し，スマートフォンに保存されている電話帳，メール，音声，動画，画像及び文書ファイルを，利用者が意識することなく，クラウドサービスのサーバに定期的にコピーする自動同期機能を利用できる。 ・一部の機種では，デフォルトの状態で，アプリケーションが導入・設定済みであり，自動同期機能が有効になっている。

Ｙ氏は，スマートフォンからのリモートアクセス環境の案として，スマートフォンにメール及びメールアドレスを保存せずにメールを送受信できるようにする案１をま

とめた。

案 1 は，ネットワーク構成，実現方式，セキュリティ対策，スマートフォン利用手続及びセキュリティ規程から成っている。案 1 におけるネットワーク構成を図 1 に示す。以下，ネットワーク構成及びファイアウォール（以下，FW という）の設定において，各機器の冗長化，負荷分散装置，DNS に関する記載は省略する。

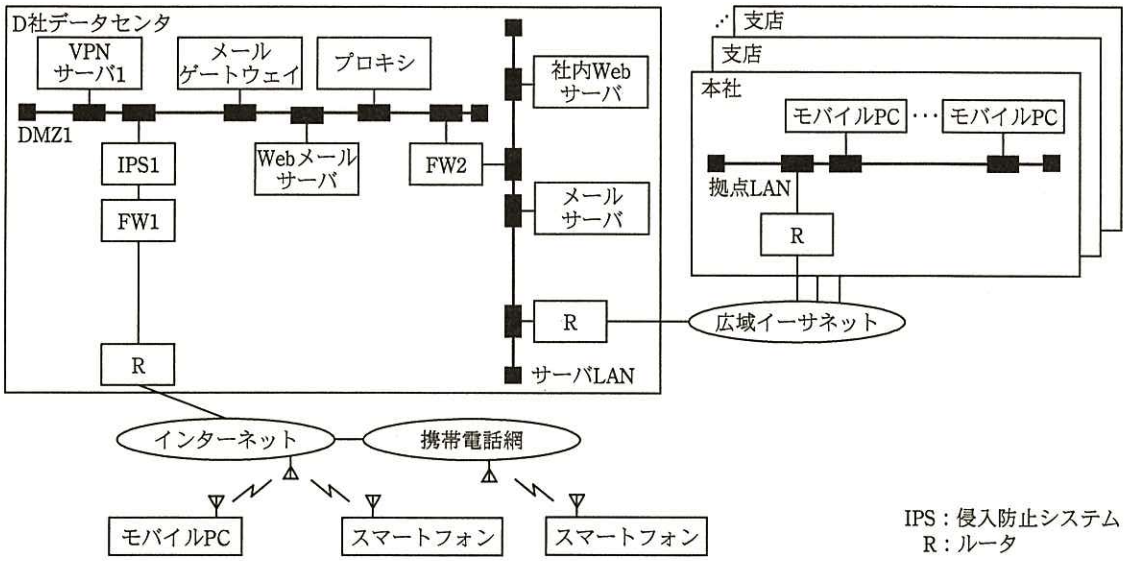

図 1　案 1 におけるネットワーク構成

案 1 における実現方式は次のとおりである。

(1) スマートフォンの VPN クライアント機能を用いて，L2TP over IPsec で既存の VPN サーバ 1 に接続する。L2TP は，イーサネットフレームが変換された PPP フレームをカプセル化して UDP で送受信するプロトコルであり，これと IPsec を組み合わせたものが L2TP over IPsec である。スマートフォンもモバイル PC も VPN サーバ 1 に接続された状態では，DMZ1 のネットワークセグメントの IP アドレスが割り当てられ，DMZ1 に接続されているのと同じように通信できる。

(2) Web メールサーバを構築し，スマートフォンのブラウザから利用できるようにする。Web メールサーバは，メールサーバに対してはメールクライアントとして動作し，スマートフォンに対してはアドレス帳とメールクライアントの機能を Web で提供する。スマートフォンのメールクライアントからメールサーバにアクセスするこ

とは禁止する。

案1におけるセキュリティ対策を図2に，FW1及びFW2で許可する通信を表3及び表4に，スマートフォン利用手続を図3に，セキュリティ規程を図4に示す。

1. FW1及びFW2の設定によって，インターネットとDMZ1間の通信及びDMZ1とサーバLAN間の通信は，業務上必要な通信に限定する。
2. スマートフォンからVPNサーバ1への接続においては，VPN認証情報による利用者認証を行う。
3. スマートフォンからWebメールサーバへのアクセスにおいては，メールサーバ認証情報による利用者認証を行う。
4. Webメールサーバの設定によって，メールの添付ファイルをスマートフォンに保存できないようにする。
5. ウイルス対策とFWの機能をもつ製品Fを，スマートフォンに導入・設定する。
6. スマートフォンの盗難及び紛失に備え，次の対策を行う。
   - 第三者に推測されにくいデバイスパスワードを設定する。
   - 盗難又は紛失の届出があった場合，VPNサーバ1の設定において当該利用者のVPNアカウントを停止する。

図2　案1におけるセキュリティ対策

表3　案1においてFW1で許可する通信

送信元	宛先	プロトコル
Any	VPNサーバ1	L2TP over IPsec
Any	メールゲートウェイ	SMTP
メールゲートウェイ	Any	SMTP
プロキシ	Any	HTTP
プロキシ	Any	HTTP over TLS

表4　案1においてFW2で許可する通信

送信元	宛先	プロトコル
DMZ1	メールサーバ	POP3
DMZ1	メールサーバ	SMTP
メールサーバ	メールゲートウェイ	SMTP
DMZ1	社内Webサーバ	HTTP
DMZ1	社内Webサーバ	HTTP over TLS
拠点LAN	プロキシ	HTTP
拠点LAN	プロキシ	HTTP over TLS

1. 利用申請

個人所有のスマートフォンA又はBを業務に利用することを選択した従業員は，スマートフォンを特定する次の項目を機器登録申請書に記入して所属長から承認を得た後，情報システム部に提出する。

(1) スマートフォンの種別（A又はBを選択）

(2) 携帯電話事業者名

(3) 機種名

(4) シリアル番号（スマートフォンAの場合）又はMACアドレス（スマートフォンBの場合）

2. スマートフォンの設定

スマートフォンの業務利用が承認された従業員は，次の設定を行う。

(1) H社ストア又はT社ストアから，製品Fをスマートフォンに導入し，ウイルス定義ファイルの自動更新を有効にする。

(2) スマートフォンのVPNクライアント機能に接続方法，接続先，VPN認証情報などを設定する。

(3) デバイス保護機能を次のように設定する。

(a) スマートフォンを操作しなかった場合は15分以内にロックが掛かり，デバイスパスワードを入力しないとロックを解除できないようにする。

(b) デバイスパスワードには，英字と数字の両方を含む8桁以上の文字列を設定する。

図3　案1におけるスマートフォン利用手続

1. スマートフォンの業務利用は，Webメールサーバを利用したメールの送受信に限定する。
2. 業務利用の必要性がなくなった場合は，スマートフォンから接続方法，接続先，VPN認証情報などを消去する。
3. メールを社外のメールアドレスに自動転送することを禁止する。
4. Jailbreak（脱獄）やroot化など，スマートフォンに設けられた制限を取り外す行為（以下，改造という）を禁止する。
5. アプリケーションは，H社ストア，T社ストア又は携帯電話事業者のWebサイトから導入する。
6. OS又はアプリケーションの更新通知があった場合は，速やかに更新する。
7. 情報システム部が配布するのぞき見防止フィルタを画面に貼り，第三者に画面を見られないよう注意する。
8. スマートフォンを盗まれたり，紛失したりした場合，速やかに所属長及び情報システム部に届け出る。

図4　案1におけるセキュリティ規程

Y氏は，案1について，Z主任のレビューを受けた。Z主任は，①D社が認めていないアクセスが技術的に可能になっている問題と，②スマートフォンの盗難又は紛失の届出があったときにとられる対策によって引き起こされる問題を指摘し，解決策をアドバイスした。また，Z主任は，セキュリティ規程に，“従業員はスマートフォンを業務に利用するか否かを自由に選択できる”と追記すること，及びスマートフォンを利用したリモートアクセス環境において想定されるセキュリティリスクと対策をまとめることをアドバイスした。

Y氏は，案1にZ主任のアドバイスを反映させた案2をまとめた。案2におけるネットワーク構成を図5に，想定されるセキュリティリスクと対策を表5に，それぞれ示す。

なお，FW1 及び FW2 の設定は表 3，4 と同じである。

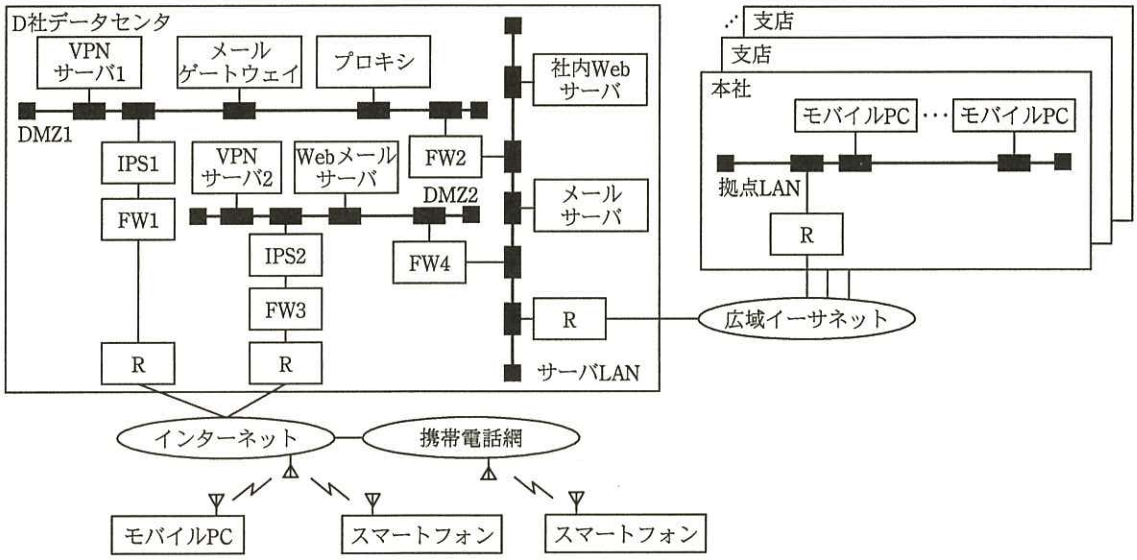

図 5　案 2 におけるネットワーク構成

表 5　案 2 において想定されるセキュリティリスクと対策

セキュリティリスク	対策
R1. インターネットから DMZ，サーバ LAN 及び拠点 LAN への侵入	C1. FW 及び IPS の設置
	C2. DMZ 上のサーバの要塞化 ・不要なサービスの停止 ・最新のセキュリティパッチの適用 ・デフォルト設定の管理者アカウントの変更
	C3. 情報システム部による，定期的な脆弱性診断
R2. インターネットにおける通信の盗聴	C4. VPN による暗号化通信
R3. 正規利用者へのなりすまし (盗難及び紛失時を含む)	C5. デバイス保護機能の設定
	C6. VPN サーバにおける利用者認証
	C7. メールサーバにおける利用者認証
	C8. 盗難及び紛失時の VPN アカウントの停止
R4. スマートフォンからの情報漏えい	C9. 業務メール及びメールアドレスのスマートフォンへの保存の禁止
R5. 画面からの情報漏えい	C10. のぞき見防止フィルタの利用
R6. メールサーバからの情報漏えい	C11. 業務目的以外でのメール転送の禁止
R7. スマートフォンの脆弱性の悪用	C12. 最新の OS の利用
	C13. 最新のアプリケーションの利用
	C14. 改造の禁止
R8. スマートフォンにおける不正コード	C15. アプリケーションの安全性審査
	C16. H 社ストア，T 社ストア及び携帯電話事業者の Web サイト以外からのアプリケーション導入の禁止
	C17. ウイルス対策ソフトの導入・設定

Y氏は，案2について，Z主任のレビューを受けた後，X部長の承認を得た。

D社は，案2に基づいたリモートアクセス環境を構築し，運用を開始した。

〔リモートアクセス環境の改善〕

スマートフォンを利用したリモートアクセス環境の運用開始から1年後，D社では約半数の従業員がスマートフォンを業務に利用するようになった。情報システム部は，スマートフォンを業務に利用している従業員に対してアンケートを行い，満足度及び利用状況を調査した。調査の結果，次のことが分かった。

(1) スマートフォンを利用したリモートアクセス環境に対する満足度は高いが，顧客から送られてきたメールの添付ファイルをスマートフォンにダウンロードして，ドキュメントビューアで閲覧できるようにしてほしいという要望が多い。

(2) スマートフォンの通信料金を節約するために，携帯電話網を介したデータ通信を無効化して，無線LAN経由でリモートアクセスを行っている従業員が多い。

一方，スマートフォンのアプリケーションの中には，利用者の位置情報，電話番号及び電話帳の情報をインターネット上のサーバに送信するものがあることが報道されている。

情報システム部はこれらの状況を踏まえ，リモートアクセス環境の改善に向けた検討を開始した。

X部長は，メールの添付ファイルをスマートフォンに保存することを認めた場合，スマートフォンに導入したアプリケーションが利用者の意図しない動作をし，情報漏えいが起きるリスクがあると考えた。そこで，必要となるセキュリティ対策を調査した上で，リモートアクセス環境の改善を検討するよう，Y氏に指示した。

Y氏が調査した結果，スマートフォンA，Bの設定，OS及びアプリケーションをサーバから一元管理する製品Eが販売されていることが分かった。製品Eは，スマートフォンに導入するEエージェントと，スマートフォンを管理したり通信を中継したりするEサーバから成る。EエージェントとEサーバは，互いにTCP/IPのプロトコルで通信することによって，次の機能を提供する。

・デバイス保護機能の設定及びスマートフォンの設定の監視と強制

・改造されたスマートフォンの検知

・OS 及びスマートフォンに導入されているアプリケーションの名称及びバージョンなどの取得
・スマートフォン及び外部記憶媒体に保存されたデータの暗号化
・スマートフォン及び外部記憶媒体に保存された全データのリモート消去

Y 氏は，従業員の利便性を更に向上させるために，案 3 をまとめた。案 3 では，スマートフォン及び外部記憶媒体にメールの添付ファイルを保存することを認める一方，現在のリモートアクセス環境に製品 E を適用してスマートフォンのセキュリティ管理を強化する。Y 氏は，スマートフォンを管理する E サーバ 1 をサーバ LAN に，E サーバ 1 と E エージェント間の通信を中継する E サーバ 2 を DMZ2 に，それぞれ配置し，FW3 及び FW4 で必要な通信を許可することにした。案 3 において追加したセキュリティ対策を図 6 に示す。

1. 製品 F が導入・設定されていることを，製品 E によって監視する。製品 F が導入されていない又は正しく設定されていないスマートフォンが検知された場合，情報システム部は，当該従業員（所有者）とその所属長に通知する。当該従業員は，一定期間内に製品 F を導入・設定する。
2. 古い OS 又はアプリケーションを利用しているスマートフォン，若しくは安全性が疑わしいアプリケーションを導入しているスマートフォンを，製品 E によって検知する。情報システム部は，必要と判断した場合，当該従業員とその所属長に通知する。当該従業員は，一定期間内に最新の OS 又はアプリケーションを導入したり，安全性が疑わしいアプリケーションを削除したりする。
3. スマートフォン及び外部記憶媒体に保管した業務データを保護するために，製品 E の機能を利用してスマートフォン及び外部記憶媒体上の全データの暗号化を行う。
4. スマートフォン中の業務データをバックアップする場合，所有者はバックアップデータを暗号化する。バックアップデータの保管先として利用できるのは，D 社の規程に基づいて管理されている機器だけとし，D 社の管理及び規程が及ばないサービス又はシステムを利用することを禁止する。
5. スマートフォンの盗難又は紛失の届出があった場合，情報システム部は，当該従業員に，モバイル PC のブラウザから E サーバ 1 にアクセスしてスマートフォン及び外部記憶媒体に保管された全データを消去する方法を伝える。当該従業員は，スマートフォン及び外部記憶媒体に保管された全データを消去する。

図 6　案 3 において追加したセキュリティ対策

Y 氏は，案 3 をまとめた後に，スマートフォンの盗難又は紛失時のデータ消去手段として，製品 E を利用する方法以外に，携帯電話事業者のデータ消去サービスがあることを知った。そこで，どちらの方法を採用すべきかを，Z 主任に相談した。携帯電話事業者のデータ消去サービスには，製品 E と同等の機能を提供するサービスと，③携帯電話網を介したデータ通信を用いて，スマートフォン及び外部記憶媒体に保存したデータを消去するサービスの 2 種類があり，携帯電話網を介したデータ通信を用い

るサービスだけを提供している携帯電話事業者もあることが分かった。Z主任は，図5を示しながら，スマートフォンの状態によっては，携帯電話網を介したデータ通信を用いる方法ではデータ消去が行えないので，製品Eを利用する方法で統一すべきであることをY氏に説明した。Y氏は，Z主任の説明を受けて案3を具体化し，Z主任のレビューを受けた。

案3のレビューにおいて，Z主任は，スマートフォンの仕様の一部が，D社の業務データ取扱事項違反の原因となり，セキュリティリスクがあることを指摘した。また，その対策として，スマートフォン利用手続にスマートフォンの設定について項目を追加することと，正しく設定されているかを製品Eの機能によって情報システム部が監視することをアドバイスし，それがどのような場合に効果があるかを説明した。

Y氏は，案3にZ主任のアドバイスを反映させた案4をまとめた。

〔同意書の検討〕

Y氏が案4についてX部長に説明したところ，“スマートフォンの盗難又は紛失時における製品Eによるデータ消去は，業務データをスマートフォンに保存する場合のリスクに対する対策であるが，D社として，消去されるデータを具体的に示した上で従業員から事前に同意を得ておく必要がある”との指摘がX部長からあった。

X部長の指摘を受けて，Y氏は，製品Eによるセキュリティ対策の内容をセキュリティ規程に追記するとともに，スマートフォンの利用手続に同意書の提出を義務付ける項目を新たに設け，案5とし，X部長の承認を得た。

D社は，案5に基づいて，リモートアクセス環境の運用を開始した。

X部長は，今後，スマートフォンの高機能化に伴い，新しい脆弱性が発見されたり，対策技術が変化したりする可能性があると考え，Y氏に，スマートフォンの利用におけるセキュリティリスク及び対策技術の動向について，定期的に調査し，報告することを指示した。

設問 1　〔スマートフォンを利用したリモートアクセス環境の構築〕について，(1)～(4)に答えよ。

(1) 本文中の下線①について，D 社が認めていないアクセスとは何から何へのアクセスか。二つ挙げ，それぞれ 25 字以内で述べよ。また，下線①で述べた問題に対して，案 2 において講じられている対策を二つ挙げ，それぞれ 50 字以内で述べよ。

(2) FW3 及び FW4 において許可する通信を，表 3 及び表 4 の記述形式に倣って FW3 については一つ，FW4 については二つ答えよ。

(3) 本文中の下線②の問題を，50 字以内で述べよ。また，この問題に対して，案 2 において講じられている対策を，50 字以内で述べよ。

(4) 表 5 中の対策 C1～C17 の中から，対策の内容及び実施について D 社の管理が及ばないものを一つ選び，記号で答えよ。

設問 2　〔リモートアクセス環境の改善〕について，(1)～(3)に答えよ。

(1) 本文中の下線③のサービスについて，製品 E を利用すればデータを消去できるが，下線③のサービスではデータを消去できないのは，スマートフォンがどのような状態のときか。30 字以内で述べよ。

(2) Z 主任が，“D 社の業務データ取扱事項違反の原因となる”と指摘したスマートフォンの仕様を，40 字以内で述べよ。また，Z 主任がアドバイスした，スマートフォン利用手続に追加する項目の内容を，20 字以内で述べよ。

(3) 案 2 において従業員が行っていた対策のうち，案 4 においては情報システム部が製品 E を利用して監視するとしているものを，表 5 中の対策 C1～C17 の中から全て選び，記号で答えよ。

設問 3　〔同意書の検討〕について，X 部長が考えた，従業員から事前に得ておく同意とはどのような内容か。50 字以内で具体的に述べよ。