問3　業務委託先への情報セキュリティ要求事項に関する次の記述を読んで，設問 1 ～ 4 に答えよ。

X 社は，携帯通信事業者から通信回線設備を借り受け，データ通信サービス及び通話サービス（以下，両サービスを併せて X サービスという）を提供している従業員数 70 名の企業である。X 社には，法務部，サービスマーケティング部，情報システム部，利用者サポート部（以下，利用者サポート部を US 部という）などがある。X 社では，最高情報セキュリティ責任者（CISO）を委員長とした情報セキュリティ委員会（以下，X 社委員会という）を設置している。X 社委員会では，情報セキュリティ管理規程の整備，情報セキュリティ対策の強化などが審議される。X 社委員会の事務局長は US 部の S 部長である。各部の部長は，X 社委員会の委員及び自部における情報セキュリティ責任者を務め，自部の情報セキュリティに関わる実務を担当する情報セキュリティリーダを選任している。US 部の情報セキュリティリーダは G 課長である。

US 部には，25 名の従業員が所属している。主な業務は，X サービスを利用している顧客，及び X サービスへの新規の申込みを検討している潜在顧客（以下，X サービスを利用している顧客及び潜在顧客を併せて X 顧客という）からの問合せへの対応業務（以下，X 業務という）である。

〔US 部が利用しているコールセンタ用サービスの概要〕

US 部では，X 業務を遂行するためにクラウドサービスプロバイダ N 社の SaaS のコールセンタ用サービス（以下，N サービスという）を利用している。N サービスは ISMS 認証及び ISMS クラウドセキュリティ認証を取得している。N サービスには，会社から貸与された PC の Web ブラウザから，暗号化された通信プロトコルである［ a ］を使ってアクセスする。N サービスは，図 1 の基本機能及びセキュリティ機能を提供している。

1 基本機能
1.1 管理画面上で手動で実行できる機能（以下，手動実行機能という）
・顧客情報の検索，閲覧
・顧客との通話
（省略）
1.2 自動で実行される機能（以下，自動実行機能という）
・顧客との通話の録音
（省略）
2 セキュリティ機能
2.1 手動実行機能
2.1.1 アクセス制御の設定
・N サービスにアクセスできる IP アドレスの登録，更新，削除
2.1.2 アカウント管理
・N サービスのログイン用のアカウントの登録，更新，削除
2.1.3 顧客情報の操作権限の設定
・各アカウントに対する顧客情報の登録，更新，閲覧，削除の権限の設定
（省略）
2.2 自動実行機能
2.2.1 監査ログ収集
・N サービスへのログイン及び手動実行機能を実行した時刻，アカウント，アクセス元 IP アドレスなどのログの収集
（省略）

図 1　N サービスの基本機能及びセキュリティ機能

N サービスのデータベース（以下，NDB という）に，氏名，年齢，住所，利用中のサービスプラン，問合せ対応記録その他の X 顧客に関する情報（以下，X 情報という）は暗号化されて，また，検索用キーは平文で保存されている。①X 情報は，US 部の従業員に貸与している PC にだけ格納した暗号鍵を用いて，US 部の従業員が復号できる仕組みになっている。PC へのログインには利用者 ID とパスワードが必要である。

X 社では，N サービスのセキュリティ機能のうち手動実行機能は，管理者アカウントをもつ US 部の特定の従業員だけが実行できる。X 社利用分の監査ログは，X 社の情報システム部が常時監視している。

US 部では，業務効率化の一環として，2019 年 10 月に X 業務の 3 割を外部に委託し，残りの業務は継続して N サービスを利用しながら US 部内で遂行することにした。その委託先の第一候補が Y 社である。Y 社を選んだ理由は，次の 2 点である。

・他の候補と比較してサービス内容に遜色がなく，しかも低価格であること

・秘密保持契約を締結した上で，業務委託に関わる範囲を対象とした，情報セキュリティ対策の評価に協力してくれること

〔Y社の概要〕

Y社は，次のコールセンタサービス（以下，Yサービスという）を提供する従業員数200名の企業である。

・委託元に代わって顧客からの製品やサービスに関する様々な問合せや苦情などを受け付ける。
・委託元の製品やサービスの評判を新聞，雑誌などのメディア，インターネット上のSNS，掲示板などを基に調査し，委託元に報告する。著作物を複製する場合は，著作権者の許諾を得て行う。

Y社はコールセンタシステム（以下，Yシステムという）を構築し，通常はそれを利用してYサービスを提供している。

Y社の組織の主な業務及び体制を表1に示す。

表1　Y社の組織の主な業務及び体制（抜粋）

| 組織 | 主な業務 | 体制 |
|---|---|---|
| 人事総務部 | （省略） | （省略） |
| 営業部 | （省略） | （省略） |
| カスタマサービス部（以下，Y-CS部という） | ・Yサービスの企画立案<br>・Yサービスの提供 | T部長<br>課長：1名<br>主任：4名<br>一般従業員：5名<br>パートタイマ：50名 |
| システム管理部 | ・Yシステム，Y社内に導入している入退管理システムなどのシステムの企画，開発，運用<br>・情報セキュリティに関わる企画，開発，運用<br>・Yシステムのデータベースの管理，障害対応及び機能改修[1)] | 部長：1名<br>F課長<br>主任：2名<br>一般従業員：8名<br>パートタイマ：0名 |

注記　一般従業員とは，管理職及びパートタイマを除く従業員をいう。主任以上を管理職という。
注[1)]　本業務を実施する際に従業員がデータベースのデータにアクセスすることがある。

Y社は，従業員を対象に，原則4月及び10月の1日に社内の定期人事異動がある。また，これらの時期以外でも組織再編，業務の見直しなどの理由で人事異動がある。

Y-CS 部のパートタイマは，1 年間で約 2 割が退職する。人事総務部は，欠員補充のために，ほぼ同数を新規に採用している。

〔Y 社の情報セキュリティ対策〕

Y 社は，東京都内の 7 階建てビルの 3～5 階に入居しており，他の階には別の企業が入居している。ビルの出入りは誰でも可能であり，階段やエレベータを使用して，各階に移動できる。Y 社の入退管理を図 2 に示す。

・各階には業務エリアが一つずつある。各業務エリアには出入口が 2 か所あり，入室時に 6 桁の暗証番号によってドアを解錠する入退管理システムが設置されている。
・暗証番号は各業務エリアで異なる。
・システム管理部は，4 月及び 10 月の 1 日に各業務エリアの暗証番号を更新する。暗証番号は，各業務エリアの入室権限を与えた従業員だけに事前に通知する。
・システム管理部の通知後は，人事異動によって配属された従業員への暗証番号の通知は各部で行う。
・共連れで入室すること及び他部の従業員に暗証番号を教えることは禁止している。
・Y 社の従業員以外が視察や情報セキュリティ調査などの目的で業務エリアに入室する場合，Y 社の管理職が同行し，入室中は指定のネックストラップを常時着用させる。
・各業務エリアの出入口付近には監視カメラが設置されており，毎日 24 時間録画している。
・業務エリアに出入りする際の持ち物検査は行っていない。

図 2　Y 社の入退管理

3 階は Y-CS 部の，また，4 階及び 5 階は他部の業務エリアである。

Y-CS 部の管理職及び一般従業員は，5 階の会議室で営業部の従業員と会議をすることが多いので，3 階及び 5 階への入室権限が与えられている。

3～5 階には，複合機が 2 台ずつ設置されており，コピー，プリント，スキャンの機能が使用できる。Y-CS 部はスキャンの機能を使用して，新聞，雑誌などに紹介された委託元の製品やサービスに関する記事を PDF 化し，委託元に報告している。スキャンした PDF ファイルは電子メール（以下，電子メールをメールという）にパスワードなしで添付されて，スキャンを実行した本人だけに送信される。PDF ファイルの容量が大きい場合は，PDF ファイルを添付する代わりにプリントサーバ内の共有フォルダに自動的に保存され，保存先の URL がメールの本文に記載されて送信される。その際，メールの送信者名，件名，本文及び添付ファイル名の命名規則などは，複合機の初期設定のまま使用している。そのため，誰がスキャンを実行しても，メー

ルの送信者名などは同じになる。複合機のマニュアルはインターネットに掲載されている。

管理職にはデスクトップ PC 及びノート PC が，その他の従業員にはデスクトップ PC が貸与されている。ノート PC は，社内会議での資料のプロジェクタによる投影，在宅での資料作成などに利用する。Y 社が貸与している PC（以下，Y-PC という）の仕様及び利用状況を表 2 に示す。

表 2　Y-PC の仕様及び利用状況（抜粋）

| PC の種類 | 仕様及び利用状況 |
|---|---|
| デスクトップ PC | 1　セキュリティケーブルを使用して机に固定しており，鍵はシステム管理部が保管している。<br>2　社内の有線 LAN だけに接続できる。<br>3　インターネットには，DMZ 上のプロキシサーバを経由してアクセスする。 |
| ノート PC | 1　社内外の無線 LAN に接続できる。有線 LAN には接続できない。<br>2　社外又は社内からインターネットにアクセスする場合，まず 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。その後，DMZ 上のプロキシサーバを経由してアクセスする。<br>3　盗難防止のために，離席時はセキュリティケーブルを使用する。 |
| 共通 | 1　次の二つの制御が実装されている。<br>・USB メモリなどの外部記憶媒体は，データの読込みだけを許可する。<br>・アプリケーションソフトウェアは，Y 社が許可しているものだけを導入できる。<br>2　業務上，外部記憶媒体へのデータの書出しが必要な場合及びアプリケーションソフトウェアの追加導入が必要な場合は，Y 社内のルールに従って，システム管理部に申請する。<br>3　業務で使用する Web ブラウザ及びメールクライアントが導入されている。<br>4　マルウェア対策ソフトが導入されており，1 日に 1 回，ベンダのサーバに自動的にアクセスし，マルウェア定義ファイルをダウンロードして更新する。<br>5　表示された画面を画像形式のデータとして保存できる。 |

プロキシサーバには次の機能があるが，現在は使用していない。

・指定された URL へのアクセスを許可又は禁止する機能（以下，プロキシ制御機能という）

・利用者 ID 及びパスワードによる認証機能（以下，利用者認証機能という）

プロキシサーバのログ（以下，プロキシログという）はログサーバに転送され，3 か月間保存される。プロキシログは，ネットワーク障害，不審な通信などの原因を調

査する場合に利用する。プロキシログには，アクセス日時及びアクセス先 IP アドレスが記録されるが，利用者認証機能を使用すると，Web サイトにアクセスした従業員の利用者 ID も記録される。

VPN サーバにはパケットフィルタリングの機能及びあらかじめ設定したドメインへの通信を禁止する機能（以下，両機能を併せて VPN 制御機能という）があるが，現在は使用していない。

〔Y 社からの提案〕

Y 社が X 業務に利用するシステム又はサービスは表 3 に示す 2 案がある。X 社から特段の要求がなければ，Y 社は案 1 を採用する。

表 3　Y 社が X 業務に利用するシステム又はサービス

| 案 | X 業務に利用するシステム又はサービス | アクセスできる従業員 |
|---|---|---|
| 案 1 | Y システム | ・Y-CS 部の主任のうち 2 名，一般従業員のうち 2 名，パートタイマのうち 4 名が Y システムにアクセスできる。 |
| 案 2 | N サービス | ・Y-CS 部の主任のうち 2 名，一般従業員のうち 2 名，パートタイマのうち 4 名が N サービスにアクセスできる。<br>・主任 2 名は，N サービスの監査ログから X 業務での操作履歴を確認できる。 |

〔X 社委員会における案 1 及び案 2 の検討〕

X 社委員会は，案 2 では，案 1 のもつ［ b ］できるので，案 2 の採否について議論した。X 社委員会では，業務委託後の残留リスクを受容できると判断できた場合は，Y 社に委託することにした。そこで，CISO は，業務委託に関わる範囲を対象として Y 社の情報セキュリティ対策を確認し，X 社委員会に報告するよう S 部長に指示した。

S 部長は，G 課長に Y 社の情報セキュリティ対策を確認して報告するよう指示した。S 部長は，情報システム部に技術面での協力を依頼し，同部の H 主任が G 課長に協力することになった。

〔X社の情報セキュリティ要求事項と評価〕

G 課長と H 主任は，自社の情報セキュリティ管理規程を基に，X 業務の外部への委託における情報セキュリティ要求事項（以下，X 要求事項という）を取りまとめた。

X社とY社間で秘密保持契約を締結した後，G課長は，Y社を訪問した。G課長はY 社の承諾を得た上で，X 要求事項を基に，Y-CS 部従業員へのヒアリング及び設備状況の目視による確認などを行った。その際，T 部長及び F 課長に同行を依頼した。その後，表 4 のとおり評価結果と評価根拠をまとめて Y 社に事実確認を依頼したところ，“事実だ”との回答があった。評価結果は次のルールに従って記入した。

・要求事項を満たす場合：“OK”

・要求事項を満たさない場合：“NG”

表 4　X 要求事項に対する Y 社の対策の評価結果と評価根拠（抜粋）

| 項番 | 要求事項 | 評価結果 | 評価根拠 |
|---|---|---|---|
| 5 | X 業務で N サービスへのアクセスが可能な業務エリアは Y-CS 部の業務エリアだけに限定すること | NG | ・現状のままでは，Y 社で N サービスにアクセスできるようになったら，［ c ］が，3 階以外から N サービスにアクセスできてしまう。<br>・（省略） |
| 8 | X 業務を実施する業務エリアへの入室は，入室権限が与えられている従業員だけに制限すること | NG | 入室権限に，次の 2 点の不備がある。<br>・［ d ］<br>・［ e ］ |
| 12 | （省略） | NG | ・②複合機が初期設定のままになっている。 |
| 13 | X 業務には，Y 社貸与の PC を使用すること | OK | （省略） |
| 14 | X 業務で使用する PC では，外部記憶媒体へのアクセスを禁止すること | NG | ・Y-PC で実装している技術的な制限では，外部記憶媒体のデータの読込みが可能となっている。 |
| 18 | インターネット上の Web サイトへの X 情報の持出しをけん制する対策があること | NG | （省略） |

〔評価結果に対する対応案の検討〕

後日，G 課長は T 部長と F 課長に，Y 社と業務委託契約をしたいと伝え，その前提として，評価結果が“NG”の要求事項への対応を依頼した。Y 社は G 課長に③対応案を伝えた。G 課長は H 主任と相談の上，対応案を S 部長に報告した。

S 部長が表 4 及び対応案を X 社委員会に報告したところ，Y 社に X 業務を委託することが承認され，無事に業務が開始された。X 社は Y 社への業務委託によって業務の効率化を進めることができた。

設問 1　〔US 部が利用しているコールセンタ用サービスの概要〕について，(1)，(2)に答えよ。

(1) 本文中の［ a ］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 DKIM | イ DomainKeys | ウ HTTP over TLS |
| エ IMAP over TLS | オ POP3 over TLS | カ SMTP over TLS |

(2) 本文中の下線①について，情報セキュリティ上のどのような効果が期待できるか。次の (i) ～ (vi) のうち，期待できるものだけを全て挙げた組合せを，解答群の中から選べ。

(i) NDB の DBMS の脆弱性を修正し，インターネットからの不正なアクセスによる情報漏えいのリスクを低減する効果

(ii) NDB を格納している記憶媒体が不正に持ち出された場合に X 情報が読まれるリスクを低減する効果

(iii) N 社の　　従業員が NDB に不正にアクセスすることによって X 情報が漏えいするリスクを低減する効果

(iv) X 情報へのアクセスが許可された US 部の従業員が NDB を誤って操作することによって X 情報を変更するリスクを低減する効果

(v) 攻撃者によって NDB に仕込まれたマルウェアを駆除する効果

(vi) 攻撃者によって NDB に仕込まれたマルウェアを検知する効果

解答群

| | | |
|---|---|---|
| ア (i)，(ii) | イ (i)，(ii)，(iii) | ウ (i)，(v) |
| エ (ii)，(iii) | オ (ii)，(v) | カ (iii)，(iv) |
| キ (iii)，(vi) | ク (iv)，(v) | ケ (iv)，(v)，(vi) |

設問2　本文中の［　b　］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。

b に関する解答群

ア　X 業務に従事しない Y-CS 部の従業員による X 情報の不正な持出しリスクを低減

イ　X 業務に従事する Y-CS 部の従業員による X 情報の不正な持出しリスクを N 社に移転

ウ　X 業務に従事する Y-CS 部の従業員による X 情報の不正な持出しリスクを回避

エ　システム管理部の従業員による X 情報の不正な持出しリスクを回避

設問3　〔X 社の情報セキュリティ要求事項と評価〕について，(1) ～ (4) に答えよ。

(1)　表 4 中の［　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。

c に関する解答群

ア　F 課長

イ　T 部長

ウ　X 業務に従事する Y-CS 部の 2 名の一般従業員

エ　X 業務に従事する Y-CS 部の 2 名の主任

オ　X 業務に従事する Y-CS 部のパートタイマ

(2) 表 4 中の［ d ］，［ e ］に入れる評価根拠として適切なものを，解答群の中から選べ。

d，e に関する解答群

ア　Y-CS 部の従業員が 3 階の業務エリアに入室できる。

イ　Y-CS 部のパートタイマが 5 階の業務エリアに入室できる。

ウ　営業部の従業員が 3 階の業務エリアに入室できる。

エ　システム管理部の従業員が 5 階の業務エリアに入室できる。

オ　退職者の一部が 3 階の業務エリアに入室できる。

カ　元 Y-CS 部の従業員が，他部門に異動した後も，3 階の業務エリアに入室できる。

(3) 表 4 中の下線②は，どのような情報セキュリティリスクが残留していると考えたものか。次の (i) ～ (v) のうち，残留している情報セキュリティリスクだけを全て挙げた組合せを，解答群の中から選べ。

(i) X 業務に従事する従業員が，攻撃者からのメールを複合機からのものと信じてメールの本文中にある URL をクリックし，フィッシングサイトに誘導される。

(ii) X 業務に従事する従業員が，攻撃者からのメールを複合機からのものと信じて添付ファイルを開き，マルウェア感染する。

(iii) X 業務の中で，複合機から送信されるメールが攻撃者宛に送信される。

(iv) 攻撃者が，複合機から送信されるメールの本文及び添付ファイルを改ざんする。

(v) 攻撃者が，複合機から送信されるメールを盗聴する。

解答群

| | | |
|---|---|---|
| ア (i)，(ii) | イ (i)，(ii)，(iii) | ウ (i)，(iii)，(iv) |
| エ (ii)，(iii) | オ (ii)，(iii)，(iv) | カ (ii)，(iv)，(v) |
| キ (iii)，(iv) | ク (iii)，(iv)，(v) | ケ (iv)，(v) |

(4) 表 4 中の項番 14 について，Y 社が追加の対策をとり，要求事項を満たすことによってどのような情報セキュリティリスクが低減できるか。次の (i) ～ (iv) のうち，適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) Y-PC 内のデータを外部記憶媒体に保存して持ち出される。

(ii) Y-PC 内のデータを複合機でプリントして持ち出される。

(iii) Y 社で許可していないアプリケーションソフトウェアが保存されている USB メモリを Y-PC に接続されて，Y-PC に当該ソフトウェアが導入される。

(iv) マルウェア付きのファイルが保存されている USB メモリを Y-PC に接続されて，Y-PC がマルウェア感染する。

解答群

| | | |
|---|---|---|
| ア (i) | イ (i)，(ii)，(iv) | ウ (i)，(iii) |
| エ (i)，(iv) | オ (ii) | カ (ii)，(iii) |
| キ (ii)，(iii)，(iv) | ク (iii) | ケ (iii)，(iv) |
| コ (iv) | | |

設問4　〔評価結果に対する対応案の検討〕について，(1)，(2)に答えよ。

(1) 本文中の下線③について，表4中の項番5の要求事項への有効な対応案はどれか。解答群のうち，最も有効なものを選べ。

解答群

ア　Nサービスのアクセス制御の設定機能でX社及びY社以外からのアクセスを禁止する。

イ　Nサービスの監査ログを監視し，3階の業務エリア以外からのアクセスを検知する。

ウ　Nサービスの顧客情報の操作権限の設定機能で，X情報の閲覧だけ許可する。

エ　VPNサーバのVPN制御機能を使用して，ノートPCからNサービスへのアクセスを禁止する。

オ　Y-CS部の管理職は，Nサービスへのアクセスを禁止する。

カ　プロキシサーバのプロキシ制御機能を使用して，Nサービスへのアクセスを禁止する。

(2) 本文中の下線③について，表 4 中の項番 18 の要求事項への有効な対応案としてどのようなものがあるか。次の (i) ～ (v) のうち，有効なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) N サービスにログインできる従業員のデスクトップ PC から Web ブラウザを削除し，導入が必要な場合にだけ，システム管理部に申請する。

(ii) N サービスにログインできる従業員は，デスクトップ PC は使用せずに，ノート PC だけを使用して X 業務を実施する。

(iii) N サービスにログインできる従業員を対象に，プロキシサーバの利用者認証機能を使用し，プロキシログを監視する旨を通知する。

(iv) デスクトップ PC からは N サービスだけにアクセスすることを社内ルールに明記し，N サービスにログインできる従業員を対象に，通知する。

(v) プロキシサーバのプロキシ制御機能を使用して，N サービス以外へのアクセスを禁止する。

解答群

| | | |
|---|---|---|
| ア (i) | イ (i)，(v) | ウ (ii) |
| エ (ii)，(iii) | オ (ii)，(v) | カ (iii) |
| キ (iii)，(iv) | ク (iv) | ケ (iv)，(v) |
| コ (v) | | |