問3　情報セキュリティの自己点検に関する次の記述を読んで，設問1～6に答えよ。

マンション管理会社 Q 社は，マンションの管理組合から委託を受けて管理業務を行っており，契約している管理組合数は 3,000 組合である。東京の本社には，経営企画部，営業統括部，人事総務部，経理部，情報システム部，監査部などの管理部門があり，東日本を中心に 30 の支店がある。従業員数は，マンションの管理人（以下，管理員という）3,300 名を含めて 3,800 名である。管理業務の内容は，管理組合の収支予算書及び決算書の素案の作成，収支報告，出納，マンション修繕計画の企画及び実施の調整，理事会及び総会の支援，清掃，建物設備管理，緊急対応，管理員による各種受付・点検・立会い・報告連絡などである。

Q 社は 3 年前に全社で ISMS 認証を取得しており，最高情報セキュリティ責任者（CISO）を委員長とする情報セキュリティ委員会を設置し，JIS Q 27001 に沿った情報セキュリティポリシ及び情報セキュリティ関連規程を整備している。CISO は情報システム担当常務が務め，情報セキュリティ委員会の事務局は情報システム部が担当している。また，本社各部の部長及び各支店長は，情報セキュリティ委員会の委員，及び自部署における情報セキュリティ責任者を務め，自部署の情報セキュリティを確保し，維持，改善する役割を担っている。各情報セキュリティ責任者は，自部署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。

U 支店には，支店長，主任 2 名，管理組合との窓口を務めるフロント担当者 10 名が勤務している。U 支店の情報セキュリティ責任者は B 支店長，情報セキュリティリーダは第 1 グループの A 主任である。U 支店に勤務する従業員には，一人 1 台のノート PC（以下，NPC という）が貸与されている。NPC にはディジタル証明書をインストールし，Q 社のネットワークに接続する際に端末認証を行っている。U 支店では，Q 社の文書管理規程に従い，顧客情報などの重要な情報が含まれる電子データは，U 支店の共有ファイルサーバの所定のフォルダに保管する運用を行っている。U 支店の共有ファイルサーバは，1 日 1 回テープにバックアップを取得し，1 週間分のテープを世代管理している。

U 支店が契約している管理組合数は 80 組合であり，フロント担当者 1 名当たり 5～10 の管理組合を担当している。U 支店が担当する管理組合のマンションはそれぞれ，管理事務室が 1 か所設置されており，管理員が 1～2 名勤務している。管理事務室には，管理員以外に，Q 社従業員，マンション居住者が立入ることがある。多くの

マンションでは，管理事務室の入室にマンションごとの暗証番号が必要である。暗証番号はおおむね 2 年ごとに変更される。管理事務室には，管理組合の許可を受けた上で，管理員と U 支店の連絡用に，LTE 通信機能付き NPC を 1 台設置し，インターネット VPN 経由で Q 社のネットワークと接続している。①管理事務室に複数の管理員が勤務する場合には，管理員間で NPC，利用者 ID，パスワード，メールアドレスを共用している。

〔自己点検の規程及びチェック項目〕

Q 社では，自己点検規程及び内部監査規程を，表 1 のとおり定めている。

表 1　自己点検規程及び内部監査規程（概要）

項目	自己点検規程	内部監査規程 [1)]
実施者	管理員を含めた全従業員自らが実施する。	監査部が実施する。監査人は，専門職としての知識及び技能を保持し，監査対象部署からの［a1］を確保しなければならない。
報告先	情報セキュリティリーダが自部署の従業員の回答を評価し，情報セキュリティ責任者が確認の上，その結果を情報セキュリティ委員会に提出する。	監査責任者は，監査手続の結果とその関連資料から作成された監査調書に基づき，監査報告書を作成し，CISO に提出する。
実施頻度	月 1 回実施する。	年 1 回実施する。また，自己点検の結果に応じて適時実施する。
対象	管理員を含めた全従業員を対象とする。	監査対象をサンプリングによって抽出する。
評価の観点	［a2］を遵守して ISMS を運用しているかを点検する。点検する項目は，各部，各支店では，情報セキュリティ責任者が，情報セキュリティ委員会の定めた自己点検における標準チェック項目を基に自己点検チェック項目（以下，チェック項目という）として設定している。	［a2］を遵守して ISMS を運用しているか，［a2］が，情報セキュリティポリシに準拠しているか，また法令の改正や，環境の変化に合わせて適切に改定されているかを評価する。
評価の手法	（省略）	規程文書などを確認して準拠性を評価し，［a3］への質問・閲覧・観察などによって遵守性を評価する。
結果に対する改善	自己点検の結果に基づき，改善が必要な場合には，情報セキュリティ責任者が，情報セキュリティの改善及びチェック項目の見直しを行う。	（省略）

注 [1)]　本規程は，経済産業省“情報セキュリティ監査基準”及び“システム監査基準”を基に Q 社が作成した。

また，U支店では，チェック項目を図1のとおり設定している。

1　クリアデスクを実施している。
2　クリアスクリーンを実施している。
3　NPCのOSの更新履歴によって，自動更新の正常終了を確認している。
4　NPCのアプリケーションソフトウェア（以下，アプリケーションソフトウェアをアプリという）のバージョンが最新かをヘルプメニューで確認している。
5　退出時にNPCをセキュリティケーブルでロックしている。
6　退出時に顧客情報などの重要な情報を含む書類をキャビネットに施錠保管している。
7　プリンタに印刷物を放置していない。
8　顧客情報などの重要な情報が含まれる電子データを，NPC上ではなくU支店の共有ファイルサーバの所定のフォルダに保管している。
9　個人所有PCを業務で使用していない。
（省略）

図1　U支店のチェック項目

〔アプリの更新漏れ〕

A主任は情報処理推進機構（IPA）の情報セキュリティサイトを見た際に，PDF閲覧ソフトにおいて任意のコードが実行されるという深刻な脆弱性に対する注意喚起が，2週間前から掲載されていることに気付いた。そこで，A主任が第1グループメンバのNPCについて，PDF閲覧ソフトのバージョンが最新かを確認したところ，最新ではないNPCが2台あった。1週間前に実施した自己点検では，チェック項目4に全員が“はい”と回答していた。A主任が2台のNPCの利用者に確認したところ，他のアプリの更新は確認していたが，PDF閲覧ソフトの確認が漏れていたことが判明した。

A主任が，IPAの情報セキュリティサイトの参考情報から，脆弱性対策情報データベースを確認したところ，図2のとおり記載されていた。

JVNDB-20XX-XXXXXX
PDF 閲覧ソフトにおける任意のコードを実行される脆弱性
CVSS v3 による深刻度
[b] 値 [1] : 9.8 ([c])
・攻撃元区分 [2] : ネットワーク
・攻撃条件の複雑さ : [d1]
・攻撃に必要な特権レベル : [d2]
・利用者の関与 : [d3]
・機密性への影響 (C) : 高
・完全性への影響 (I) : 高
・可用性への影響 (A) : 高

注 [1] 値は，0～10.0 で表現される。
[2] 区分には，ネットワーク，隣接，ローカル及び物理がある。

図 2　PDF 閲覧ソフトに対する CVSS v3 の脆弱性評価結果（抜粋）

次は，図 2 についての情報システム部の R 課長と A 主任の会話である。

R 課長：CVSS v3 の [b] 評価基準は，脆弱性そのものの特性を評価する基準であり，評価には，攻撃の容易性及び情報システムに求められる三つのセキュリティ特性である，機密性，完全性，可用性に対する影響といった基準を用います。[b] 評価基準は，時間の経過や利用環境の差異によって変化せず，脆弱性そのものを評価する基準です。図 2 を見ると，この PDF 閲覧ソフトの脆弱性の深刻度は [c] であり，“攻撃条件の複雑さ”，“攻撃に必要な特権レベル”，“利用者の関与”の全てにおいて，攻撃が成功するおそれが最も高い値を示しています。したがって，PDF 閲覧ソフトは早急に更新が必要です。

A 主任：アプリのバージョンが最新かを，簡単にチェックする方法はありませんか。

R 課長：方法は二つあります。一つ目は，“MyJVN バージョンチェッカ”という IPA から無償提供されているソフトウェアを使う方法です。各利用者が NPC にインストールされているアプリのバージョンが最新かを簡単にチェックすることができます。二つ目は [e] を導入する方法です。情報システム部で，各 NPC のアプリのバージョンが最新かを管理し，一括してチェックすることが可能ですが，導入には費用が掛かります。実は，“MyJVN バージョンチェッカ”を全社で利用する準備のために，試用部署を探していました。

しかるべき手続を経て，情報セキュリティ委員会の承認を受けるので，U 支店で試用してもらえませんか。

A 主任は，B 支店長の許可を得て“MyJVN バージョンチェッカ”の試用を開始し，“MyJVN バージョンチェッカ”がフロント担当者や管理員の IT リテラシでも問題なく使用できることを確認し，B 支店長と R 課長に報告した。

報告を受けた B 支店長は，“MyJVN バージョンチェッカ”を全社に先駆けて U 支店で継続して試用することについて，情報セキュリティ委員会の承認を受けた。

〔個人所有スマートフォンの業務利用〕

最近，フロント担当者の K さんが仕事中に度々個人所有スマートフォン（以下，スマートフォンをスマホという）を使っているので，A 主任が K さんに尋ねたところ，個人所有スマホを業務に使うことがあるとのことであった。

K さんは，②スマホの個人利用者向けチャットアプリ（以下，M アプリという）を利用して，K さんが担当する P マンションの管理組合（以下，P 組合という）の理事からの問合せに回答したり，業務に関する情報を送信したりしているとのことであった。P 組合の理事長から，次の理由で，M アプリの使用を求められて，やむを得ず従ったとのことであった。

・P 組合では，理事同士の情報共有に M アプリを利用している。
・問合せに対する K さんの返信がいつも遅く，おおむね 3 営業日以上掛かっている。M アプリを利用すれば，K さんがいつメッセージを読んだかが把握できる。

なお，Q 社は，③従業員が個人所有スマホを業務に利用することを，会社として許可していない。

A 主任は，K さんが個人所有スマホを業務利用していること，及びスマホ用アプリの業務利用によって問題が発生することについて，B 支店長に報告した。

〔チェック項目の見直し〕

これまでの報告を受けて，B 支店長は，図 1 のチェック項目の見直しが必要であると判断し，A 主任に対して見直しを指示した。④A 主任が示した見直し案を B 支店

長が承認し，見直されたチェック項目が翌月から使用されることになった。

〔M アプリの調査〕

K さんは，P 組合に M アプリが使用できなくなったことを連絡したが，P 組合は，M アプリの利用を強く要望するとのことであった。相談を受けた A 主任が，M アプリの機能と特徴を調べたところ，図 3 のとおりであった。

・M アプリの連絡先（以下，AP 連絡先という）に登録された相手とだけ，メッセージの送受信ができる。
・送信相手がいつメッセージを読んだかを確認できる。
・M アプリのメッセージは，スマホに保存される。
・M アプリのアカウントは，スマホの電話番号に対応付けて登録される。
・スマホのアドレス帳（以下，アドレス帳という）に登録された相手と，自分の双方が M アプリを使用し，かつ，それぞれの M アプリに，アドレス帳へのアクセス許可を与えている場合，M アプリのアカウントが相互の AP 連絡先に自動登録される。
・宛先グループを作成し，宛先グループ全員にメッセージを同時に送信できる。また，そのメッセージを宛先グループの各メンバがいつ読んだかを確認できる。
・写真，音声，ビデオ，ファイル，URL などを，メッセージに添付して送信できる。
・メッセージに JPEG ファイルを添付した場合，撮影時に格納される各種データは自動的に削除される。
・現在地の位置情報を自動的に取得して，メッセージに添付して送信できる。

図 3　M アプリの機能及び特徴（抜粋）

A 主任は，図 3 から，⑤M アプリを業務連絡に利用することには，幾つかのリスクがあると考えた。更に調査したところ，M アプリに業務用の機能を追加したアプリ（以下，BM アプリという）が存在することが分かった。BM アプリで追加された機能は，図 4 のとおりである。

・他のスマホの M アプリ又は BM アプリとの間でメッセージを送受信できる。
・BM アプリを導入した組織において，BM アプリの管理者を指定できる。
・管理者が，AP 連絡先の管理を行え，AP 連絡先の自動登録を禁止できる。
・管理者が，BM アプリのデータを遠隔から消去できる。
・管理者が，BM アプリを導入したスマホでのスマホ用アプリの利用を制限できる。
・誤って送ったメッセージの送信を取り消すことができる。

図 4　BM アプリで追加された機能（抜粋）

A 主任は，図 4 から，BM アプリには適切なセキュリティ機能が備わっていると考

え，情報システム部に，個人所有スマホ及び BM アプリの業務利用について検討を依頼した。

情報システム部は，個人所有スマホの業務利用に対する情報セキュリティリスクアセスメント及び⑥BM アプリの利用に対する情報セキュリティリスクアセスメントを実施した。さらに，その結果を情報セキュリティ委員会に報告し，許可を受けた上で BM アプリを試験導入し，問題がないことを確認した。

P 組合から強い要望を受けてから半年後，情報セキュリティ委員会は，必要な情報セキュリティ関連規程を整備し，チェック項目を再度見直した上で，全社的に個人所有スマホの業務利用を BM アプリなど会社が認めたスマホ用アプリに限定して許可した。これによって，Q 社は P 組合の要望に応えることができた。また，BM アプリの利用を広げたことによって，Q 社と顧客との間の連携が強化された。

設問 1　本文中の下線①について，次の (i) ～ (iv) のうち，共用することによって高くなるリスクはどれか。該当す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) NPC を操作した者を特定できないという状況を狙われて，不正に操作されるリスク

(ii) 異動者や退職者など，利用資格を失った者に NPC を不正に操作されるリスク

(iii) 共用者の 1 人がパスワードを変更した際に，他の共用者に変更後のパスワードを伝えるためのメモを書き，そのメモからパスワードが漏えいし，不正に操作されるリスク

(iv) クリアスクリーンをし忘れ，その隙に不正に操作されるリスク

解答群

ア (i)　　イ (i), (ii)

ウ (i), (ii), (iii)　　エ (i), (ii), (iv)

オ (i), (iii)　　カ (i), (iii), (iv)

キ (i), (iv)　　ク (ii), (iii)

ケ (ii), (iv)　　コ (iii), (iv)

設問2　〔自己点検の規程及びチェック項目〕について，(1)，(2)に答えよ。

(1)　表1中の［a1］～［a3］に入れる字句の組合せはどれか。aに関する解答群のうち，最も適切なものを選べ。

aに関する解答群

	a1	a2	a3
ア	機密性	情報セキュリティ関連規程	監査対象部署
イ	機密性	情報セキュリティ関連規程	監査部
ウ	機密性	文書管理規程	監査対象部署
エ	責任追跡性	情報セキュリティ関連規程	監査対象部署
オ	責任追跡性	情報セキュリティ関連規程	監査部
カ	責任追跡性	文書管理規程	監査対象部署
キ	独立性	情報セキュリティ関連規程	監査対象部署
ク	独立性	情報セキュリティ関連規程	監査部
ケ	独立性	文書管理規程	監査対象部署

(2)　図1中のチェック項目3～8のうち，NPCにおけるランサムウェアの脅威に対する管理策だけを全て挙げた組合せを，解答群の中から選べ。

解答群

ア　3，4，5　　イ　3，4，8

ウ　3，5，7　　エ　3，6，7

オ　4，5，6　　カ　4，6，8

キ　4，7，8　　ク　5，6，7

設問3　〔アプリの更新漏れ〕について，(1) ～ (4) に答えよ。

(1)　図 2 及び本文中の［ 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　環境　　イ　基本　　ウ　現状

(2)　図 2 及び本文中の［ 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　危険　　イ　緊急　　ウ　警告　　エ　重要

オ　注意　　カ　レベル 4　　キ　レベル 5

(3)　図 2 中の［ d1 ］～［ d3 ］に入れる字句の適切な組合せを，d に関する解答群の中から選べ。

d に関する解答群

	d1	d2	d3
ア	高	低	不要
イ	高	低	要
ウ	高	不要	不要
エ	高	不要	要
オ	低	高	不要
カ	低	高	要
キ	低	低	不要
ク	低	低	要
ケ	低	不要	不要
コ	低	不要	要

(4) 本文中の［ e ］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。

e に関する解答群

ア BI ツール

イ CASB（Cloud Access Security Broker）

ウ IT 資産管理ツール

エ UEBA（User and Entity Behavior Analytics）

オ ソフトウェア構成管理ツール

カ 特権 ID 管理ツール

キ ポートスキャナ

設問4 本文中の下線②及び下線③のような行為を表す字句の適切な組合せを，解答群の中から選べ。

解答群

	下線②	下線③
ア	グリーン IT	BYOD
イ	グリーン IT	CDN
ウ	グリーン IT	VPN
エ	サンクション IT	BYOD
オ	サンクション IT	CDN
カ	サンクション IT	VPN
キ	シャドーIT	BYOD
ク	シャドーIT	CDN
ケ	シャドーIT	VPN

設問5　本文中の下線④について，次の (i) ～ (iii) のうち，A 主任が見直しを行った図1のチェック項目と見直しの内容だけを全て挙げた組合せを，解答群の中から選べ。

(i) 3 と 4 を“MyJVN バージョンチェッカによって，NPC のアプリのバージョンが最新かを確認し，最新でなければ更新している。”に統合する。

(ii) 4 を“NPC のアプリのバージョンが最新かを MyJVN バージョンチェッカで確認し，最新でないアプリは，MyJVN バージョンチェッカの指示に従って更新する。”に修正する。

(iii) 9 を“PC やスマホなどの個人所有端末を業務で利用していない。”に修正する。

解答群

ア (i)　　イ (i)，(iii)

ウ (ii)　　エ (ii)，(iii)

オ (iii)　　カ 当てはまるものはない

設問6　〔Mアプリの調査〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑤のリスクについて，次の(i)～(iii)のうち，該当す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)　業務と関係のない宛先グループや友人とも M アプリでやり取りできるので，業務と関係のない友人や宛先グループに，誤って業務情報を送付してしまうリスク

(ii)　写真（JPEG ファイル）を添付した場合，写真には撮影場所を特定できるものが写っていなくても，撮影場所が特定されるリスク

(iii)　見知らぬ人が AP 連絡先に登録されてしまう場合があるので，見知らぬ人にメッセージを送ってしまうリスク

解答群

ア　(i)　　イ　(i)，(ii)

ウ　(i)，(ii)，(iii)　　エ　(i)，(iii)

オ　(ii)　　カ　(ii)，(iii)

キ　(iii)　　ク　当てはまるものはない

(2)　本文中の下線⑥で実施することについて，次の(i)～(v)のうち，該当す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)　リスク共有

(ii)　リスク特定

(iii)　リスク評価

(iv)　リスク分析

(v)　リスク保有

解答群

ア　(i)，(ii)，(iii)，(iv)　　イ　(i)，(ii)，(iii)，(iv)，(v)

ウ　(i)，(iii)，(iv)　　エ　(i)，(iii)，(iv)，(v)

オ　(i)，(iii)，(v)　　カ　(ii)，(iii)，(iv)

キ　(ii)，(iv)　　ク　(iii)，(iv)