問2　アカウント乗っ取りによる情報セキュリティインシデントに関する次の記述を読んで，設問1～4に答えよ。

P社は，従業員数300名の食品メーカである。東京に本社があり，関東に営業所と工場が点在している。本社には，製造部，流通管理部，営業部，情報システム部などがある。営業所は，営業部の管轄であり，担当地域の取引店への営業，配送管理などを担当している。Q県を担当するR営業所には，所長と副所長のほかに，15名の営業担当者，2名の流通担当者，2名の事務担当者が配置されている。

P社では，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（以下，P社委員会という）を設置し，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。P社委員会の事務局は，情報システム部が担当し，情報システム部のL課長が情報セキュリティインシデント（以下，インシデントという）発生時のインシデント対応責任者を務めている。さらに，本社の各部の部長，各営業所の所長，及び各工場の工場長は，P社委員会の委員，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を確保，維持及び改善する役割を担っており，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。R営業所の情報セキュリティ責任者はA所長であり，情報セキュリティリーダはB副所長である。

P社では，全従業員が基盤情報システムを利用して日々の業務を行っている。基盤情報システムは，サーバ，ネットワーク及び各従業員に貸与される端末から構成され，設定と運用管理は，情報システム部が行っている。貸与される端末にはノートPC（以下，NPCという），デスクトップPC（以下，DPCという），及びスマートフォン（以下，スマホという）がある。図1にサーバの概要を，表1に端末の概要を示す。

1 VPN サーバ及びプロキシサーバ
1.1 セキュリティベンダが提供する，悪意のあるサイトへのアクセスを遮断する URL フィルタリングサービスが導入されている。
1.2 アクセス成功とアクセス失敗の両方に関して，アクセス先 URL，アクセス元 IP アドレス，アクセス日時及びアクセス成否がアクセスログに記録され，直近 3 か月分が保存される。
1.3 設定の変更及びログの確認は，情報システム部だけが行える。
2 ファイルサーバ
2.1 営業所ごとに，業務で利用するファイルを保存するためのファイルサーバがあり，従業員は所属する営業所のファイルサーバだけを利用できる。

図 1　基盤情報システムのサーバの概要（抜粋）

表 1　基盤情報システムの端末の概要（抜粋）

項目	NPC	DPC	スマホ
機器を貸与される者	営業所の所長，副所長及び営業担当者	NPC を貸与されない従業員	本社の課長以上の管理職，並びに営業所の所長，副所長及び営業担当者
Web ブラウザでのインターネット閲覧	P 社の社内 LAN に直接接続している場合はプロキシサーバを経由し，それ以外の場合は VPN サーバを経由して閲覧する。	プロキシサーバを経由して閲覧する。	携帯通信網を経由して閲覧する。
ファイルサーバの利用	P 社の社内 LAN に直接接続している場合は社内 LAN だけを経由し，それ以外の場合は VPN サーバ及び社内 LAN を経由して利用する。	社内 LAN を経由して利用する。	利用できない。
セキュリティ機能	マルウェア対策ソフトの定義ファイルの更新機能，マルウェアスキャンの機能が有効になっている。	マルウェア対策ソフトの定義ファイルの更新機能，マルウェアスキャンの機能が有効になっている。	マルウェア対策ソフトの定義ファイルの更新機能，マルウェアスキャンの機能，URL フィルタリング機能 [1] が有効になっている。

注 [1]　URL フィルタリング機能は，悪意のあるサイトへのアクセスを遮断するブラックリスト型である。アクセスを遮断した場合だけ，アクセス先 URL 及び日時がスマホ内にログとして記録され，直近 7 日分のログだけが保存される。

〔チャットサービス〕

P 社では，製造した食品の取引店への配送を，配送業者に委託している。交通事情などによって配送が遅延する場合，配送業者は，各営業所の流通担当者に電子メール

（以下，電子メールをメールという）で連絡する。配送業者から連絡を受けた流通担当者は，メールで営業担当者に連絡し，営業担当者が各顧客に連絡している。

R 営業所が担当する地域では，交通事情による遅延の頻度が高いので，流通担当者が営業担当者にメールを見たかどうかを電話で確認することも多く，連絡の煩雑さが問題となっている。R 営業所の流通担当者である K さんは，この問題を解決するために，V 社が提供している SaaS 形式のチャットサービス（以下，V サービスという）を配送の連絡に利用すること，及び業務効率化のために V サービスを R 営業所におけるその他の連絡にも利用することを A 所長に提案した。A 所長はこの提案を P 社委員会に諮り，承認を得た。V サービスのサービス仕様を図 2 に示す。

1 基本機能
1.1 利用者は PC の Web ブラウザ，又はスマホの Web ブラウザ若しくは V サービス専用アプリケーションソフトウェア（以下，V アプリという）を利用してアクセスする。
1.2 同一利用者が PC とスマホの両方から同時にログインできる。
2 ワークスペース（以下，WS という）
2.1 利用者は，WS を作成することができる。WS を作成した利用者は，作成した WS の管理者権限をもつ。
2.2 WS の管理者権限をもつ利用者（以下，WS 管理者という）は，他の利用者を WS に参加させること，WS に参加している利用者（以下，WS 参加者という）に管理者権限を付与すること，及び WS を削除することができる。
3 グループチャット（以下，GC という）
3.1 WS 管理者は，WS 内に GC を作成し，WS 参加者を GC に参加させることができる。
3.2 利用者は，V サービスにログイン後，自身が参加している WS 及び GC にアクセスできる。
3.3 利用者は，GC 内で文字列のメッセージ（以下，GC メッセージという）及びファイルを送信できる。GC メッセージ及びファイルは GC 内に保存され，GC に参加している利用者（以下，GC 参加者という）だけが閲覧できる。
3.4 GC メッセージ及びファイルには，送信した利用者のアカウント名及び送信日時（以下，GC 送信情報という）が記録される。
3.5 送信された GC メッセージは GC ごとに直近の 1,000 件分が，ファイルは GC ごとに直近の 100 件分が保存され，それより前のものは自動的に削除される。削除された GC メッセージ及びファイルについての GC 送信情報も同時に削除される。
3.6 WS 管理者は，WS 内の GC メッセージ，ファイル，及び GC 送信情報を削除できる。

図 2　V サービスのサービス仕様（抜粋）

4 セキュリティ機能

4.1 V サービスへの接続には，HTTP over TLS を使用する。

4.2 各利用者のアカウントは，メールアドレスを利用者 ID として登録し，ログイン時の利用者認証のためのパスワードを設定する。パスワードは英大文字，英小文字，数字，記号の文字種の全てを組み合わせ，8 文字以上でなければならない。

4.3 Web ブラウザを閉じた場合は，一定時間後に自動的に V サービスからログアウトされる。V アプリを閉じた場合は，その時点で自動的に V サービスからログアウトされる。

4.4 利用者が自身のパスワードを変更した場合，利用中の全てのセッションで V サービスからログアウトされ，再度ログインを求められる。

4.5 利用者は追加の利用者認証機能（以下，V 認証機能という）を有効にすることができる。

・V 認証機能を有効にした場合は，V サービスへのログイン時に，利用者 ID とパスワードによる利用者認証に加え，あらかじめ登録しておいた電話番号に SMS で送信される 6 桁の数字，又は利用者 ID として設定されたメールアドレスに送信される 6 桁の数字を入力することによる追加の利用者認証を実施する。

・V サービスは，スマホの端末識別番号，又は V サービスへのログイン時に発行される Cookie の有無を基に，初めて V サービスを利用する端末かどうかを判断する。

・V 認証機能を有効にした場合，同じ端末での 2 度目以降の V サービスへのログイン時の追加の利用者認証を 30 日間省略する機能（以下，V 省略機能という）を有効にすることができる。

図 2　V サービスのサービス仕様（抜粋）（続き）

B 副所長は，A 所長の指示を受け，図 3 に示す R 営業所での V サービスの利用ルール（以下，V サービス利用ルールという）を策定した。

1　利用者 ID には，自身の P 社のメールアドレスを登録すること。

2　GC で送信する全てのファイルをパスワードで保護すること。

3　V サービスのパスワード及びファイルを保護するためのパスワードは，他人に推測されにくく，他のサービスのパスワードとして利用していない文字列とすること。

4　V サービスのパスワードは他人に知られないように適切に管理すること。

5　ファイルを保護するためのパスワードは，V サービスのパスワードとは別の文字列を利用し，ファイルを送信した GC 内で別の GC メッセージとして送信すること。

図 3　V サービス利用ルール（抜粋）

A 所長は，V サービスの利用開始を B 副所長に指示した。B 副所長は，V サービスで R 営業所用の WS を作成し，R 営業所の全従業員を WS に参加させ，自身のほか事務担当者だけに WS の管理者権限を付与した。また，表 2 に示す GC を作成した上で，R 営業所の全従業員に，V サービス利用ルールを周知した。次に，R 営業所の全ての NPC，DPC 及びスマホの Web ブラウザのブックマークに V サービスの URL を登録してもらった上で，6 月 1 日に利用を開始した。

表2　R営業所で利用するGC

GC番号	GC名	GC参加者	主な用途
GC-1	管理職	R営業所の所長，副所長及び事務担当者	業務連絡
GC-2	R営業所	R営業所の全従業員	業務連絡
GC-3	営業	R営業所の所長，副所長，営業担当者及び事務担当者	勤務スケジュール連絡，業務連絡
GC-4	配送	R営業所の流通担当者，営業担当者及び事務担当者	配送スケジュール連絡

〔インシデント発生〕

7月3日の15時5分，B副所長のもとにKさんが報告に来た。報告内容は次のとおりであった。

・営業担当者であるDさんから，表3に示すGCメッセージが送られてきた。

・不審に思ったので，Dさん本人が送信したGCメッセージであるかどうかを同日15時に①D さんに電話で確認したところ，本日は，社外研修を受講しており，当該GCメッセージは送信していないとの回答であった。

表3　Dさんのアカウントから送信されたGCメッセージ

番号	GC番号	日時	内容
1	GC-4	7月3日 13時35分	アカウントの確認が必要です。 https://www.v-service.example.com/にアクセスしてください。

B副所長は，Dさんになりすました何者か（以下，なりすまし者という）がDさんのアカウントに不正にログインしたおそれがあると考え，A所長に報告した。

報告を受けたA所長は，インシデントの発生を宣言し，VサービスのGCを利用しないようR営業所の全従業員に通知するとともに，このインシデントについてCISO及びL課長に報告した。B副所長はL課長と協力し，②被害拡大の防止策を実施した。

〔被害状況の把握と影響範囲の調査〕

次は，インシデントの被害状況と影響範囲に関するL課長とB副所長の会話である。

L 課長　：表 3 の GC メッセージ中の URL（以下，URL-P という）は V サービスの URL ではありません。悪意のあるサイトの URL と考えられるので，URL-P へのアクセスの成功が記録されている可能性のある［　a　］のログについて調査しましたが，該当する記録はありませんでした。［　a　］のログだけでは確認できないので，③R 営業所の従業員のうち，必要がある者に対して URL-P にアクセスしたかどうかをヒアリングしましたが，全員がアクセスしていないという回答でした。D さんのアカウントへの不正ログインによる情報漏えいの有無についてはどうでしたか。

B 副所長：事務担当者からの報告によると，なりすまし者がアクセスした可能性のある［　b　］の GC メッセージを調査した結果，P 社の業務に関する情報はありましたが，会社が秘密と規定した情報（以下，秘密情報という）は含まれていませんでした。しかし，④現時点で確認可能な GC メッセージの調査だけでは十分な調査とはいえません。

L 課長　：［　b　］を利用していた利用者にヒアリングが必要ですね。ところで，GC に送信されたファイルはどうでしたか。

B 副所長：10 ファイルありましたが，全て V サービス利用ルールを満たしたパスワードで保護されていました。

L 課長　：今回の場合，パスワードで保護されていても，⑤なりすまし者が短時間にパスワードを入手又は特定して，ファイルの内容を閲覧できたと思われます。ファイルにはどのような情報が含まれていたのでしょうか。

B 副所長：業務に関する情報は含まれていましたが，秘密情報は含まれていませんでした。

L 課長　：分かりました。調査結果を A 所長及び CISO に報告しましょう。

〔原因調査〕

次は，原因に関する B 副所長と L 課長の会話である。

B 副所長：D さんにヒアリングしたところ，V サービスにアクセスしてアカウントの確認をするように求めるメールが V サービスから来たので，すぐに NPC

でメール中の URL（以下，URL-R という）にアクセスし，メールアドレスとパスワードを入力したとのことでした。調べてみると，メールの時刻は 7 月 3 日 11 時 22 分でした。

L 課長　：URL-R はフィッシングサイトと考えられます。URL-P と URL-R は，D さんが URL-R にアクセスした時点では，URL フィルタリングサービスに悪意のあるサイトの URL として登録されていませんでした。しかし，現在は登録されていますし，フィッシング対策協議会のサイトに緊急情報として掲載されています。他の従業員が同様のメールを受信し，URL-R にアクセスしていないかも調査します。念のため，D さんが利用していた NPC（以下，NPC-D という）は，証拠として保全し，詳細に調査します。詳細調査には，1 週間掛かります。

B 副所長：1 週間掛かると，⑥D さんの業務に影響があります。

L 課長　：NPC-D を初期化し，セキュリティ修正プログラムを適用してから，文書作成ソフトなどのアプリケーションソフトウェアを再インストールするという対応も考えられます。しかし，NPC-D を初期化すると，⑦詳細調査に影響があります。⑧D さんの業務への影響を軽減する策を講じれば大丈夫ですか。

B 副所長：それなら大丈夫です。

〔対策の検討〕

B 副所長及び L 課長は，詳細調査の結果を基に，R 営業所での V サービス利用における問題点と対策を表 4 のように整理した。

表 4　R 営業所での V サービス利用における問題点と対策（抜粋）

番号	今回の問題点	今後の対策
1	URL-R が悪意のあるサイトの URL として URL フィルタリングサービスに登録されるよりも前に，D さんが URL-R にアクセスしてしまった。	・［　c　］ことを確実に実施する。 ・フィッシング対策に関する従業員研修を実施する。
2	利用者認証に利用者 ID とパスワードだけを利用していたので，不正ログインされてしまった。	V 認証機能を有効にする。

次は，表4に関するB副所長とL課長の会話である。

B副所長：番号 2 の対策では，ログインが煩雑になり利便性が低下してしまうことを懸念しています。

L課長　：それでは，［ d ］ことにすれば，利便性も保てます。

B 副所長と L 課長は，詳細調査の結果と今後の対策を A 所長に報告し，承認を得た。また，A 所長は P 社委員会に報告し，承認を得た。その後，必要な対策を実施し，V サービスの業務利用を再開した。今回の V サービス活用による業務効率化は，高く評価された。その後，V サービスは P 社全体に導入され，業務効率向上に貢献した。

設問1　〔インシデント発生〕について，(1)，(2)に答えよ。

(1) 本文中の下線①について，K さんが，電話ではなく，V サービスで D さんに連絡した場合に想定される被害はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア　K さんが，なりすまし者とのやり取りの結果，表 3 の GC メッセージが D さんからのものと信じ，URL-P にアクセスすることによって，K さんのパスワードが窃取される。

イ　K さんが，なりすまし者に GC メッセージを送ることによって，V サービスで利用している B 副所長のアカウントが，なりすまし者によって不正に利用される。

ウ　K さんがなりすまし者への連絡のために送った GC メッセージが，なりすまし者以外の第三者に盗聴され，内容が第三者に漏えいする。

エ　K さんが連絡した直後に，なりすまし者によって証拠隠滅が図られ，D さんのアカウントが利用されて GC メッセージが削除される。

(2) 本文中の下線②について，次の (i) ～ (v) のうち，実施した防止策として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) D さんに，V サービスのパスワードを変更するよう指示する。

(ii) R 営業所の全従業員に，URL-P にアクセスした場合は B 副所長に報告するよう指示する。

(iii) R 営業所の全従業員に，URL-P にアクセスしないよう指示する。

(iv) V アプリをスマホにインストールしている R 営業所の従業員に，V アプリを再インストールするよう指示する。

(v) WS 管理者のパスワードを変更する。

解答群

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

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

設問2 〔被害状況の把握と影響範囲の調査〕について，(1) ～ (5) に答えよ。

(1) 本文中の［ a ］に入れる適切な字句はどれか。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 URL フィルタリング機能

イ VPN サーバ

ウ VPN サーバ及び URL フィルタリング機能

エ VPN サーバ及びプロキシサーバ

オ プロキシサーバ

カ プロキシサーバ，VPN サーバ及び URL フィルタリング機能

キ プロキシサーバ及び URL フィルタリング機能

(2) 本文中の下線③について，最低限，R 営業所のどの従業員にヒアリングをする必要があるか。解答群のうち，最も適切なものを選べ。

解答群

ア 営業担当者

イ 所長，副所長，営業担当者及び事務担当者

ウ 所長，副所長及び営業担当者

エ 所長及び副所長

オ 流通担当者及び事務担当者

(3) 本文中の [b] に入れる適切な字句を，解答群の中から選べ。

b に関する解答群

ア GC-1，GC-2 及び GC-3

イ GC-1，GC-2 及び GC-4

ウ GC-1，GC-3 及び GC-4

エ GC-2

オ GC-2 及び GC-3

カ GC-2，GC-3 及び GC-4

キ GC-2 及び GC-4

ク GC-3

ケ GC-3 及び GC-4

コ GC-4

(4) 本文中の下線④について，十分な調査とはいえない理由はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア Dさんのアカウントでは確認できないGCメッセージがあるから

イ URL-P にアクセスした結果，マルウェアをダウンロードした従業員がいる可能性があるから

ウ なりすまし者がDさんのアカウントに不正にログインした後，GCメッセージのうち秘密情報を含むものを選んで削除した可能性があるから

エ なりすまし者が D さんのアカウントに不正にログインしていた間は閲覧可能であったが，その後に削除されたGCメッセージがあった可能性があるから

オ 表3に示すGCメッセージを閲覧していない従業員がいるから

(5) 本文中の下線⑤について，パスワードを入手又は特定した方法はどれか。解答群のうち，最も適切なものを選べ。

解答群

ア Dさんのスマホを物理的に入手しフォレンジックすることによって特定する。

イ GCメッセージから特定する。

ウ 辞書攻撃を行うことによって特定する。

エ 他のサービスから流出したパスワードのリストから特定する。

設問3　本文中の下線⑥～⑧について，“詳細調査の間の D さんの業務への影響”，“詳細調査への影響”及び“詳細調査への影響なしに D さんの業務への影響を軽減する策”を，次の (i) ～ (x) 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。

[詳細調査の間の D さんの業務への影響]

(i) D さんが NPC を業務に利用できない。

(ii) D さんが URL-P にアクセスできない。

(iii) D さんが配送業者からの連絡を受け取ることができない。

[詳細調査への影響]

(iv) D さんが参加している GC のメッセージが消去され，内容を追跡できない。

(v) NPC-D 内に保存されているデータが消去されてしまい，調査できない。

(vi) NPC-D の OS の設定変更が発生してしまい，V サービスに D さんのアカウントでログインしても，内容を調査できない。

[詳細調査への影響なしに D さんの業務への影響を軽減する策]

(vii) D さんが業務で利用しているファイルを，詳細調査の対象から外す。

(viii) D さんに，新たに NPC を手配し，詳細調査の間は追加で貸与する。

(ix) D さんの業務終了後の時間帯に詳細調査を行う。

(x) NPC-D に保存されているファイルを全てバックアップし，バックアップファイルを詳細調査する。

解答群

ア (i)，(v)，(vii)	イ (i)，(v)，(viii)
ウ (i)，(v)，(ix)	エ (i)，(vi)，(ix)
オ (ii)，(iv)，(ix)	カ (ii)，(v)，(viii)
キ (ii)，(v)，(x)	ク (ii)，(vi)，(vii)
ケ (iii)，(iv)，(viii)	コ (iii)，(v)，(x)

設問4　〔対策の検討〕について，(1)，(2)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　VPNサーバ，プロキシサーバ及びスマホに，悪意のあるサイトのIPアドレスを基にサイトへの接続を遮断する機能をもつセキュリティ対策ソフトを追加導入する

イ　Vサービスに対して，P社が指定する監査法人による監査を毎年実施するよう要求し，実施しない場合は，Vサービスの利用を停止する

ウ　Vサービスの代わりに，これまでフィッシング対策協議会の緊急情報にフィッシングメールが報告されたことがない別のチャットサービスを利用し，緊急情報を毎日確認する

エ　従業員がWebブラウザからVサービスにアクセスするときは，必ずブックマークからアクセスする

オ　フィッシングサイトにアクセスしたときに，それが確実に記録されるように，NPC又はDPCからだけVサービスを利用する

(2) 本文中の［ d ］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。

d に関する解答群

ア　P 社内でフィッシング対策についての従業員研修を行い，研修を終えた従業員は，V 認証機能を無効のままにできるよう V サービス利用ルールを更新する

イ　R 営業所の全従業員について V 認証機能及び V 省略機能を有効にする

ウ　R 営業所の全従業員について V 認証機能を有効にし，V サービスのパスワードの長さを 32 文字以上に設定した従業員だけ，V 省略機能を有効にする

エ　V サービスのパスワードを 30 日ごとに変更するよう V サービス利用ルールに定め，V 認証機能を有効にしない

オ　V サービス利用ルールを満たしたパスワードを利用しているか，ツールによって確認し，満たしている従業員は，V 認証機能を無効にする