問２　情報機器の紛失に関する次の記述を読んで，設問１，２に答えよ。

Ｚ社は，従業員数 2,000 名の生命保険会社であり，東京に本社をもち，全国に支社が点在している。以下，本社及び各支社を拠点という。

Ｚ社では，拠点の営業員が，会社貸与の持出し用ノート PC（以下，NPC という）を携帯して顧客を訪問し，商品説明資料，見積書，契約書の作成などを行っている。Ｚ社の本社情報システム部は，NPC の情報セキュリティ対策とその持出し管理のために，表１に示すルールを定めている。

表１　NPC の情報セキュリティ対策と持出し管理ルール

全 PC のための情報セキュリティ対策	・次の情報セキュリティ対策を行う。 (a) OS へのログインパスワード設定 (b) BIOS パスワードの設定 (c) CD 及び DVD からの起動禁止設定 (d) OS，ソフトウェアの最新化（脆(ぜい)弱性対応） (e) ウイルス対策ソフトのパターンファイル最新化及び定期的なフルスキャン (f) ５分間無操作でスクリーンをロックし，パスワード入力要求 (g) 外部記憶媒体の接続制限（Ｚ社が従業員に貸与する USB メモリだけが接続可）
NPC のための情報セキュリティ対策	・(a)～(g)に加えて，次の情報セキュリティ対策を行う。 (h) ハードディスクドライブ（以下，HDD という）全体の暗号化 (i) クラウドサービスで提供される契約管理システム（以下，L システムという）を利用するためのクライアント証明書[1]のインストール ・(h)，(i)の情報セキュリティ対策を施した NPC に“対策済 NPC”の文字列と有効期限日（最長６か月）を記載したシールを貼り付ける。
NPC による情報の持出し管理	・NPC に情報を保存して持ち出す場合は，本社情報システム部が運用する NPC 持出し申請システムを利用して，その都度，所属する部課の長の承認を得る。その際，持ち出すファイルのリストを NPC から出力し，NPC の資産管理番号と合わせて申請する。 ・NPC の持出し頻度が高く，都度申請では支障が生じる場合には，部課の長は，最長１か月の“NPC 期間持出し”を承認することができる。

注[1]　L システムでは，クライアント認証とパスワード認証の組合せによる２要素認証の仕組みが提供されている。クライアント認証は公開鍵暗号方式を利用する。NPC 上のクライアント証明書と秘密鍵は，NPC の故障などに備えるためにエクスポート可能にしている。L システムの利用アカウントは本社情報システム部が管理している。L システムでは顧客情報を含む契約書を管理している。

Ｚ社は，各拠点に情報セキュリティ管理責任者とその配下の情報セキュリティリー

ダを置いている。また，各拠点に配置された情報システム担当は，各拠点で利用するPC などの情報機器の貸出し，表 1 に示した情報セキュリティ対策の設定と維持，持出し管理の実施指導，本社情報システム部と連携した情報システムの運用管理，利用支援などを行っている。

Z 社の情報セキュリティ管理規程では，顧客情報を含め Z 社が秘密として管理している情報（以下，秘密情報という）の漏えい及びその可能性がある情報セキュリティインシデント（以下，情報セキュリティインシデントをインシデントという）が発生した場合の対応手順を定めている。そのうち，従業員に貸与している情報機器の紛失・盗難が発生した場合の対応手順は図 1 のとおりである。

1. インシデントの発生

紛失・盗難の発生又はその可能性がある事象を発見した従業員は，直ちに，所属する部課（以下，当該部課という）の長に報告する。報告を受けた長は，直ちに，その時点で確認した事実関係を，当該部課がある拠点（以下，当該拠点という）の情報セキュリティ管理責任者に報告する。情報セキュリティ管理責任者は，情報機器への不正なアクセスのおそれ，秘密情報の紛失・漏えいの発生又はその可能性があると判断した場合には，インシデントの発生を宣言する。

2. 初動対応

情報セキュリティ管理責任者は，配下の情報セキュリティリーダに対して，直ちに，初動対応の体制の編成及び初動対応の開始を指示する。情報セキュリティリーダは，当該拠点の情報システム担当と協力して，インシデントの事実関係を整理し，情報機器に保存されていた情報の内容及び量，並びに暗号化，アクセス制御などの情報セキュリティ対策の実施状況を確認する。保存されていた情報に情報システムのアカウント情報が含まれる場合は，パスワードの変更やアカウントの停止を行うなど，インシデントの影響拡大を防止する措置をとる。情報セキュリティリーダは，確認結果と防止措置を当該拠点の情報セキュリティ管理責任者に報告する。情報セキュリティリーダは，必要に応じてインシデントの対応に当たるメンバを指名することができる。

以下省略（“3. 調査”，“4. 通知，報告及び公表”，“5. 復旧”，“6. 事後対応”が続く）。

図 1　情報機器の紛失・盗難発生時の対応手順（抜粋）

〔情報機器の紛失〕

R 支社は，従業員数 100 名の支社であり，営業員が 60 名いる。R 支社では，支社長が情報セキュリティ管理責任者を務め，各部課の長が情報セキュリティリーダを務めている。

10 月 12 日（水）10 時 30 分頃，R 支社の営業部 1 課の F さんが，客先から R 支社

に戻る途中，電車の網棚にかばんを置き忘れるという事象が発生した。かばんの中には，NPC が入っていた。

報告を受けた R 支社長は，インシデントの発生を宣言し，営業部 1 課の情報セキュリティリーダである K 課長に対して，直ちに初動対応を開始するよう指示した。また，R 支社長の指示によって，K 課長，各部の部長，及び R 支社の情報システム担当として初動対応に当たる W 主任が出席して，インシデント対策会議が開催されることとなった。

幸い，当日の 15 時頃にかばんとその中の NPC を回収することができた。しかし，紛失している間に，外部の者によって NPC を操作されたり，NPC から情報を窃取されたりした可能性は否定できない。K 課長は，調査を継続しつつ，16 時 30 分に開催予定のインシデント対策会議に向けてインシデント報告書案を作成することにした。

〔インシデント報告書案の作成〕

K 課長は，まず，F さんが置き忘れた情報機器（以下，紛失機器という），紛失機器に保存されていた情報，及び紛失機器における情報セキュリティ対策の実施状況を表 2 のとおり整理した。

表 2　インシデント報告書案（抜粋）

紛失機器	・NPC（1 台） 資産管理番号：ZR00XXXX NPC 持出し申請システムにおいて，10 月 3 日に，1 か月間の NPC 期間持出しを承認した記録あり。 ・補足：会社貸与のスマートフォンは紛失していない。 当日，会社貸与の USB メモリなどの外部記憶媒体は持ち出していない。
紛失機器に保存されていた情報の内容及び量	・NPC 持出し申請システムにおいて，会社紹介資料，商品説明資料の持出し申請の記録あり。どちらも自社 Web サイトで社外に公開している資料。 ・持出し申請以後に保存した情報は調査中。
紛失機器における情報セキュリティ対策	・全 PC 及び NPC のための情報セキュリティ対策は，本社情報システム部が定める手順に従い正しく実施されていたことを，PC 管理ツールが NPC 紛失当日の朝に収集した情報を基に，W 主任が確認した。 なお，F さんのログインアカウントには情報セキュリティ対策を変更する権限はない。 ・“対策済 NPC” シールは 7 月 25 日に発行されたものである。

続いて，K 課長は，インシデント報告書案の一部として，インシデント発生とその初動対応の経緯を図 2 のとおり整理した。

NPC の紛失から初動対応及び NPC の回収までの経緯		
(1) インシデントの発生及び報告		
09:45	F さん	訪問先を出る。
10:00	F さん	会社に戻るために，○○駅から××線に乗車。混んでいたので，立ったまま，かばんを目の前の網棚に置く。会社貸与のスマートフォンで電子メールを閲覧。
10:05	F さん	目の前の座席が空いたので，座る。かばんは網棚に置いたまま。
10:20	F さん	△△駅に到着。下車した後，網棚にかばんを置き忘れたことに気付く。
10:30	F さん	△△駅の係員にかばんの紛失を届ける。内容物は NPC，パンフレット，筆記用具など。その時点で，駅において該当する拾得物の届出はなし。
10:45	F さん	スマートフォンを使って，K 課長に，かばんの紛失を電話で連絡。 紛失した状況，かばんに NPC が入っていたこと，その NPC は持出しを承認されているが，紛失時にどのような情報を保存していたかは定かではないことを報告。
	K 課長	F さんに対し，警察に連絡するように指示。
10:55	K 課長	R 支社長に対し，第一報として，F さんからの報告内容を報告。
	R 支社長	インシデントの発生を宣言。K 課長に，直ちに体制を編成して初動対応を開始するように指示。
(2) 初動対応		
11:00	K 課長	関係者を召集して状況説明。初動対応を次のとおり開始。 (a) K 課長の実施内容 ・紛失物の捜索活動の支援 ・情報機器紛失時の状況など，事実関係の確認 ・[a] (b) W 主任の実施内容 ・紛失機器の特定 ・紛失機器における [b] ・[c] システムの特定 ・上記で特定したシステムにおいて F さんのアクセス権の無効化 ・上記で特定したシステムにおいて [d]
11:10	K 課長	R 支社長に電話で状況報告。
	R 支社長	対応の継続を指示するとともに，15:00 にインシデント対策会議を開催することを決定し，事実関係を整理するよう指示。
	W 主任	NPC 持出し申請システムにおける F さんの持出し申請記録を確認し，K 課長に連絡。
11:15	F さん	最寄りの警察署に，遺失届出書を提出。
11:20	W 主任	L システムにおいて F さんのアクセス権が無効化されたことを K 課長に報告。

図 2　インシデント発生とその初動対応の経緯

11:45	F さん	R 支社に帰社。
	K 課長 W 主任	事実関係を確認するために F さんにヒアリング。
12:30	K 課長	この時点までに確認した事実関係と対応状況を R 支社長に報告。
(3) NPC の回収		
14:10	F さん	△△駅からかばんが見つかった旨の電話連絡を受ける。□□駅で，乗客が届けてくれていた。
	K 課長	R 支社長にインシデント対策会議延期を申し入れ，16:30 開始に決定。
14:50	F さん	□□駅でかばんとその中身を確認し，受領。
	K 課長	すぐに NPC を受け取る。
15:05	K 課長	R 支社長に電話で報告。

図 2　インシデント発生とその初動対応の経緯（続き）

〔インシデントの影響及び対応〕

16 時に，K 課長は W 主任に声を掛け，インシデント対策会議の事前確認のための打合せを行った。次はその時の会話である。

K 課長 ：F さんは，NPC にはどのような情報が入っていたか定かではないと言っていました。契約書などの顧客情報は入っていたのでしょうか。

W 主任 ：NPC の持出し申請の時点では，顧客情報は含まれていませんでした。ただし，①持出しの承認の後でも，NPC に顧客情報を追加で保存できてしまいます。

K 課長 ：分かりました。②当社で定めた手順のうち，NPC 紛失時に NPC の中の情報を盗まれるリスクを低減する手順は，施されていたでしょうか。

W 主任 ：はい。もちろんです。

K 課長 ：紛失時点で顧客情報が NPC に保存されていたかどうか，紛失後に NPC に誰かがアクセスしていたか，確認をお願いします。ところで，今，F さんは L システムにアクセスができない状態ですね。

W 主任 ：はい。F さんの NPC 内にあるクライアント証明書と秘密鍵が盗用される可能性を考慮した措置です。もし，F さんの利用アカウントで認証に成功したとしたら，F さんが担当する全ての顧客の情報にアクセスできてしまいます。

K 課長 ：すばやく対応してくれましたね。

W 主任：秘密鍵の漏えいの有無を調査するために，何者かが F さんの秘密鍵を使い，クライアント認証して [e1] が L システムの [e2] のログ中にないか確認しました。確認したログの範囲では，不審な点はありませんでした。F さんがまた L システムにアクセスできる状態にするために，[f]，アクセス権を有効にする予定です。

K 課長 ：F さんの NPC は，今後どのようになるのでしょうか。

W 主任 ：一時的にでも自社の管理を離れたことによって情報が盗まれたり，マルウェアが入れられたりした可能性があるので，[g1]。

K 課長 ：[g2]。

こうして K 課長はインシデント対策会議に臨み，インシデント報告書案に沿って事実関係，対応状況及び今後の調査予定を報告し，R 支社長の了解を得た。

2 日後，W 主任から，NPC 内に顧客情報は追加保存されていなかったこと，及び F さんが NPC を紛失していた間に NPC がアクセスされた痕跡はなかったことの報告があり，このインシデントは収束が宣言された。

設問1　〔インシデント報告書案の作成〕について，図2中の［　a　］～［　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。

aに関する解答群

ア　Fさんが紛失した情報の内容及び量の特定

イ　Fさんが持ち出した情報の持出し方法の特定

ウ　インシデントによる損害額の検討

エ　インシデントの再発防止策の策定

bに関する解答群

ア　“対策済NPC”シール発行記録の確認

イ　Fさんの利用記録の確認

ウ　資産管理番号とFさんへの貸与記録の確認

エ　情報セキュリティ対策の実施状況の確認

cに関する解答群

ア　Fさんがオフィスで使っている

イ　Fさんが外出先からアクセスできる

ウ　Fさんが顧客情報を保管している

エ　Fさんが顧客訪問の際に画面を見せてもらったことがある

dに関する解答群

ア　Fさんが当日訪問した顧客に関する顧客情報がダウンロードされていないかどうかに絞った確認

イ　社外から操作ログが改ざんされていないかどうかの確認

ウ　社外からパスワードリスト攻撃が行われていないかどうかの重点的な確認

エ　社外から不審なアクセスがないかどうかの幅広い確認

設問２　〔インシデントの影響及び対応〕について，(1) ～ (5) に答えよ。

(1)　本文中の下線 ① について，どのような方法が考えられるか。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)　1 か月間の NPC 期間持出しの承認を得るとその期間中に，NPC を会社に持ち帰り，追加で保存できる。

(ii)　NPC の持出しとは別に，会社貸与の USB メモリに保存して持ち出すことによって，NPC に保存できる。

(iii)　外出先から L システムにアクセスして，NPC にダウンロードして保存できる。

(iv)　外出先で，公衆無線 LAN に接続して，インターネット上で他社の公開 Web サイトを閲覧し，NPC にダウンロードして保存できる。

(v)　顧客訪問先で，顧客から借りた USB メモリからコピーして保存できる。

解答群

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

(2)　本文中の下線 ② について，表 1 に記載されている対策のうち，NPC 紛失時に，NPC 内のデータが読み取られるリスクを低減するための対策として最も効果的なものを，解答群の中から選べ。

解答群

ア　(a)	イ　(b)	ウ　(c)
エ　(d)	オ　(e)	カ　(f)
キ　(g)	ク　(h)	ケ　(i)

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

e に関する解答群

	e1	e2
ア	アクセスを試みた形跡	本日 00:00 から 11:20 まで
イ	アクセスを試みた形跡	本日 00:00 から 15:30 まで
ウ	情報をダウンロードした形跡	本日 00:00 から 11:20 まで
エ	情報をダウンロードした形跡	本日 00:00 から 15:30 まで

(4) 本文中の [f] に入れる適切な字句を，解答群の中から選べ。

f に関する解答群

ア　F さんの L システムの利用アカウントのパスワードを変更した後

イ　F さんの従来のクライアント証明書を失効させてから，新しい鍵ペアを生成しクライアント証明書を発行し直した後

ウ　F さんの秘密鍵のバックアップを取り寄せた後

エ　本社情報システム部で L システムのログを保全した後

(5) 本文中の [g1] , [g2] に入れる字句の組合せはどれか。g に関する解答群のうち，最も適切なものを選べ。

g に関する解答群

	g1	g2
ア	HDD を複製し，今日中には返却します	入念な調査をお願いします
イ	証拠保全をした上で調査しています	F さんには新しい NPC を手配しましょう
ウ	直ちに HDD を取り出し，データを消去した上で，破壊し，破棄します	情報漏えいがないように，確実にお願いします
エ	直ちに NPC を初期化して，OS から入れ直します	それなら安心ですね
オ	返却前に，F さんに NPC の中のファイルを点検してもらいましょう	私も立ち会います