問4　ノートPCの情報漏えい対策に関する次の記述を読んで，設問1～5に答えよ。

E社は，事業戦略策定などに関するコンサルティングを業務としている中堅のコンサルティング会社である。オフィスのフリーアドレス化及び出先での業務推進のため，E社に所属する200名のコンサルタント（以下，従業員という）にはノートPC（以下，NPCという）が配布されている。従業員は，社内や顧客オフィスでNPCを用いて業務を行う。また，従業員には通信カードも配布されており，社外からも，E社の情報システムにアクセスしている。

ここ最近，E社では，通勤途中の従業員が，顧客の重要情報を保存したNPCやUSBメモリを紛失するという事故が連続して発生した。それによって，顧客からは，E社のセキュリティ管理状況に対して強い不信の念をもたれることとなった。

そこで，E社の幹部は，情報セキュリティの専門家であるH氏の支援の下，再発防止プロジェクトチーム（以下，対策チームという）を立ち上げ，情報漏えい事故に対して抜本的な対策を実施することにした。

〔管理状況の把握〕

対策チームではまず，NPCやUSBメモリを紛失した従業員及びE社の各部門から選んだ数名の従業員に対してヒアリングを行い，NPC及びUSBメモリにおける顧客の重要情報の管理状況について把握することにした。その結果，次のような管理状況が明らかになった。

(1) E社の規程では，重要情報をNPC又はUSBメモリに保存する場合，暗号化しなければならないことになっている。しかし，E社指定の暗号ソフトでは，保存の都度，ファイル単位で暗号化の操作を行う必要がある。その手間を嫌い，平文のままファイルを保存してしまう場合が多い。

(2) E社指定の暗号ソフトでは，暗号化の際，復号のためのパスワードを入力する必要があるが，パスワードを忘れることを懸念して，自分の名前や顧客名，ファイル名など，単純なものをパスワードにしている場合が多い。

これらの管理状況に対するH氏のコメントは，次のとおりである。

(a) 暗号化を利用するのであれば，重要情報を確実に暗号化できるような仕組みを考

える必要がある。

(b) 幾ら強力な暗号ソフトを利用しても，現在の管理状況では，簡単に復号されてしまう可能性がある。

(c) (a) への対応のためには，ハードディスク全体を暗号化し，データの暗号化と復号を利用者に意識させることなく行う方法が有効である。ただし，この方法では，スリープ状態で NPC を持ち運んでいると，紛失や盗難時の情報漏えい対策として暗号化が意味を成さなくなることがあるので注意が必要である。

(d) 暗号化の代わりとして，シンクライアントシステムと呼ばれる仕組みを導入することで，NPC 上にデータを保存せずに済ませるという対策も考えられる。

(e) USB メモリへの重要情報の保存についても，データを確実に暗号化するための対策が必要である。USB メモリの利用を禁止するという対策も考えられる。

〔対策の検討〕

対策チームでは，H 氏のコメントの (c) 及び (d) で挙げられた，ハードディスク全体の暗号化による対策とシンクライアントシステムによる対策の二つについて検討を進めた。シンクライアントシステムには，幾つかの方式が存在しているが，従業員に配布済の NPC を有効に活用するため，NPC にシンクライアント用ソフトウェアを導入する方式を前提に検討することにした。表 1 は，二つの対策について，幾つかの観点から比較した内容を整理したものである。

表1　ハードディスク全体の暗号化とシンクライアントシステムの比較

比較項目	ハードディスク全体の暗号化	シンクライアントシステム
PC の紛失や盗難時の情報漏えい対策	(ア) 暗号鍵が漏えいしない限り，情報漏えいを防止できる。	(イ) 重要情報が NPC 上に保存されないため，情報漏えいを防止できる。
USB メモリ紛失や盗難時の情報漏えい対策	(ウ) USB メモリ上のデータについても利用者に意識させることなく暗号化することによって，USB メモリからの情報漏えいを防止できる。	(エ) USB メモリを使用禁止にすることによって，結果的に USB メモリからの情報漏えいを防止できる。
パフォーマンス	(オ) ファイルの読み書きの都度，暗号化又は復号の処理に伴うオーバヘッドが生じるが，最近の PC の性能から考えて，業務効率に与える影響は少ない。	(カ) サーバと接続しているネットワークや通信回線の速度に大きく依存するが，モバイルでの利用であっても，最近の高速モバイル通信であれば，E 社の業務には支障がない。
懸念事項	(キ) NPC をスリープ状態で持ち運んでいて，紛失したり盗難に遭ったりした場合，暗号化が意味を成さなくなることがある。 (ク) 製品の仕様上の問題や利用者の不適切な運用によって，暗号鍵が適切に管理されない場合，漏えいした暗号鍵によってデータを復号されてしまう可能性がある。 (ケ) 暗号鍵が紛失又は破損した場合，若しくは暗号鍵を保護するパスワードを忘れた場合は，NPC 上のデータにアクセスできなくなる。	(コ) データへアクセスするためにネットワーク接続が必須となる。

対策チームは，表1中の比較項目の検討と並行して，従業員の NPC 及び USB メモリの利用形態について調査した。その結果，図1のことが判明した。

(i) 顧客先などインターネットによる通信ができない場所で，NPC に保存された資料のデータにアクセスしなければならないことが多い。
(ii) 顧客先で資料のデータを顧客に渡す必要が出る場合が多く，USB メモリの利用頻度が高い。

図1　従業員の NPC 及び USB メモリの利用形態についての調査結果

シンクライアントシステムによる対策は，［a］や［b］といった点から，ハードディスク全体の暗号化による対策に比べて情報漏えいのリスクをより小さくできる点が評価されたものの，［b］や［c］といった点が現状の E 社の業務形態に合わない点が問題とされた。一方，ハードディスク全体の暗号化による対策には，表1中の(キ)，(ク)，(ケ)といった懸念事項があるものの，いずれも技術的に対応可能であると考えられた。

以上から，対策チームは，シンクライアントシステムの導入を今回は見送ることにし，情報漏えい対策としては，NPC のハードディスク全体の暗号化による対策を実施することにした。

〔製品の選定〕

対策チームは，ハードディスク全体を暗号化できる製品の選定を進めた。H 氏から実績が豊富な製品として挙げられた P 社，Q 社及び R 社の製品が候補となった。いずれも，NPC の起動時にパスワードを入力することによって，暗号化されたハードディスクにアクセスできるようになるという製品である。表 2 は各社の製品の比較表である。

表2　製品の比較

比較項目	P社製品	Q社製品	R社製品
暗号化の対象となるデバイス	ハードディスク及び USB メモリ	ハードディスク及び USB メモリ	ハードディスク（USB 接続のものを除く）
データ鍵(1)の保管方法	ハードディスク上に暗号化して保管する。	ハードディスク上に暗号化して保管する。	ハードディスク上に暗号化して保管する。データ鍵を使用するためには，保管時に指定したパスワードの入力が必要である。
マスタ鍵(2)の保管方法	鍵メモリ(3)に暗号化して保管する。マスタ鍵を使用するためには，保管時に指定したパスワードの入力が必要である。	PC 内にある TPM（Trusted Platform Module）(4) に保管する。マスタ鍵を使用するには，マスタ鍵の保管時に指定したパスワードの入力が必要である。	マスタ鍵に相当する鍵はない。
PC 利用開始時の操作	鍵メモリを PC に接続した上で，パスワードを入力する。 PC を利用している間は，常に鍵メモリを接続している必要がある。	パスワードを入力する。	パスワードを入力する。
USB メモリによるデータ交換のサポート	USB メモリ上のファイルを暗号化する PC 及び復号する PC の双方に P 社製品のインストールが必要である。	自己復号ファイル(5)として書き出すこともできるので，復号する PC への Q 社製品の導入は不要である。	USB メモリへの書出し時は暗号化されない。
スリープ状態からの復帰	パスワードの入力が必要である。	パスワードの入力が必要である。	パスワードの入力は不要である。
パスワードを忘れたときの対応	管理ツールによって，リカバリ用のパスワードを発行できる。	特にない。	特にない。

注(1) ハードディスク上のデータの暗号化に用いる鍵
注(2) データ鍵の暗号化に用いる鍵
注(3) マスタ鍵を保管する USB メモリ
注(4) 暗号化やハッシュの演算，プラットフォームの完全性検証の機能をもったセキュリティチップで，TPM 内に保管された暗号鍵は，チップ外へ読み出すことができない。物理的な方法によって無理に読み出そうとしても，チップの動作停止や回路の物理的破壊などによって，攻撃を防ぐようになっている。
注(5) 復号のためのプログラムと暗号化データを一体化した実行可能形式のファイルで，ファイルを実行することでデータを復号することができる。

Q 社製品の利用には TPM を内蔵した PC が必要であるが，E 社が従業員に配布している NPC は TPM 内蔵のモデルであり，この点は問題にならなかった。また，NPC に内蔵された TPM は，TPM に保管されたパスワードを間違えた場合，一定時間，マスタ鍵へのアクセスがロックされるという機能をもっている。

対策チームは，表1に挙げられた(キ)，(ク)，(ケ)といった懸念事項を中心に各社の製品を評価し，結果を表3にまとめた。

表3　製品の評価結果（一部）

評価の観点	優れている製品	理由
懸念事項(キ)への対応	P社製品，Q社製品	スリープ状態のNPCが盗まれてもパスワードが分からなければデータにアクセスできない。
懸念事項(ク)への対応	d 社製品	〔懸念事項(ク)に関する製品比較〕に記述
懸念事項(ケ)への対応	P社製品	従業員がパスワードを忘れても，データへのアクセスが可能となる。
USBメモリによるデータ交換への対応	e 社製品	f

〔懸念事項(ク)に関する製品比較〕

〔管理状況の把握〕の(2)から考えて，マスタ鍵を保護するパスワードとして，総当たり攻撃によって解析可能な程度の強度しかもたないものが設定される可能性がある。その点を踏まえて，対策チームでは，懸念事項(ク)への対応については，図2のような検討を行った。

(i)　P社製品を利用するとした場合，NPCと鍵メモリを同時に持ち歩く必要がなく，両方が同時に紛失したり盗難に遭ったりする可能性が低いならば，P社製品が優れている。
(ii)　P社製品を利用するとした場合，NPCと鍵メモリを同時に持ち歩く必要があり，両方が同時に紛失したり盗難に遭ったりする可能性が高いならば，Q社製品が優れている。

図2　懸念事項(ク)に関する製品比較

〔製品の選定と懸念事項(ケ)への対応〕

対策チームは，表3に基づいてQ社製品を選定し，NPCのハードディスク全体の暗号化を推進した。ただし，Q社製品では，懸念事項(ケ)への対応が不十分なことから，対策チームは，NPC上のデータをバックアップしておき，NPC上のデータにアクセスできなくなっても，バックアップ先から復旧できるようにしておくことで懸念事項(ケ)に対応することにした。

設問1　本文中の［　a　］～［　c　］に入れる適切な字句を，表 1 中の (ア)～(コ) から選び，記号で答えよ。

設問2　〔管理状況の把握〕において H 氏がコメント (b) の指摘をした理由を，40 字以内で述べよ。

設問3　〔管理状況の把握〕における H 氏のコメント (c) にあったスリープ状態での NPC の持ち運びについて，(1)，(2)に答えよ。

(1) 紛失や盗難時の情報漏えい対策として暗号化が意味を成さなくなることがあるのは，どのような場合か。35 字以内で述べよ。

(2) (1)の場合に暗号化が意味を成さなくなる理由を 40 字以内で述べよ。

設問4　E 社従業員の USB メモリの利用形態から考えて，表 3 中の［　e　］に入れるべき，USB メモリによるデータ交換への対応が優れていると考えられる製品を P～R から選び，記号で答えよ。また，表 3 中の［　f　］に入れるべき理由を，40 字以内で述べよ。

設問5　〔懸念事項 (ク) に関する製品比較〕について，(1)～(3) に答えよ。

(1) 図 2 中の (i) で P 社製品が優れているとした理由を，30 字以内で述べよ。

(2) 図 2 中の (ii) で Q 社製品が優れているとした理由を，マスタ鍵を保護するパスワードの強度に関する懸念を踏まえて 50 字以内で述べよ。

(3) E 社従業員の NPC の利用形態も踏まえて，表 3 中の［　d　］に入れるべき，懸念事項 (ク) への対応が優れていると考えられる製品を P～R から選び，記号で答えよ。