問3　情報漏えい対策に関する次の記述を読んで，設問1～4に答えよ。

E社は，雑貨やアイディア商品の企画・販売を行う従業員数100名の会社である。大手通販会社や生活用品店，雑貨店，全国チェーンのドラッグストアなどを顧客にもち，E社ブランド商品の販売のほか，顧客のプライベートブランドで販売されるOEM商品の企画や各種イベントとタイアップした商品の企画なども手掛けている。

〔情報漏えい事故の発生と対策の指示〕

ある日，E社の従業員が帰宅後も資料を作成するために，USBメモリに商品の企画書をコピーして持ち帰り，そのUSBメモリを紛失するという事故が起こった。USBメモリにコピーした企画書は，顧客であるL社のプライベートブランドで販売される予定のOEM商品に関するものであり，L社への事情説明と謝罪に加え，商品の企画をやり直す事態となった。

当該商品が企画の初期段階であり，幸い大事に至らなかったが，今後，業務情報の社外持出しに起因する重大な情報漏えい事故が発生しないとも限らないとE社社長は考えた。そこで，E社社長は，情報システム部長を通じて，情報システム部のY課長に，E社における業務情報の社外への持出しの現状を調査し，必要であれば情報漏えい対策を検討するよう指示した。

〔業務情報の持出しに関する現状調査〕

Y課長は，まず，“業務情報の持出し”を，“会社貸与のノートPC（以下，貸与PCという）や会社貸与のUSBメモリ（以下，貸与USBメモリという）に業務情報を保存して社外に持ち出すこと”と定義した上で，業務情報の持出しの状況についての調査と対策の検討を進めることにした。一方，電子メールやファイル転送などによる社外への情報の送信についての調査と対策の検討は，別途実施することにした。

Y課長は，E社における業務情報の持出しの現状を調査するために，情報システム部のZ君とともに従業員のうちの何人かにヒアリングを行った。

ヒアリングの結果，従業員が業務情報を持ち出す目的は，顧客との打合せ（以下，Mという）か，自宅での資料作成（以下，Hという）のいずれかであることが分かった。現状，いずれの場合においても申請や承認などについて規定されていない。

Z君は，E社の業務情報の持出しの状況について，概要を表1に整理した。

表1　E社の業務情報の持出しの状況

持ち出す目的	持ち出す者	持出先	持ち出す業務情報（以下，持出情報という）と開示可能範囲		現状の持出手段
			持出情報の内容	開示可能範囲	
M	E社営業担当者	顧客先	E社ブランド既存商品の情報	制限なし	貸与PC
			OEM商品やタイアップ商品の企画書及び提案書	E社内の案件関係者並びにOEM又はタイアップ先の顧客	
H	E社従業員	自宅	・公開前のプレスリリース ・E社ブランド商品の企画書 ・キャンペーン，プロモーションなどの企画書	E社内の案件関係者	貸与PC又は貸与USBメモリ
			E社ブランド既存商品の情報	制限なし	
			OEM商品やタイアップ商品の企画書及び提案書	E社内の案件関係者並びにOEM又はタイアップ先の顧客	

貸与PCで業務情報が持ち出された場合は，M，Hのいずれにおいても，持出先での業務情報へのアクセスには，その貸与PC自体が利用されている。一方，Hにおいて，貸与USBメモリで業務情報が持ち出された場合は，従業員が私有するPC（以下，私有PCという）を利用して業務情報にアクセスすることがあると判明している。

Mについては，顧客に資料を提示しなければならないという業務上の必要性があるのに対し，Hについては，E社オフィス内で資料作成を実施すればよく，必要性に乏しい。そこでY課長は，Hのための持出しについては，禁止することを会社規則として規定した上でそれを全社に周知することとし，Mについては，情報漏えい対策の検討をZ君に指示した。

〔Mにおける情報漏えい対策の検討〕

Z君は，Mにおける情報漏えい対策を検討するに当たって，Mのための業務情報の持出しに関連した情報漏えいリスクへの現状の対応状況を表2に整理した。

表２　M のための業務情報の持出しに関連した情報漏えいリスクへの現状の対応状況

情報漏えいリスク		リスクに対して有効と考えられる対策	E 社における左記対策の実施状況
(ア) 盗難，紛失	持出中に貸与 PC が盗まれる又は紛失する。	・情報を秘匿するための［ a ］ ・①貸与 PC の安全な持運びに関する注意点の周知	・情報は［ a ］していない。 ・貸与 PC の社外での取扱方法に関する規定はない。
(イ) マルウェアに感染	・持出中に貸与 PC がマルウェアに感染する。 ・マルウェアに感染した貸与 PC で情報を持ち出す。	・社外でのインターネット接続の禁止 ・ウイルス対策ソフトの導入 ・会社指定ソフトウェア以外のインストール禁止 ・セキュリティパッチ適用の徹底	・貸与 PC による社外でのインターネット接続は禁止していない。 ・貸与 PC にウイルス対策ソフトを導入済 ・会社指定ソフトウェアの規定はないが，従業員に貸与 PC の管理者権限が与えられていないので，管理者権限が必要なソフトウェアのインストールはできない。 ・貸与 PC に対してセキュリティパッチの強制適用を定期的に実施している。
(ウ) 不正開示	持出中に E 社従業員が，開示が許可されている対象者以外に（故意又は過失で）情報を開示してしまう。	開示可能範囲の周知	開示可能範囲は規定されているが，それを制限する技術的な対策は導入していない。
(エ) 盗み見	持出中に貸与 PC の画面をのぞき見られる。	・プライバシフィルタの利用 ・第三者から見られる場所での利用を禁止した規定の周知	・プライバシフィルタは利用していない。 ・貸与 PC の社外での取扱方法に関する規定はない。

M では，営業担当者が持出情報を持ち歩いていることに加え，②日常業務に利用している貸与 PC を持ち出していることで，万一，情報漏えい事故が発生すると被害が大きくなるおそれがあることから，Z 君は，営業担当者が業務情報を持ち出す必要をなくし，貸与 PC の社外への持出しも禁止することが情報漏えい対策として望ましいと考えた。そこで，情報漏えい対策として，ハードディスクなどの記憶装置をもたず USB メモリなどの外部記憶媒体も利用できないシンクライアント端末（以下，専用端末という）を利用する案（以下，案 1 という）と，公開 Web サーバのディスク領域を利用する案（以下，案 2 という）の二つの案を提案することにした。それぞれの案では，貸与 PC の社外への持出しは禁止した上で，図 1 のような手順によって，業務情報を持ち出すことなく顧客に見せることができる。

（案1の場合）
(1) E社内のサーバ上に，専用端末からアクセス可能なディスク領域をあらかじめ作成しておく。
(2) E社の営業担当者は，(1)で作成したディスク領域に業務情報を保存する。
(3) E社の営業担当者は，専用端末を用いて顧客先からそのサーバにVPNでリモートアクセスする。

（案2の場合）
(1) E社の公開Webサーバ上に，各顧客専用のディスク領域をあらかじめ作成しておく。
(2) 各顧客には，専用のディスク領域にアクセスするためのIDとパスワードを登録しておいてもらう。
(3) E社の営業担当者は，業務情報を当該顧客専用のディスク領域にアップロードした上で，当該顧客にダウンロードをしておくよう依頼する。

図1　案1及び案2による顧客への業務情報の提示手順

案2の場合は，③万一，公開Webサーバが不正アクセスされても，業務情報が漏えいするリスクをできるだけ小さくするための運用上の対策を併せて実施する。

案1，案2は，いずれも表2の(ア)及び(イ)のリスクを［ b ］することができる。表2の(ウ)のリスクについては，業務として特定顧客向けの業務情報を取り扱う以上，案1と案2のいずれであっても［ b ］することはできないので，［ c ］策を取ることとし，案1と案2のそれぞれの場合についてどの程度［ c ］できるかを検討し，次のようにまとめた。

（案1の場合）

業務情報ごとに開示が許可されている範囲を明確にし，ディスク領域に保存することを周知することはできるが，E社従業員の故意又は過失による他社への情報開示を技術的に禁止することは困難である。

（案2の場合）

アップロード時に故意又は過失で当該顧客向け業務情報を他社に開示するリスクがあるが，業務情報のアップロードに際して，④アップロードする営業担当者の上司による確認がなされれば，そのリスクを［ c ］することができる。

表2の(エ)のリスクについては，案2では顧客が業務情報をダウンロードすることによって［ b ］できる一方で，案1では［ b ］できない。

Z君は，以上の検討結果から，Mにおいては案2を採用するという対策をまとめ，Y課長に報告し，了承を得た。

〔対策案の見直し〕

Y 課長が情報漏えい対策について情報システム部長に報告したとき，部長から次のコメントがあり，H のための業務情報の持出しについて追加の検討をすることになった。

(a) E 社では，テレワーキングの導入を検討しており，H は，近い将来，許可される方向にある。

(b) 当面は H を禁止することを前提として検討を進めて構わないが，テレワーキングの導入に伴って H が許可された場合の対策も併せて検討しておいてほしい。

Y 課長と Z 君は，H が許可された場合の対策を検討するに当たって，表 2 の内容を見直し，H のための業務情報の持出しの対応状況も含めて整理することにした。

なお，表 3 は，変更後の表 2 から，(ア) 及び (イ) の行を抜粋したものである。

表 3　M と H のための業務情報の持出しに関連した情報漏えいリスクへの対応状況（変更後の表 2 の抜粋）

情報漏えいリスク		リスクに対して有効と考えられる対策	E 社における左記対策の実施状況
(ア) 盗難，紛失	持出中に貸与 PC 又は貸与 USB メモリが盗まれる又は紛失する。	・情報を秘匿するための［a］ ・貸与 PC 及び貸与 USB メモリの安全な持運びに関する注意点の周知	・情報は［a］していない。 ・貸与 PC 及び貸与 USB メモリの社外での取扱方法に関する規定はない。
(イ) マルウェアに感染	・持出中に貸与 PC 又は貸与 USB メモリがマルウェアに感染する。 ・マルウェアに感染した貸与 PC 又は貸与 USB メモリで情報を持ち出す。 ・マルウェアに感染した私有 PC で持出情報を扱う。	（表 2 から変更なし）	（表 2 の内容に次を追記） ・私有 PC におけるマルウェアの対策状況を定常的に把握できていない。 ・私有 PC については，インストールできるソフトウェアを会社指定のものだけに制限できていない。 ・私有 PC については，セキュリティパッチの適用は徹底できていない。

表 3 に基づいて，Y 課長と Z 君は，M について検討した案 1 と案 2 を H のための案として読み替えたものを対策候補として検討を進めた。H の場合，⑤案 2 では，(イ) のリスクに対する有効な対策を取ることが困難なので，案 1 の方が有効であると考えら

れる。(ウ) と (エ) のリスクも検討の上で総合的に判断し，Y 課長と Z 君は，M は案 2，H は案 1 で対応することとした。手順が複数となることで業務効率上の問題が生じた場合は，手順の一本化について後日検討することとした。

Y 課長は，これらを情報システム部長に報告し，了承を得た。また，社長にも概要報告がなされ，了解が得られた。

設問 1　表 2 及び表 3 中の [a] 並びに本文中の [b]，[c] について，(1)，(2) に答えよ。

(1) [a] に入れる適切な字句を 3 字以内で答えよ。

(2) [b]，[c] に入れる適切な字句の組合せを解答群の中から選び，記号で答えよ。

解答群

	b	c
ア	移転	回避
イ	回避	低減
ウ	低減	移転
エ	低減	回避

設問 2　表 2 中の下線①の持運びに関する注意点を 15 字以内で具体的に述べよ。

設問 3　〔M における情報漏えい対策の検討〕について，(1)～(3) に答えよ。

(1) 本文中の下線②について，被害が大きくなるおそれがある理由を 45 字以内で述べよ。

(2) 本文中の下線③とは，どのような運用上の対策か。45 字以内で述べよ。

(3) 本文中の下線④では，何を確認すべきか。35 字以内で述べよ。

設問 4　〔対策案の見直し〕について，本文中の下線⑤の有効な対策を取ることが困難な理由を 55 字以内で述べよ。