問３　LAN 分離に関する次の記述を読んで，設問 1～4 に答えよ。

N 社は，新薬創出を事業内容とする，いわゆる創薬ベンチャ企業である。従業員は 10 名で，研究開発員が 5 名，その他の事務員が 5 名である。N 社のネットワーク構成を図 1 に示す。図 1 中の全ての機器には固定の IP アドレスを割り当てている。また，インターネット経由で N 社が利用しているクラウドサービスを表 1 に示す。

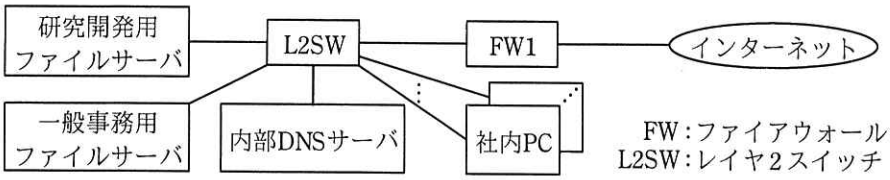


図 1　N 社のネットワーク構成

表 1　利用しているクラウドサービス

サービス名称	内容
電子メールサービス	社内 PC にインストールされた電子メールソフトからのアクセスに応じて，電子メールの送受信を行う。
Web プロキシサービス	社内 PC と社内のサーバからインターネット上の Web サイトへのアクセスを中継する。FW1 では，社内 PC と社内のサーバから，Web プロキシサービスを経由しないでインターネット上の Web サイトへアクセスすることを禁止している。
更新ファイル提供サービス	社内 PC と社内のサーバに，脆(ぜい)弱性修正プログラム（以下，パッチという）とマルウェア定義ファイル（以下，パッチとマルウェア定義ファイルを併せて更新ファイルという）を提供する。更新ファイルは，社内 PC 又は社内のサーバが，HTTP 通信を利用し，Web プロキシサービスを経由してこのサービスへアクセスし，取得する。

〔リスクアセスメント〕

N 社は，事業拡大のために，研究開発員を 30 名程度に増員する計画を立てた。これまで，情報管理を従業員の裁量に任せていたが，増員に伴い，社内の情報管理方法，特にファイルの漏えい防止対策を強化することになり，B 取締役がその責任者に，ネットワーク管理に最も詳しい R さんが担当者に，それぞれ指名された。社外の情報処理安全確保支援士（登録セキスペ）である A 氏の支援を受けることにし，漏えい防止対策の強化について検討を開始した。

次は，その時の会話である。

B 取締役：当社では情報資産の漏えい防止が重要な課題ですが，まずは有望な新薬候補に関するファイル（以下，新薬ファイルという）の保護に絞って見直そうと思います。

A 氏　　：分かりました。新薬ファイルは，どこに保管しているのですか。

R さん　：主に研究開発用ファイルサーバに保管していますが，一部は研究開発員が使用する社内 PC にも保管しています。

A 氏　　：保護の見直しの最初に，サーバや社内 PC に保管中の新薬ファイルについてリスクアセスメントを行うことが必要です。JIS Q 31000:2010 及び JIS Q 31010:2012 では，リスクアセスメントは，［　a　］，リスク分析，［　b　］の三つのプロセスの順に進めると定義されています。まず，［　a　］のプロセスですが，ファイルに影響を及ぼす一般的なリスクの一覧を私から提供しますので，これを基に進めるとよいでしょう。

B 取締役と R さんは，A 氏の支援の下で［　a　］のプロセスを完了した。その結果，新薬ファイルに影響を及ぼすリスクの一覧として表 2 が得られた。

表 2　リスク一覧（抜粋）

項番	リスク	内容
リスク 1	インターネットからの不正侵入による新薬ファイルの漏えい	インターネット経由で，ファイルサーバに侵入されることによって，新薬ファイルがインターネットに流出する。
リスク 2	標的型攻撃による新薬ファイルの漏えい	電子メールによって N 社を標的としたマルウェアが送り込まれ，社内 PC 又は社内のサーバがマルウェアに感染することによって，新薬ファイルがインターネットに流出する。
リスク 3	従業員の故意又は過失によるインターネット経由の新薬ファイルの漏えい	従業員の故意又は過失によって，新薬ファイルが不適切な宛先に電子メールで送信される又は SNS に書き込まれることによって，インターネットに流出する。

続いて，リスク分析のプロセスとして，JIS Q 31000:2010 及び JIS Q 31010:2012 に沿って，［　c　］と，［　d　］を組み合わせてリスクのレベルを決定した。最後に，［　b　］のプロセスとして各リスクへの対応の要否を検討した。その結果，B 取締役は，表 2 のリスク 2 への対応が必要と判断した。

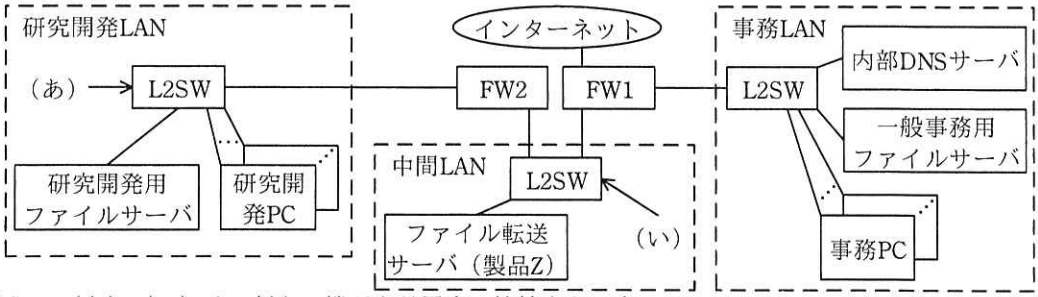
〔LAN 分離案の検討〕

B 取締役と R さんは，表 2 のリスク 2 への対応として，新薬ファイルを保管している機器を収容する LAN（以下，研究開発 LAN という）と，それ以外の機器を収容する LAN（以下，事務 LAN という）に分離する LAN 分離案を検討することにした。事務 LAN はインターネットとの通信を許可するが，研究開発 LAN はインターネットとの通信を一切許可しない。この LAN 分離に伴い，社内 PC は，研究開発 LAN だけに接続する研究開発用の研究開発 PC と，事務 LAN だけに接続する一般事務用の事務 PC に分かれる。研究開発員は，事務 PC と研究開発 PC の 2 台を利用する。

R さんは，業務遂行のために必要な要件を研究開発員から聞き，図 2 にまとめ，ファイル転送のための中間 LAN を加えた図 3 の LAN 分離案を作成した。

1. 社外から届いた電子メールの添付ファイルを，研究開発 PC に転送できること
2. 社外の共同研究者とデータを共有するために，社外のファイル交換用 Web サイトから事務 PC にダウンロードしたファイルを，研究開発 PC に転送できること
3. 研究開発用ファイルサーバ内の新薬ファイルのうち，社外の共同研究者と共有するために承認を受けた新薬ファイルを研究開発 PC 上で編集した後，編集結果を事務 PC に転送し，事務 PC からインターネット上のファイル交換用 Web サイトにアップロードできること

図 2　業務遂行のために必要な要件



注記　（あ），（い）は，新たに機器を設置する接続点を示す。

図 3　LAN 分離案

この案では，研究開発 LAN と事務 LAN の間のファイル転送を行うために，ファイル転送サーバとして広く利用されている U 社製の製品 Z を導入する。図 3 中の FW1 と FW2 の設定内容を表 3 に示す。また，ファイルを転送する際の操作手順を図 4 に示す。

表3　FW1 と FW2 の設定内容

機器名	許可する通信	禁止する通信
FW1	・事務 LAN 上の機器から N 社が利用しているクラウドサービスへの必要な通信 ・事務 PC からファイル転送サーバへの必要な通信	・他の全ての通信
FW2	・研究開発 PC からファイル転送サーバへの必要な通信	・他の全ての通信

注記 1　研究開発 LAN 上の機器は，内部 DNS サーバを利用していない。
注記 2　FW1 及び FW2 は，ステートフルパケットインスペクション型である。

研究開発 PC から事務 PC へのファイル転送時の操作手順

1. 研究開発 PC の Web ブラウザからファイル転送サーバのアップロード用 URL にアクセスし，表示される画面で利用者ごとに異なる利用者 ID 及びパスワードを入力してログインする。
2. ログイン後に表示されるアップロード画面で，研究開発 PC 内のファイルを一つ選択して，アップロードする。アップロードが正常に完了すると，完了メッセージとともにアップロード画面が再度表示される。ここで次のファイルを続けてアップロードすることも，ログアウトボタンをクリックして，ログアウトすることもできる。
3. 事務 PC の Web ブラウザからファイル転送サーバのダウンロード用 URL にアクセスし，表示される画面で利用者ごとに異なる利用者 ID 及びパスワードを入力してログインする。
4. ログイン後に表示されるダウンロード画面では，その利用者 ID でアップロードされたファイルの一覧が表示されるので，ファイルを一つ選択してダウンロードする。ダウンロードが完了すると，サーバ内のダウンロードされたファイルが削除された後，完了メッセージとともにダウンロード画面が再度表示される。ここで次のファイルを続けてダウンロードすることも，ログアウトボタンをクリックして，ログアウトすることもできる。ダウンロードされなくてもアップロードしてから 4 時間たつとファイルは削除される。

注記　事務 PC から研究開発 PC へのファイル転送時の操作手順は，図中の研究開発 PC を事務 PC に，事務 PC を研究開発 PC に，それぞれ置き換えて読むものとする。

図4　ファイルを転送する際の操作手順

LAN 分離を進めると，研究開発 PC 及び研究開発用ファイルサーバは更新ファイルの提供を受けられなくなるので，新しい仕組みが必要になる。R さんは，更新ファイル提供サービスと同じ動作をするパッチ配信兼マルウェア対策管理サーバ（以下，配信サーバという）を用意することにした。

図 3，表 3 及び図 4 を見た A 氏は，幾つかのシナリオを仮定して図 3 の LAN 構成で想定されるマルウェア感染被害について表 4 のとおり評価した。表 5 に，各 OS を利用している機器を示す。

表4　マルウェア感染被害の評価（抜粋）

項番	仮定したシナリオ	想定される被害
1	・HTTP 通信を悪用して管理者権限を奪取できる脆弱性 v が発見されたが，パッチはリリースされていない。 ・事務 PC，研究開発 PC 及びファイル転送サーバには，脆弱性 v が存在している。 ・事務 PC が，脆弱性 v を利用して能動的に感染を広げるマルウェア α に感染した。	・事務 PC からファイル転送サーバが感染する。 ・脆弱性 v を利用して，ファイル転送サーバから①研究開発 PC が感染する可能性は低い。 ・配信サーバの設置位置によっては，配信サーバが感染する可能性がある。
2	・攻撃者が，N 社が製品 Z を使用していることを知っており，製品 Z のアクセス手順を組み込んだマルウェア β を作成し，電子メールを利用して N 社に送り込んだ。 ・事務 PC が，マルウェア β に感染した。 ・マルウェア β が，[e]，[f]，[g] の情報を窃取して，ファイル転送サーバにアクセスした。	・ファイル転送サーバに不正なファイルがアップロードされる。 ・その不正なファイルが原因となって②研究開発 PC が感染する可能性は低い。
3	・ファイル共有プロトコルを悪用して管理者権限を奪取できる脆弱性 w が，OS-P で発見される。 ・OS-Q には，脆弱性 w は存在しない。 ・事務 PC，研究開発 PC 又は配信サーバのいずれかが，脆弱性 w を利用して能動的に感染を広げるマルウェア γ に感染した。 ・更新ファイルの提供に使用するプロトコルは，ファイル共有プロトコルではない。	・配信サーバの設置位置によっては，脆弱性 w を利用して，事務 PC，研究開発 PC 及び配信サーバの間で感染が拡大する可能性がある。

表5　各 OS を利用している機器

OS の名称	その OS を利用している機器
OS-P	事務 PC，研究開発 PC，配信サーバ，内部 DNS サーバ
OS-Q	研究開発用ファイルサーバ，一般事務用ファイルサーバ，ファイル転送サーバ

この結果から，図 3 の LAN 分離案は研究開発 LAN 内の新薬ファイルの漏えい防止に有効だとの結論を得て，B 取締役は社内ネットワークの変更を進めることにした。

さらに，表 4 の項番 3 について，マルウェアの感染が広がることを防ぐために，R さんは配信サーバの設置位置を，表 6 を用いて検討した。検討の際に，FW1 と FW2 の設定は必要最小限の通信だけを許可するものとした。

表6　配信サーバの設置位置の検討内容

感染経路	図3中の（あ）に設置した場合	図3中の（い）に設置した場合
事務 PC から配信サーバへ	(省略)	結論：感染する可能性が低い。 理由：FW1 によって感染活動を遮断できるから
研究開発 PC から配信サーバへ	結論：感染する可能性が［ h ］。 理由：［ i ］	結論：感染する可能性が［ j ］。 理由：［ k ］
配信サーバから事務 PC へ	(省略)	(省略)
配信サーバから研究開発 PC へ	(省略)	(省略)

検討の結果，R さんは B 取締役に配信サーバの適切な設置位置を提案して，社内ネットワークを変更した。

〔不審な操作ログ〕

社内ネットワークの変更から半年ほどたったある日，ファイル転送サーバのログを調べていた R さんが，研究開発員の S さんの研究開発 PC がファイル転送サーバへ頻繁にアクセスしていたことを発見した。S さんの研究開発 PC を調査したところ，規程で利用を禁止しているリムーバブルメディアを利用した形跡があった。そのリムーバブルメディア経由で研究開発 PC がマルウェアに感染し，S さんが研究開発 PC を操作していない時に，マルウェアが研究開発 PC 内のファイルをファイル転送サーバにアップロードしていたことが分かった。ただし，ファイル転送サーバからダウンロードされてはいなかった。

このマルウェアの情報を調べたところ，次の機能をもっていることが分かった。

・図4の操作手順による，ファイル転送サーバへのファイルのアップロード

・図4の操作手順による，ファイル転送サーバからのファイルのダウンロード

今回，インターネットへのファイルの流出には至らなかったが，S さんの事務 PC もマルウェアに感染していた場合は直ちにインターネットへのファイルの流出に至るので，R さんはファイル転送サーバに何らかの対策が必要だと考えた。

Rさんが A 氏に，この対策について相談したところ，“製品 Z には，正当なファイル転送であることを確認するために，図 4 の手順 2 の後に [l] の手順を追加し，その手順の完了をもってダウンロードが可能となる拡張機能が用意されているので，それを利用してはどうか”との回答を得た。R さんは，この拡張機能は効果があると考え，B 取締役の承認の下，導入した。

その後，N 社では情報管理上の大きな事故もなく，順調に事業を拡大している。

設問 1　〔リスクアセスメント〕について，(1)，(2)に答えよ。

(1)　本文中の [a]，[b] に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　リスク回避　　イ　リスク対応　　ウ　リスク特定

エ　リスク評価　　オ　リスク保有　　カ　リスクモニタリング

(2)　本文中の [c]，[d] に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　リスクが顕在化したときの結果　　イ　リスク対応の実践の優先度

ウ　リスクの起こりやすさ　　エ　リスク保有の利点

設問 2　〔LAN 分離案の検討〕について，(1)～(3)に答えよ。

(1)　表 4 中の下線①で，A 氏が低いと判断した理由は何か。40 字以内で述べよ。

(2)　表 4 中の [e] ～ [g] に入れる適切な字句をそれぞれ 15 字以内で答えよ。また，これら全ての情報をまとめて窃取する方法を，30 字以内で具体的に述べよ。

(3)　表 4 中の下線②で，A 氏が低いと判断した理由は何か。50 字以内で述べよ。

設問 3　表 6 中の [h] ～ [k] に入れる適切な内容を，[h] 及び [j] については“低い”又は“高い”のいずれかで答え，[i] 及び [k] についてはそれぞれ 30 字以内で述べよ。

設問 4　本文中の [l] に入れる適切な手順を，15 字以内で答えよ。