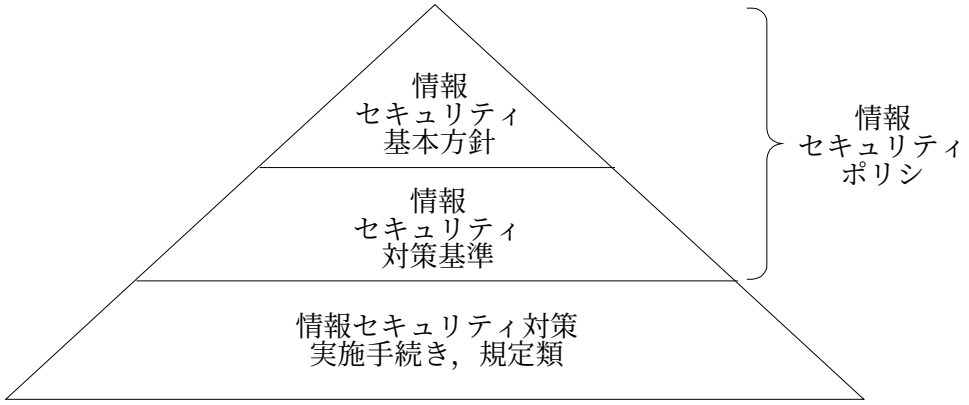
# 平成１３年度　秋期　情報セキュリティアドミニストレータ　午後Ｉ問題

**情報セキュリティポリシの位置づけ**



**問１**　不正侵入対策に関する次の記述を読んで，設問１～４に答えよ。

Ｘ社は，ソフトウェアの開発及び販売を行っている中堅のソフトウェア会社である。

Ｘ社には，ソフトウェアの開発を行う部署として開発部がある。開発部に所属する社員には，クライアントマシンとして最低一人 1 台のパソコンが与えられており，さらに，個々の開発課ごとに 1 台のサーバが設置されている。各パソコン及びサーバは，すべて LAN に接続されている。開発部の LAN は，他部署の LAN とともにファイアウォールを介してインターネットに接続されている。加えて，開発部の LAN 上にはリモートアクセスサーバ（以下，RAS という）が設置されており，開発部の社員が自宅や外出先から社内のサーバにアクセスするために利用されている。RAS には開発部のほぼ全社員がアカウントをもっている。RAS へのログインに際しては，アカウント名とパスワードによる認証が必要であるが，それ以外のアクセス制限は行われていない。

Ｘ社のネットワーク構成を図に示す。

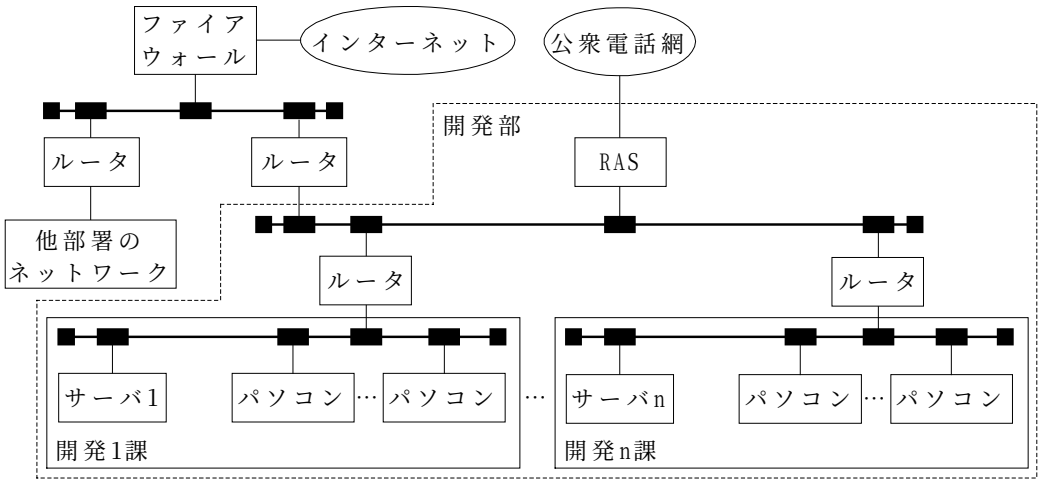



**図　Ｘ社のネットワーク構成**

Ｘ社には，ネットワークやサーバの情報セキュリティ管理を行う専門の部署はない。また，社内ネットワーク及びインターネットについての利用規程はあるものの，禁止事項を幾つか列挙しただけのものであり，全社的な情報セキュリティポリシは存在しない。結果として，ネットワークや各サーバの情報セキュリティ管理については，社員の知識や良識に強く依存している。

社員に与えられたパソコンは，その社員自身が管理を行うことになっており，各開発課のサーバについては，その開発課のメンバのうち 1，2 名が管理者として任命されている。また，ネットワーク機器や RAS といった開発部内の共有リソースについては，各機器についての知識の豊富な社員が開発部全体から選ばれて管理を任されている。RAS については，現在，開発 1 課のＹ係長が管理者になっている。

〔不正侵入の発生と検知〕

Ｖ君は，開発部の開発 1 課に所属するプログラマである。本来の業務であるプログラミングのほか，開発 1 課のサーバ 1 の管理も担当している。

Ｖ君はある日，サーバ 1 上で利用している開発ツールの不具合について調査するため，サーバ 1

上のログをチェックしていた。そのとき，E課長のアカウントによるサーバ 1 へのログインの試みが数回記録されているのに気が付いた。E課長はV君とは別の開発 2 課のメンバであり，サーバ 1 上にアカウントをもっていない。そのため，ログインの試みはすべて失敗していた。V君は，このアクセスを不審に思ったが，操作ミスのたぐいであって大した問題ではないと判断し，サーバ 1 に実害がなかったこともあって，上司への報告はしなかった。

それから 10 日ほど経ったころ，開発 2 課のサーバ管理者であるK主任は，開発 2 課のサーバ 2 に，病欠中のE課長がログインしているのを発見した。不審に思ったK主任が直ちにE課長の自宅に電話で確認したところ，E課長本人はログインしていないとのことであった。そのため，だれかがE課長のアカウントを不正に利用していることが明らかになった。不正利用されているE課長のアカウントが RAS からログインされていることを確認したK主任は，Y係長に連絡した。

〔開発部の対処作業〕

Y係長は，侵入者が公衆電話網からアクセスしてきていることを確認の上，RAS を［　a　］から切り離した。続いて，各開発課のサーバ管理者に不審なアクセスの記録がないかどうか調査するよう連絡するとともに，開発部の全社員に対して，早急に各自のもつすべてのパスワードを変更するように通知した。

一方，K主任は，サーバ 2 を［　b　］から切り離した上で，①現状のディスクの内容をテープに保存した。その後，サーバ 2 上に保存されている開発中のプログラムや各種ドキュメントに対する改ざんや破壊の有無を調査した。その結果，開発中の複数のプログラムにでたらめな文字列が書き込まれていたことが判明した。K主任は，改ざんされたプログラムをバックアップテープから［　c　］して，対処作業を終了した。

ほかの開発課のサーバに関しては，V君が発見したのと同様にE課長のアカウントによるログインの試みが記録されていた。しかし，いずれのサーバにもE課長のアカウントが存在しないので，それらの試みはすべて失敗していた。よって，実際に不正侵入されたのはサーバ 2 だけであろうと考えられた。

〔原因究明〕

Y係長が RAS のアクセスログを調べたところ，10 日ほど前にE課長のアカウントを始めとして，複数のアカウントに対するログインの失敗がまとまって記録されていることが判明した。E課長以外のアカウントに関しては，いずれも 10 回ほどの失敗が記録されているだけなのに対し，E課長のアカウントについては，3 回の失敗の後，ログインに成功していた。Y係長は，E課長が容易に推測可能なパスワードを利用していたので，アカウントを不正利用されたのではないかと考えた。

その後の調査で，ログインの失敗が記録されていた日とV君が不審なアクセスを発見した日が同じであったこと，及びE課長のパスワードがE課長のアカウント名を逆順にしただけのものであったことが判明した。

〔トラブルの再発〕

K主任が対応作業を終了してから数日後，Y係長あてに，“ あなたのサイトのものと思われる xxx.xxx.xxx.xxx という IP アドレスをもつマシンからポートスキャンをされている。早急な対処を願う ” という内容の電子メール（以下，メールという）が届いた。メールの送信者によれば，

WHOIS データベースでX社のドメイン名を調べ，技術担当者として登録されているY係長のメールアドレスにメールを送信したとのことである。この抗議メール自体がいたずら又は勘違いによるものである可能性も考えられたが，Y係長は，念のため，調査を開始することにした。

メール本文に記述された IP アドレスは，X社のファイアウォールのものであった。X社は，ファイアウォールで［　d　］を実施しているので，社内 LAN 上にあるすべてのマシンが社外へのアクセスに際してこの IP アドレスを使用することになる。調査の結果，サーバ 2 上の NTP サーバが，別のプログラムと入れ替えられており，これが社外のサイトに対してポートスキャンを行っていることが判明した。E課長のアカウントを不正利用した侵入者が，管理者権限を不正に取得した上で“トロイの木馬”を残していったものと考えられた。K主任は，②正常な NTP サーバを再インストールすることによって対処した。

Y係長は，抗議メールの送信元へ，原因が“トロイの木馬”であり，それを除去することによって対処したことを付記した謝罪のメールを返信した。

〔事故の報告〕

今回の事故の報告を上司のZ課長から求められたY係長は，事故の経緯と対処作業について報告書にまとめるとともに，不正侵入の早期発見のための技術的対策として監視ツールの導入提案を報告書に付記した。Z課長は，たとえ監視ツールを導入したとしても，③管理者が，今回の事故におけるV君のような対応を取った場合には，十分な効果が望めないと考えた。そこで，根本的な対策のためには全社的な情報セキュリティポリシの策定と社内体制の整備が急務であるとの意見書を作成し，Y係長の報告書とともに開発部長へ提出した。

**設問１**　本文中の［　a　］～［　d　］に入れる適切な字句を，それぞれ 8 字以内で答えよ。

**設問２**　Y係長が，既にパスワードが漏えいしているE課長だけでなく，全社員にパスワードの変更依頼を通知したのはなぜか。その理由を 30 字以内で述べよ。

**設問３**　サーバ 2 への対処に関する次の問いに答えよ。

(1) K主任が下線①の作業を行った理由を 20 字以内で述べよ。

(2) 下線②の作業だけでは，“トロイの木馬”への対処として不十分である。その理由と，本来とるべき対処作業をそれぞれ 30 字以内で述べよ。

**設問４**　Z課長が下線③のように考えた理由を 30 字以内で述べよ。

**問２**　営業支援システムの導入に伴うリスク分析に関する次の記述を読んで，設問１～４に答えよ。

M社は，都市部に 10 店舗をもつインテリア用品の販売会社である。2 年前に始めた自社企画品の販売が成功し，売上を大きく伸ばしている。社長は，自社企画品の売上を更に拡大するとともに，今後 3 年間で店舗数を 30 に増やす計画である。

昨年，M社は，全店舗に POS システムを新規導入し，本社営業部員及び商品企画部員に一人 1 台のノートパソコンを配布した。一方，全社の売上管理や仕入管理などの業務システムについては，Ｐ社が提供するアウトソーシングサービスの利用に切り替えた。また，インターネット接続についても，Ｐ社のレンタルサーバサービスを利用し，社外との電子メールの送受信を可能にした。これまで業務システムが稼働していたサーバは，本社営業部のファイルサーバとして使用することにした。

その後，企業向け販売担当の本社営業部から，“ノートパソコンを使用している者のほとんどは，社外に持ち出して使用している。顧客対応の迅速化を図るために，ファイルサーバにある営業情報を社外からもアクセスできるようにしてほしい”という要望が出された。そこで，M社は，営業支援システムを構築することにした。

営業支援システムの要件が具体的になった段階で，社長は，経営企画室長（以下，室長という）に対し，営業支援システム導入に伴うリスク分析を実施するように指示した。

〔M社の情報システム〕

M社の業務システムの概要と営業支援システムの要件は，次のとおりである。

(1) 業務システムの概要

① 本社及び各店舗の機器は，業務システムと VPN で接続されている。インターネット経由で業務システムにアクセスすることはできない。

② 店舗の POS 端末で入力した売上データや仕入データは，ストアコントローラを経由し，一定時間ごとに業務システムに送信されている。

③ 本社営業部の売上データは，リアルタイムで業務システムに登録されている。

(2) 営業支援システムの要件

① 過去及び受注前の見積情報や提案情報をデータベースに登録し，検索を行う。

② 売上データを業務システムから受け取り，データベースを構築する。

③ 本社にリモートアクセスサーバ（以下，RAS という）を設置し，社外から各データベースへのアクセスを可能にする。RAS へのアクセスは，ID とパスワードによる認証によって制御する。

営業支援システム稼働後のM社情報システムの構成は，図のとおりである。

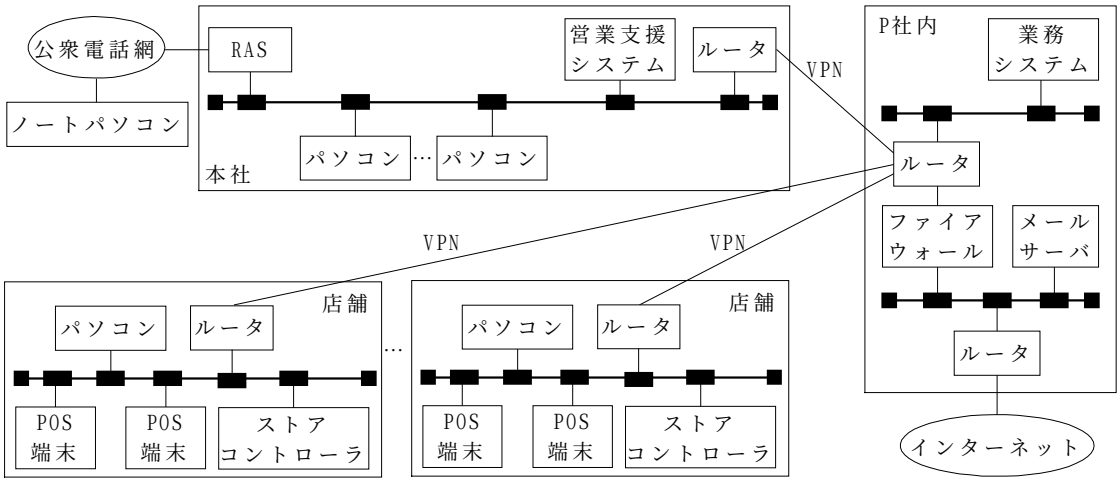



**図 M社情報システムの構成**

〔営業支援システム導入に伴う情報セキュリティの調査〕

室長は，情報システム部出身のＬ君に，営業支援システム導入に伴うリスク分析を実施するように指示した。また，3 年後の店舗数を前提に影響度を定量化し，報告するように加えて指示した。

室長から指示を受けたＬ君は，ぜい弱性を洗い出すために，まず，情報セキュリティの調査方法を検討した。この結果，Ｌ君は，次の方法で調査することにした。

(1) 社内の情報セキュリティ調査

① ノートパソコンを使用している部門については，チェックリストを作成し，全員に記入を依頼することにした。

② 上記の①以外の部門については，機器の使用状況や設置場所など [ a ] 調査を実施することにした。

③ 情報システムについては，システム化要求仕様書の [ b ] を行うとともに，システムの要件を取りまとめた担当者に [ c ] を実施することにした。

(2) 社外の情報セキュリティ調査

自社企画品の生産を委託している複数の工場については，商品企画部と電子メールを利用してサンプル商品の生産依頼や生産進捗の確認を行っているので，調査を実施する。しかし，これらの工場については，情報化のレベルが不明なので，各工場の情報システム担当者に対して [ c ] を行うとともに，機器の使用状況や設置場所などについて [ a ] 調査を実施することにした。

なお，各工場に，調査への協力を依頼する文書を社長名で事前に送付した。

〔リスク分析の定量化〕

調査を終了したＬ君は，調査結果を基にしてぜい弱性の洗い出しを行うとともに，影響度を考慮してリスクの定量化を行った。Ｌ君は，リスク分析の結果を表にまとめ，予想される 1 年当たりの損失額を [ d ] 万円，費用を [ e ] 万円と算出した。

**表　L君が作成したリスク分析のリスト**

| 情報資源 ＼ 脅威 | 営業支援システム及びパソコン | | | 業務システム |
|---|---|---|---|---|
| | 受注前情報 | 販売実績情報 | 商品企画情報 | 売上情報，仕入情報など |
| 漏えい | 受注前情報が漏れ，失注<br>・ノートパソコンの紛失，盗難<br>・RAS から営業支援システムへの侵入<br>〔損失額〕<br>・過去の営業案件提案額 平均 1,000 万円／回<br>・想定発生件数 年 3 回 | 販売実績情報が外部に漏れ，得意先からのクレームに対する対応<br>・店舗設置パソコンからの漏えい<br>〔費用〕<br>・対応費 5 万円／回<br>・想定発生件数 年 1 店舗 1 回×10 店舗 | 商品企画情報が外部に漏れ，対抗品の発売による売上減<br>・生産委託工場のパソコンからの漏えい<br>〔損失額〕<br>・過去の企画品売上額 平均 1 億円／回<br>・売上減率 20%<br>・想定発生件数 年 2 回 | なし |
| 改ざん | 受注前情報が改ざんされた場合の復旧処理<br>・RAS から営業支援システムへの侵入<br>〔費用〕<br>・復旧作業費 20 万円／回<br>・想定発生件数 年 1 回 | なし | なし | なし |
| 破壊 | 受注前情報が破壊された場合の復旧処理<br>・RAS から営業支援システムへの侵入<br>〔費用〕<br>・復旧作業費 10 万円／回<br>・想定発生件数 年 1 回 | なし | なし | なし |

損失額は本来獲得できるはずであったが獲得できなかった売上金額であり，費用は被害を受ける前の状態に戻すために発生する金額である。

〔リスク分析の結果報告〕

L君は，リスク分析の結果を室長に報告した。室長は，このリスク分析のリストを見て，“定量化の前提が指示した内容と異なる”と指摘した。 L君は，室長の指摘を受けて，リスク分析の定量化をやり直すことにした。

**設問１**　本文中の［ a ］～［ c ］に入れる適切な字句を，それぞれ 10 字以内で答えよ。また，［ d ］，［ e ］に入れる適切な数値を答えよ。

**設問２**　ノートパソコンを使用している部門の調査方法について，チェックリストによる調査を選択したのはなぜか。その理由を二つ挙げ，それぞれ 20 字以内で述べよ。

**設問３**　〔リスク分析の結果報告〕に関する次の問いに答えよ。

(1) 定量化の前提が室長の指示と異なる事項を 30 字以内で述べよ。
(2) 表中に列挙された受注前情報の損失額や費用には見落としがある。その見落としを二つ挙げ，それぞれ 40 字以内で述べよ。

**設問４**　室長は，営業支援システムの導入計画を聞いたころから，業務システムに新たなリスクが発生するのではないかと考えていた。それは何か，35 字以内で述べよ。

**問３**　電子商取引の情報セキュリティ対策に関する次の記述を読んで，設問１～４に答えよ。

Ａ社は，中堅規模の製造業者である。自社商品の生産に必要な主要原料を，限られた取引相手先から年間契約に基づき購入している。購買調達部門の要望によって，この業務は，“発注システム”としてシステム化されている。システムを通して，Ａ社から取引相手先への見積依頼，取引相手先から見積りや納期納品条件の提示，Ａ社から正式な発注書，取引先から発注請け書の送受信が行われている。その後，取引先から実際の商品及び請求書が送られてくる。この“発注システム”は，Ａ社の情報システムの一部としてＡ社に設置してあり，取引先各社は，各社に設置した“発注システム”専用端末と公衆電話網で接続している。

なお，Ａ社及び取引先各社は，この“発注システム”への接続のために発信者番号の確認機能が付いたモデムを設置し，特定の相手先以外からの着信を拒否している。

この“発注システム”は，製造部門からの要求があり，受発注に伴う製品情報や製品設計図の送受信を行うことができるよう機能を追加した。しかし，Ａ社の製品情報が漏れたり，取引先と共同で作成し修正した製品設計図が，取引先経由で他社に流用されたりする事態が発生した。Ａ社は，取引に先立ち，製品情報や製品設計図に関する［　a　］条項及び設計図面の［　b　］権を，あらかじめ契約書として取り決めておく必要に迫られ，対応した。

その後，“発注システム”が軌道に乗ると，購買調達部門から事務機器や梱包材，用紙類などの間接材取引もシステム化したいという追加要望が挙がった。Ａ社の情報システム部のＢ主任は，この要望を実現する“新調達システム”の基本検討を担当することになった。

検討が進むと，該当する間接材を電子的に調達できる仕組み（以下，マーケットプレイスという）による購買調達サービスが他社から開始されることが判明した。Ｂ主任は，Ａ社が単独で，“発注システム”と同様のシステムを個別に取引先相手ごとに構築するより，このマーケットプレイスに参加した方が容易にシステム化が図れると考えた。さらに，有利な条件で調達できる可能性があるのではないかと考え，このサービスへの参加を前提に“新調達システム”の検討を進めることにした。

〔Ｂ主任と購買調達部門のＧ課長との会話〕

Ｂ主任：いま，“マーケットプレイス”という購買調達サービスの提供が始まろうとしていますが，ご存知ですか。ご要望の“新調達システム”にこのサービスを利用すると，システム化を取引先相手ごとに調整する手間が省けますし，より有利な条件で調達できる可能性があるので，この際是非検討したいのですが。

Ｇ課長：話には聞いたことがある。インターネット上に構築された仮想市場のことだろう。でも，見ず知らずの会社を相手にコンピュータ上で取引して問題ないのだろうか。このごろインターネット上でのオークションや取引で，トラブルも多いと聞いているが。

Ｂ主任：確かにインターネットのもつ匿名性を悪用されたり，ID を盗用されたりするために発生する［　c　］による詐取のリスクはあります。そのため，マーケットプレイスでは参加する企業に対し，暗号技術を利用した［　d　］の仕組みを使って，相手企業の確認を行うそうです。

G課長：どの程度のチェックができるのかね。

B主任：幾つかレベルがあるようです。発行団体の［ d ］が付いた［ e ］書を取得するには，その発行団体に会社登記簿謄本などの提出が義務付けられています。また，仮に参加企業の中に異変があった場合，参加企業全体に速やかに報告されるそうです。

G課長：［ d ］による確認が行われるなら，間接材の“新調達システム”としても悪くないね。

この後，A社で検討が行われ“新調達システム”においては，このマーケットプレイスのサービスに参加することになった。

“新調達システム”が稼働してしばらく過ぎたころ，それまで順調に取引していた相手先からA社の発注した品物が納期を過ぎても入荷してこないというトラブルが発生した。調べてみると，発注した相手企業の［ e ］書が一部悪用され，［ c ］によって取引が混乱したので，その企業の［ e ］書の利用が既に停止されていたことが分かった。

今回のトラブルを受けて，A社では様々な検討を進めた。その一つとして，取引に先立ち相手企業に対する信用調査を強化して取引先を厳選する対策を実施した。

“新調達システム”稼動前に制定されていたA社の情報セキュリティ対策基準の抜粋を次に示す。

情報セキュリティ対策基準（抜粋）

1．目的　（省略）
2．対象者
　本情報セキュリティ対策基準（以下，本基準という）は，当社経営者及びすべての従業員に適用し，経営者及びすべての従業員は，これを遵守しなければならない。本基準を遵守しなかった場合，就業規則に基づき罰則を適用する。
3．適用範囲
　本基準は，当社が業務で使用する当社管理下の情報及び情報システムを含む情報資産すべてを対象とする。
4．情報セキュリティ文書体系　（省略）
5．情報セキュリティ組織
　①　情報セキュリティ主管
　　経営会議において担当役員を任命し，情報セキュリティ室を設置する。
　　情報セキュリティ室は，情報セキュリティに関する諸規定の策定，改定，遵守状況の監視，チェック，トラブルの把握及び緊急事態への対処の指揮指導を行う。
　②　情報セキュリティ対策組織
　　情報セキュリティに関するトラブルが発生した場合，情報セキュリティ室は，必要に応じて業務担当部署から要員を選出し，対策プロジェクトを設置する。
6．情報セキュリティの範囲と責任
　①　対象とする情報の範囲と分類
　　当社業務で利用するすべての情報を対象とする。情報を入れる媒体としては，紙，伝票類などの紙媒体及びWebページ，電子メールなどの電子媒体を問わない。
　　また，極秘，関係者外秘，部外秘，社外秘，公開の5種類に分類し，分類に応じた取扱方法をとる。

② 対象情報システム範囲
当社の業務に供し当社管理下にあるすべての情報システムを対象とする。その構成要素としては，システム構成機器，ソフトウェア，ネットワーク及びネットワーク機器と稼働に必要な電源，空調，施設設備を含めた範囲とする。
③ 情報資産の管理責任
すべての情報資産に対して管理部署を決定し，管理部署は，社員の中から管理責任者を任命する。管理責任者は，情報資産へのアクセス，取扱方法を定め，効果的に守られていることを恒常的に監視監督する。ただし，この監視監督業務は，外部委託を認める。また，情報セキュリティ室はこれらのアクセス，取扱方法及び監視監督の有効性について，定期的又は必要に応じて検証を行う。検証に関しては，第三者機関への委託を認める。
７．ネットワーク接続及び運用
① ネットワーク接続
当社情報システムに対する情報機器の接続は，その管理のため，会社施設内での接続に限定する。会社施設外からのアクセスは，緊急対応時，定期的診断及び保守作業に必要な場合に限り一時的に認める。
② ネットワークの運用
当社情報ネットワークに関しては，情報システム部が管理責任を負う。ただし，運用に関しては外部委託を認める。
８．アクセス制御
① アクセス制御方針
情報及び情報システムに関するアクセスの許認可及び管理は，“６．情報セキュリティの範囲と責任”の“③情報資産の管理責任”に従う。管理者は，情報システム運用者に対し，アクセスに対する措置の申請・解除などの手続をとる。情報システムの運用に関しては，外部委託を認める。
② ユーザアクセス管理
ユーザのアクセスに関して“6．情報セキュリティの範囲と責任”の“③情報資産の管理責任”に従い，状況を監視監督する。
（以下省略）

**設問１**　[ a ] ～ [ e ] に入れる適切な字句を，それぞれ 8 字以内で答えよ。

**設問２**　情報セキュリティ対策基準に関する次の問いに答えよ。

(1) 現在の基準では，“発注システム”の考慮がなされていなかった。“発注システム”の特徴から，基準で最も不適合を起こしている箇所の項目番号を挙げ，その理由を 20 字以内で述べよ。

(2) “新調達システム”を導入する上で，上記の(1)以外でＡ社の基準に変更が必要な箇所の項目番号を挙げ，変更に盛り込むべき内容を 35 字以内で述べよ。

**設問３**　“新調達システム”で発生した本文中の下線のトラブルの対策として，ITU-T X.509 に定められた，あるデータを確認する方法が考えられる。対策として，Ａ社が確認すべきものは何か。6 字以内で答えよ。また，このトラブルを防止するために，その運用上注意すべきことは何か。15 字以内で述べよ。

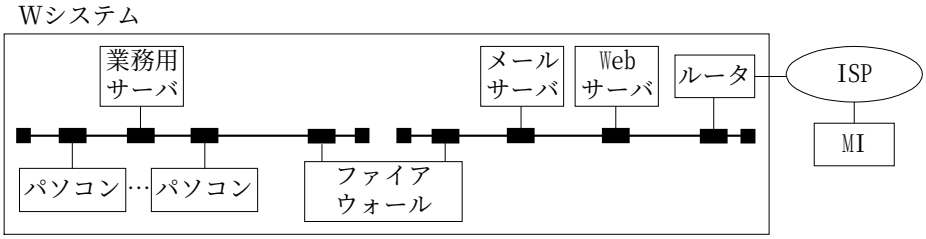
**設問４**　設問３の対策だけでは，納期を過ぎても入荷されないというトラブルを完全に防ぐことはできない。それはなぜか。40 字以内で具体的に述べよ。ただし，情報システムでは正常に発注処理が行われたものとし，事故や犯罪によって引き起こされたトラブルは対象外とする。

**問４**　電子メールによるウイルス感染と対策に関する次の記述を読んで，設問１～４に答えよ。

N社は，文房具の中堅小売業者である。東京に店舗があり，関東一円を商圏にしている。N社では，Web を利用して企業に文房具を販売するシステム（以下，Wシステムという）を導入した。Wシステムは，Web サーバ，電子メール（以下，メールという）サーバ，注文請求処理を行う業務用サーバなどから構成され，インターネットサービスプロバイダ（以下，ISP という）に接続されている。

文房具を購入する企業は，ブラウザから注文を入力する。このデータは，SSL を用いてWシステムに送られる。Wシステムは，データを受信すると，企業に注文受付メールを送る。企業は，注文受付メールの内容を確認して，注文確認メールを出す。N社では，注文確認メールを受け取ると，担当者が受注処理を行い，商品を発送する。また，N社は，このWシステムの Web サーバ及びメールサーバを関連会社に利用させている。

なお，N社では，図に示すように，過去の取引の関係でWシステム以外に ISP のメールサービスも利用している。



MI：ISPの提供するメールサーバ

**図 システムの構成**

〔ウイルス被害の発生〕

Wシステムによる販売は，顧客企業に大変好評で，売上は予想を大きく上回った。しかし，N社では，請求処理が追い付かず，大量のバックログを抱えて決算を迎えた。5 月の第 1 日曜日に事件が起きた。N社のＴ君が，休日出勤の朝，注文確認のメールボックスを開いた。そこには，いつも注文をくれるＣ社のＵ氏からの注文確認メールが多数あった。Ｃ社は在庫節減のため文房具の注文単位が小さく，N社は頻繁に注文を受けている。Ｔ君がこのメールを開いたところ，メールの本文は，“I LOVE YOU ”で冗談のような内容であった。Ｔ君は，Ｕ氏独特の冗談と考えた。同時にU氏から到着していたほかのメールも同様であった。このメールには，実行形式のファイルが添付されていた。Ｔ君は不審に思ったが，この添付ファイルを実行した。画面には何も変化がなかったので，注文確認処理を続けていたところ，メールサーバの応答が悪くなった。1 時間ほどして，N社の情報システム部のＳ部長が飛び込んできた。

Ｓ部長：Ｄ社から，ウイルスの付いたメールを受けたと言ってきた。何をしたのだ。
Ｔ君：はい。今朝からいつものように，注文確認処理と受注処理を行っているところです。Ｄ社からの発注はないので，メールは送っていません。
Ｓ部長：Ｄ社からは，10 分ほど前に，ウイルスの付いた冗談めいたメールが送られてきたと言って

きている。何かおかしいのではないか。

T君：そう言えば，U氏からよく似たメールがありました。関連があるのかな。

S部長：メールプログラムの送信記録は，今，どうなっている。

T君：大量のメールの送信記録が残っています。こんなことは初めてです。

〔ウイルス対策〕

S部長は，ネットワークと情報セキュリティを担当しているH主任を呼び出し，メールサーバを停止させた。H主任は，これがウイルス感染によるものと判断し，部下のJ君とウイルス検査ソフトを用いて全社のパソコンに対策を施した。休日なので，出社している社員は少なかった。ただ，経理部は，決算処理プログラムを実行中であり，ウイルス対策を実施できなかった。そこでH主任は，ウイルス感染を伝え，ウイルス検査ソフトによる対策の実施を口頭で依頼した。その後，Wシステムのメールサーバを LAN から切り離して立ち上げ，スプール内のウイルスの付いたメールを削除した。最後に，H主任らは，ほかのサーバが感染していないことを確認してWシステムを再開し，S部長に報告した。

H主任：これは Love letter ワームと呼ばれるウイルスによるものです。U氏からのメールで感染したと思われます。ところで，D社以外に連絡はないのですか。

S部長：あとは，F 社から連絡があっただけだ。ウイルスというとフロッピーディスクの［ a ］に感染して，伝染していくもののことか。

H主任：それは，昔のウイルスの話です。最近のウイルスには，ワープロの文書を制御する言語を介して伝染するものや，OS に常駐するプログラムを置き換えて，メールのクライアントプログラムを外部から制御するものなどがあります。Love letter ワームなどでは，［ b ］あてにウイルスの付いたメールを送るので，被害が急速に広がります。大切なのは，ウイルスの予防策です。ところでJ君，ウイルス検査ソフトの［ c ］の更新はどうしている。

J君：月に 1 回は行っています。ほかにはどんな予防策があるのですか。

H主任：［ c ］の更新は週に 1 回は行う必要があります。新しいファイルは，常に検査してから利用すること。さらに，ウイルスによる被害を最小限にするために，日頃から定期的に重要なファイルの［ d ］を採取しておくこと。また，万が一感染したときは，パソコンを正常な状態に戻せるように［ e ］を用意しておくこと。これらの予防策は，被害を少なくするために必須です。

J君：パソコンが多いので管理が大変です。ほかに方法はありませんか。

H主任：メール用のウイルス検査サーバを設置してはどうだろうか。

S部長：ISP のメールサーバの利用も制限する必要があるだろう。

H主任：はい。LAN 内部から ISP のメールサーバに POP 接続する利用を制限すべきですね。また，今回のようにWシステム利用会社にも迷惑を与えてしまうので，メールサーバをN社内利用向けとWシステム利用会社向けの二つに分けるべきではないでしょうか。そうすれば，N社内利用向けのメールサーバをより安全な内部に設置できます。

S部長：ウイルス検査サーバを設置し，メールサーバを分離する案を作成してもらいたい。

〔ウイルス被害の再発とN社の営業部のR部長からのクレーム〕

ところが，1 時間後にウイルスの付いたメールが社内を巡った。今回も，サーバを停止して対策をとった。

S部長：H主任，対策をとったのではなかったのか。なぜ，再発したのか。
H主任：すみません。［　f　］。
S部長：そうか。困ったな。私からもウイルス対策を依頼するようにしよう。

N社の営業部のR部長から電話が入った。

R部長：S部長，対策が遅い。先ごろ社長をヘッドにしで情報セキュリティポリシを作成したが，実行しないと意味がないな。ところで，社長には連絡したのか。
S部長：社長は，家族旅行中なので連絡していません。情報システム部だけで対応しました。また，情報セキュリティポリシのウイルス対策は予防対策についてしか述べておらず，今回のような感染時の復旧措置や事後対策はありません。
R部長：ウイルス対策には，情報システム部だけではなく，組織的に取り組まないとだめなのではないのか。

**設問１**　本文中の［　a　］～［　f　］に入れる適切な字句を答えよ。なお，［　b　］については，ウイルス伝染の仕組みを表すように，20 字以内で述べよ。また，［　f　］については，再発理由を 25 字以内で述べよ。

**設問２**　ウイルス対策に関する次の問いに答えよ。

(1) H主任がWシステムのウイルス対策を行う際，メールサーバを LAN から切り離した理由を 35 字以内で述べよ。

(2) ウイルス検査サーバの設置だけでは，ウイルス対策が十分ではない。個々のパソコンにウイルス検査が欠かせない理由を 25 字以内で述べよ。

**設問３**　メール用ウイルス検査サーバとメールサーバの設置に関する次の問いに答えよ。

(1) ウイルス検査サーバ（V），N社内利用向けメールサーバ（Ma）及びWシステム利用会社向けメールサーバ（Mb）をどの位置に設置すればよいか。解答欄の図を完成させよ。サーバ名には，略号（V，Ma，Mb）を用いること。

(2) ISP のメールサーバの利用を許可する場合の条件を 20 字以内で述べよ。

**設問４**　N社には，情報セキュリティポリシ（基本方針と対策基準）と情報セキュリティ体制に問題点がある。これに関する次の問いに答えよ。

(1) ウイルス感染を検出したときにとるべき復旧措置について，情報セキュリティ対策基準に追加すべきものは何か。25 字以内で具体的に述べよ。

(2) R部長が言うウイルス対策への組織的な取組とは何か。35 字以内で具体的に述べよ。