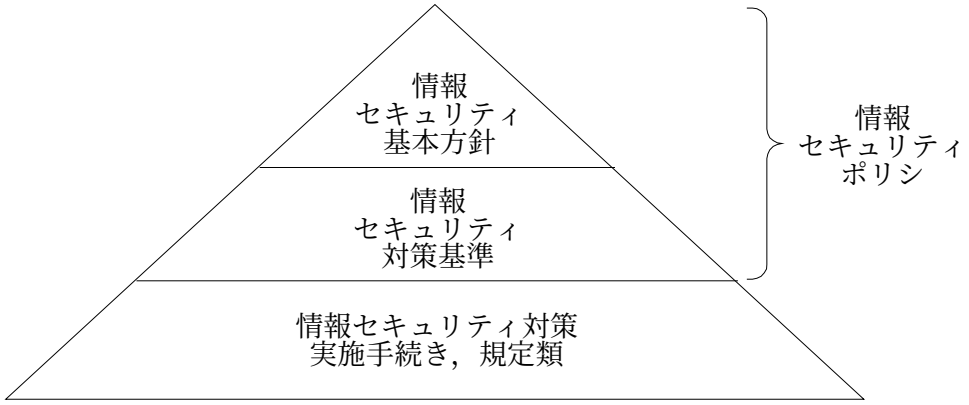
平成１４年度　秋期　情報セキュリティアドミニストレータ　午後Ⅰ問題

情報セキュリティポリシの位置づけ



問１　アウトソーシングにおける情報セキュリテイに関する次の記述を読んで，設問 1～4 に答えよ。

A社は，全国に営業拠点をもつ従業員数約 5,000 名の企業で，自社ブランドの住宅設備製品を販売しており，顧客情報管理，販売情報管理，修理情報管理など 40 を超える業務システムを運用している。住宅設備製品は，安全管理上の理由から，販売した製品情報と顧客情報の関連付けが必要で，顧客情報管理システムがほとんどの業務システムと連携している。これらの業務システムの運用は，10 年前からA社が 100%出資する情報システム子会社の K 社によって行われていた。

K 社の社員約 200 名の半数以上が，A社からの出向者であった。このため，A社と K 社の間では，よい意味でも悪い意味でも“身内感覚”で仕事を進めてきており，システムの運用に関して，サービス内容とその品質が規定されていなかった。情報セキュリティに関しては，A社の情報セキュリティポリシの中で顧客情報を適切に取り扱うよう明確に定められ，A社及び K 社の全社員に対して周知徹底されていたので，A社と K 社内には顧客情報保護の意識が浸透していた。

2 年前，A社は，情報セキュリティを重視した企業であることを社会的にアピールするために，［ a ］を取得する方針を打ち出した。これは，“個人情報保護に関するコンプライアンス・プログラムの要求事項”（JIS Q 15001）に適合し，電子計算機処理にかかわる個人情報を保護するための体制を整備している事業者に対して認定される制度である。K 社との委託契約には，“個人情報に関する［ b ］義務契約”，“再委託に関する事項”，“事故時の責任分担”及び“契約［ c ］時の個人情報の返却及び消去”の四つの内容が盛り込まれていた。

〔資本参加型アウトソーシングの契約〕

昨年，A社は，自社のコアコンピタンスを強化するため，情報サービス事業者の E 社に対して，K 社への資本参加を要請し，10 年間のアウトソーシング契約を締結することで合意した。E 社の K 社への出資比率は 51%であった。A社と K 社の契約金額については，K 社から提出された 10 年間の見積額を基に，前年度実績を踏まえて，毎年見直すという取決めであった（図１）。

K 社は E 社の子会社になったので，E 社から多くの社員が出向してきた。K 社の情報セキュリティポリシは，E 社の情報セキュリティポリシに基づいて，新たに制定され，K 社内に周知徹底された。A社でも組織の見直しが行われ，100 名在籍していた情報システム部員の半数以上は，K 社に転籍した。A社の情報システム関連業務は，システム企画，予算管理及び K 社への委託業務管理だけで，ほかの業務に関しては K 社にアウトソーシングし，業務システムの実務経験がない経営企画部システム管理課の 10 名が担当することになった。

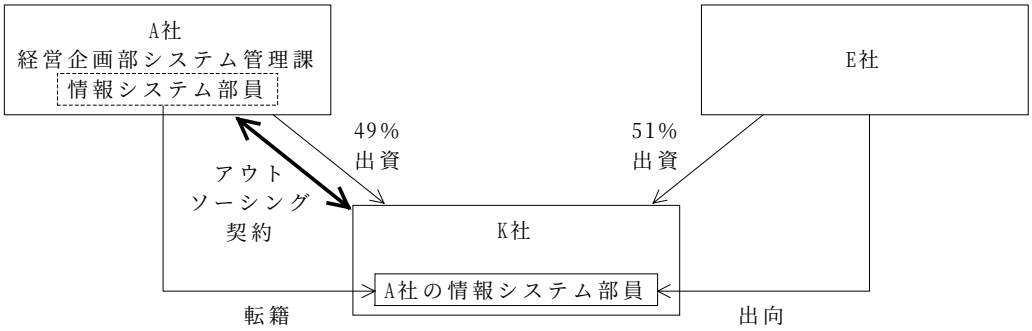


図１　Ｅ社資本参加型アウトソーシング契約後のＫ社の位置付け

Ａ社のシステム管理課の X 課長は，この体制で情報セキュリティを確保することは難しいのではないかと考えていた。ソフトウェアの情報セキュリティ上の不具合に関する情報は，インターネットから簡単に入手できるものの，その量は膨大であり，対策を講じなかった場合，Ａ社にどのような影響があるのかについて，システム管理課では見極めることができなかった。また，K 社との関係及び K 社内の体制が変更されたことから，顧客情報を従来どおり守れるかどうかといった不安があった。

〔サービスレベルの定義〕

Ａ社と K 社は，アウトソーシング契約締結時にシステムの運用委託に関するサービスレベルの目標値と提供されるサービス内容について合意した。昨年度のウイルス対策に関するサービスレベルの目標値は図２のとおりであり，サービス内容は表のとおりである。

年間延べウイルス感染率　　：サーバ台数とクライアント台数のそれぞれ 5%以内 ウイルス被害からの復旧期間：3 営業日以内

図２　ウイルス対策に関するサービスレベルの目標値

表　ウイルス対策に関するサービス内容

・最新のウイルス定義ファイルの更新サービス（以下，更新サービスという） 社内ネットワークに接続されたサーバ及びクライアントにウイルス対策ソフトを導入し，ウイルス定義ファイルを最新のものに更新するサービス（ライセンス費用も含む） 年間サービス回数：24 回 作業工数／回：1 人日／10 サーバ，1 人日／300 クライアント
・情報セキュリティ修正プログラムの適用サービス（以下，パッチ適用サービスという） ソフトウェアの情報セキュリティ上の不具合を修正するプログラムを適用するサービス 年間サービス回数：全サーバ及び全クライアント 1 回 作業工数／回：1 人日／サーバ，1 人日／30 クライアント
・ウイルス感染時の事故対応サービス（以下，事故対応サービスという） ウイルス感染による被害の拡大防止，応急及び復旧措置を行うサービス 年間サービス回数：5 回 作業工数／回：100 人日

（契約条件）工数単価：40,000 円／人日
規模：サーバ台数 200 台，クライアント台数 6,000 台

K 社の事故対応サービスにおいて，サービス利用回数の実績が年間 4 回以下であっても，契約金額は同じである。また，ウイルス被害からの復旧期間の目標値は，営業日単位で設定され，その目標値を短くすると緊急に人員を手配する必要がある。そのため，事故対応サービスの契約金額は，復旧期間を 3 営業日以内とする場合と比較して，2 営業日以内の場合で 1.25 倍，1 営業日以内の場合で 3 倍になる。

〔事故の発生と対応〕

インターネット上のホームページを閲覧するだけで感染するウイルスがA社内に侵入し，顧客情報管理システムが停止するという事態に至った。最新の情報セキュリティ修正プログラムを適用していなかったサーバに感染し，そこから社内にまんえんした（感染サーバ 3 台，感染クライアント 250 台）。停止時間は，金曜日の営業開始直後から休日 2 日間を挟んで火曜日の営業終了直前までに及んだ。その間，手作業で対応せざるを得ない業務が発生し，対応費用として 1 営業日当たり 200 万円を要した。

A社内では，K 社の今回の対応に不満を漏らす声が多く出た。X 課長は，K 社の担当者である D 氏に今回の事故の説明を求めた。D 氏は，年 1 回のパッチ適用サービスを実施していたこと，及びウイルス感染による被害時の復旧目標値である 3 営業日以内で復旧したことから，K 社側に落ち度がない旨を主張した。さらに，情報セキュリティ修正プログラムは昨今数多く発表されており，それらをすべて適用すると，業務システムの安定稼働を維持するために，ばく大な作業工数を要すると発言した。X 課長は，D 氏の説明に納得し，パッチ適用サービスの回数が極力少なくて済むための新サービスの提案を依頼した。

〔サービスレベルの見直し〕

X 課長は，今年度のウイルス対策に関するサービスレベルの目標値を昨年度と同じにすべきであると考えた。K 社は，提案中の新サービスを追加すれば，ウイルスの脅威が増大している状況下であっても，昨年度のサービス内容の工数を変更しないで済むと説明した。X 課長は，K 社の提案が妥当かどうか判断できなかったので，第三者の専門業者にコンサルティングを依頼した。依頼を受けた業者は，K 社の提案を妥当であると評価した。また，復旧期間の目標値に関しては，費用を最小化するという観点から，復旧までの営業日を短縮すべきであると提案した。

設問１　本文中の [a] ～ [c] に入れる適切な字句を答えよ。[a] については 10 字以内，[b] については 4 字以内，[c] については 2 字以内で答えよ。

設問２　X 課長は，アウトソーシングによって，顧客情報の機密性を保持することに不安があると考えている。K 社に実施させるべき具体的対策を，30 字以内で述べよ。

設問３　顧客情報管理システムが停止した事故に関する次の問いに答えよ。

(1) D 氏は，情報セキュリティ修正プログラムをすべて適用すると，ばく大な作業工数を要すると発言しているが，その作業項目とは何か。15 字以内で述べよ。

(2) X 課長が，情報セキュリティ修正プログラムの適用回数を少なくするため，K 社に依頼した新サービスとは何か。40 字以内で述べよ。

設問４　ウイルス対策のサービスレベルに関する次の問いに答えよ。

(1) 昨年度の更新サービスと事故対応サービスの契約金額を，それぞれ求めよ。

(2) 復旧期間の目標値の見直しに関して，コンサルティングを依頼した専門業者が提案した内容を具体的に 10 字以内で述べよ。また，その理由について 45 字以内で述べよ。

問２　認証システムに関する次の記述を読んで，設問１～５に答えよ。

B 社は，本社を東京にもち，複数の事業所を有する大手製造業者である。本社と各事業所は，社内ネットワークで結ばれている。社外への情報提供のために，非武装セグメント（DMZ）に Web サーバを設置している。B 社は，早くから情報化に取り組んでおり，社員に 1 人 1 台のパソコンを配布している。また，社内の各種業務サービスの多くは，ブラウザからアクセスできる。このうち，人事や経理など一部のシステムは，ID とパスワードによるアクセス制御を行っている。電子メールについては，4 月と 10 月の年 2 回の定期人事異動のたびに電子メールアドレスが変わることがないよう，所属部門に依存しないアドレス形式に統一されている。

昨年，経営トップの交代があり，情報化戦略強化の一環として，公開かぎ基盤（以下，PKI という）の構築が打ち出された。情報システム部の S 部長は，直ちに，T 課長，U 主任とともに PKI の導入計画を策定し，システム設計を開始した。その概要は，次のとおりである。

(1) PKI の導入によって，クライアント認証の強化を図る。具体的には，サーバへのアクセス時のクライアント認証，社外から B 社システムへのアクセス時のクライアント認証に適用する。
(2) 公開かぎ証明書の発行対象は，全社員とする。失効事由が発生した場合には，直ちに失効手続を取るが，人事異動で失効にならないよう設計に留意する。
(3) 公開かぎ証明書を発行する認証局の主管は，情報システム部とする。認証局は，社員の秘密かぎを保持しない。
(4) 社外から社内サーバへのアクセスは，100 人規模のパイロットシステムによって 3 か月間の評価を実施し，その後，全社展開を行う。

社員は，配布されたツールを使用して，あらかじめ秘密かぎと公開かぎのかぎペアを生成し，公開かぎ証明書を取得する。

図 1 に，B 社システムの構成を示す。

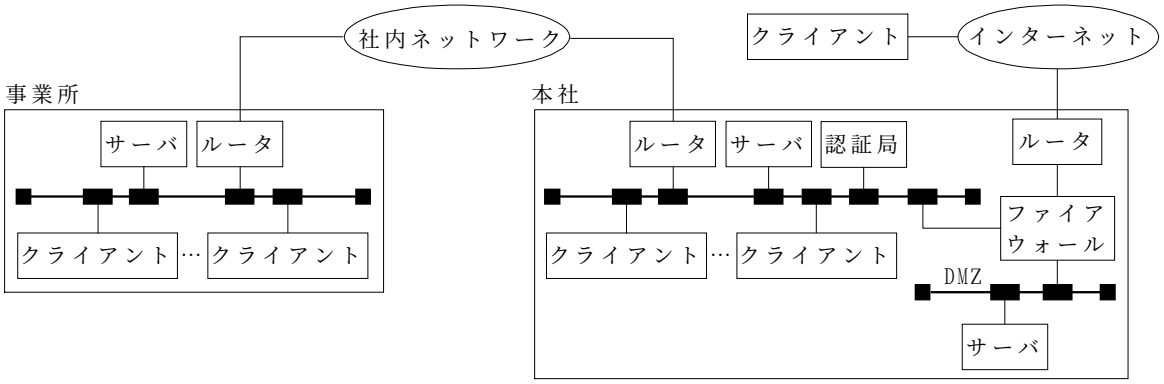


図１　Ｂ社システムの構成

S 部長は，①ID とパスワードによる認証方式が利用者にとって負担になり，結果としてセキュリティの水準を低くしているという問題意識をもっていたことから，PKI 導入によって，一気にこの問題を解決できると考えた。

PKI 設計のかなめは，公開かぎ証明書の設計である。S 部長，T 課長及び U 主任の 3 人は，図 2 に示す公開かぎ証明書に記載する“対象者名（subject）”と“有効期間”について議論した。

シリアル番号
発行者名
有効期間
対象者名
公開かぎ
発行者の署名

図２　公開かぎ証明書（主な内容）

S 部長：公開かぎ証明書は，印鑑証明書のようなものなので，“対象者名”をユニークにする必要がある。

T 課長：社員番号，電子メールアドレス，所属と氏名などいろいろ考えられますが，公開かぎ証明書を画面で見てすぐ確認できることと，社内で使うものですから，所属と氏名を記載したらいかがでしょうか。

S 部長：②その案には賛成できないな。ユニークにするといっても，社員番号ではだれだか分からないので問題だが，電子メールアドレスなら既に電子メールが社内に普及しているので，問題は少ないと思う。無論，氏名と社員番号の組合せや，氏名と電子メールアドレスの組合せでも構わないと思うが。

T 課長：それでは，氏名と社員番号の組合せにしましょう。

S 部長：公開かぎ証明書には，有効期間があったはずだが，どれくらいだったかな。

U 主任：4 年です。

S 部長：有効期間が切れる前に，次の公開かぎ証明書を発行する必要があると聞いているが，それはいつごろを計画しているのかな。

U 主任：全社規模になりますと，数日で次の公開かぎ証明書を発行するのは難しいと思いますので，有効期間が切れる 1 か月前からにしたいと思います。

パイロットシステムによる評価は，以前から情報システム部門に協力的な営業部と技術部が行うことになった。早速，両部の部員に対して操作方法や公開かぎ証明書の取得の仕方などの説明会が開かれ，翌日から公開かぎ証明書の発行申請の受付が始まった。公開かぎ証明書の発行申請及び取得は，Web から行うことができるようになっており，このときに入力する本人確認用の“初期パスワード”は手渡しで配付した。1 週間のうちに全員が手続を済ませた。

1 か月ほど経ったある日，U 主任に技術部の C 君から電話が入り，秘密かぎと公開かぎ証明書が入ったパソコンを紛失してしまったと連絡があった。③U 主任は，認証局の運用規定に従って C 君が本人であることを確認し，速やかに処置を行った後，C 君に次にとるべき処置を指示した。このような場合に社員がとるべき行動については，説明会で配付した説明書や Web ページにも掲載してあるが，試行期間中でもあったので，どうすればよいかを懇切丁寧に説明した。

パイロットシステムによって，社外から社内サーバにアクセスできるようになったことから，営業部の部員には好評であった。パイロットシステムによる試行が始まると同時に，S 部長をはじめとするプロジェクトチームは，全社展開に向けて準備を開始した。

S 部長：今度は全社規模であり，試行時のように本人に手渡しするわけにもいかないので，何か工夫が必要だと思うが。

T 課長：はい。公開かぎ証明書の発行申請及び取得は Web から行い，④発行申請前と取得後にそれぞれこのような内容の電子メールを送付して通知しようと思います。（と言いながら，電子メールで通知する内容を書いた説明書を S 部長に提示する。）

S 部長：なるほど。これなら問題ない。話は変わるが，この前，我が社と似たような規模の W 社の F 部長に会ったときの話だと，W 社は PKI を利用したディジタル署名システムを試行するそうだ。⑤公開かぎ証明書の有効期限は 4 年で半分の 2 年経ったところで次の公開かぎ証明書を発行するといっていたが，我が社は 1 か月前で大丈夫か。

U 主任：大丈夫です。問題ありません。クライアント認証のためなので，1 か月前で十分です。

設問１　本文中の下線①で，ID とパスワードによる認証方式が抱えている，利用者にとって負担になる問題とは何か。セキュリティ確保の観点から二つ挙げ，それぞれ 25 字以内で述べよ。

設問２　本文中の下線②で，S 部長が反対した理由を 30 字以内で述べよ。

設問３　本文中の下線③で，U 主任が行うべき処置と，U 主任が C 君に対して指示すべき処置は何か。U 主任が行うべき処置を 15 字以内，U 主任が C 君に対して指示すべき処置を 30 字以内で述べよ。

設問４　本文中の下線④の電子メールの内容は何か。公開かぎ証明書の発行申請前と取得後の電子メールの内容について，それぞれ 20 字以内で述べよ。

設問５　本文中の下線⑤で，W 社は有効期間が切れる 2 年前に次の公開かぎ証明書を発行するのに対して，B 社では有効期間が切れる 1 か月前の発行を予定している。なぜ，更新時期がこのように大きく違うのか，80 字以内で述べよ。

問３　社員向け情報セキュリティ教育に関する次の記述を読んで，設問１～５に答えよ。

M 社は，社員数 200 人規模の会社である。ほとんどすべての社員が，社内ネットワークに接続された 1 人 1 台のパソコンを使って，日々の業務を遂行している。社内ネットワークは，情報システム部の管理の下でインターネットに接続されており，一般社員が利用するパソコンからインターネットを利用することができる。ただし，利用できるインターネットサービスは，ファイアウォールによって制限されている。

M 社は，既に情報セキュリティポリシを定めており，その基本方針の中で，図１のように規定していた。

> 社員は，情報セキュリティポリシを遵守すること。情報セキュリティポリシの規定事項に著しく反する行為があった社員は，取締役会の審議を経て懲戒を受ける場合がある。

図１　情報セキュリティ基本方針(抜粋)

しかし，新入社員から，“ このような抽象的な指示では，具体的に何を守らなければならないのかが分かりにくい ” という声があがったので，情報システム部を中心にして，社員が守るべき事項を周知するための教材を作成することになった。

情報システム部の Y 部長の指示で，Z 主任が教材の作成を担当することになった。まず，教材の構成を検討するために, 情報セキュリティ対策基準(以下, 対策基準という)を参照することにした。

次は，Y 部長と Z 主任の会話である。

Y 部長：先日頼んでおいた教材の作成の件だが，検討状況を報告してくれないか。

Z 主任：はい。まず，教材の構成は，当社の対策基準の項目に沿って整理を進めています。まだ，必要な項目すべてを網羅してはおりませんが，今日までの検討結果を報告いたします。教材の冒頭では，社員が当社の情報セキュリティポリシを熟読し，すべての内容を理解することが重要であることを明記します。

Y 部長：なるほど。情報セキュリティを考える上で，一番大切な文書だからな。ところで，当社の対策基準の章立ては，どうなっていたかね。

Z 主任：はい。図 2 のとおりです。

(1) 組織及び体制
(2) 情報の分類と管理
(3) 物理的セキュリテイ
(4) 人的セキュリテイ
(5) 技術的セキュリテイ
(6) 運用
(7) 法令遵守
(8) ポリシ [a] への対処
(9) 評価と見直し

図２　対策基準の章立て

Y 部長：いろいろな項目があるが，どこから検討を開始したらいいだろうか。

Z 主任：はい。この対策基準は，管理する側の視点で構成されていますので，各項目の中から利用者が守るべき事項を抜き出して整理し直すつもりです。その中でも，新入社員が仕事を進める上で一番身近な問題である情報システムの利用に関する部分から始めようと思います。[b] や Web といった，最も代表的なインターネットサービスの正しい使い方を説明する予定です。また，当社の対策基準で，“社員は，[b] や Web の利用に当たっての脅威を十分に理解すること”と規定されていますので，そうした脅威についても説明します。もう少し具体的に述べますと，[b] を受け取ったときに，そこに書いてある送信者の情報が [c] され，なりすましが行われていないかどうかを確認すること，[d] していないかどうかを専用のソフトウェアを用いて確認すること，[b] を社外に送るときには，正しい受取人に届くように必ず [e] を確認すること，などを推奨するつもりです。さらに，会社にとって重要な情報を扱う場合には，配送経路上での [c] を検出したり，[f] を防止したりするために，[g] 技術の利用を検討することも奨励します。

Y 部長：普段何気なく使っている [b] も様々な脅威が存在するということだな。ところで話は変わるが，社員がパスワードを管理する上で注意すべき事項を説明する必要はないだろうか。当社の対策基準では，(4)章で適切なパスワード管理を社員に義務付け，(5)章でパスワードに関する技術的な要求事項を述べるなど，分散していてとても分かりにくい。

Z 主任：そうですね。大事なことを忘れていました。利用者の立場に立って項目を整理します。まず，簡単に見破られるようなパスワードを使わないこと，利用開始時に設定された初期パスワードを直ちに変更すること，パスワードを定期的に変更すること，を追加します。本来は，このような固定式のパスワードではなく，[h] パスワードを利用する方が情報セキュリティ対策上は望ましいのですが，固定式に比べて費用がかさむので，今後の検討課題とします。それと，パスワードといわれて思い出したのですが，①パソコンを使用中に会議などで席をはずす場合に注意すべきこととして，ログオフすることがありました。また，不在時に電源を入れていない自分のパソコンを他人に勝手に起動されないように注意すべきこととして，パソコンの電源投入時に必要な起動用のパスワードを設定する

こともありました。これらも追加しておきます。さらに，単に利用者に義務を課すだけでは操作が煩雑になり，実効性を欠く可能性があるので，利用者の負担を減らす工夫も盛り込もうと思います。

Y 部長：ところで，対策基準の運用の章で，緊急時の対応に関する原則が規定されていたはずだな。以前から気になっていたのだが，万が一，情報セキュリティに関連する事故が発生した場合に，社員がどのような行動をとるべきなのかを知らせておいた方がよいのではないか。

Z 主任：おっしゃるとおりです。ただし，一口にセキュリティ事故といっても，いろいろな場面がありますので，何通りかに分けて説明しようと考えています。

Y 部長：どのように分けるのかね。

Z 主任：はい。まず，情報セキュリティ管理者にどのような現象を報告すべきかということと，その報告手段について詳しく述べるつもりです。次に，もしもその現象が，明らかなセキュリティ事故であった場合にとるべき行動，ソフトウェアの予期しない動作であった場合にとるべき行動，まだ事故は発生していないが事故を起こす原因になるぜい弱性を発見した場合にとるべき行動，に分けて説明します。特に注意しなければならないのは，ぜい弱性を発見した場合に，自分でそれを確認しようとしたり，解決しようとしたりしないことです。もし，発見者がそのような行動をとると，場合によっては，不正な使い方をしていると見なされてしまう可能性があるからです。

Y 部長：確かにそうだな。社員を守るためには，そのような考え方も重要だろう。

Z 主任：はい。もう一つ，ソフトウェアが予知しない動作をした場合にも，自分だけで解決しようとしないことが重要です。それというのも，［　d　］したことが原因で予期しない動作を起こした場合に，②経験のない社員が原因の除去を行おうとすると，かえってシステムを破壊したりして被害を拡大する可能性があるからです。

Y 部長：なるほど。こうして考えてみると，ただ単に規則を守るようにと教育するだけではなく，身の回りにどのような脅威が存在するのかについて，正しい知識をもってもらうことも重要なのだな。

Z 主任：はい。そうです。

Y 部長：では，今日のところはここまでとしよう。この調子で，残りの部分も頑張ってくれたまえ。

設問１　本文中の［　a　］～［　h　］に入れる適切な字句を，それぞれ 9 字以内で答えよ。

設問２　パスワードを管理する上で，社員が注意すべき点は何か。本文中で Z 主任が例示した以外の注意点を二つ挙げ，それぞれ 15 字以内で述べよ。

設問３　セキュリティ事故を発見した際にも，ぜい弱性を発見したときと同様に，発見者に自ら対処させず，情報セキュリティ管理者への報告を義務付けるべきであるが，それはなぜか。発見者が自分で対処した場合に怠りがちな事柄と，その結果，生じる可能性がある問題点について，それぞれ 15 字以内で述べよ。

設問４　パソコンの不正操作や画面からの情報漏えい防止の対策として，本文中の下線①に示した規則を定めて単に義務を課すだけでは，十分に対策が徹底されない場合がある。利用者の負担を減らし，対策の実効性を担保するためには，システム面でどのような工夫が考えられるか。35 字以内で述べよ。

設問５　本文中の下線②に示したように，被害が拡大する原因として考えられる誤操作を二つ挙げ，それぞれ 45 字以内で述べよ。

問４　リモートアクセスシステムに関する次の記述を読んで，設問 1～4 に答えよ。

H 社は，中堅の製造業者である。本社は，営業拠点も兼ねて東京にあり，近郊に研究所と工場がある。市場は主に国内であり，全国主要都市に営業所がある。数年前から社内業務の電子化を進めており，昨年までに 1 人 1 台のパソコンの設置が完了した。最近では，社長をはじめ全社員が電子メールを使って連絡，指示及び報告を行うようになった。昨年から，社外向けホームページを開設して，積極的な情報発信も行っている。また，Web サーバを利用した社内の情報共有化も進んでおり，24 時間いつでも必要な情報にアクセスできる。これは，情報共有 Web サーバへの事例登録件数を社内電子化推進への貢献に対する指標として評価するという社長の方針が大きく影響しており，部門業績の評価項目にもなっている。さらに，営業部門に対しては，1 人 1 台の携帯電話を貸与し，販売活動の円滑化を図っている。

これまで H 社は，先端技術を使用していることもあって，セキュリティ確保を最優先にし，社外から社内のサーバへのアクセスを原則禁止にしてきた。ところが，先ごろの役員会で営業活動の更なる効率化が議題に挙がり，営業や技術サポート部隊が客先や出張先から社内のサーバに直接アクセスすることができれば，営業活動を効率的かつ効果的に行うことができるとの判断から，リモートアクセスを解禁することが決定された。

情報システム部の G 部長は，この決定を受けて，現行システムの構築に最初から携わっている入社 6 年目の R 主任に直ちに検討に入るように指示した。

1 か月後，R 主任は，次のような内容を骨子とする計画案を作成し，G 部長に提出した。

(1) 情報セキュリティポリシを見直し，社内システムへのアクセスに関する対策基準と実施手順を追加規定する。
(2) 社外からアクセス可能な社内サーバは，メールサーバ(SMTP 及び POP)と特定の情報共有 Web サーバに限定する。
(3) 情報セキュリティ対策及びライセンス管理上, 社外から社内システムにアクセスするための PC カード付きノート型パソコンは，会社から貸与する。
(4) ノート型パソコンには，紛失を考慮してファイル暗号化ソフトを組み込む。また，本人以外が起動できないように起動パスワードを設定する。
(5) 社外から社内システムへのアクセスは，当面，リモートアクセスサーバ(以下，RAS という)経由だけにする。RAS へのアクセス記録は，本人あてに電子メールで送付する。

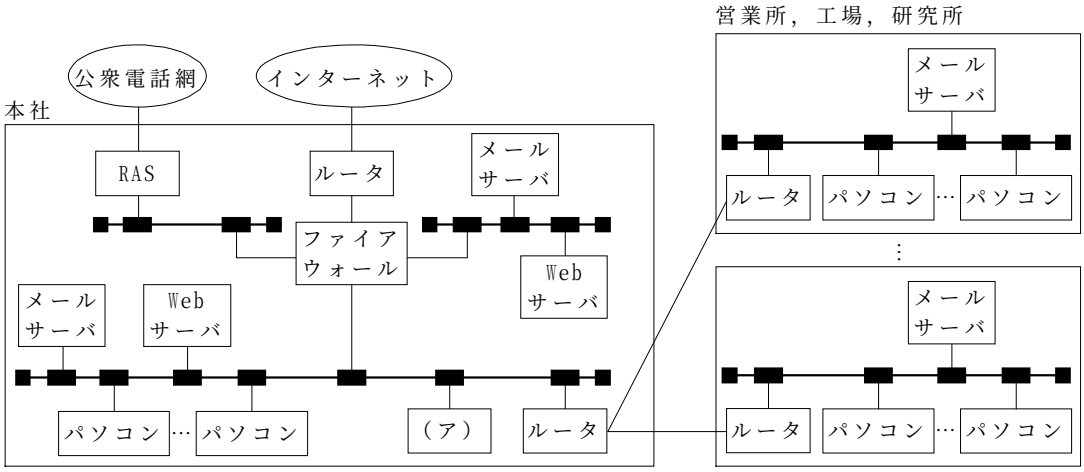


図　H社のネットワーク構成（業務サーバを除く）

次は，この計画案に対するG部長とR主任の会話である。

G部長：我が社のシステムも本格的にリモートアクセスが可能になるわけだが，セキュリティの観点からのポイントを説明してもらいたい。

R 主任：はい。不正侵入の［　a　］，不正侵入の早期［　b　］，侵入された場合の対応体制の整備やウイルスチェックなど，システム側としての対策は無論ですが，ノート型パソコンの紛失や無許可使用などのリスクに対しても十分な手を打つことを心掛けました。

G部長.：不正侵入の［　a　］対策として，具体的にどのような手が打たれているのか，図のH社のネットワーク構成を用いて簡単に説明してもらいたい。

R主任：はい。リモートアクセスユーザを確認するため，発信者番号通知に基づく発信元確認を行うとともに，図中の(ア)に［　c　］サーバを設置してRASへの接続時にパスワードのチェックを行います。また，RASと社内ネットワークとの間には，ファイアウォールを設置しています。

G 部長：早期［　b　］を行うための，本人あてのアクセス記録の送付頻度はどうなっているのかね。

R主任：とりあえず，翌日の朝に前日分をまとめて送付するというやり方でスタートしてみようかと思います。

G部長：ところで，<u>①会社から貸与するノート型パソコンだが，ウイルスの感染防止及び機密情報の漏えい防止の観点からの禁止規定が抜けているな</u>。アタックの踏み台にされて，我が社だけでなくほかの企業にも迷惑を掛ける可能性もあるからな。

R主任：分かりました。<u>②ウイルスの感染防止及び機密情報の漏えい防止の観点からは，個人所有のパソコンに言及した禁止規定も必要ですね</u>。

G部長：そうだな。それはそうと，ファイルの暗号化は守られるだろうか。社内でも暗号メールは，なかなか浸透しないようなので少し心配だが。

R主任：貸与するノート型パソコンに組み込むファイル暗号化ソフトは，あらかじめ対象ファイルを定義しておけば，自動的にファイルの暗号化を行いますので，利用者はいちいち意識す

る必要はありません。

G 部長：なるほど。最近，他社では，携帯電話機から社内の Web サーバにアクセスしている所もあるようだが。

R 主任：はい。今回は入っていませんが，その場合は，インターネット経由のアクセスになりますので，情報セキュリティ対策上ゲートウェイサーバを追加設置します。[c] サーバは，リモーアクセスと共有できます。

G 部長：③インターネットを経由するとなると，なりすましに対する対策が必要だな。

新システム稼働後のある日の午後 1 時過ぎ，営業部の N 担当から電話が入った。

N 担当：営業部の N ですが，PC カード付きノート型パソコンを紛失したのですが。

R 主任：（N 担当に関する情報を検索しつつ）紛失した場所と時刻，最後にアクセスした時刻を教えてください。

N 担当：昼に立ち寄った店に置き忘れたのですが，気が付いて戻ったときにはもうありませんでした。最後にアクセスしたのは，午前 11 時ごろです。

R 主任は，直ちに N 担当のアカウント停止措置をとった後，[d] を見て不審なアクセスがなかったかどうかを調べた。幸い，その間に不審なアクセスはなかった。

その後，しばらくは平穏な日々が続いたが，ある日の朝一番に営業部の P 部長から電話が入った。

P 部長：営業部長の P だが，携帯電話から社内ネットワークにつなぐときのパスワードを忘れた。何とかしてくれ。

R 主任：P 部長とおっしゃいましたね。念のため内線電話番号と電子メールアドレスを教えて頂けますか。電子メールで新しいパスワードをお送りしますので，それを使ってください。(R 主任は，電話で応対しながら P 部長のアドレス情報を検索し，内線番号と電子メールアドレスが一応正しいことを確認した。)

P 部長：今，ホテルからなんだ。電子メールが読めないので，今ここでパスワードを教えてくれないか。

R 主任：申し訳ありません。それはできかねます。

P 部長：肝心なときに役に立たんな。今朝，重要顧客の L 社の専務から電話があり，電子メールを送ったので至急見てほしいと連絡があったんだ。何とかならんか。

R 主任：L 社ですか。④分かりました。それでは，“ hysk74pt ”を使ってください。

P 部長：分かった。ありがとう。

設問１　本文中の [a] ～ [d] に入れる適切な字句を答えよ。

設問２　本文中の下線③についての対策事項を，15 字以内で述べよ。

設問３　本文中の下線④の R 主任の行動には，情報セキュリティ対策上問題がある。それは何か。25 字以内で述べよ。また，どのように行動すべきだったかを，40 字以内で述べよ。

設問４　本文中の下線①及び②で，G 部長と R 主任が必要であると思った追加規定を，それぞれ 45 字以内で述べよ。