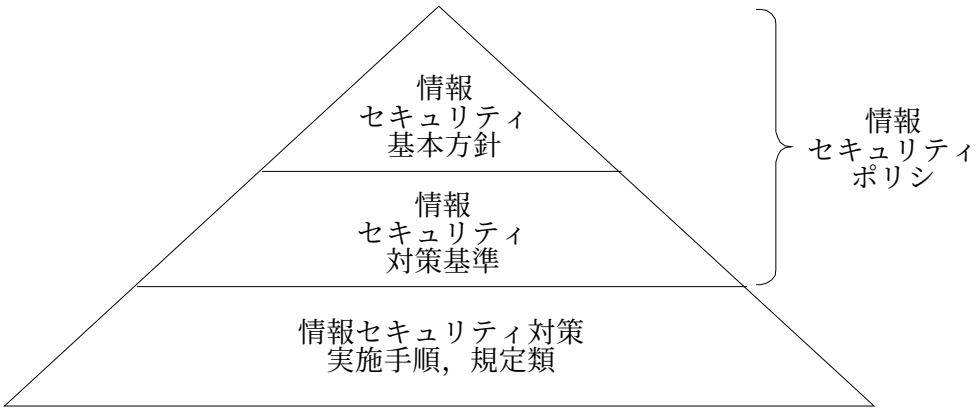
平成１６年度　秋期　情報セキュリティアドミニストレータ　午後Ⅰ問題

〔情報セキュリティポリシの位置付け〕

情報セキュリティポリシの位置付けは、次のとおりとする。



問１　情報セキュリティポリシの教育に関する次の記述を読んで，設問１～４に答えよ。

A 社は，従業員数 2,000 名の不動産会社で，戸建て住宅，マンションの販売及びオフィス賃貸事業を全国に展開している。A 社では，社内業務の効率向上のために，5 年前から全従業員に対して，ネットワークに接続されたパソコンが配備されている。3 年前からは，インターネットによる空き室情報の提供や申込受付などのサービスを開始し，順調に売上を伸ばしている。また，インターネットによるサービスの開始と同時に，外部からの不正侵入を阻止するために，ファイアウォールを設置した。

A 社の組織構成を図に示す。インターネットを利用した事業を推進する上で，情報セキュリティポリシが必要不可欠であると判断し，社長を委員長とする情報セキュリティ委員会を社内に新設した。委員には各部の部長が選任され，情報システム部の N 部長と若手の T 主任の 2 名が事務局となった。

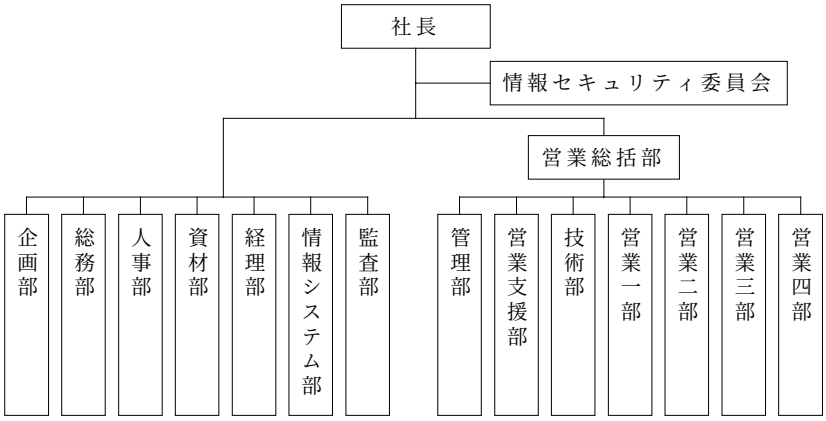


図　A社の組織構成

この委員会は，3 か月間で情報セキュリティポリシを策定した。A 社は，インターネットによる情報の活用促進を重要視する一方で，会社の秘密情報が外部に流出することを防止するために，会社の情報資産を重要度に応じて分類し，その分類ごとに適切に取り扱うように情報セキュリティポリシの中で規定している。

T 主任は，情報セキュリティポリシを社内に周知徹底させるに当たって，数年前に情報システム部が“電子メール利用上の注意”を社内に浸透させようとしたときの方法について調べた。このときは，情報システム部の担当者が各部に直接出向いて説明会を開き，全従業員に受講させていた。それにもかかわらず，“電子メール利用上の注意”が従業員に浸透しているとはいえなかった。T 主任は，“電子メール利用上の注意”を浸透させようとした際に実施したアンケートの調査結果を読み直してみた。その結果，“情報システム部の説明が理解しにくい”，“注意事項はもっともだが，それでは仕事の実態からずれている”などの問題点が指摘されていることに気付いた。

T 主任は，アンケートの調査結果を踏まえ，社内への周知方法について N 部長と話し合った。その結果，説明の時間や回数を増やすのではなく，方法を変えてみることにした。それは，情報システム部による一斉集合教育から，段階的なトップダウン教育に変更するというものであった。具体的には，まず，情報システム部が各部の総務担当の課長に対して指導者養成のための教育を行い，次に，各課長が所属

する部の従業員に対して教育を行うというものであった。教育用マニュアルは，専門用語を避け，一般従業員でも理解しやすい表現にした。

次は，各課長に対する教育での質疑応答である。

①B 課長：情報セキュリティポリシの教育といっても，情報システム部がファイアウォールを設置したし，システムに利用者 ID とパスワードを設定しているから，当社の情報セキュリティは十分だと思うが。

②T 主任：まだまだ不十分です。まず，どの情報が会社の秘密情報なのか分かりにくい状況です。次に，秘密情報と思われるものが机の上に無造作に置かれていて，業務上必要のない従業員が簡単に見ることができます。

③B 課長：確かにそうだ。

④N 部長：基本的なことだが，部外者が許可なく室内に出入りできなくするための入退管理も大切なことではないか。

⑤B 課長：休日出勤したときや最後に退社する際に，かぎの管理が甘いのではないかと感じることがある。しかし，それと情報セキュリティとは，どう関係するのだろうか。

⑥N 部長：情報セキュリティを確保するためには，様々な脅威に対して，物理的，人的，技術的対策などを網羅的に実施する必要がある。

⑦C 課長：人的対策を実施するとは，具体的にどうすればいいのでしょう。

⑧N 部長：例えば，従業員の雇用契約の中に守秘義務にかかわる条項を入れることなどがある。

⑨C 課長：当社の雇用契約には，守秘義務にかかわる条項が含まれている。その一方で，外部への業務委託が増えているので，各社との契約の中に守秘義務に関する条項があるかどうかを確認する必要がありそうだ。改めて聞くが，なぜ今，情報セキュリティを強化しなくてはならないのかね。

⑩T 主任：激化する競争に勝ち抜くために，当社のような企業では，情報の活用が不可欠です。その一方，企業内や企業間のネットワーク化によって情報が共有され，活用が推進されて，情報が外部に流出するリスクが増大していることを当社の大部分の従業員は気付いていないのです。情報セキュリティを確保するためには，情報セキュリティへの従業員の無関心を何とか解決しなくてはなりません。

⑪D 課長：コンピュータに詳しくなくても，他人のネットワークに不正侵入を試みることができるソフトウェアも出回っているようだね。

⑫N 部長：そのような行為を防止するために，［　a　］が 2000 年に施行されたわけだ。

⑬D 課長：最近，新聞などに個人情報とプライバシの問題が採り上げられているね。確かに今，情報を利用するときのモラルについて教育することも不可欠だと思うね。

⑭T 主任：情報セキュリティに対する意識や知識が不足していると，自分では気付かずに法に触れてしまうこともあります。第三者のホームページの記事を許可なく転載すると，［　b　］権を侵害する場合があります。また，ソフトウェアを無断でコピーし利用すると，［　b　］権だけでなく，進歩性のあるアイデアを保護する［　c　］権も侵害する場合があります。

⑮B 課長：情報漏えいは，内部の人間によるものが多いという新聞記事を見た。

⑯N 部長：過去の情報漏えいの事例を見ると，やはり内部の人間が持ち出すケースがほとんどだね。従業員の管理を徹底させることが重要だ。

⑰C 課長：内部の人間による不正を防ぐためには，教育と併せて，社内のチェック体制を確立することも大事だ。外部への業務委託のチェック体制としては，委託先に管理者を置き，その管理者に任せるようにしよう。ところで，万が一，秘密情報が漏えいした場合，その使用と開示を差し止めることはできるのか。

⑱T 主任：差し止めることができる法律としては，不正競争防止法があります。ただし，差止め権を行使することができるのは，［ d ］情報のうち，顧客情報や製造方法など事業活動に［ e ］技術上又は営業上の情報であり，客観的に秘密情報として管理されていることが必要条件になります。

⑲B 課長：訴訟になった場合，企業における情報管理が問われるわけか。

⑳T 主任：そこで，被害を最小限にとどめるために，会社の秘密情報をどのように管理すべきかを情報セキュリティポリシの中でうたってあります。

㉑D 課長：今までの説明で，情報セキュリティポリシの教育の背景やねらいなどを理解することはできたが，うまく説明できるかどうかが心配だ。

㉒N 部長：教育用のマニュアルやツールについては，分かりやすいものを用意したので，ぜひともよろしくお願いしたい。

設問１　本文中の［ a ］～［ e ］に入れる適切な字句を答えよ。

（1）［ a ］については，当てはまる法律名を 20 字以内で述べよ。

（2）［ b ］，［ c ］については，それぞれ 2 字以内で答えよ。

（3）［ d ］，［ e ］については，解答群の中から選び，記号で答えよ。

解答群

ア　希少な　　イ　貴重な　　ウ　自社の　　エ　非公知の　　オ　有用な

設問２　本文中の質疑応答の中で，人的対策の観点から不十分な発言がある。該当する発言番号を①～㉒の中から一つ選び，その理由を 30 字以内で述べよ。

設問３　本文中の質疑応答の T 主任の発言内容から，A 社の秘密情報の管理は不十分であるといえる。万が一，秘密情報が漏えいした場合，法的に不正使用を差し止めるには，A 社の情報管理をどのように変更すべきか。T 主任の発言内容を踏まえて要件を二つ挙げ，それぞれ 25 字以内で述べよ。

設問４　情報セキュリティポリシの教育に関する次の問いに答えよ。

（1）A 社に情報セキュリティポリシを周知徹底させる上で，T 主任が考えている最大の障害は何か。25 字以内で述べよ。

（2）情報セキュリティポリシを周知徹底させるために，T 主任は従業員に対する教育を各部の総務担当の課長にお願いした。各部の総務担当の課長が実施するメリットは何か。45 字以内で述べよ。

問２　ログの設定と監視に関する次の記述を読んで，設問１～４に答えよ。

M 社は，社員数 200 名の中堅商社である。M 社では，会社からの社員への連絡や社員間の情報共有のために，Web ベースのグループウェア（以下，GW という）を利用している。この GW には，Web メール，掲示板，予定管理，文書管理，電話帳（社員の氏名，所属，役職，内線番号，メールアドレスを調べられる）といった機能があり，それぞれの機能はソフトウェアモジュールで実現されている。GW は，社内 LAN に設置されたサーバ 1 上で稼働している（図 1）。サーバ 1 上では，GW のほかに Web サーバとメールサーバが稼働している。

M 社では，営業社員が社外からサーバ 1 にアクセスできるようにするため，DMZ に設置されたサーバ 2 上で VPN ソフトを稼働させ，インターネットからサーバ 1 への VPN によるアクセスを許可している。

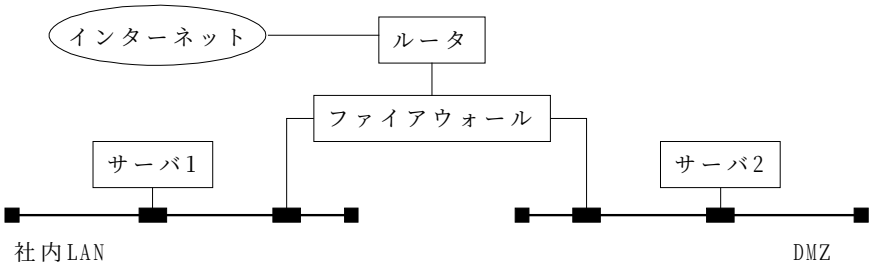


図１　M社のネットワーク構成（一部）

〔ログ管理の見直し〕

M 社の社内 LAN に設置されたサーバ（以下，社内サーバという）のログの設定は，OS やアプリケーションをインストールしたときの初期設定のままであり，これまで監視や分析は行っていなかった。

このような状況下で，ある日，社内サーバにワームがまん延するという事故が起きた。ワームそのものは，ウイルス定義ファイルを更新したウイルス対策ソフトによって比較的簡単に駆除できたが，感染経路を特定できなかった。それは，ほとんどの社内サーバが，いつ，どこから，どのようなアクセスがあったのかを検知できるだけのログを取得していなかったからである。

情報システム部の L 部長は，社内サーバのログ管理がほとんどできていない現状では，ワームの感染経路の特定だけでなく，社内情報が漏えいした場合の調査などにも支障が出る可能性を懸念した。また，ログを適切に監視していれば，ワームへの感染なども早期に検知できると考え，L 部長は情報システム部の K 係長に対して，社内サーバのログ管理について検討するよう指示した。そこで K 係長は，手始めにサーバ 1 のログの設定を見直すことにした。

〔脅威の洗出し〕

K 係長は，サーバ 1 に関して想定される脅威と，それを検知し，調査するための情報を，表 1 のとおりに整理した。

表１　脅威と，それを検知し，調査するための情報

脅威	説明	検知し，調査するための情報
ウイルス，ワーム	ウイルス，ワームへの感染	ネットワークアクセス情報
なりすまし	他人のアカウントを利用したシステムへのログイン	ログインの成功／失敗の記録 ログイン元マシンの IP アドレス
情報の漏えい	許可範囲を超えた情報の配付，又はアクセス権限のない者による情報へのアクセス	ファイルへのアクセス記録 ファイルの転送記録 電子メールの送信記録
情報の破壊や改ざん	情報の不正な変更，又は削除	ファイルへのアクセス記録 ファイルの変更記録

〔取得すべきログ〕

続いて，K 係長は，サーバ 1 が取得できるログのうち，表 1 に挙げられた情報が記録できるものを調べた（表 2）。その後，サーバ 1 の設定を変更し，表 2 のログを取得できるようにした。

表２　サーバ１のログ

構成要素	記録されるイベント	記録される項目
OS	A：ログイン／ログアウト	時刻，アカウント名，操作内容（ログイン／ログアウト），状態コード（成功／失敗）
	B：ネットワークアクセス	時刻，送信元 IP アドレス，プロトコル（TCP／UDP／ICMP），送信元ポート番号，あて先ポート番号
Web サーバ	C：ブラウザからのアクセス	時刻，送信元 IP アドレス，HTTP 要求，状態コード（成功／失敗），転送バイト数
メールサーバ	D：電子メールの受信	時刻，メッセージ ID，送信元 IP アドレス，送信者メールアドレス，受信者メールアドレス，メールサイズ，状態コード（成功／失敗）
	E：送信キューへの格納	時刻，メッセージ ID，送信者メールアドレス，受信者メールアドレス，メールサイズ，状態コード（成功／失敗）
	F：送信キューからの送信	時刻，メッセージ ID，あて先 IP アドレス，送信者メールアドレス，受信者メールアドレス，メールサイズ，状態コード（成功／失敗）
GW	G：ログイン／ログアウト	時刻，アカウント名，操作内容（ログイン／ログアウト），状態コード（成功／失敗）
	H：各モジュールでのデータアクセス	時刻，アカウント名，モジュール名，アクセス内容（読出し／書込み／削除），アクセス対象データ，状態コード（成功／失敗）

表 3 は，表 1，2 に基づいて，サーバ 1 において脅威を検知し，調査するために監視又は分析すべきログを示したものである。

表３　監視又は分析すべきログ

脅威	ログ（記録されるイベント）
ウイルス，ワーム	a
なりすまし	A，B，C，G
情報の漏えい	b，c，d，e
情報の破壊や改ざん	b，c

〔なりすましの監視〕

サーバ 1 では，アカウントをもっている各社員の所属部署や役職に応じて，アクセス可能なデータを制限している。ところが最近，自分のアカウントではアクセスできないデータを参照するために，ほかの社員のアカウントを借りる例が散見されるようになってきた。ほかの社員のアカウントを利用したまま，うっかり掲示板に意見を書き込んでしまって物議を醸した事例が何件か発生し，問題になっていた。

この問題に関しては，社員への啓発やデータのアクセス権限の見直しといった対策が取られてきているが，アカウントの貸し借りの監視などは行われていない。監視できれば，アカウントの貸し借り抑止にもなると考えた L 部長は，今回設定したログによって監視できないか，K 係長に相談した。

アカウントの貸し借りが，表 1 に示したなりすましの脅威に当たると考えた K 係長は，監視の可能性を検討した。その結果，①なりすましの発生をログの監視によって直接検知することは困難であると判断した。K 係長は，ログでは不審な挙動を検知できるだけで，脅威の発生そのものの監視はできないことを L 部長に報告した。ただし，不審な挙動の検知をきっかけとした調査によって，脅威の発生の予防又は早期発見につながる可能性があるので，監視することは有益である点も併せて報告した。

K 係長の報告を受けた L 部長は，早速，ログの監視を実施するよう K 係長に指示した。K 係長は，ログの監視によって，②ログイン／ログアウトのパターンが普段と異なっているアカウントを発見した場合に，そのパターンを不審な挙動とみなすことにした。

〔複数のログの取扱い〕

K 係長は，サーバ 1 以外の社内サーバについても，順次，ログの設定の見直しを進めた結果，各社内サーバで必要なログを取得できるようになった。K 係長は，それらのログの相互参照を容易にし，③ログに対する脅威に対抗するために，社内サーバのログを収集するサーバ（以下，ログサーバという）を社内 LAN に設置し，ログを一元管理することにした。各社内サーバは，ログをローカルに保存するとともに，ログサーバにもログを送信するように設定された。

さらに，K 係長は，各社内サーバで取得されているログを相互に対照できるように，すべての社内サーバに関して，④ログの設定以外にもシステム的な設定を行った。この設定によって，例えば，ワームがどのように感染を広げていったかを，別々の社内サーバのログ情報を見比べることで把握できるよう

になる。このことが，感染経路の特定につながると期待された。

設問１　表 1，2 に基づいて作成された表 3 中の [a] ～ [e] に入れる適切な記号を，表 2 中の A～H から選べ。

設問２　本文中の下線④のシステム的な設定内容を，20 字以内で述べよ。

設問３　本文中の下線③に関する次の問いに答えよ。

（1）脅威の内容を，5 字以内で答えよ。

（2）ログサーバの導入が(1)の脅威の対抗策となる理由を，35 字以内で述べよ。

設問４　〔なりすましの監視〕に関する次の問いに答えよ。

(1) K 係長が本文中の下線①のように判断した理由を，表 2, 3 を参考にして 50 字以内で述べよ。

（2）ログの監視によって本文中の下線②を検知するために，表 3 に示したログ A，B，C，G を利用して，日常的に行っておくべきことがある。その内容を，60 字以内で具体的に述べよ。

問３　情報系システムのウイルス対策に関する次の記述を読んで，設問１～４に答えよ。

E 社は衣料品を扱う，社員数 300 名の中堅商社である。E 社では，全社員が情報を収集するための社外の Web サイトの閲覧と電子メールの利用ができるほか，商品情報などを提供する Web サイトを自社で運用している。情報系システムはシステム部が所管し，S 君が利用者からの問合せに対応している。問合せに関して専門家のアドバイスが必要な場合は，設計，構築を行ったシステムインテグレータの F 社に有償で支援を依頼している。

E 社の情報系システムの構成とファイアウォール（以下, FW という）のフィルタリング設定内容は，図 1 のとおりである。

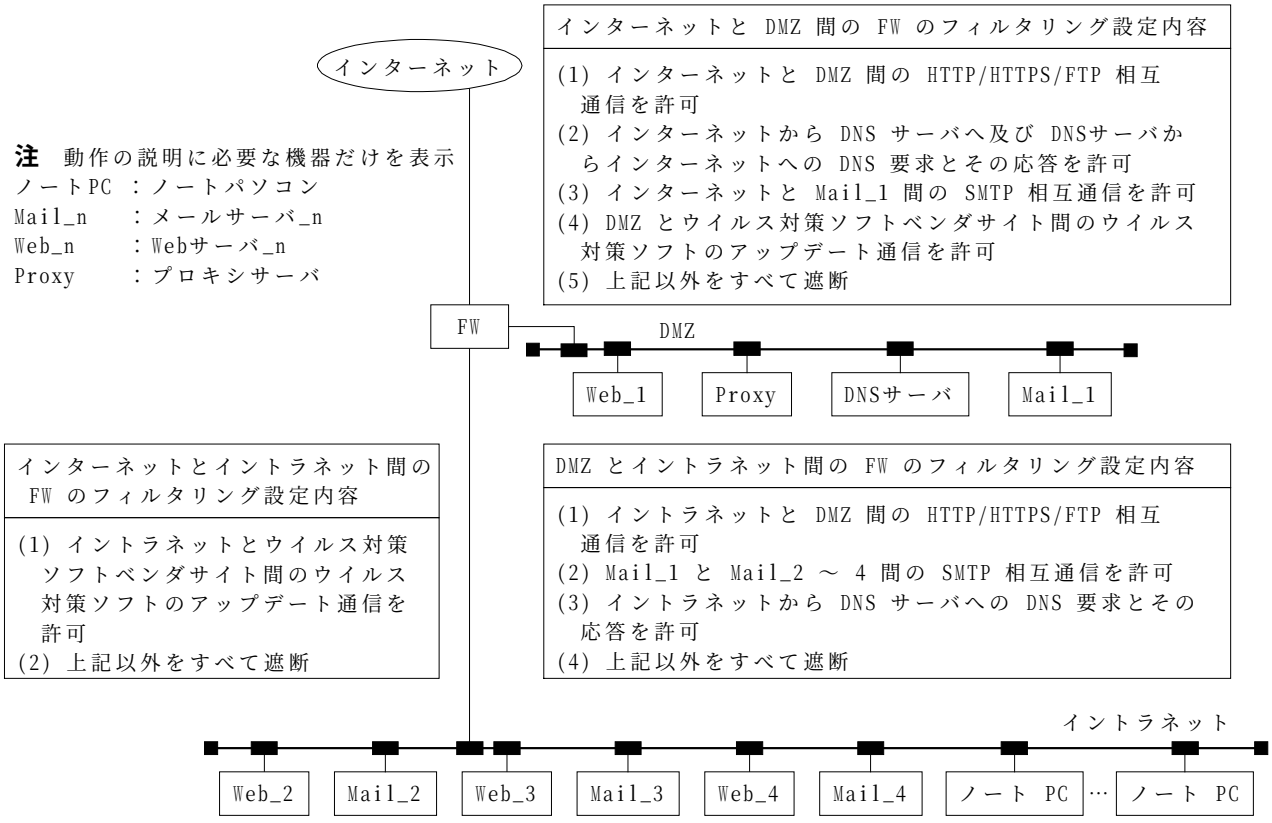


図１　Ｅ社の情報系システムの構成とＦＷのフィルタリング設定内容

(1) イントラネットには，各部が運用する Web_2～4 の 3 台の Web サーバが設置され，社内の情報共有などに利用されている。営業部が運用する Web_3 では，最新の商品情報などが常に更新されている。

(2) Web_1 は社外向け Web サーバであり，会社情報と商品情報の発信のほか，商品に対するアンケート収集を行っている。発信する商品情報は，CGI プロセスがイントラネットに設置された Web_3 から最新の情報を取得している。Web_1 の CGI プロセスは Web_3 とだけ通信していて，プロトコルは HTTP を使っている。アンケートの結果は Web_1 のフォームから入力を受け，個人情報や商品情報などを含んだテキストファイルとして格納される。担当者が，システム部立会いのもとでサーバ

コンソールから随時ログインし，アンケート結果を取得した後，当該ファイルを削除している。

（3）社員のメールボックスは，各部が運用する Mail_2～4 に設置されている。社員は，クライアント PC から所定のメールボックスに接続して電子メールを送受信する。外部との送受信は，すべて DMZ に設置された Mail_1 を経由して行われている。

（4）社員が社外の Web サイトを閲覧するとき，及び社外の FTP サーバとファイルをやり取りするときは，すべて Proxy を経由して行う。

（5）Mail_1～4 及びイントラネットの全ノート PC にウイルス対策ソフトが導入されウイルスやワームを常時監視している。ウイルスやワームが発見された場合は，アラームメールが S 君に送られるようになっている。その場合，S 君は運用マニュアルに従って初動措置を行い，必要に応じて F 社にサポートを依頼する。ウイルス対策ソフトのアップデートは，毎日自動的にウイルス対策ソフトベンダサイトと通信して行われるほか，緊急時には，S 君が全社員に電子メールなどでアナウンスし，社員各自が速やかに実行する規則になっている。

（6）FW のフィルタリングは，図 1 のように設定されている。

〔第 1 の事件〕

ある日，“ Mail_3 にワーム U が侵入しようとしたので駆除した ”というアラームメールが S 君に届いた。ウイルス対策ソフトベンダサイトで検索したところ，図 2 のようなワームであることが判明した。

クライアントでの動作：

クライアント実行型ワーム U が，電子メールの添付ファイルとしてクライアント PC に侵入し，利用者がこれを実行すると，アドレス帳にある任意のメールアドレスに対してクライアント実行型ワーム U を添付した電子メールを送信する。さらに，IP アドレスをランダムに設定して，侵入可能なセキュリティホールがある Web サーバを検索する。侵入可能な Web サーバを発見すると，サーバ実行型ワーム U をプロトコル FTP で送り込み，実行させる。

サーバでの動作：

サーバ実行型ワーム U は，自身が動作中の Web サーバにアクセスしてくるブラウザにセキュリティホールを発見すると，クライアント実行型ワーム U をプロトコル HTTP で送り込み，実行させる。また，ファイルのアクセス権限を変更し，サーバ上のテキストファイルを外部から読取り可能にする。

図２　ワームUの特徴

ワーム U はウイルス対策ソフトによって駆除されたので緊急に対処する必要性は低くなったが，感染経路を不審に思った S 君は，社内のウイルス対策ソフトの設定状況を一斉点検した。その結果，Mail_3 を使用する営業部員 1 人のノート PC のウイルス対策ソフトが削除されていることを発見した。ウイルス対策ソフトを再インストールしたところ，ノート PC がワーム U に感染していることが判明した。この営業部員は，日ごろから自宅や外出先でもこのノート PC を使っていたという。

以上から，S 君は今回の事件を次のように推定した。ワーム U が添付された電子メールを，営業部員が自宅か外出先で受信し，ノート PC がワーム U に感染した。そのノート PC をイントラネットに接続し，ワーム U に感染した電子メールを発信した。この感染した電子メールを，Mail_3 のウイルス対策

ソフトが検出した。

S 君は，①規則どおりにウイルス対策ソフトを運用するよう，全社員に徹底させた。

〔第 2 の事件〕

事件が解決した直後，イントラネットでウイルス対策ソフトのアラームが多発した。さらに，見知らぬ G 社から“貴社の Web サイトにアクセスしたら，ワーム U に感染した”との苦情が届いた。調査したところ，Web_1 がワーム U に感染していて，アクセスしてきた利用者のブラウザにセキュリティホールがある場合に，感染が広がる可能性があることが分かった。緊急事態と判断したシステム部長は，感染経路の究明と感染防止対策の検討を S 君に指示する一方，図 2 に示すサーバでの動作を見て，感染拡大のほかにも②重大な問題が発生している可能性があると考え，調査を行った。

S 君は F 社の J 氏に支援を依頼した。J 氏は，図 1，2 を見て，Web_1 への感染経路として，次の二つの可能性を指摘した。

（1）インターネット上の，ワーム U に感染している［　a　］から，サーバ実行型ワーム U がプロトコル［　b　］で Web_1 に送り込まれた。

（2）ワーム U に感染した，営業部員のノート PC からイントラネット経由で，［　c　］型ワーム U がプロトコル FTP で Web_1 に送り込まれた。

こうした状況を踏まえ，今後，新種のウイルスやワームへの感染を防止するために，S 君は次の対策を提案した。

（1）［　d　］

（2）［　e　］

（3）FW のフィルタリング設定において，③必要以上に通信が許可されている設定があるので，制限を強化する。

この提案は経営者に承認され，早速実行に移された。

設問１　本文中の［　a　］～［　c　］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　FTP	イ　HTTP	ウ　HTTPS
エ　SMTP	オ　Web サーバ	カ　クライアント PC
キ　クライアント実行	ク　サーバ実行	ケ　メールサーバ

設問２　S 君の取った行動は，本文中の下線①だけでは不十分であった。ワーム U の特徴が判明していたことを考えると，更にどの機器を対象に，どのような調査を行うべきであったか。35 字以内で述べよ。

設問３　本文中の下線②に示した重大な問題とは何か。対象となる情報とセキュリテイ事故について，20 字以内で述べよ。

設問４　ウイルス，ワームへの感染防止に関する次の問いに答えよ。

(1)本文中の下線③に示した,必要以上に通信が許可されている設定とは何か。機器間通信のうち，FTP 通信に関する不要な例を一つ挙げ，15 字以内で述べよ。

(2) S 君が本文中の［ d ］，［ e ］で提案している，ウイルス，ワームへの感染防止対策とは何か。対象機器と実施事項を含めて，それぞれ 30 字以内で述べよ。

問４　インターネットデータセンタ選定時の情報セキュリティ要件定義に関する次の記述を読んで，設問１～３に答えよ。

H 社は，社員数 200 名の中堅の衣料品小売業者である。今までは，郵送カタログによる商品紹介と電話やファックスによる注文受付が大半を占めていたが，最近ではインターネットを活用した，Web での商品紹介や注文受付の比重が高くなってきている。その結果，商品紹介や注文受付に必要なサーバ類が新商品の売出し直後など注文の多い時期に停止すると，売上に大きな影響を及ぼすようになってきた。

これまで，H 社では，商品紹介や注文受付に必要なサーバ類を社内のサーバルームに設置していた。しかし，H 社が借りているオフィス用賃貸ビルは，物理的セキュリティ面での不安や法定点検時の全館停電など，サーバ類の 24 時間 365 日安定稼働に支障があった。また，サーバ類の運用を行っている H 社情報システム部には，部長を含めて 5 名の要員しかいないので，夜間や休日も含めた十分な運用体制を組むことは事実上無理であった。

そこで，常時稼働が必要なサーバ類を，物理的セキュリティ対策や無停電対策が整っているインターネットデータセンタ（以下，IDC という）に移設するとともに，各サーバ類の運用を IDC にアウトソーシングすることにした。

まず, 移設先の選定や移設スケジュールなどを検討するために, 3 名からなる検討チームを編成した。検討チームのリーダには H 社情報システム部の P 部長が就任し，メンバとして情報システム部の Q 主任と，他部門から異動したばかりで経験の浅い R 君が指名された。検討チームは移設後のシステム構成を検討し，図 1 のように決定した。

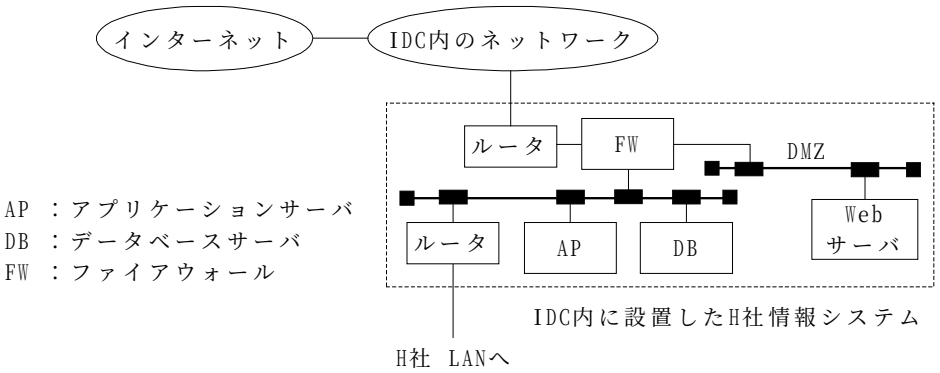


図１　移設後のシステム構成

次に，Q 主任が中心になり，IDC について集められるだけの資料を入手して，書類選考によって 5 社を選択した。選択した 5 社は，使い勝手や価格体系の面でほぼ似通っていて，簡単には優劣をつけがたい状況であった。

そこで，P 部長を含むメンバ全員で各社の IDC を訪問調査して，情報セキュリティに関連する事項を中心に，更に比較検討することにした。訪問調査を始めるに際して，検討チームで調査項目の洗出しを行い，表 1 に示す調査項目について調査することになった。

表１　調査項目（情報セキュリティに関連する事項の抜粋）

調査項目	調査ポイント
サーバ運用サービスの内容	稼働監視，ログ確認，…
敷地，建物への入退管理の実施状況	入館手続，個人識別手段，…
監視設備の状況	監視カメラ，警報装置，…
電源設備の状況	受電設備，非常用電源，…
空調設備の状況	空調容量，空調方式，…
防火対策と消火設備の状況	センサ種別，消火方式，…
そのほかの状況	建材，内装，…

さらに，表 1 の調査項目を基に，R 君が Q 主任の指示に従って，IDC に求めるべき情報セキュリティ要件を検討した。R 君がまとめた要件の抜粋を，図 2 に示す。

1. サーバ運用
（1）IDC 内に設置したサーバ類（以下設置サーバという）について，24 時間 365 日にわたって稼働状況を監視すること
（2）設置サーバに対するインターネット経由の不正アクセス（以下，不正アクセスという）の有無を，24 時間 365 日にわたって監視すること
（3）不正アクセスなどの緊急事態が発生した場合に，迅速な対処が可能であること
2. 入退管理
（1）すべての IDC 社員（派遣契約社員，外注者を含む。以下同様とする）及び外来者を入退管理の対象にし，更に外来者については，事前の届出を必須にすること
（2）入館時には，IDC 社員，外来者を問わず，身分証明書を提示させること
（3）外来者には所持品検査を行い，入退記録簿への記入を求め，外来者用の［ a ］を貸与すること
（4）コンピュータ室への出入りの際には，［ a ］を使った個人識別と記録を実施すること。さらに，共連れ（1 人の認証で，複数人が出入りする行為）やすれ違いを抑止するために，アンチパスバック機能（2 回連続して入室できず，また 2 回連続して退室できない機能）を利用していること
3. 監視設備
（1）建物外壁の窓ガラスに，振動や開閉を検知するセンサを設置し，昼夜を問わず侵入者を自動検知すること
（2）建物のすべての出入口に［ b ］を設置し，警備室から終日監視すること
（3）コンピュータ室内及び通路の要所にも［ b ］を設置し，警備室から終日監視すること
4. 電源設備
（1）2 系統受電，ループ受電などの受電方式を採用し，ビル内の配電経路を二重化していること
（2）商用電源の瞬断や停電時には，非常用電源によって電力を供給できること
（3）非常用電源として，起動から発電開始までの時間が短いガスタービン発電機を設置していること
5. 空調設備
（1）空調機は，現用系 N 台＋予備系 1 台で構成されていること
（2）大規模な地震時の可用性向上のために，水冷式の空調機を採用していること
6. 防火対策と消火設備
（1）室内の建材や備品などには，不燃材，準不燃材又は難燃材を使用していること
（2）コンピュータ室には，超高感度煙検知機と連動した泡消火設備を設置していること
7. コンピュータ室の設置に関する要件
（1）不正侵入防止のために，外壁窓ガラスは網入りガラスを使用していること
（2）地震発生時に，照明器具が落下，損傷しないような措置を講じていること

図２　ＩＤＣに求めるべき情報セキュリティ要件（抜粋）

訪問調査の結果，各社が提供するサーバ運用サービスには一長一短があることが分かった。そこで，この 5 社から更に候補を絞り込むために，移設予定のシステムのハウジングを想定したサーバ運用サービスの内容について，各社に提案を依頼した。Q 主任は，不正アクセス防止策を比較するために，各社からの提案を基に，FW に関するサーバ運用サービスの内容を表 2 にまとめた。

Q 主任が P 部長に表 2 を示して相談したところ，不正アクセス防止策として，①FW に関する表 2 の

サーバ運用サービスは，図2で規定したサーバ運用に関する要件を満たしていないと指摘された。そこで，各IDCと相談して，図1に示したH社情報システムに新たなハードウェアを追加せずに②付加できる，FWに関するサーバ運用サービスの内容と，新たなハードウェアを追加した場合に③付加できるサーバ運用サービスの内容について，それぞれ代案の提示を求めた。

表２　不正アクセス防止策のためのＦＷに関するサーバ運用サービス水準の比較

社名 / セキュリティ関連のサービス項目	V社	W社	X社	Y社	Z社
ハードウェアの稼働監視 (1)	1回／5分	1回／5分	1回／10分	1回／10分	1回／5分
プロセスの稼働監視 (2)	（なし）	1回／5分	1回／10分	1回／10分	1回／5分
ログの確認(3)	1回／日	1回／週	1回／月	1回／日	1回／日
設定変更の対応 (4)	休日，深夜を除く随時	随時	随時	随時	休日，深夜を除く随時
ハードウェアの障害対応 (5)	休日，深夜を除く随時	随時	随時	随時	休日，深夜を除く随時

注　(1) ハードウェアが稼働しているか否かを，あらかじめ定めた間隔でpingを用いて監視するサービス
(2) FWプロセスが正常に動作しているか否かを，あらかじめ定めた間隔で監視するサービス
(3) FWプロセスが出力するログをあらかじめ定めた間隔で確認し，不正アクセスと思われる通信が行われていないか否かを調査するサービス
(4) サービス上の都合や新たなぜい弱性の発見など，何らかの理由でFWの設定を変更する必要が生じた場合に，設定を変更するサービス
(5) 障害を起こしたハードウェアの切分けやベンダへの保守コールなどを実施するサービス

設問１　図2中の［　a　］，［　b　］に入れる適切な字句を，それぞれ6字以内で答えよ。

設問２　図2中の4～7には，コンピュータの設置場所の条件として，経験の浅いR君の誤解や理解不足に基づく誤った要件記述がそれぞれ一つずつある。不適切と思われる記述を選び，図2中の(1)～(3)の番号で答えよ。また，それらの記述が不適切である理由と，本来の望ましい要件を，それぞれ20字以内で述べよ。

設問３　本文中の下線①～③に示したサーバ運用サービスの内容に関する次の問いに答えよ。
（1）P部長が，下線①で“満たしていない”と指摘した要件を，図2中の番号で答えよ。
（2）下線②の“付加できる，FWに関するサーバ運用サービスの内容”を，20字以内で述べよ。
（3）下線③の“付加できるサーバ運用サービスの内容”を，想定される追加ハードウェアを含めて，30字以内で述べよ。