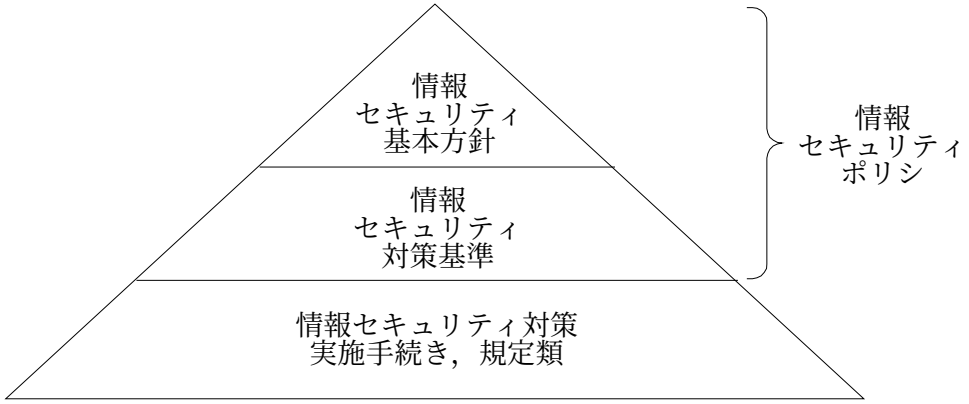
平成１３年度　秋期　情報セキュリティアドミニストレータ　午後Ⅱ問題

情報セキュリティポリシの位置づけ



問１　ネットワークのぜい弱性分析とその対処に関する次の記述を読んで，設問１～５に答えよ。

X 社は，各種の電子部品やパソコンの周辺機器を製造，販売している中堅の電子機器メーカである。パソコンの周辺機器については，パソコンメーカに相手先ブランドで供給するとともに，自社ブランドによる一般消費者への販売も行っている。

X 社の組織は，図１のとおりである。ある地方都市の郊外に本社ビルがあり，同じ敷地内に工場が隣接している。そのほか，東京，大阪及び名古屋に営業所が設置されている。

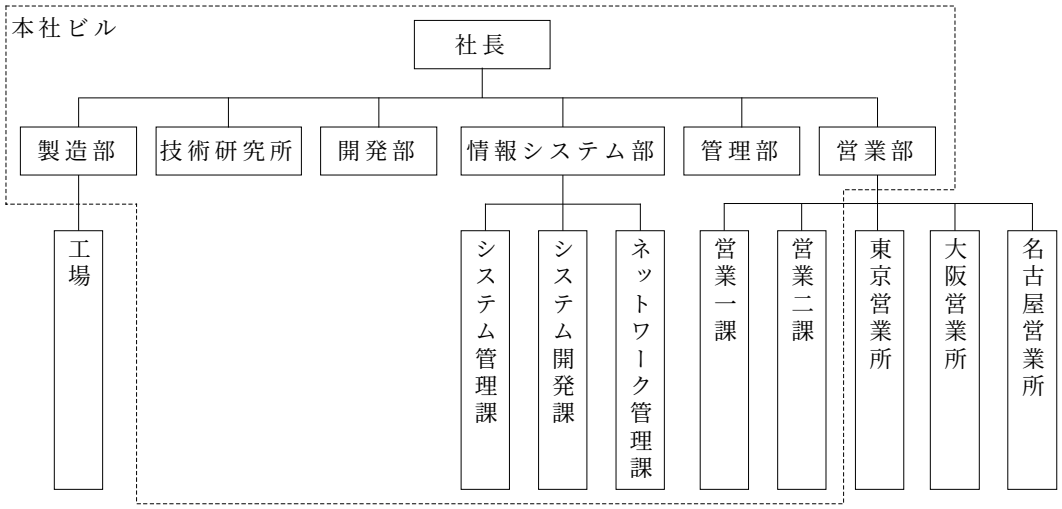


図１　X社の組織

〔インターネットへの接続と情報セキュリティポリシの策定〕

技術研究所（以下，研究所という）は，先端技術の研究を行うという業務の性格上，各種の技術情報を効率的に収集する必要がある。また，大学や各種研究機関と共同で研究を行う機会も多くなっている。そのため，研究所では，X 社のほかの部門でネットワークが導入される以前からインターネットへの接続環境を整備し，情報収集や共同研究の際の情報交換などに活用していた。

今から 5 年ほど前，X 社では業務の効率化を目指し，販売管理システムの構築と全社的なネットワーク（以下，業務用ネットワークという）の導入が推進された。業務用ネットワークの管理を行う部署として情報システム部の下にネットワーク管理課が新設された。

業務用ネットワークの整備が開始されるのと同時に，社長から，“ 当社は今後，情報セキュリティを重視していく ”との方針が出され，部門を横断した組織として情報セキュリティ委員会（以下，委員会という）が設置された。この委員会を中心として，X 社の情報セキュリティポリシが策定された。

当時，インターネットの普及が本格化してきたことから，業務用ネットワークはインターネットへ接続されることになった。業務用ネットワークのインターネットへの接続は，新たに契約した専用線で行われた。それに伴い，研究所が利用していた専用線は，解約される予定であった。しかし，研究所から“ 各種ネットワークプロトコルの研究やネットワーク機器の相互接続性の実証実験など

に利用可能な環境がほしい”との強い要望が出されたので，研究所のインターネット接続環境は，そのまま実験用ネットワークとして残されることになった。ただし，情報セキュリティポリシに従って，実験用ネットワークは，実験用機器の設置と実験データの収集にだけ用いることにした。研究所が従来から行ってきた情報収集，情報交換，実験データの解析及び資料作成には，業務用ネットワークを用いることが決められた。

結果として，X 社のインターネットへの接続環境は，図２のようになった。業務用ネットワークはネットワーク管理課が，実験用ネットワークは研究所が，それぞれ管理している。

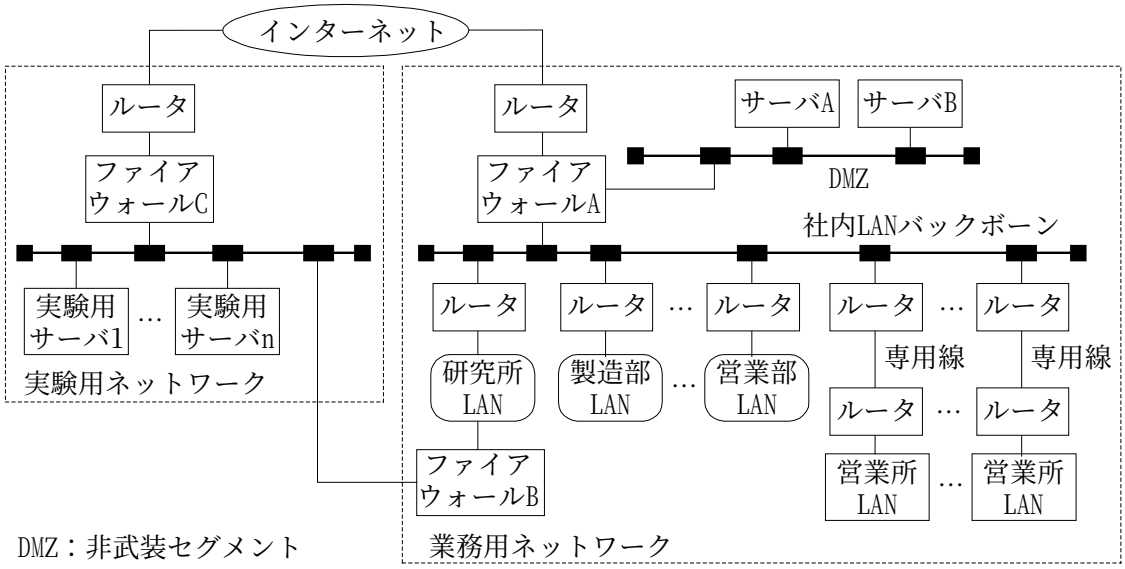


図２　X社のネットワーク構成

業務用ネットワークから実験用ネットワークへのアクセスは，ファイアウォール B によって，研究所 LAN からの TELNET，FTP，HTTP 及び SSH に制限されている。また，ファイアウォール B は，研究所 LAN と実験用ネットワーク間の経路情報しか保持していないので，研究所 LAN から実験用ネットワーク経由でインターネットへ直接アクセスすることはできない。

実験用ネットワークには，実験用のサーバやネットワーク機器を実験内容に応じて接続している。したがって，機器の台数や構成は一定していない。ファイアウォール C は，実験用ネットワークからインターネットへの IP パケット及びその応答パケットだけを許可している。ただし，実験の内容によっては，設定が変更されることもある。

業務用ネットワークの DMZ 上には，2 台のサーバが設置されている。サーバ A では Web サービスが，サーバ B では電子メール（以下，メールという）サービス（SMTP サーバと POP サーバ）が，それぞれ稼働しており，X 社の社員は，サーバ B 上の POP サーバにアクセスしてメールを読んでいる。この POP サーバは，外出先でも社員がメールを読めるように，インターネットからもアクセスが可能になっている。また，ファイアウォール A では，SMTP と HTTP で受信したデータに対するウイルススキャンと URL のフィルタリングが機能している。

インターネットから POP サーバへのアクセスについては，情報が漏えいする可能性があるので難色を示した委員もいたが，委員会での検討の結果，利便性を重視してアクセスを可能とすること

になった。

〔電子商取引サイトの立ち上げとスパムメール〕

今から 1 年ほど前，パソコンの周辺機器を直接消費者に販売する電子商取引（以下，EC という）サイトを立ち上げる案が役員会で検討され 承認された。この EC サイトは，情報システム部のシステム開発課が中心となって構築を進めていくことになった。仕組みは，次のとおりである。

(1) 業務用ネットワークの DMZ 上にサーバ C を追加し，これに DBMS をインストールする（図３）。この DBMS には，X 社が製造しているパソコンの周辺機器の製品情報データベースを載せる。

(2) サーバ A 上に，この DBMS と連携できるアプリケーションサーバ（以下，AS という）をインストールし，この AS を利用して，商品の検索と注文ができるホームページを用意する。

(3) 消費者は，この注文用ページを利用して購入したい周辺機器の注文をする。

(4) 注文内容は，営業部の EC サイト担当者あてのメールとして，サーバ A によって自動的にサーバ B へ送られる。担当者は，注文品の在庫と納期を確認した後，受注確認のメールを注文者あてに送信し，商品の発送手続を行う。

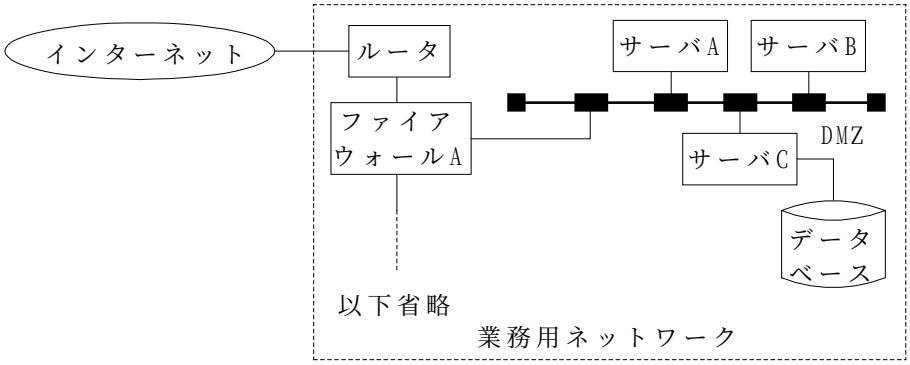


図３　ＥＣサイトの構成

EC サイトを立ち上げて間もなくのある日の早朝，ネットワーク管理課の Y 係長は，営業部の EC サイト担当者から POP サーバの応答が悪いという連絡を受けた。Y 係長が調査したところ，サーバ B 上の SMTP サーバの送信キューには大量の未送信メールが，また，受信スプールにはあて先不明によるリターンメールがそれぞれ大量にたまっており，サーバ B が過負荷状態になっていることが判明した。何者かがサーバ B を踏み台にして，大量のスパムメールを送信したようであった。Y 係長は，上司である Z 課長に事態を報告し，指示を仰いだ。

X 社のセキュリティ管理者でもある Z 課長は，報告を受けると，直ちにサーバ B をネットワークから切り離すよう Y 係長に指示するとともに，すぐさま復旧作業に取り掛かるよう命じた。Y 係長は，メールの送受信プロセスを停止させた後，①復旧作業を実施した。また，事故の再発防止のため，サーバ B 上の SMTP サーバのメール配送ルールを表 1 のように設定し，第三者中継を防ぐようにした。

なお，ルール 3 は，外出先の X 社社員がサーバ B を利用してメールを送信できるようにするた

めのものである。

表　ＳＭＴＰサーバのメール配送ルール

ルール	接続元	発信側のメールアドレス	受信側のメールアドレス	中継／受信
1	社外	任意	a	許可
2	社外	b	c	不許可
3	社外	X 社のドメイン	d	許可
4	社内	X 社のドメイン	任意	許可

〔ぜい弱性分析の実施〕

Z 課長は，X 社のインターネットの接続環境には，サーバ B の第三者中継以外にもセキュリティ上の問題があるのではないかと考え，専門業者にぜい弱性分析を依頼した。

〔ぜい弱性分析の結果〕

専門業者からの報告で，早急に対処が必要とされた問題は次の 3 点である。

・問題点 1

サーバ B 上で稼働している POP サーバの幾つかのアカウントのパスワードを，辞書攻撃によって破ることができた。これは，第三者によってメールを読み出されてしまう可能性が極めて高い状態になっていることを意味している。また，第三者中継への対処が不十分なので，X 社のアカウントを詐称すればサーバ B を踏み台にすることが可能になる。

・問題点 2

ファイアウォール C 上で HTTP のプロキシサーバが稼働している。このプロキシサーバの設定が不適切なので，第三者がこのプロキシサーバを踏み台にして社外の Web サーバへアクセスすることができるようになっている。

・問題点 3

サーバ A 上で稼働している AS には，最近になって不正侵入に結びつくセキュリティホールが報告された。サーバ A では，このセキュリティホールに対する対策が取られておらず，実際にシステムに侵入可能であることが確認された。

“問題点 1”～“問題点 3”のそれぞれに対し，専門業者から提示された対処法は次のとおりである。

・問題点 1 の対処法

簡易なパスワードを設定している社員に対して，パスワードの変更を指示することが急務である。

なお，②インターネット経由で POP を利用することは，望ましくない。外出先から会社あてのメールを読む必要のある社員が少数であれば，③特定のアカウントにだけリモートアクセスを許可するような仕組みにした方がよい。

また，現状の構成のまま，X 社の社員が外出先からサーバ B 上の SMTP サーバを利用してメー

ルを送信できるようにしたいのであれば，［ e ］などを利用して，第三者中継を防ぐ必要がある。

・問題点 2 の対処法

ファイアウォールの設定を見直し，プロキシサーバが踏み台にされないように設定を変更する。

・問題点 3 の対処法

この問題に対する対処法には，次の三つの方法がある。

（a） ベンダから提供されている対策パッチを適用する。

（b） AS を最新のものにバージョンアップする。

（c） ほかのベンダの AS に切り替える。

ただし，いずれの方法にも一長一短がある（表 2 を参照）ので，どう対処するかに関しては検討が必要である。

表２　各対処法の得失

対処法	工数	AS 上のアプリケーションの書換え	問題点
（a）	少	不要	パッチ適用後，メモリリークが発生
（b）	中	一部必要 （AS 呼出しの構文仕様変更のため）	特になし
（c）	多	ほぼ全面的に必要 （移行ツール付属の AS もあり）	新たな AS をサポートできるように担当者の再教育が必要

〔Z 課長の調査〕

“問題点 2”のプロキシサーバは，研究所 LAN からインターネット上の Web サイトへアクセスするために用いられていることが判明した。

ファイアウォール C を管理している研究員によれば，“ファイアウォール A でブロックされている複数の Web サイトへアクセスするためにプロキシサーバを立ち上げた”とのことである。業務上アクセスの必要な Web サイトがファイアウォールでブロックされている場合，フィルタリングの設定変更の申請をするのが本来の手続である。しかし，研究に関連する Web サイトへのアクセスがブロックされることが頻繁にあり，そのたびに申請をするのが煩わしいことや，申請してから設定が変更されるまでに時間がかかることといった不満が，バックドアの作成に結び付いたようである。

“問題点 3”に関しては，専門業者，システム開発課の EC サイト担当者及び営業部の EC サイト担当者から事情を聞いた結果，次の点が明らかになった。

（1）X 社の EC サイトのアクセス状況から考えて，対処法（a）のメモリリーク対策のためには，最低でも 1 日 1 回は AS の再起動が必要である。

（2）現在，システム開発課の社員は，販売管理システムの改訂作業に追われており，ほかの作業に人手を割く余裕がほとんどない。

（3）対処法（b）の場合，アプリケーションの変更作業とそのテストが必要であるが，上記の（2）の理由によって，対処が終了するまで 1，2 か月が必要である。

（4）対処法（c）については，移行ツール付属の AS へ切り替えたとしても，対処法（b）に比べて更に多くの時間が必要である。また，担当者に対するトレーニング費用も発生する。

（5）EC サイトは，思いのほか好評で売上も好調である。機会損失を最小にする意味からも，なるべくサイトを停止させたくない。

Z 課長は，表 2 と上記の（1）～（5）を勘案した上で，“ 未対処のままの期間の長短 ”，“ 対処作業の工数とコスト ”，及び “ 対処後に EC サイトの可用性を低下させる要因の有無 ” を考慮し，“ 問題点 3 ” の対処作業案を作成した。

Z 課長は，上記の内容と各問題点に対する対処作業案についてまとめた上で，委員会を召集した。

〔委員会での検討〕

“ 問題点 1 ” については，当面，次のように対処することにした。

（1）POP アカウントをもつ全社員に対し，適切なパスワードに変更するよう周知徹底する。

（2）社外からは，APOP による認証を行うことにする。

（3）第三者中継に対する対策として［　e　］を導入する。

また，委員会では，“ 専門業者のアドバイスに従って，外出先からのメールの読出しを，申請されたアカウントに限って期限付きで許可するべきである ” との意見が大勢を占めた。そこで，Z 課長以下ネットワーク管理課が，その仕組みを提案することになった。

“ 問題点 2 ”については，ファイアウォール C の設定を変更するよう研究所に指示するとともに，フィルタリングの設定変更処理を迅速化するための体制について検討することにした。

“ 問題点 3 ” については，Z 課長から提案された対処作業案が了承された。

設問１　本文中の［　a　］～［　e　］に入れる適切な字句を答えよ。

設問２　本文中の下線①で行った復旧作業の内容を 60 字以内で述べよ。

設問３　“ 問題点 1 の対処法 ” に関する次の問いに答えよ。

（1）本文中の下線②の理由を 25 字以内で述べよ。

（2）本文中の下線③の理由を 30 字以内で述べよ。

設問４　“ 問題点 2 の対処法 ” に関する次の問いに答えよ。

（1）URL のフィルタリングの運用に関して，変更処理の迅速化のほかにも検討した方がよいことがある。その検討内容を 50 字以内で述べよ。

（2）現在の X 社のネットワーク構成及び管理体制では，実験用ネットワークを介したバックドアの作成が今後も発生する可能性がある。それを防ぐため，ネットワーク構成と管理体制の面からとるべき具体的な対処作業案を，それぞれ理由とともに 60 字以内で述べよ。

設問５　Z 課長が作成した “ 問題点 3 ” の対処作業案は，どのようなものと考えられるか。理由とともに 140 字以内で述べよ。

問２　情報セキュリティポリシの策定及び運用に関する次の記述を読んで，設問１～５に答えよ。

A 社は，従業員が 700 人規模のエネルギ関連企業で，エネルギの購入，備蓄，精製及び卸販売を行っている。

エネルギの購入及び卸販売の業務は，主に本社部門が行っている。これらの事務処理業務のシステム化は，情報システム部が担当している。情報システム部は，事務処理の効率化のため，10 年ほど前にネットワーク（以下，事務処理系ネットワークという）を敷設し，本社部門のパソコンをネットワークに接続した。昨年，購入や卸販売業務でインターネットの利用が必要になったので，事務処理系ネットワークをインターネットに接続した。これによって，電子メールと社外のホームページ検索（以下 Web 検索という）が可能になり，従来からの社員間の情報交換に加え，社外との情報交換も可能になった。

インターネットの接続時にファイアウォールを設置し，電子メールと Web 検索だけを可能にした。特にウイルス対策としては，社外及び社内用メールサーバでウイルス検査を行い，感染のおそれがある場合には，中継を保留する措置を講じた。

生産部門では，エネルギを備蓄するためのタンクとエネルギを精製するための装置（以下，これらを総称してプラントという）を管理している。安定稼働とコストダウンの観点から，プラントの操業の自動化が推進されてきており，20 年前にコンピュータが導入された。プラントの制御及び監視の一元管理，並びに計測情報の分析及び解析のため，10 年ほど前にプラント制御系ネットワークが敷設された。また，プラントのメンテナンス業務を効率化するため，リモートアクセスサーバ（以下，RAS という）を設置している。これらについては，生産部門が構築し，維持管理を行っている。

A 社ではこれまで，本社部門と生産部門の間で方針や施策に関して意見の食い違いが多く発生し，意思決定に時間を要していた。本社部門と生産部門の連携を強化するため，両部門間の人事ローテーションを活発に行うこと，及び 1 年後に本社部門を生産部門の隣に移転することを経営会議で決定した。また，本社部門の移転時に，ネットワーク全体の見直しを図ることも決定した。

〔情報セキュリティポリシの策定〕

情報システム部の B 課長は，本社部門の移転計画を契機に，情報セキュリティポリシを作成し，セキュリティレベルの向上を図ることが必要であると考えた。そこで，B 課長は，社長を委員長とする情報セキュリティ委員会の設置と情報セキュリティ基本方針の骨子（図１）を経営会議に提案した。経営会議では，“本社部門の移転までの 10 か月間で情報セキュリティポリシの導入を完了し，移転後に運用を開始すること”及び“ウィルス対策を強化すること”という指示が出た。

次は，経営会議での質疑応答である。

C 役員：短期間で完了するためには，同業他社で作成した情報セキュリティポリシを流用して一部修正するのが効率的ではないか。

B 課長：効率的に作業を進めるため，外部の専門会社の支援を仰ぐつもりですが，情報セキュリティ基本方針の骨子で述べたような情報セキュリティポリシを策定するには，自分たちが中心となって作成したいと考えています。

社員は，エネルギ事業を継続的かつ安定的に行う上で，情報資産の重要性を認識し，情報資産の重要度とリスクに応じたセキュリティ（機密性，完全性及び可用性）の確保に努めなければならない。特に，プラント関係のシステムについては，可用性の確保に努めなければならない。

当社は，情報セキュリティ委員会を設置し，すべての情報資産のセキュリティを確保するため，実効性のある施策を情報セキュリティポリシとして定めるとともに，必要な諸手続を整備する。情報セキュリティポリシに関する教育，有効性の評価及び遵守状況の監視を行うことによって，セキュリティを維持，向上させる。

情報資産のセキュリティを損ねる行為を行った社員は，就業規則に基づき懲罰される。

図１　情報セキュリティ基本方針の骨子

情報セキュリティポリシ策定の支援を依頼された外部コンサルティング会社からは，失敗しないためのポイントとして，次の三つが提示された。

① 各部門の代表者からなる横断的な組織を形成し，全社での協調体制を構築する。
② 既存の文書管理規則や電子メールの利用規定との整合性を確保する。
③ 責任の所在が明確になるように，利用部門及び管理部門の権限範囲を規定する。

B 課長は，会社全体の実情に詳しく，また，他の部門のメンバと調整した経験のある情報システム部の W 主任を，情報セキュリティ対策の担当者に選任した。W 主任は，情報セキュリティポリシを策定し，その後，本社部門の移転までに教育を完了するというスケジュールを立案した。それを見た B 課長は，経営会議の指示に対して，作業が完了しない項目がでるおそれがあると考え，情報セキュリティポリシの策定スケジュールを早めるように W 主任へ指示した。

次は，情報セキュリティ委員会での会話である。

F 課長：今回の適用対象に紙の情報を含めるのか。ワープロで作成された電子化情報だけを対象にすれば十分ではないか。

W 主任：プリンタで出力すれば電子化情報も紙として存在しますので，含めたいと思います。紙の情報の機密レベルは，既に文書管理規則で規定されております。今後，情報の機密レベルについては，情報セキュリティポリシに一本化する方向で文書管理規則の担当者と合意しております。

F 課長：生産部門のプラント制御系システムを，今回の情報セキュリティポリシの対象から外すべきだ。利用している OS などの技術基盤が異なるからだ。

W 主任：本社部門の移転後，事務処理系とプラント制御系のネットワークを接続する予定です。確かに，プラント制御系システムは，汎用性の低い専用のハードウェアとソフトウェアで構成されていますが，以前よりも汎用化が進んでいます。やはり対象とすべきではないでしょうか。

F 課長：我々の生産部門は，安定稼働を至上命題にシステムやネットワークを構築した。事務処理系システムよりも高い可用性レベルを維持している。そもそも，事務処理系のネットワークやシステムとはセキュリティ要件が異なる。無理やりすべての情報資産を同じレベルで管理しようとすると，かえって我々のシステムのレベルが下がってしまう。

W 主任：生産部門のシステムは，確かに高い可用性レベルを維持しています。しかし，基本方針の骨子にも，すべての情報資産を対象にするとあり，一部を外すわけにはいきませんので，対象に含めるべきではないでしょうか。

F 課長：これでは平行線で，話がまとまらん。

B 課長：今回の移転は，本社部門と生産部門の連携強化がねらいだが，すぐに実現することは難しいので段階的に進めていくのはどうだろう。W 君，何かいい方法はないかね。

W 主任：それでしたら，プラント制御系ネットワークを 2 つに分けるのはどうでしょうか。汎用性の高い方は，情報セキュリティポリシの対象とし，もう一方は対象から外します。

F 課長：それぞれが基本方針や対策基準を策定し，運用していくということだな。それがいい。運用状況を見て，1 年後に統合するかどうかを検討するのはどうだろうか。

B 課長：了解した。当面，ネットワークの所管については，従来どおりでいこう。

W 主任：話は変わりますが，電子メールによる情報の漏えいを防ぐため，外部に送信する場合には，上司に控えを送信するというようにしたいのですが，いかがでしょう。

F 課長：私の部下は 30 人もいて，いちいち見ていられない。

B 課長：電子メールによる機密情報の漏えいを予防するため，協力をお願いしたい。

〔ネットワークの見直し計画〕

情報セキュリティ委員会の委員及び関係者で協議し，ネットワーク構成を見直した結果，図 2 のようになった。

（1）プラント制御系ネットワークを制御系と制御情報系の二系統に分離する。

（2）制御系ネットワークは，プラントの制御及び監視を行う。ネットワークプロトコルや OS などは，専用的な技術基盤を利用する。

（3）制御情報系ネットワークは，プロセスコンピュータ（以下，プロコンという）を用いて，計測情報や各種構成情報など，重要で最も機密性の高い情報を管理する。ネットワークプロトコルや OS などは，汎用的な技術基盤を利用する。

（4）制御情報系ネットワークは，内部ファイアウォールを経由して事務処理系ネットワーク，ゲートウェイを介して制御系ネットワークと接続する。制御情報系ネットワーク上のパソコンから社内共用ネットワークへの接続，電子メールや Web 検索の利用が可能である。

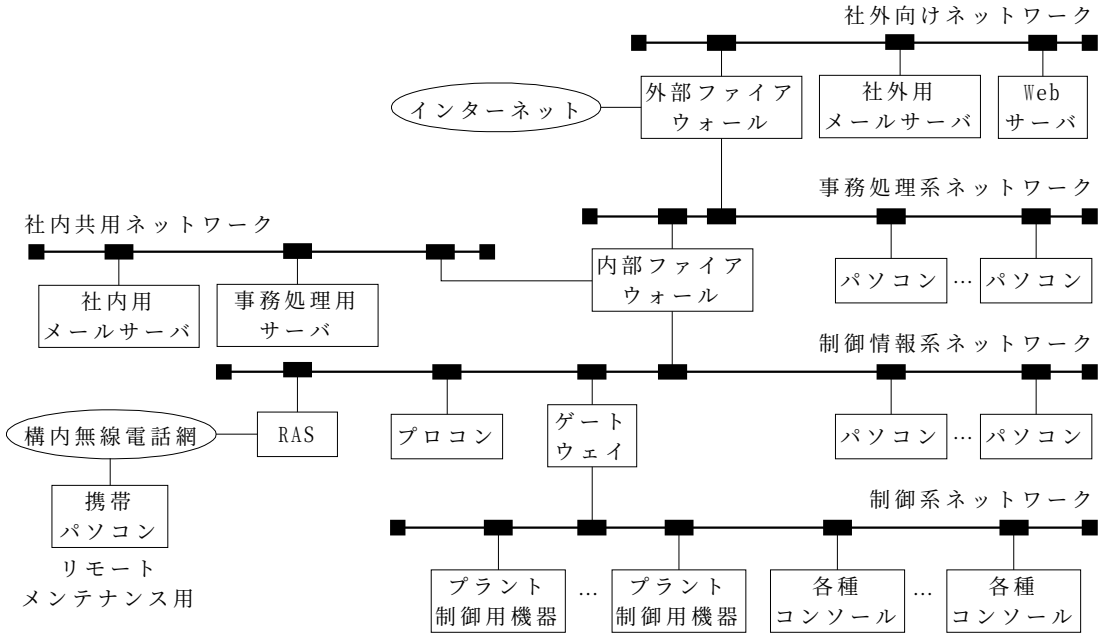


図２　本社部門の移転後のＡ社ネットワーク構成

表は，各ネットワークに対して要求されるセキュリティレベルをそれぞれの所管がまとめたものである。

表　各ネットワークのセキュリティ要件

区分	適用対象	所管	セキュリティ要求レベル		
			機密性	完全性	可用性
社外向けネットワーク	対象	情報システム部	低	低	低
事務処理系ネットワーク	対象	情報システム部	中	中	中
社内共用ネットワーク	対象	c	高	高	中
制御系ネットワーク	a	生産部門	中	高	e
制御情報系ネットワーク	b	d	高	高	高

注　適用対象は，情報セキュリティポリシの適用対象に含めるか含めないかを示す。

本社部門の移転の 5 か月前に，図３の情報セキュリティポリシが策定された。

Ⅰ．目的

情報資産（情報及び情報システム）の機密保護，運用及び保全に関する取扱いを定め，その方針や基準を明確化することによって，セキュリテイ（機密性，完全性及び可用性）を確保することを目的とする。

Ⅱ．適用範囲

① 当社に所有権又は管理責任のある情報資産，及びこれを利用又は管理する者（以下取扱者という）に対して適用される。

② プラントを制御する情報システム（ハードウェア，ソフトウェア及びネットワーク）のうち，制御系ネットワークで稼動するものは適用対象外とする。

（途中省略）

Ⅴ．情報資産の重要度分類

（1）情報は，次の三つの機密レベルに分類して取り扱う。

① 極秘　：関係者以外への配布を禁止する。ネットワークを経由して配布，共有する場合，暗号化などによる秘匿化措置やアクセス制御を実施しなければならない。

② 取扱注意：社外への配布を禁止する。ただし，事前に管理責任者の許可を得て，ネットワークを経由して社外へ配布する場合，暗号化などによる秘匿化措置を講じなければならない。

③ 一般情報：取扱いに制限はない。

なお，電子メールの利用は，ネットワークを経由した配布に該当する。また，社外へ電子メールを送付する場合は，上司に控え（ブラインドカーボンコピー）を送付しなければならない。

（2）情報システムは，次の三つの可用性レベルに分類して取り扱う。

① 無停止　：安定稼働を最優先したホットスタンバイ構成にする。稼働状況の監視を常時実施する。

② 即時復旧：費用対効果を勘案するが，安定稼働を重視したコールドスタンバイ構成にする。稼働状祝の監視を定期的に実施する。

③ 通常復旧：費用対効果を勘案した構成にする。稼働状況の監視は，必要に応じて実施する。

（途中省略）

Ⅷ．運用管理項目

① 情報資産へのアクセス管理と取扱者の認証を適宜行わなければならない。

② 情報システムは，適切に設計され，維持管理されなければならない。

③ 情報システムを構成する機器類は，適切な場所と環境に設置し，維持管理されるとともに，定期的に保守されなければならない。

④ 情報システムが正常に稼働していることを把握しなければならない。

（途中省略）

付則：本情報セキュリティポリシの適用範囲は，施行 1 年後に見直すものとする。

図３　A社の情報セキュリティポリシ（抜粋）

〔情報セキュリティポリシの遵守状況の確認〕

B 課長は，情報セキュリティポリシが適切に運用されるように，次の二つの方策を検討し，本社部門の移転後に実施することにした。

インターネットからの不正侵入による脅威が増大し続けているので，年 1 回，外部の専門家によるペネトレーションテスト（疑似侵入攻撃）を実施し，ファイアウォールによる対策に不備がないかどうかを検証することにした。

また，電子メールの適正な利用を推進するため，社外に送信する電子メールであて先に上司が含まれていない（ブラインドカーボンコピーがない）場合，送信を保留して本人へ返送する仕組みを導入することにした。また，これを導入するに当たって，［ f ］の問題で会社と社員との間にあつれきが生じないように，事前に周知することにした。

〔事故の発生〕

本社部門の移転後，しばらくしてプロコンのデータが一部消失するという事故が発生した。調査の結果，次のことが分かった。

（1） 本社部門の移転時にプラントのメンテナンス用機器が盗まれ，その機器を利用して RAS 経由で不正侵入された。RAS への接続には構内無線電話が利用されており，安全であるとの認識から，接続時に ID とパスワードの設定はなかった。しかし，工場の外壁の外側からテストしたところ，RAS への接続が可能であった。

（2） メンテナンス用機器の利用者は，盗難に気付いていたが報告していなかった。

（3） プロコンの管理者用の ID とパスワードが容易に推測できるものであった。また，プロコンの OS のセキュリティに関する設定が初期値のままであった。

（4） プロコンに保管されている各種構成情報からゲートウェイのアドレスが発覚し，攻撃を仕掛けられたが，侵入までには至らなかった。

〔対策の実施〕

事故発生後，次の対策を講じた。

（1） メンテナンス用機器の紛失時の連絡体制を整備し，周知徹底した。

（2） RAS 及びプロコンの ID とパスワードの管理方法を見直した。

（3） プロコンの OS に対する設定を見直した。

今回の事故を通じて，B 課長は，情報セキュリティを確保する上でのポイントは何であるかを痛感した。

設問１　本文中の［ a ］～［ f ］に入れる適切な字句を答えよ。

設問２　情報セキュリティ対策に関する次の問いに答えよ。

（1） B 課長は，W 主任の提示したスケジュールでは，“ 作業が完了しない項目がでるおそれがある ” と考えた。そのような作業項目を 15 字以内で述べよ。

（2） W 主任は，情報セキュリティポリシの策定に当たって，B 課長の期待どおりに活躍しているが，それはどのような点か。二つ挙げ，それぞれ 30 字以内で述べよ。

（3） B 課長は，経営会議の質疑応答で，“ 自分たちが中心となって作成したい ” と答えている。B 課長のねらいは何であるか。50 字以内で述べよ。

設問３　電子メールの情報セキュリティ対策に関する次の問いに答えよ。

（1）情報セキュリテンポリシの導入によって，従来からのウイルス対策の効果が一部低下するおそれがある。それは現在の運用方法から考えてどのような点か。30 字以内で述べよ。

（2）電子メールの適正な利用を推進するための対策について，運用上の課題を二つ挙げ，それぞれ 30 字以内で述べよ。

設問４　不正侵入に関する次の問いに答えよ。

（1）W 主任は，ほかのネットワークと比較して制御系ネットワークのリスクが小さいと分析した。その理由を二つ挙げ，それぞれ 15 字以内で述べよ。

（2） プロコンに対する対策は，不正侵入防止という点から不十分である。とるべき対策を 20 字以内で述べよ。

設問５　B 課長は，今回の事故を通じて，A 社の情報セキュリティを向上するために改善すべき内容とその解決策は何であると考えているか。改善すべき内容を 30 字以内で述べよ。また，その解決策を 70 字以内で述べよ。