**問4**　情報セキュリティ技術者の育成に関する次の記述を読んで，設問1～4に答えよ。

K社は，従業員数9,000名の機械製造会社であり，本社の他，全国に工場が8か所，営業所が10か所ある。図1に示すとおり，K社には本社，工場及び営業所を接続した社内ネットワークが構築されており，全社でサーバが200台，PCが5,000台接続されている。社内ネットワーク，サーバ及びPCの運用管理は，主として本社に勤務する情報システム部員が担当しているが，各工場にも情報システム部員を配置して，現地でなければ実施できない運用管理を行っている。

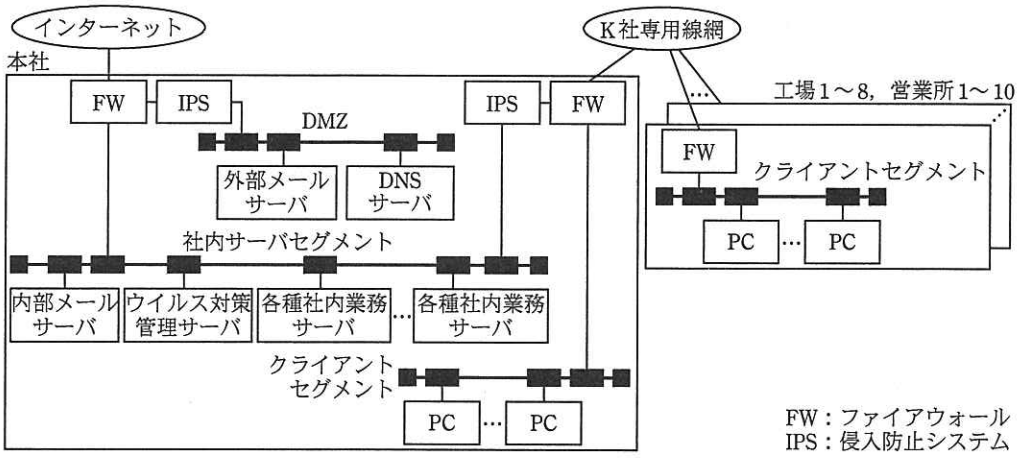


**図1　K社ネットワーク全体構成図**

全てのPCにはウイルス対策ソフトが導入されており，図1中のウイルス対策管理サーバは，このウイルス対策ソフトの管理とウイルス定義ファイルの配信を行っている。ウイルス対策ソフトはウイルス定義ファイルに基づきパターンマッチングによってウイルスを検出するものであり，ウイルス定義ファイルは最低でも1日に1回は更新されている。

〔K社の情報セキュリティ対策の現状〕

K社では過去に多くの情報セキュリティインシデントが発生しており，そのうちの幾つかはK社の製品に関する機密情報の窃取を狙ったものと推測されている。K社ではこの事態を重くみて，2年前，総務部内に総員10名の情報漏えい対策チーム（以下，

P チームという）を常設組織として設置し，文書，口頭，ネットワークなど，全ての経路での情報漏えいの予防及び情報漏えい発生時の緊急対応を実施してきた。この P チームは，幾つかの班に分かれており，そのうちの技術班のリーダが T 主任である。

〔標的型攻撃への対策の検討〕

T 主任は，K 社を取り巻く最近の状況から，悪意あるプログラムを電子メール（以下，メールという）の添付ファイルとして送付してくる攻撃に注意が必要であると考えていた。特に，①メール本文やタイトルに K 社に関連した内容が含まれるなど高度な偽装が施されており，かつ，②新たに作成された悪意あるプログラムを含んだファイルが添付されている，いわゆる標的型攻撃メールに対して危機感を持っており，その対策について検討を始めていた。

検討を進める中で T 主任は，セキュリティコンサルティング会社から，標的型攻撃に対応する演習のための教材一式を入手することができた。その教材には，実際に標的型攻撃に使用されたメール及び攻撃用プログラムを基にした，メール本文例及び疑似攻撃プログラムであるプログラム S が含まれていた。教材は，演習用環境で不正な通信が発見されてから，その通信が発生した原因を突き止めるまでの演習を対象範囲にしている。T 主任は，この教材を利用して P チーム内で標的型攻撃に対応する演習を行い，その結果に基づいてインシデント対応方法の改善を目指すことにした。

〔標的型攻撃に対応する演習の準備〕

T 主任は演習の対象者として，P チーム内で 1 年間ほどインシデント対応を担当している U 君を選抜した。この演習に当たって，T 主任は図 2 に示す演習用環境を構築した。

なお，この演習用環境は他の全てのネットワークから切り離されている。

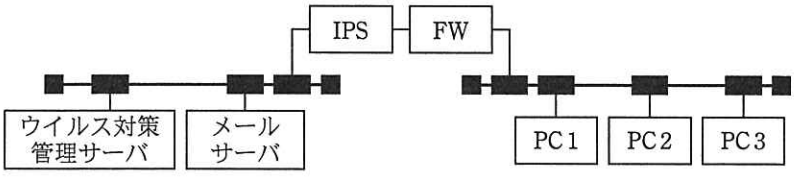


**図 2　演習用環境**

また，インシデント対応において必要になる可能性が高いと考えて，図 2 の環境とは別にパケットキャプチャ装置を用意して解析用の隔離環境を整えた。

T 主任は，演習用環境内の PC1 が標的型攻撃に遭遇した状況を作るために，図 3 に示す準備を行った。演習に使用したプログラム S の動作は図 4 のとおりであった。ただし，図 3 及び図 4 の内容は U 君には知らせなかった。

(1) 教材のメール本文例を参考に，K 社に関連した内容を含んだ標的型攻撃用メールを作成した。
(2) 標的型攻撃用メールには，プログラム S を添付した。プログラム S は実行形式であるが，受信者のメールソフト上では文書形式ファイルのアイコンが表示されるように偽装している。
(3) 標的型攻撃用メールを，PC2 からメールサーバ経由で PC1 の利用者のメールアドレス宛てに送信した。送信に当たっては社内の実在するメールアドレスからの送信であるように偽装した。
なお，他のメールも 100 通ほど送信し，標的型攻撃用メールが他のメールに紛れるようにした。
(4) 各 PC にはウイルス対策ソフトを導入した。さらに，演習で用いるウイルス定義ファイルを使用した場合でも，プログラム S がウイルスとして検出されないことを確認した。
(5) プログラム S が動作する際の通信が，IPS によって不正な通信として検出されることを確認した。
(6) 演習の開始直前に PC1 にログインしてメールを受信し，メールの添付ファイルであったプログラム S を実行した。

**図 3　演習の準備**

(1) 実行すると，利用者に気づかれないように PC に常駐する。
(2) 自セグメント及び近隣のセグメントに接続されたコンピュータにアクセスを試みる。その際に，相手のコンピュータのセキュリティホールを利用する。
(3) (2)でアクセスに成功したらファイルの取得を試みる。ファイルが取得できたら，そのファイルを攻撃者のメールアドレスに送信する。
(4) 他のコンピュータに自身をコピーして，常駐させる。ただし，演習用なので，コピーする台数，世代数には制限を設けている。また，指定された期日を過ぎると動作を停止する。
(5) リムーバブルメディアが接続されたことを検知して，利用者に気づかれないように他のコンピュータへの感染経路として利用する。

**図 4　プログラム S の動作**

〔標的型攻撃に対応する演習〕

演習用環境の準備を整えた後，T 主任は U 君に演習の開始を告げた。次は，その時の会話である。

T 主任：それでは演習を開始します。この後 IPS が不正な通信を検出するので，その検出をきっかけにインシデント対応を実行してみてください。

U 君　：はい。本番だと思ってやってみます。

T 主任：早速 IPS で不正な通信が検出されたようですよ。

対応を開始した U 君は，まず IPS による不正な通信の検出結果を確認した後，ウイルス対策管理サーバ，FW 及び IPS のログ分析を開始した。

FW 及び IPS のログ分析の結果，U 君は PC1 からメールサーバに対して不審なアクセスが行われていると思われるログを発見した。次は，その時の会話である。

T 主任：ここまでの演習で，標的型攻撃への理解は深まりましたか。

U 君　：はい。ウイルスとしては検知されないんですね。こうなると，PC1 に原因があるとは即座に絞り込むことができないので，IPS での誤検知や送信元 IP アドレスの IP スプーフィングの可能性も調べないといけませんね。

T 主任：そうですね。ただ，PC1 から不審なアクセスが行われている可能性があると分かった時点で，PC1 を早めに切り離した方がよかったのではないでしょうか。

その後，U 君は PC1 を演習用環境から切り離す措置をとった。切り離した PC1 は，解析用の隔離環境に接続し，PC1 の解析を行った。2 時間ほどしたところで U 君が行き詰まっているのに気が付いた T 主任は，U 君に声を掛けた。

T 主任：どうやら苦戦しているようですね。

U 君　：解析用の隔離環境で行ったパケットキャプチャの結果全体と，パケットの送信元 IP アドレスを見て，PC1 から不正な TCP 通信が行われていることは確認できたのですが，PC1 でどのような悪意あるプログラムが動いているかが分かりません。起動中の常駐プログラム名の一覧を確認したのですが，正常な PC との差異はありませんでした。

T 主任：常駐プログラムに目を付けたのはいいけれど，プログラム名を見ただけでは十分とは言えませんね。プログラム名ぐらいは簡単に偽装できますよ。

U 君　：そうなんですか。では，悪意あるプログラムを特定するには，何を糸口にすればよいのでしょうか。

T 主任：パケットキャプチャの結果を分析すれば，不正な通信の詳細情報が分かりま

す。その情報の中には，当然 TCP セッション情報が含まれていますよね。それが糸口になりませんか。

U 君　：なるほど。今の話で③悪意あるプログラムを特定する方法を思い付いたので解析作業に戻ります。

T 主任：ところで，本番のインシデントでは証拠保全の必要があります。PC1 は重要な証拠であり保全の対象となるので，本来であれば PC1 の複製を使用して解析を行うことになります。今回は演習なので証拠保全の措置は省略しましたが，インシデント対応手順を考える上で証拠保全は必要な措置となるので覚えておいてください。

U 君　：はい，分かりました。

この後 U 君は，下線③の方法を使って悪意あるプログラムを特定し，さらに PC1 の利用者のメールアドレス宛てに到着したメールの中から不審な添付ファイルを見つけ出した。利用者がこの添付ファイルを実行したことによって悪意あるプログラムが常駐してしまい，他のコンピュータへの不正な通信を行っていたことを突き止めた。

〔演習の振返り〕

U 君　：今回は何とか不審な添付ファイルを見つけることができましたが，メール本文は総務部からの社内連絡を装っている上，送信元のメールアドレスも実在するものであり，添付ファイルのアイコン偽装以外は不審な点は一切見当たりませんでした。実際の状況を想定してみると，標的型攻撃は，発見が難しいものなんですね。

T 主任：そうなんです。この演習は他社で過去に起きた事例を参考にしたものです。だから，当社にもこの程度の攻撃があると想定しなければいけません。このような標的型攻撃による被害を未然に防ぐためには，全従業員への指導も併せて行っていく必要があるのです。

演習の後，U 君は従業員が社内ネットワーク上の PC で今回のような標的型攻撃メールを受信して添付ファイルを実行してしまった場合，どのような被害が発生するか，その被害への対応をどうすべきかを検討して，インシデント対応手順にまとめた。ま

た，インシデント対応のため，PC を LAN から切り離して解析作業を行っている間に，その PC の利用者から内蔵ハードディスク内のファイルが欲しいと言われる可能性が高いと考えた。そこで，証拠保全が可能な方法によって PC を複製した後に，④複製した PC からファイルを取り出す手順をインシデント対応手順に記載した。さらに，インシデントを未然に防ぐための標的型攻撃対策を作成した。

その後，T 主任はインシデント対応手順及び標的型攻撃対策を承認し，P チーム内の正式ドキュメントとして発行した。標的型攻撃対策に基づき，P チームは全従業員に対して標的型攻撃に関する指導を行った。K 社では，このような対策の効果もあり，標的型攻撃による被害を未然に防ぐことに成功している。

**設問 1**　攻撃者が本文中の下線①及び下線②のような細工をする目的を，下線①について 40 字以内，下線②について 30 字以内で述べよ。

**設問 2**　本文中の下線③の悪意あるプログラムを特定する方法とは何か。その方法を 50 字以内で述べよ。

**設問 3**　本文中の下線④について，ウイルス感染を広めることのないように，利用者が必要とするファイルを PC から取り出すにはどのような方法をとればよいか。その方法を 50 字以内で具体的に述べよ。ただし，取り出すべきファイルはウイルスに感染していないものとする。

**設問 4**　本文中の下線①及び下線②の特徴を持った標的型攻撃メールを受信した場合の被害を回避するためには，従業員にどのような指導を行えばよいか。添付ファイル付きメールの取扱いについて指導すべき内容を 40 字以内で述べよ。