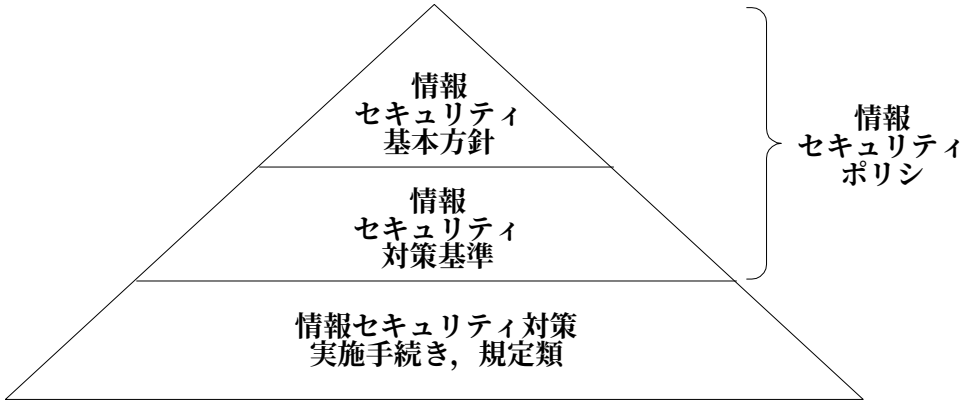
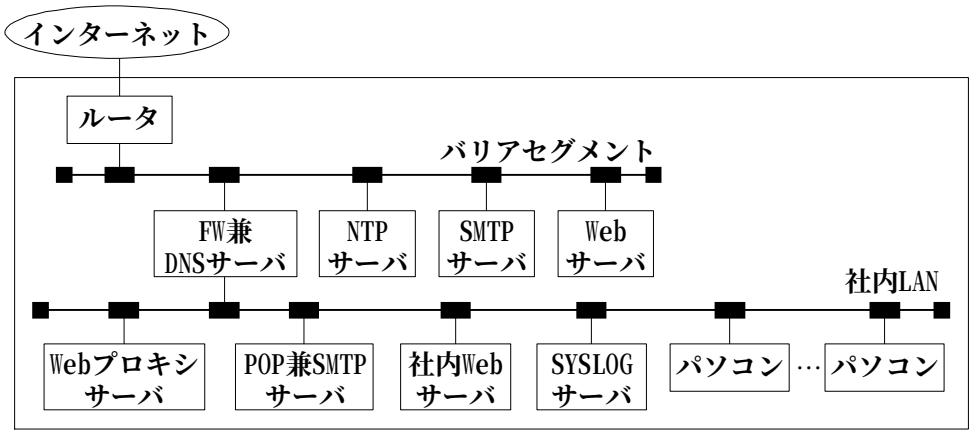
平成１５年度　秋期　情報セキュリティアドミニストレータ　午後Ⅱ問題

情報セキュリティポリシの位置づけ



問１　セキュリティ事件への対応に関する次の記述を読んで，設問１～５に答えよ。

A社は，社員数が 300 名ほどの健康食品の輸入と販売を行う商社である。これまで，A社では，Web を利用した商品の宣伝や社外との電子メール（以下，メールという）のやり取りのために，インターネットサービスプロバイダ（以下，ISP という）が提供する小規模事業者向けの各種のサービスを利用してきた。具体的には，ダイヤルアップによるインターネット接続サービス，ISP が提供する Web サーバのホスティングサービスやメールアカウント利用サービスなどである。しかし，ダイヤルアップによる接続では，顧客とのメールのやり取りが遅れがちで業務に支障が出始めていた。そこで，昨今，高速なインターネット常時接続サービスが低価格で利用できるようになってきたことや，A社内の情報システムの拡充に伴って情報システム課の課員が増強されたことなどから，自社内に Web サーバやメールサーバなどのインターネット向け情報システム（以下，新システムという）を構築し，インターネットに常時接続することにした。A社の情報システム課のB課長をリーダとする 3 名でチーム（以下，構築チームという）を組み，新システムの構築を推進することになった。図１に，新システムの構成を示す。



FW：ファイアウォール
注　SYSLOGサーバは，新システムの構成要素が出力するSYSLOGを収集し，蓄積する。

図１　新システムの構成

構築チームによる検討の結果，新システムは，図２に示すような方針で運用することにした。

（1）ルータ
・DNS サービス，SMTP サービス，HTTP サービス及び NTP サービスに必要のないインターネットからの通信は，ルータですべて遮断する。
（2）FW 兼 DNS サーバ
・FW 兼 DNS サーバ上で FW 機能及び DNS サービスを提供する。
・インターネット側からの DNS の問合せに対しては，バリアセグメントの情報だけを返す。
・社内 LAN からの DNS の問合せに対しては，バリアセグメント，社内 LAN 及び外部ドメインに関する情報を返す。
・インターネットから社内 LAN へのアクセスは，FW 機能ですべて遮断する。
・バリアセグメントから社内 LAN へのアクセスは，SMTP サーバから POP 兼 SMTP サーバへの SMTP による通信と，バリアセグメント上の各サーバから SYSLOG サーバへの SYSLOG による通信だけを許可し，それ以外は FW 機能で遮断する。
（3）NTP サーバ
・NTP サーバを設置し，ISP が提供する時刻同期用のサーバと時刻を同期させる。
・バリアセグメントと社内 LAN 上の全サーバ，FW 及びパソコンは，NTP サーバと時刻を同期させる。
・NTP サーバの運用及び保守は，社内 LAN から FW 兼 DNS サーバを経由する telnet 通信で行う。
・NTP サーバ上では，NTP サービスと運用及び保守に必要のないネットワークサービスをすべて停止する。
（4）SMTP サーバ及び POP 兼 SMTP サーバ
・社外から社内に送られてくるメールは，SMTP サーバで中継され，POP 兼 SMTP サーバに転送される。
・社内で交換されるメールは，POP 兼 SMTP サーバ上で処理される。
・社内から社外に送られるメールは，POP 兼 SMTP サーバから，SMTP サーバを経由して転送される。
・SMTP サーバの運用及び保守は，社内 LAN から FW 兼 DNS サーバを経由する telnet 通信で行う。
・SMTP サーバ上では，メールの送受信と運用及び保守に必要のないネットワークサービスをすべて停止する。
（5）Web サーバ（社外向けの情報発信）
・Web サーバを用いて，社外向けに情報発信を行う。
・Web コンテンツの更新時には，更新したいコンテンツをフロッピーディスクや CD－R などの記録媒体にいったん格納し，それを Web サーバのドライブに挿入して，データを更新する。
・Web コンテンツの更新を除く Web サーバの運用及び保守は，社内 LAN から FW 兼 DNS サーバを経由する telnet 通信で行う。
・Web サーバ上では，HTTP サービスと運用及び保守に必要のないネットワークサービスをすべて停止する。
（6）Web プロキシサーバ（社内からインターネット上にある Web を閲覧）
・社内 LAN 上のパソコンから，インターネット上にある Web を閲覧するためには，Web プロキシサーバを経由させる。

（7）SYSLOG サーバ
・バリアセグメント及び社内 LAN 上の各サーバが出力するログは，すべて SYSLOG サーバに転送される。SYSLOG サーバは，定期的に書き込み専用の記録媒体へログを出力する。
（8）そのほかの共通事項
・各サーバでは，毎日午前 3 時から早朝にかけて，バックアップを採取する。バックアップ媒体は，3 世代分を保管する。

図２　新システムの運用方針

情報システムへの投資に対する予算の制約もあり，必要なハードウェアやソフトウェアの選定，調達及び設定まで，構築チームがすべての作業を実施することになった。

〔新システムのぜい弱性の検査〕

3 か月ほどの期間を経て，新システムの構築がほぼ一段落した。そこで，構築チームのメンバである情報システム課のC主任が，新システムをインターネットに接続する前に，新システム全体の情報セキュリティの状況について確認することになった。

C主任は，新システムで利用する OS やアプリケーションソフトウェアに関連したぜい弱性の情報を集め，各種の設定ファイルの内容や修正パッチの適用状況などを調査した。その結果，Web サーバに関連するセキュリティ上の問題が二つ発見された。

次は，それらの問題に関するB課長とC主任の会話である。

C主任：新システムの Web サーバで，セキュリティ上の問題が二つ発見されました。インターネットに接続する前に，これらの問題を解決しておく必要があります。

B課長：それはどのような問題かね。もう少し具体的に説明してほしい。

C主任：一つは，クロスサイトスクリプティング（以下，XSS という）と呼ばれるぜい弱性に関する問題です。このぜい弱性を悪用されてしまうと，［　a　］といった被害の発生する可能性が考えられます。

B課長：それは大きな問題だな。この問題を解決するには，どのような対策を実施すればよいのだろう。

C主任：XSS の問題を解決するためには，幾つかの対策を実施しなくてはなりません。詳細は，改めて文書で報告いたしますが，一つだけ例を挙げますと，Web ブラウザからのリクエストに対して Web サーバが返す Web コンテンツ中に［　b　］が存在した場合には，それらに対する［　c　］処理を Web サーバが実施しなければならないといったことがあります。

B課長：ほかにも問題はあったのかね。

C主任：もう一つは，バッファオーバフロー（以下，BOF という）と呼ばれるぜい弱性に関する問題です。このぜい弱性を悪用されてしまうと，遠隔地からインターネットを経由した不正な［　d　］や，［　e　］といった被害の発生する可能性が考えられます。

B課長：それでは，新システムへの移行時期を少し延期した方がよさそうだな。

C主任：2 週間ほど時間をいただけないでしょうか。その間に，XSS や BOF の対策として必要な修正を加えた上で，再度，確認試験を行いたいと思います。

B課長：分かった。それでは，担当役員を通じて取締役会に報告し，承認を得た上で延期することにしよう。

〔新システムへの移行〕

2 週間ほどたって，C主任からB課長に Web サーバで発見されたぜい弱性への対策を終了したとの報告があった。B課長は，その結果を担当役員を通じて再度取締役会に報告し，新システムへの移行について承認を得た。

この承認を受けて，A社では，新システムへの移行が実施された。B課長は引き続き新システムの運用責任者に任命され，構築チームは解散した。新システムでは，インターネットとの常時接続や回線速度の増強などが実現され，顧客や社員に極めて好評であった。新システムへの移行が終了してから数週間は，大きなトラブルもなく，順調であった。

〔事件の発生〕

新システムに移行してから数週間が過ぎたある日，某社（以下，X社という）のサイト管理者からA社のサイト管理者のメールアドレスあてに，図３に示すようなメールが届いた。

To：root@A-Company.co.jp
From：root@X-Company.co.jp
Subject：貴社ホストからの不審なアクセスについて
Date：20 Mar 2003 16:47:46 +0900

私は，X社のサイトを管理している者です。
この 1 週間ほど，貴社サイト内のホスト（Web サーバ）が発信源と推測できる不審なアクセスを観測し続けています。アクセスの内容は，当社の DNS に登録している外部公開サーバ群に対するポートスキャンです。
これまでのところ，当社ホストには不正侵入といった深刻な被害は発生しておりませんが，貴社ホストが何者かに悪用されている可能性がありますので，状況を調査していただくとともに，不審なパケットの送出を停止していただくようお願いいたします。
下記に，当社のルータで捕そくした貴社ホストからのアクセスのログを添付いたします。
（以下，ログは省略）

図３　X社のサイト管理者から届いたメール

このメールは，直ちに情報システム課のメンバに伝達され，状況調査が行われた。図４に，新システムの状況調査の結果を示す。

（1）インターネットに接続するルータ自身には，不正アクセスを受けた形跡はない。
（2）Web サーバ上に隠しディレクトリが作られており，その中に構築チームのだれも知らないデータファイルが置かれていた。
（3）FW 兼 DNS サーバには，不正アクセスを受けた形跡はない。

図４　新システムの状況調査の結果

C主任は，①Web サーバに置かれていた不審なデータファイルを削除し，再度 Web サーバ上の OS やアプリケーションソフトウェアについて，各種の設定ファイルの内容や修正パッチの適用状況などの確認作業を行ったが，ほかに問題は発見できなかった。

〔事件の再発〕

C主任が確認作業を行ってから数時間後に，Web ページを見た顧客からの連絡で，Web サーバのコンテンツが改ざんされたことが分かった。インターネットに接続した状態では更に何が起こるか分からなかったので，C主任は，B課長と相談の上，Web サーバのネットワーク接続を一時的に切断し，徹底的な原因の究明を行って，再発防止の対策を実施することにした。

B課長は，直ちに情報システム課のメンバを召集して対策会議を開いた。しかし，このような事件に対してどのようなステップで対応すべきかについて，経験のあるメンバがおらず，明確な対策を打ち出せずにいた。

そこで，B課長は，このような事件に対する一般的な対応手順について，C主任に至急情報を収集するように命じた。C主任は，情報システム課のメンバの D 君と協力して情報を収集し，図５に示す一般的な対応手順を取りまとめ，B課長に報告した。

(1) 責任者及び担当者への連絡
　セキュリティ事件は，だれが発見するか分からないので，事前に緊急時の連絡先を定めておくこと。事件を発見した者は，直ちに定められた連絡先の担当者に状況を報告して適切な指示を受けること。責任者は，事前に定めた手順に沿って対応すること。もし，手順が定められていなければ，(2) 以降の記述を参考にして対応すること。
(2) 事実の確認
　セキュリティ事件の内容や状況などについて，事実関係を明らかにすること。
(3) システムの利用状況の記録とハードディスクの内容の保存
　後日の調査及び対応処置に備えるために，事件を発見したら，なるべく早い段階で，システムの利用状況を記録し，ハードディスクの内容を保存しておくこと。
(4) ネットワーク接続の遮断又はシステムの停止
　不正侵入が継続しているなど，他システムへの影響や被害の拡大が想定される場合には，ネットワーク接続を遮断するか，システムを緊急に停止すること。
(5) 影響範囲の特定
　どのような範囲に対して，どのような影響が生じたのかを正確に把握すること。
(6) 関係サイトへの連絡
　自組織のサイトを踏み台にして不正にアクセスされたサイト又は自組織のサイトに不正にアクセスしてきたサイトに対して，事実の報告と対応の依頼を行うこと。
(7) 要因の特定
　ホストに対して不正にアクセスが行われた時間的順序を明らかにし，不正なアクセスの経路を特定すること。さらに，その経路から，不正なアクセスを許すきっかけになった要因を特定すること。
(8) システムの復旧
　システムが改ざんや破壊などの被害を受けた場合，又はそのような被害を受けていないという確証が得られない場合には，バックアップによるシステムの復旧又は初期インストール用のメディアによるクリーンインストールを実施すること。

（9）再発防止策の実施
　システムを事件発生前の状態に戻しただけでは，同じ事件が再発する可能性があるので，上記（7）で特定された要因を除去するための措置を講じること。
（10）監視体制の強化
　不正にアクセスを受けた場合には，同じ手口による不正なアクセスが再発する可能性が高いので，当面の間，そのようなアクセスに対する監視体制を強化すること。
（11）作業記録と作業結果の報告
　上記(1)～(10)の一連の作業記録を確実に保管し，作業結果を責任者に報告すること。

図５　セキュリティ事件発生時の一般的な対応手順

B課長は，C主任から報告を受けるとすぐに，新システムに関する事件発生時の全サーバ，ルータ及び FW を対象にした対応手順を，図５を参考にして検討するようC主任に指示した。図６に，事件発生時の対応手順の検討結果を示す。

（1）責任者及び担当者への連絡（省略）
（2）事実の確認
　①バリアセグメント上の全サーバ及び FW に関するログを調査し，不審なアクセスの記録について，アクセスの内容の確認を行う。
　②社内 LAN 上の全サーバについてログを調査し，上記①と同様の確認を行う。
　③社外向け及び社内向けの全サービスについて，異常の有無を確認する。異常があった場合には，その状況の調査を行う。
（3）システムの利用状況の記録とハードディスクの内容の保存
　①全サーバ及び FW について，ユーザのログインの状況，ネットワーク接続の状況及びプロセスの稼働状況を記録する。
　②全サーバ及び FW について，“ tar ”コマンドを用いてハードディスク内にある全ファイルのバックアップを採取し，保存する。
（4）ネットワーク接続の遮断又はシステムの停止（省略）
（5）影響範囲の特定（省略）
（6）関係サイトへの連絡（省略）
（7）要因の特定（省略）
（8）システムの復旧
　①保存されている最新のバックアップを用いて，システムの復旧を行う。
　②バックアップ採取時点から後の更新内容を，できる限り反映させる。
（9）再発防止策の実施
　①上記（7）で特定された要因を除去するために，不正にアクセスを受けたサーバに対して，設定ファイルの更新や修正パッチの適用などを実施する。
　②同じ手口による不正なアクセスが実行できないことを確認する。
（10）監視体制の強化（省略）
（以下省略）

図６　事件発生時の対応手順の検討結果

C主任は，B課長に図６の検討結果を報告して判断を仰いだ。B課長は，C主任が作成した②図６の対応手順を見て，二つの重大な技術上の問題点を指摘した。C主任は，B課長の指摘を受けて対応手順を修正し，直ちにその対応手順に従って対策を開始した。

翌日になり，Web サーバが復旧したところで，B課長が事件の経過を担当役員を通じて取締役会に報告したところ，情報セキュリティ対策に関する対応の不備について厳しい指摘を受けた。また，取締役会では，社長を委員長とする情報セキュリティ委員会を直ちに設置して，情報セキュリティポリシの策定をはじめ，総合的なセキュリティ対策を推進することが決議された。

設問１　本文中の［ a ］～［ e ］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　URL フィルタリング	イ　暗号化	ウ　エスケープ
エ　機密情報の漏えい	オ　コマンドの実行	カ　サービスの妨害
キ　メール中継	ク　メタキャラクタ	ケ　レイティング

設問２　本文中の下線①で実施した処置は，重大な誤りであった。そのため，A社が本来実施すべきであった対応を実施できない可能性がある。図６中の（5）に沿って，A社が本来実施すべきであったのはどのような対応か。A社の状況を踏まえて，80 字以内で具体的に述べよ。

設問３　B課長が本文中の下線②で指摘した二つの重大な技術上の問題点を，図６中から選び，それぞれ番号で答えよ。また，それらの問題点を回避するために実施すべき対応を，問題点の内容も含めて，それぞれ 80 字以内で述べよ。

設問４　図４に示した状況調査の結果だけでは，事件の影響範囲を特定し，再発を防止するには不十分であった。X社のサイト管理者からメールを受け取った時点で，更に調査の対象とすべきであった新システムの構成要素を，SYSLOG サーバ以外に二つ挙げ，図１中の字句を用いてそれぞれ答えよ。また，それらに対する調査の内容を三つ挙げ，図６中の字句を用いて，それぞれ 15 字以内で述べよ。

設問５　事件発生時のB課長の行動や判断には，情報セキュリティマネジメントを実施する上で問題がある。あなたがA社の担当役員から依頼を受けた情報セキュリティアドミニストレータであるとしたら，どのような点を助言するか。重大と思われる問題を二つ挙げ，B課長が本来実施すべきであった対応も含めて，それぞれ 70 字以内で述べよ。

問２　企業情報ネットワークの構築におけるセキュリティ対策に関する次の記述を読んで，設問１～５に答えよ。

N社は，従業員 400 名，年商 100 億円の中規模なコンピュータ周辺機器のメーカである。都心にある本社と郊外にある組立工場及び部品製造工場では，それぞれ LAN に接続されたサーバとパソコン（以下，PC という）を利用して，生産計画，生産管理及び在庫管理（以下，業務 AP という）を行っていた。N社では，本社と各工場間を必要の都度 ISDN で接続して，各サーバを参照していた。しかし，リアルタイムで頻繁に参照しようとすると，通信費が高くなるという問題があった。また，インターネットには，本社の限られた PC だけでしかアクセスできず，他社情報の収集に支障を来していた。そのため，本社と各工場間を通信事業者の IP-VPN で接続して，業務 AP を利用するN社企業情報ネットワークシステム（以下，Nネットという）を導入することにした。さらに，インターネットを利用して，取引先などとの電子メールの交換，Web での他社情報の収集，N社の企業情報や新製品情報の発信及び部品材料の購入手配（以下，新規 AP という）を行うことにした。

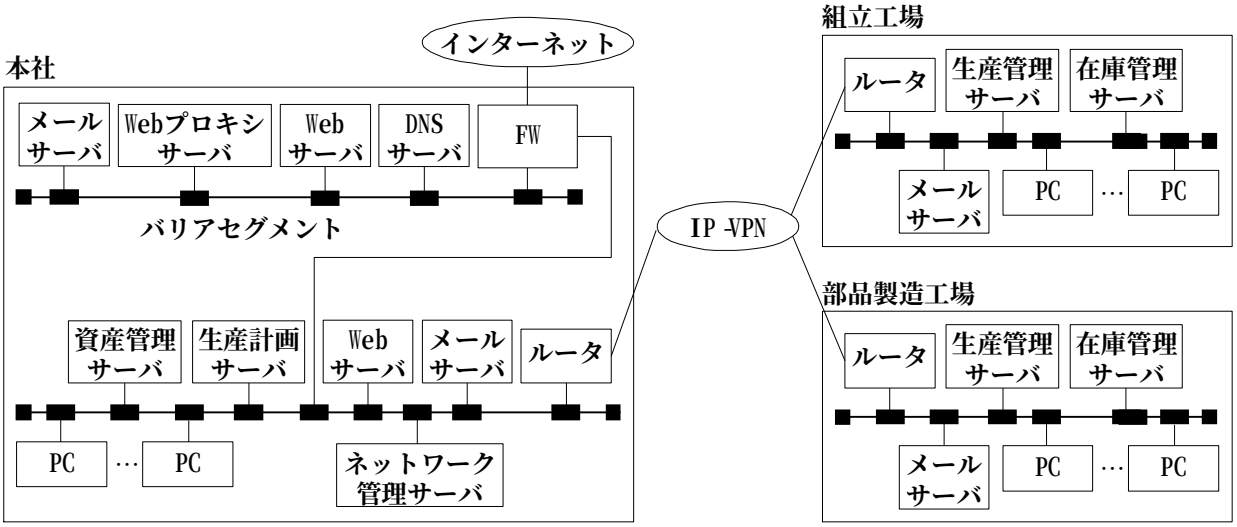
〔Nネットの基本検討〕

N社では，本社情報システム部のW部長をリーダとしたNネットの構築を行うプロジェクトチーム（以下，チームという）が，情報システム技術者，情報ネットワーク技術者のU君，情報ネットワーク管理者のX君及び情報セキュリティ管理者のY君で編成された。チームは，図１に示すNネットの技術要件をまとめた。

（1）　インターネットの利用には，インターネットサービスプロバイダと専用線で接続する。
（2）　外部の Web には，Web プロキシサーバを介してアクセスする。
（3）　N社の PC から本社や各工場のサーバにアクセスして，業務 AP を実行する。業務 AP は，既存のものを移植して使用する。
（4）　資産管理には，資産管理サーバを設置する。
（以下省略）

図１　Nネットの技術要件

U君は，図１の技術要件を基にして，図２に示すNネットの構成（案）の検討を行った。さらに，Nネットの業務 AP のトラフィックが，これまでの 2 倍に増加すると想定して設計条件を決定した。新規 AP のトラフィック条件については，類似した事例からベンダに推定してもらうことにした。



FW：ファイアウォール

図２　Ｎネットの構成（案）

〔Ｎ社の情報セキュリティポリシと情報セキュリティ対策の検討〕

Ｎ社では，部品の設計や生産計画のために，5 年前に PC を導入した。当時は，PC を利用する社員が限られていたので，情報セキュリティポリシを策定するほどではなかった。現在では，PC を利用する社員も増えてきたので，電子メールの私的利用，誤操作によって重要情報が流出する懸念及び残業時の不適切なホームページの閲覧という問題が指摘され，組織的な対応が必要になってきた。そこで，社長は，Ｎネットの導入に併せて，情報セキュリティポリシを策定することを指示した。

情報セキュリティ環境がＮネットの導入によって大きく変わるので，Ｗ部長は，Ｙ君に情報セキュリティポリシの作成及び情報セキュリティ対策要件の取りまとめを指示した。図３に，Ｙ君がＷ部長の指示の下で起案し，社長の承認を得たＮ社の情報セキュリティ基本方針，対策基準を示す。また，表１に，Ｙ君が取りまとめたＮネットの情報セキュリティ対策要件（案）を示す。

情報セキュリティ基本方針，対策基準

社長

Ⅰ．基本方針

社員など（派遣社員を含む）は，常に，N社の重要な資産である企業情報の機密漏えいの防止に努める。

（省略）

Ⅱ．対策基準

１．適用範囲

（1）本基準は，すべての社員などに適用される。

（2）本基準は，N社で利用するすべての資産（電子媒体及び紙を含む情報資産，ソフトウェア資産及び物理的資産）に適用される。

２．資産の分類及び資産管理

（1）資産には，重要度に応じて A～D のランクを付ける。設計情報,部品材料などの技術情報は，すべて重要性の高いランク A として扱う。

（2）社員などによる資産の利用は，職務遂行に必要な範囲に制限される。

（3）資産のライフサイクル管理のために，資産に関する情報をデータベース化する。

３．社内ネットワークとインターネットの利用

（1）社員などが社内ネットワークやインターネットを新たに利用する場合や利用条件を変更する場合には，所属長の許可を得て情報システム部に申請し，各サーバの利用者 ID と仮パスワードを得る。社員などは，仮パスワードを受領した後，［　a　］する。パスワードの長さは，特殊記号を含む英数字 8 文字以上とする。

（2）インターネットの利用は，電子メールと Web サイトへのアクセスに限定される。所属長又は管理者が内容を確認することがある。

４．社内ネットワークの運用

（1）インターネットからの不正侵入と攻撃に対する防御対策及びウイルス対策を行う。

（2）本社のネットワーク管理サーバで集中監視と運用管理を行う。

（3）情報セキュリティ管理者は，情報セキュリティマネジメントを適正に行う。

（4）情報ネットワーク管理者は，ネットワークの設定変更や管理を適正に行う。

５．外部委託

（1）請負事業者による資産へのアクセスは，社員の立会いの下で行い，社外への持ち出しを禁ずる。

（2）請負事業者との契約書には，守秘義務，情報セキュリティ及びリスクマネジメントに関する条項を盛り込む。

６．入退室管理

（1）ランク A の資産を扱うサーバやネットワーク管理サーバは，施錠された部屋に設置する。入室は，情報ネットワーク管理者，情報セキュリティ管理者及び特別に許可された者に限定する。入退室の際には，すべての記録をログに残す。

（省略）

９．罰則

本規定に違反する行為を行った場合には，就業規則によって懲罰を受ける。

以上

図３　N社の情報セキュリティ基本方針，対策基準

表１　Ｎネットの情報セキュリティ対策要件（案）

項目	情報セキュリティ対策要件
①FW のフィルタリング	パケットの流入出を制御する。
②本人認証	利用者 ID とパスワードで認証する。
③データベースのアクセス制御	データベース管理者が業務 AP のユーザに対し，適切なアクセス権を付与して管理する。
④不正侵入，DoS 攻撃の検知	不正侵入や DoS 攻撃などを検知するシステムを導入する。
⑤ウイルス対策	各 PC，各サーバに定期的に最新のウイルス定義ファイルを配付する。
⑥ネットワーク管理	本社で一元的に FW，ルータ及び各サーバの管理を行う。
⑦コンテンツフィルタリング	電子メールと Web サイトへのアクセスに適用する。
⑧トラフィック監視	インターネットと IP-VPN のトラフィックを監視する。
⑨資産管理	重要な資産のライフサイクル管理を行う。
⑩ネットワーク監査	ログ情報（上記①～⑨で採取）をネットワーク管理サーバに転送した後，保存して定期的にチェックを行う。

〔Ｎネットの情報セキュリティ対策の検討〕

チームは，Ｎネットを自社で設計及び運用することができるように，表 1 を基に検討を行った。まず，Ｎネットの監視と運用管理は，本社に業務を集中させて効率的に行うことにした。また，PC を利用する社員など（以下，PC ユーザという）がＮネットの各サーバに同じ利用者 ID でアクセスできるようにした。

Ｘ君は，PC ユーザに対して，申請のあったサーバへの仮パスワードを文書で連絡することにした。ただし，PC ユーザの多くが複数のサーバの利用を申請するようになった場合には，一つのアクセス制御サーバで PC ユーザを認証する［　b　］の適用を検討することにした。

次に，Ｘ君は，情報漏えいを防止し，不適切な情報を遮断するために，社外との間で送受される情報に対して，ワードブロック方式によるコンテンツフィルタリングを行うことにした。フィルタリングのソフトウェアでは，電子メールの文中で禁止字句を検出した場合，関連先（所属長など）にコピーを送信することにした。一方，Web サーバからダウンロードされたファイル中に禁止字句を検出した場合，URL と PC ユーザの IP アドレスをログ情報に残し，その旨のメッセージを情報セキュリティ管理者に送信することにした。情報セキュリティ管理者は，禁止字句のもつべき特徴を定義し，各部と協議して禁止字句を決定した。

以上の検討を基に，チームは，Ｎネットの機能要件をまとめ，Ｎ社と取引のあるベンダのＶ社と請負契約を結び，機器の調達，PC とサーバへの OS と業務 AP の導入及び設置を発注した。Ｖ社は，仕様を検討し，詳細な内容についてＮ社に問い合わせた。しかし，チームは，Ｖ社への発注において，機器の調達などが中心であると考えたので，情報セキュリティポリシに従って，セキュリティ関連情報を開示せず，Ｖ社に提案を求めた。Ｖ社は，Ｎネットの機能要件とＮ社へのヒアリングで得た情報に基づいて，Ｎ社のセキュリティ関連情報を経験から推測し，機器をリストアップしてＮ社に提示した。

〔V社による納入とN社での試験〕

V社とチームは，Nネットで使用する機器を決定し，N社への搬入，受入れ及び試験について打合せを行って，情報セキュリティ試験を含むNネットの受入プロセス（表2）について合意した。

表２　Nネットの受入プロセス

①受入基準の文書化	・搬入，受入時の検査項目及び試験項目の文書化
②移行に関する準備	（省略）
③PC ユーザへの説明	・Nネットの新機能及び切替スケジュールの説明
④類似環境での試験	・ベンダの環境における新規設備全体の搬入前試験
⑤パイロット試験	・ハードウェアの搬入と資産管理サーバへの機器の登録 ・ネットワーク機器の設定とインターネットの接続試験 ・試験データを用いた各サーバへのアクセス試験
⑥結合試験	・納入機器をすべて動作させ，機能と性能の確認 ・資産管理データベースへのデータの登録
⑦総合試験	・Nネットで想定されるトラフィックに基づいて作成した総合試験データによる，Nネット上での本人認証，アクセス制御，業務 AP 及び新規 AP の試験
⑧運用試験	・Nネットに既存の業務 AP と関連するファイルをコピーして並行運転 ・Nネットの情報セキュリティ対策要件（表1）の項目の確認 ・ネットワーク管理サーバを利用したネットワークの管理と監視 ・操作手順書の確認と修正 ・一定期間の安定稼働の確認
⑨本番への切替え	・運用試験での問題点を解決して，検収を終了

表２中の①～⑤のプロセスに，一部スケジュールの遅れがあったものの，表２中の④と⑤の試験結果が良好であったので，V社は，N社にこの状態のままで機器を納入したいと申し出た。Y君は，情報セキュリティ確保の観点から，V社が PC とサーバの OS と業務 AP の再インストールを行うべきであると主張した。しかし，V社は，これから再インストールを行うと納期が遅延すると回答した。W部長は，V社との契約書の条項を精査し，リスクに対応できると判断したので，社長にその旨を報告して，V社の申出どおり納入を認めた。社長には，V社との契約書にリスクマネジメントに関する条項が盛り込まれていると説明した。

V社とチームは，表２中の⑥の結合試験に移行し，納入機器をすべて動作させて，機能と性能を確認した。確認作業が終了した機器については，図４に示す資産管理データベースの項目に従って，データを登録した。

資産管理番号
１．資産情報
（1）管理情報
PC ユーザ名，設置場所，IP アドレス
（2）本体情報
PC 型名，製造ベンダ名，シリアル番号，ハードウェア構成，導入時期，利用期間
（3）ネットワーク情報
LAN カード，製造者名，インタフェース速度，MAC アドレス，導入時期
（4）OS 情報
OS 名，［　　ア　　］，製造者名，シリアル番号，導入時期
（5）汎用アプリケーションソフトウェア情報
ソフトウェア名，製造者名，導入時期，（省略）
（6）業務 AP 情報
生産管理クライアントプログラム名，稼働開始時期，（省略）
（以下省略）

図４　資産管理データベースの項目（ＰＣの場合）

その後，チームは，結合試験を終えて，V社の立会いの下で表２中の⑦の総合試験を行った。Nネットで想定されるトラフィックに基づいて作成した総合試験データを用いて，PC と各サーバが情報セキュリティ環境に適合するように設定を行った。チームが想定したとおりの結果が得られたので，N社は，X君，Y君及び各工場から本社に異動させた情報システム運用担当者（各 1 名）で編成されたネットワーク管理課による表２中の⑧の運用試験に移行し，V社は，電話で応対することにした。

〔ネットワークの運用試験〕

運用試験に移行した後は，リアルタイムでの各サーバへのアクセス，電子メールの利用及び Web サイトへのアクセスが好評で，PC ユーザ数や利用頻度が急速に増え続け，顧客による Web サイトへのアクセス数も増え続けた。そのため，ネットワーク管理サーバに大量のログ情報が収集されるようになった。しかし，ネットワーク管理課では，経験が不足していたので，これらの大量のログ情報の分析や対処が十分にできなかった。その結果，各サーバやネットワーク機器からの重要な警告を見落とし，障害が回避できない事態も起きた。障害には，外部からの DoS 攻撃の見落とし（外部へのアクセスができないという PC ユーザからの申告があるまで DoS 攻撃が検出できなかった）やデータベースの設定ミスによる PC ユーザのアクセス権違反の見落とし（ログ情報には警告が残っていたが，ほかのログに紛れてしまい検出できなかった）などがあった。このような障害が頻発したので，PC ユーザの不安や不満が増えてきた。

W部長は，情報セキュリティマネジメントが十分でないと考え，V社に対処を要請した。V社では，ログ情報のデータ量を削減して，重要なログだけを通報するように設定し，見落としによる障害が起きないように改善した。

その後，2 か月の運用試験を経て，W部長は，Nネットが安定稼働していると判断し，スキルのあるV社の要員によって一連の問題が解決したことと，本番運用へ切り替えることを社長に報告して検収を終え，チームを解散させた。

〔ネットワークの本番運用の開始〕

本番運用に入って，新たにNネットを利用するようになった PC ユーザから，社内ネットワークやインターネットを利用する際の PC の設定や不具合，各サーバのアクセス権限の付与や変更，コンテンツフィルタリングなどについて，問合せがネットワーク管理課に集中した。しかし，運用担当者が本社から各工場に出向いて運用業務を行っていたので，問合せに対して早急な対応ができなかった。このような状態が続いたので，ネットワーク管理課では解散したチームのメンバに協力を依頼したが，PC ユーザの不満は収まらなかった。

社長は，今後の安定した運用や障害の対策には運用管理体制の見直しが必要であると考えた。そこで，W部長に，運用試験の段階までに障害が予見できなかった原因の究明と，外部の派遣社員を活用した運用管理体制の改善を指示した。これを受けて，W部長は，PC ユーザからの問合せに対して，社内ネットワークの Web サーバに［ c ］を用意し，頻繁にある問合せを削減して，個別対応が必要な不具合に対応できるようにした。また，異動させた情報システム運用担当者を各工場に戻し，本社に経験のある派遣社員 1 名を配置することにした。

設問１　図３及び本文中の［ a ］～［ c ］に入れる適切な字句を答えよ。［ a ］，［ b ］については，それぞれ 10 字以内で答えよ。［ c ］については，5 字以内で答えよ。

設問２　資産管理データベースに関する次の問いに答えよ。

（1）図４中の［ ア ］に入れる適切な字句を二つ挙げ，それぞれ 7 字以内で答えよ。

（2）図４中の（1）～（6）のほかに，情報セキュリティマネジメントのために必要となる PC の資産情報の名称を，20 字以内で述べよ。また，その情報が必要になる理由を，45 字以内で述べよ。

設問３　コンテンツフィルタリングに関する次の問いに答えよ。

（1）禁止字句のもつべき特徴を二つ挙げ，それぞれ 20 字以内で述べよ。

（2）コンテンツフィルタリングを導入する前に，プライバシ保護の観点から，社員などに対して，どのような措置を行うべきか。40 字以内で述べよ。

設問４　Y君が，情報セキュリティ確保の観点から，PC とサーバの OS と業務 AP の再インストールを行うべきであると主張した理由は何か。40 字以内で述べよ。また，W部長が，リスクに対応できていると判断し社長に報告したのは，契約書にリスクマネジメントに関する条項としてどのような内容が盛り込まれていたからか。25 字以内で具体的に述べよ。

設問５　Ｎネットの運用に関する次の問いに答えよ。

（1）運用試験では，大量のログ情報が収集され，警告の見落としが起きた。このような見落としを防ぐためには，表２のＮネットの受入プロセスにおいて，どの段階でどのような試験をしておけばよかったか。60 字以内で述べよ。

（2）社長の指示に従って，外部の派遣社員を活用して業務を遂行するには，情報セキュリティに関する運用管理の観点から，どのような対策を実施すればよいか。二つ挙げ，それぞれ 60 字以内で具体的に述べよ。