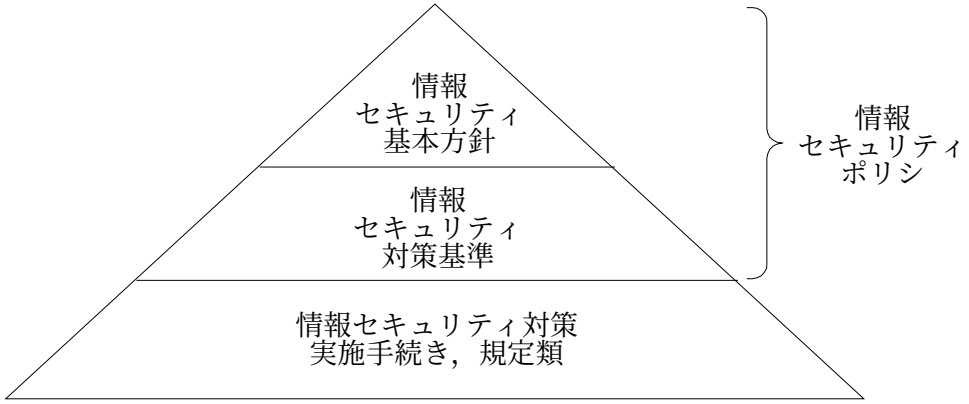
平成１４年度　秋期　情報セキュリティアドミニストレータ　午後Ⅱ問題

情報セキュリティポリシの位置づけ



問１　アンケート調査事業に関する次の記述を読んで，設問１～６に答えよ。

Ａ社は，顧客企業から依頼を受けて一般消費者向けのアンケートを実施し，市場調査を実施する会社である。従業員は 100 人ほどであり，ビルのワンフロアを借り切って事業を営んでいる。組織構成は，図１のとおりである。

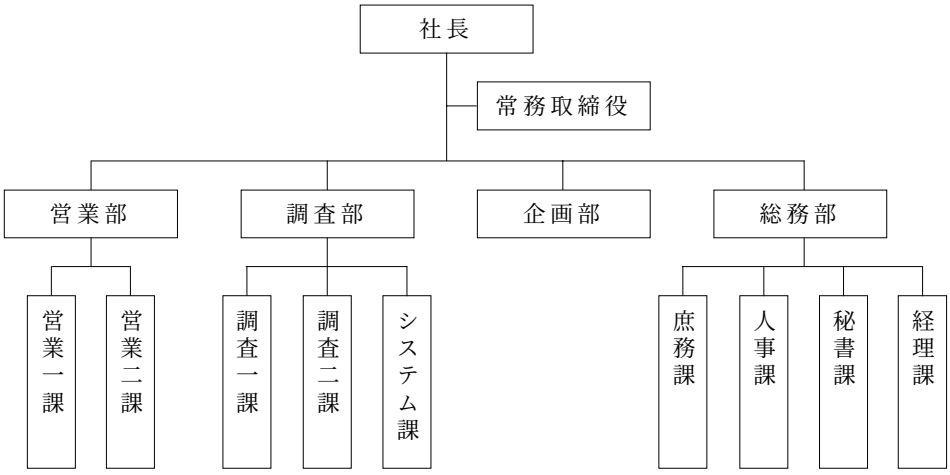


図１　Ａ社の組織構成

営業部は，顧客企業から詳細な条件を聞き出し，調査の進め方などに関する企画書と必要な費用を積算した見積書を作成する。調査部は，営業部に協力し，企画書や見積書の作成に必要な情報を営業部に提供する。受注に至ると，図２に示す作業手順に沿って業務を実施する。

(1)　アンケート調査票(以下，調査票という)の原案を作成し，顧客企業の要望を踏まえて加除訂正した上で調査票を確定する。
(2)　Ａ社が独自に情報主体から収集，又は顧客企業からの預託のいずれかの方法でアンケートの送付先候補リストを作成し，顧客企業の要望を踏まえて加除訂正した上で送付先を確定する。
(3)　郵送アンケートの場合
①　郵送物の印刷，封入及び投かんやアンケート結果のデータ入力を専業にしている B 社に調査票と送付先リストを預託し，リストに記載されたあて先に調査票を発送するように指示する。
②　アンケートの回答者から記入済の調査票がＡ社に送られてくると，その内容を確認の上，B 社に預託する。
③　調査票に記入された回答結果が B 社で電子化され，入力結果が一時記憶媒体に保管されて，調査票とともにＡ社に返却される。

④　B 社から電子化された回答結果を受け取ると，A社の調査部の担当者がA社のアンケート調査業務専用のサーバ(以下，専用サーバという)に，アンケート調査業務専用のクライアントパソコン(以下，専用 PC という)から入力する。専用サーバと専用 PC は，A社内に設置されており，通常の社内 LAN やインターネットとは独立したアンケート調査業務専用 LAN に接続されている。一時記憶媒体の内容は，入力終了後，直ちに消去される。

(4)　Web アンケートの場合

①　調査票を基にしてアンケート記入用の Web コンテンツを作成し，それを Web アンケート専用の Web サーバに掲載する。また，回答結果は，記入後，直ちにファイアウォールの内側に設置した安全な作業用サーバに転送することにし，Web サーバには，回答内容を一切保管しないように設定する。

②　アンケートを掲載した Web コンテンツの URL を，記入依頼及び記入要領とともに依頼先に電子メールを利用して送信する。

③　作業用サーバに蓄積された回答結果は，ネットワークを介さずに一時記憶媒体を用いて，専用 PC から専用サーバに入力する。一時記憶媒体の内容は，入力終了後，直ちに消去される。

(5)　市販の表計算ソフトを利用して統計処理を実施する。分析結果を報告書にまとめて顧客企業に納入し，調査業務を完了する。

図２　アンケート調査業務の作業手順

A社は，アンケート調査のために，独自に収集した一般消費者の個人情報データベースを作成して専用サーバに保管しており，これがA社の事業の競争力を維持する源泉になっている。

〔同業他社における事件の発生〕

ある日，A社の同業である C 社で，アンケートの送付先である一般消費者の個人情報が外部に漏えいするという事件が起きた。その結果，C 社は，顧客からの信頼を失い，長期間にわたって業績が悪化することが懸念された。この事件の報道記事を読んだA社の社長は，自社でも同様の事件が発生する可能性があると考え，緊急に予防対策を検討することにした。

社長の指示によって，企画部を事務局として，営業部長，調査部長，総務部長及びこれら 3 部の全課長を構成メンバとする個人情報保護対策検討委員会が組織され，委員長には，社長の特命によって常務取締役が就任することになった。

早速，第 1 回の会合が開催され，その場で，“ 個人情報保護に関するコンプライアンス・プログラム(以下，CP という)の要求事項 ” (JIS Q 15001)に沿ってA社内の個人情報保護体制を強化すること，次回の会合までに企画部長が具体的な作業手順を検討することが決定された。その決定を受けて，企画部長は，様々な資料を参照しつつ，図３に示す CP 構築の作業手順概要を作成した。

(1) 個人情報保護方針を定めて文書化する。
(2) CP 策定のための組織を編成する。
(3) CP 策定の作業計画を立てる。
(4) 個人情報保護方針を社内に周知する。
(5) 社内外の個人情報を特定する。
(6) 既存の個人情報取扱システム(規定，標準様式，体制など)を評価する。
(7) CP の構成を検討する。
(8) CP の基本になる規定を策定する。
(9) CP の詳細規定を策定する。
(10) CP を文書化する。
(11) CP に準じた体制を整備する。
(12) 役員及び従業員に対して，CP の [a] を実施する。
(13) CP に対する [b] を定期的に実施する。
(14) CP を見直し，改善する。

図３　ＣＰ構築の作業手順概要

企画部長は, 第 2 回の会合に図４に示すA社の個人情報保護方針案を提出し, 承認を得た。また, 個人情報保護対策検討委員会が CP を策定すること，次回の会合までに企画部長が CP 策定のための具体的な作業計画を立案することが決定された。

A社　個人情報保護方針

代表取締役社長　○○　○○

当社は，多数の個人情報を取り扱う企業の社会的責務として，個人情報の保護が当社の最優先課題であると認識しております。個人情報の保護を適切に実施するため，次の方針に沿つて安全対策を推進いたします。

(1) 個人情報の収集，利用及び提供に関する方針(省略)
(2) 個人情報に関連するリスクの予防及び軽減に関する方針(省略)
(3) 個人情報に関連する法令及びそのほかの規範の遵守に関する方針(省略)
(4) CP の継続的改善に関する方針(省略)

図４　A社の個人情報保護方針案(抜粋)

第 3 回の会合では，企画部長が作成した作業計画が承認され，具体的な作業が開始された。これまでA社では，業務で取り扱う情報の台帳類を全く作成していなかった。そこで，企画部長が用意した様式を用いて保護対象にしている個人情報をすべて特定するところから作業を始めることになり，営業部と調査部が保有する全個人情報を対象に調査し，表 1 に示すA社の個人情報取扱台帳を作成した。

なお，A社では，A社が独自に収集した個人情報，実施中のアンケート調査に関連する情報，顧客企業から特に保管を依頼された情報，及び法律で保管が義務付けられている情報を，すべて専用サーバ上に保管している。それらの情報を除くアンケート調査業務に関する情報は，プロジェクト完了とともに確実に消去，廃棄又は返却している。

表１　A社の個人情報取扱台帳(抜粋)

項目	XX に関するアンケート調査	YY に関する意識調査	…
個人情報	氏名，住所，電話番号，年齢など	氏名，住所，年齢，性別など	…
入手元	情報主体	顧客企業	…
入手の形態	Web アンケートによる直接収集	預託	…
取扱部署	調査部調査二課	営業一課経由で調査一課へ	…
情報の形態	専用サーバ上のファイル	預託を受けたフロッピーディスク上と，専用サーバ上のファイル	…
保管場所	専用サーバ	専用サーバ	…
保管期間	プロジェクト完了後 1 年間	プロジェクト完了まで	…
提供先	顧客企業	なし	…
廃棄方法	ファイル消去	フロッピーディスク返却とファイル消去	…
⋮	⋮	⋮	⋮

さらに，既存の個人情報取扱システムを評価するため，各種の社内規定類から関連する部分を抜き出して内容を確認した。図５に，一例として，サーバ運用規則における関連部分を示す。

第 4 章　バックアップ
第 23 条　重要な情報を収めたサーバは，別途定める期間ごとに定期的にバックアップ作業を実施すること。
第 24 条　バックアップ媒体は，3 世代管理を実施すること。
第 25 条　バックアップ媒体は，安全に保管すること。
第 26 条　バックアップ媒体は，耐用年数などを考慮して，定期的に新品に交換すること。
第 5 章　電源設備
第 27 条　(省略)

図５　サーバ運用規則(抜粋)

併せて，バックアップの実施状況を確認したところ，サーバ運用規則の第 4 章に沿って定期的にバックアップが実施されていた。また，バックアップ媒体は，調査部に備付けの施錠可能なキャビネットに保管されていた。キャビネットのかぎは，調査部長又は調査部長が不在の場合，あらかじめ指定された代行者が保管しており，自由にアクセスされることがないように管理されていた。

〔情報セキュリティマネジメントシステムの構築〕

ここまでの検討結果について，委員長が進捗報告を兼ねて社長に報告したところ，図6に示す社長からのコメントが個人情報保護対策検討委員会に寄せられた。

当社が保護すべき個人情報の範囲やそれらの取扱状況はよく分かった。だが，当社が実施すべき情報セキュリティ対策は，これまでの委員会での検討範囲だけで果たして十分なのだろうか。ほかにも実施すべき対策があるのではないか。個人情報保護については，大変重要なので引き続き検討を進めてほしい。加えて，当社が顧客の信頼を獲得し，事業を発展させる上で実施すべき情報セキュリティ対策を広く検討してほしい。

図6　社長からのコメント

この社長のコメントを受けて，委員会のメンバで調査，検討を重ねた結果，企業の情報資産を守るためには，情報セキュリティマネジメントシステム(以下，ISMS という)を構築することが重要であるとの結論に達した。そこで，個人情報保護対策検討委員会の名称を情報セキュリティ委員会に変更し，個人情報保護対策と ISMS の構築について，両者の整合を図りながら同時に進めることになった。進め方についての基本的な方針は，次のとおりである。

(1) 情報資産を保護するため，ISMS を構築する。個人情報もこの情報資産に含まれる。
(2) ISMS の適用範囲は，図7に示すとおりにする。ただし，ISMS を構築する中で必要に応じて調整する。
(3) ISMS の要求事項の一つである“準拠”の中に，個人情報保護に関する CP を位置付ける。

業　　務	：アンケート調査事業
組　　織	：調査部，営業部
場　　所	：A社所在地(ビルのワンフロア)
情報システム	：専用サーバ
情　　報	：アンケート調査事業にかかわるすべての紙文書，電子ファイルなど

図7　ＩＳＭＳの適用範囲

上記の方針を踏まえた上で，A社の ISMS の適用範囲に関連するリスクの概要を把握するため，ISMS の要求事項の実施状況を点検し，表2を作成した。

表２　ＩＳＭＳの要求事項の実施状況(抜粋)

要求事項	実施状況				判断根拠
	Y	P	N	N/A	
セキュリティ組織					
情報セキュリテイ･インフラストラクチャ					
・情報セキュリティについて検討するため，経営層を含む委員会を設置すること	○				c
・組織内の情報セキュリティを管理するため，関係する部門を横断的に調整できる体制があること	○				d
・個々の情報資産に対する保護責任及び特定の業務に関する実施責任を明確にすること		○			業務手順書やそのほかの規定類に業務の実施責任者が明示されていない。
⋮					
情報資産の分類及び管理					
情報資産に対する責任					
・情報資産を適切に管理するため資産台帳を作成し，重要な情報資産のすべてを登録すること		○			e
⋮					
通信及び運用管理					
情報システム管理					
・重要な情報及びソフトウェアのバックアップコピーを定期的に取得すること		○			サーバ運用規則は遵守されているが，その内容に不足がある。
⋮					
事業継続管理					
事業継続管理					
・ISMS の適用範囲全体を含む組織の事業継続計画を策定，維持するための管理プロセスを整備すること			○		該当する管理プロセスがなく，事業継続計画も災害復旧計画も存在しない。
⋮					

表２では，一番左側の列に ISMS の要求事項を，その隣に要求事項の実施状況と判断根拠を記すことにした。実施状況は，実施済の場合には Y 欄に，部分的に実施済の場合には P 欄に，実施していない場合には N 欄に，該当しない場合には N/A 欄に，それぞれ○印を記入することにした。

実施状況を評価した結果，既に適切な情報セキュリティ対策を実施している項目もあったが，問題点も指摘された。情報システムの構成要素のうち，専用サーバは輸入製品を使用しており，調達

に 1 か月を要する。ほかの構成要素は，通常の市販製品であり，2，3 日以内に調達可能である。調達に要する費用は，A社の事業規模からすれば，経営に深刻な打撃を与える額ではない。また，A社の事業の実態を考慮すると，被災による 1 週間程度の情報システムの停止は，許容範囲と考えられた。しかし，専用サーバ上に存在する一部のファイルは，A社の事業存続に不可欠であり，この点に関して大きな問題点が指摘された。

設問１　CP の要求事項によれば，A社が顧客企業から預託された個人情報を更に B 社に預託する際に，個人情報の管理について顧客企業に確認しなければならない点がある。それは何か。35 字以内で述べよ。

設問２　図 3 中の［ a ］，［ b ］に入れる適切な字句を答えよ。また，［ a ］，［ b ］の作業を実施しないことによって予想される悪影響を，それぞれ 15 字以内で述べよ。

設問３　本文中の下線に示した調査対象に関する次の問いに答えよ。

(1) 第 3 回の会合時点における調査対象だけでは，CP の要求事項が“保護すべき対象”として規定しているA社保有の個人情報の中で，収集できない対象がある。それは何か。15 字以内で述べよ。

(2) 上記(1)の情報を確実に収集するためには，どのような部署に記入を依頼すべきか。図 1 に示した組織名称の中から，最も適切なものを一つ選び答えよ。

設問４　表 2 中の［ c ］～［ e ］に入れる適切な字句を答えよ。

(1) ［ c ］，［ d ］については，A社の具体的な組織名称を用いて，それぞれ 35 字以内で述べよ。

(2) ［ e ］については，A社の情報資産の名称を用いて，30 字以内で述べよ。

設問５　アンケート調査事業を業務範囲と考えた場合に，ISMS の適用範囲に含まれるべき情報システムの構成要素に欠けているものがある。本文中の字句を用いて五つ挙げ，それぞれ 15 字以内で答えよ。

設問６　ISMS の構築に際しては，表 2 に示した要求事項について，具体的な実現方法を検討する必要がある。要求事項の一つである事業継続管理に関連して，火災などによるA社ビル内の情報システムへの甚大な被害発生を想定して次の問いに答えよ。

(1) 被害に遭った情報システムを 1 週間以内に確実に復旧し，A社のアンケート調査事業を維持するために実施しておくことが望ましい保護対策は何か。70 字以内で述べよ。

(2) 被災時に実施中のアンケート調査業務を継続させるため，更に対策を検討すべきリスクは何か。20 字以内で述べよ。

(3) 上記(2)のリスクを予防するためには，更にどのような対策を実施する必要があるか。30 字以内で述べよ。

問２　情報システムセキュリティの監査に関する次の記述を読んで，設問１～４に答えよ。

X 社は，中規模の部品製造会社である。X 社のもつ部品製造技術には定評があり，全世界の装置ベンダから部品の製造注文がある。X 社は，2001 年に米国の大手装置ベンダである Y 社と次世代の情報通信用装置の部品開発に関して提携を結んだ。総勢 30 名の特別プロジェクトチーム(以下，PT という)を組織編成し，開発を進めている。Y 社側も PT を組織編成している(図１)。X 社 PT では，設計システムを利用して部品のプロトタイプを製作している。両 PT は，設計のために，電子媒体を含むお互いの文書類を参照している。X 社 PT の LAN は，VPN で Y 社 PT の LAN と接続されている(図２)。PT のメンバと特別に許可された者だけが，特別プロジェクト棟に入棟できる。

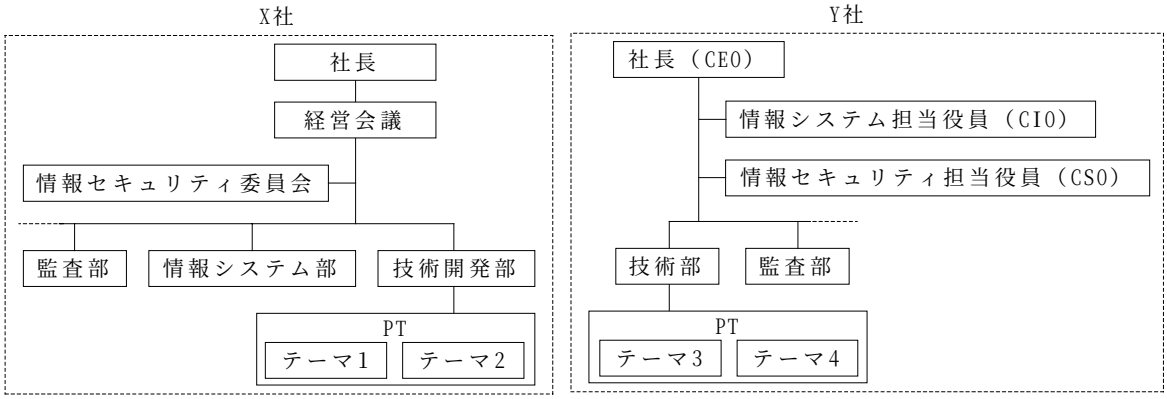
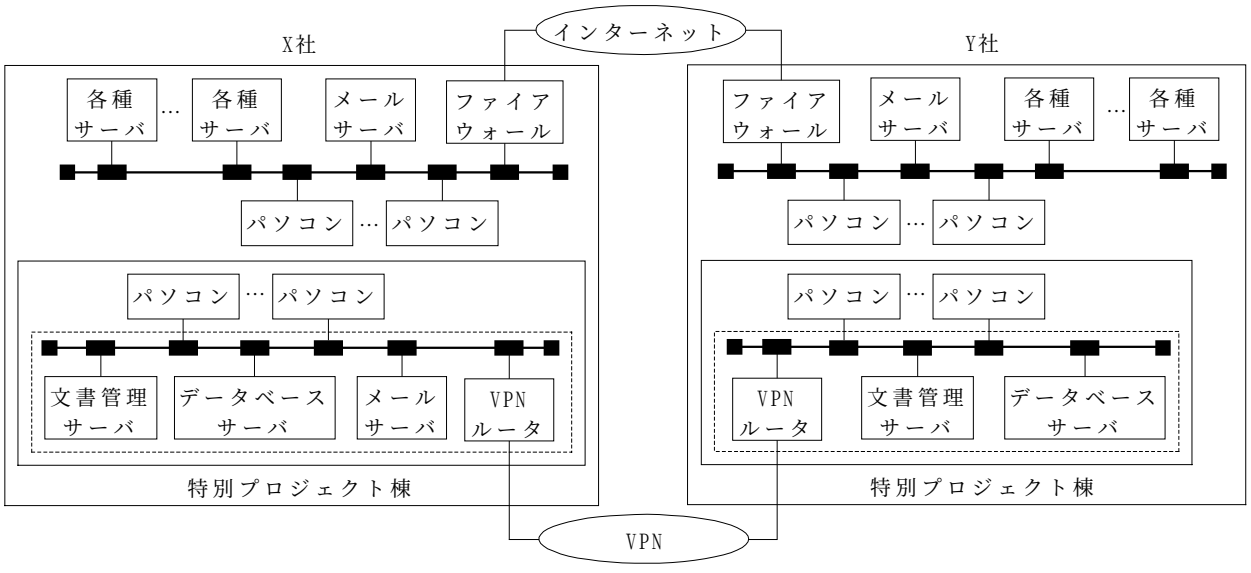


図１　ＰＴ関連組織



注　　は，物理的にアクセス制御された環境を示す。

図２　Ｘ社とＹ社のネットワーク構成

この開発は，全世界の競争相手から注目されているので，両社とも開発に関する情報セキュリティの確保には細心の注意を払っている。

ところが，開発の内容の一部が，X 社側から漏えいしたのではないかとの疑いが持ち上がった。そこで，両社は，PT の情報セキュリティを見直すことにした。早速，情報セキュリティを高めるために，X 社 PT の情報システムのセキュリティに関するシステム監査（以下，監査という）を実施することが，Y 社から提案された。

X 社の社長は，監査が将来的な情報セキュリティの向上に役立つと考え，提案を受諾した。監査チームが，Y 社監査部の J 部長をリーダとし，X 社監査部の T 課長及び Y 社監査部の L 専門担当者で構成された。監査チームは，X 社 PT に対する監査基本方針（図 3）を作成し，X 社側被監査部門の責任者である情報システム部の D 課長に必要書類の提供を求めた。

1．監査は，X 社 PT にかかわる情報セキュリティの管理状況を点検，評価し，併せて関係者の情報セキュリティ意識を高めることを目的にする。
2．監査の対象は，X 社 PT の設計業務及び入退室管理とする。また，文書管理も監査の対象とする。
3．監査は，X 社の情報セキュリティ基本方針を基に，対策基準が適切かどうか，対策基準に対応する実施規定が作成されているかどうか，実施規定が X 社 PT で適切に実施されているかどうかについて行う。
4．監査は，チェックリストを基に，現場立入調査，各種ログ分析及びヒアリングによって行うものとする。

図３　Ｘ社ＰＴに対する監査基本方針

〔監査に向けた準備〕

D 課長は，監査チームに，X 社のネットワーク構成図，組織図，“情報セキュリティ基本方針，対策基準”(図 4)及び X 社 PT に関する実施規定（図 5）を提出した。D 課長は，“情報セキュリティ基本方針，対策基準”の制定経緯について，次のように説明した。

“情報セキュリティ基本方針，対策基準”は，X 社の情報セキュリティ委員会で策定され，1998 年に経営会議で承認されて，社員（出向者，外注者，派遣者を含む）に通知された。また，X 社 PT に関する実施規定は，X 社の技術開発部長と情報システム部長によって Y 社の CSO の助言を受けて作成され，PT 発足時に関係者に通知された。

情報セキュリティ基本方針，対策基準

X 社社長

Ⅰ．基本方針

X 社は，最先端の研究成果を部品開発に生かす企業である。そのため，研究や開発に関する情報セキュリティの確保は，最も重要な経営課題である。社員は，必要の原則(need to know)に従って，情報セキュリティを常に意識して行動しなければならない。

Ⅱ．組織と役割

社長を最高責任者とし，各部長をメンバとする情報セキュリティ委員会を組織する。情報システム部長を実施責任者にする。各部に，情報セキュリティ管理者とネットワーク管理者を置く。

各部の情報セキュリティ管理者は，部長の指示に従い，基本方針，対策基準の実施，情報資産の管理及び必要の原則に基づいたアクセス権の付与に責任をもつ。各部のネットワーク管理者は，各種サーバ及びネットワークの管理業務を実施する。この際，情報セキュリティ管理者が立ち会う。

Ⅲ．対策基準

1．適用範囲

(1) 本基準は，すべての社員に適用される。

(2) 本基準は，X 社が保有するすべての情報資産に適用される。

2．情報資産管理

(1) X 社の管理する情報資産には，その重要度が高い順に A～D のランクをつける。部品開発に関する情報資産は，ランク A として扱われる。

(2) ランク A の情報資産を扱う場合には，会社が支給するパソコンやフロッピーディスクなどにデータを保存してはならず，すべて特定のデータベースに格納する。

(3) ランク A の情報資産をプリント出力し，又は社外に持ち出すときには，所属部長の許可を得る。

(4) （以下，ランク B～D の情報資産の取扱いは省略）

3．利用手続

社員は，ネットワークやデータベースを新たに利用する場合や利用条件を変更する場合，所属部長による必要の原則に基づく審査を経て，承認を受ける。承認後，ネットワーク管理者が情報セキュリティ管理者の立会いの下でアクセス権を設定する。

4．入退室管理

就業規則を適用する。

5．運用保守

サーバ，ネットワーク機器及びデータベースは，物理的に隔離された部屋に設置する。ネットワーク管理者，情報セキュリティ管理者及び情報セキュリティ委員会が許可した者（メーカ作業者など）だけが入室し，設定や変更を行うことができる。

障害修理やメンテナンスを行った場合，ネットワーク管理者は，情報システム部長に作業記録を提出する。

6．インターネットの利用

インターネットの利用は，ランク A の情報資産が流出するリスクがある場合を除き，許可する。利用者は，所属部長に申請して許可を受ける。

7. パソコン管理
(1) パソコンの設定，ネットワークへの接続，廃棄，修理及び展示やデモによる一時持ち出しは，ネットワーク管理者が情報セキュリティ管理者の立会いの下で行う。
(2) 社員は，パソコンのウイルス対策を適切に行う。
8. 記憶媒体管理
社員は，パソコンのハードディスク，フロッピーディスクなどの記憶媒体を，その取得から廃棄までのライフサイクルの各段階において，適切に管理する。また，情報セキュリティ管理者にライフサイクルの各段階での記録を逐次提出する。
9. 例外管理，セキュリティ事故への対応
（省略）
10.教育訓練
社員は，定期的に情報セキュリティの教育訓練を受ける。
11. 監査
定期的に監査を行う。
12. 罰則
本基準に違反した社員は，就業規則に従って懲戒処分を受ける。

以上

図４　情報セキュリティ基本方針，対策基準

X 社 PT に関する実施規定

X 社技術開発部，情報システム部

1. X 社 PT のメンバは，パソコンから X 社及び Y 社 PT にかかわる文書管理サーバ，データベースサーバに必要の原則の範囲内でアクセスできる。
2. X 社 PT における部品開発関連の情報資産は，すべてランク A として扱う。
3. 特別プロジェクト棟における情報のプリント出力は，技術開発部長の許可を得た後，情報セキュリティ管理者の立会いの下で，特定のパソコンから行い，必要事項を①記録簿に記載する。
4. 技術開発部長は，X 社 PT の［　　ア　　］を定期的に提出させ，チェックする。
5. ②特別プロジェクト棟におけるインターネットの利用を禁ずる。

以上

図５　Ｘ社ＰＴに関する実施規定

〔監査の実施〕
監査チームは，情報セキュリティ対策基準などの書類をチェックし，現行の運用状況についてヒアリングを行った。続いて，表 1 に示す監査チェックリストを作成し，現場立入調査を実施した。

表１　監査チェックリスト

管理区分	コントロールの内容	確認する内容，方法の一例
情報資産管理	・情報資産のランク分け	・X 社 PT の管理する情報資産は，文書，記憶媒体を問わず，ランク A～D に適正にランク分けされ，記録されていることを確認
入退室管理	・身分証を兼用する IC カードによる入退室のコントロール	・X 社 PT のメンバとそれ以外の社員の IC カードで入退室を行い，メンバ以外の社員の入退室拒否を確認 ・上記の結果をログで確認
ネットワーク機器管理	・ネットワーク構成のコントロール	・実際の機器（メールサーバ，VPN ルータなど）の設置，配線状態の確認
	・ネットワーク運用体制のコントロール	・アクセスログと作業記録が［ a ］することを確認
パソコン管理	・業務終了時のファイルのコントロール	・ランダムに選択したパソコンに［ b ］が残っていないことを確認
	・ウイルス対策	・ランダムに選択したパソコンにウイルス対策ソフトがインストールされていることを確認
	・ライフサイクルのコントロール	・パソコンの管理番号から購入記録，構成の変更記録及び［ c ］を確認
記憶媒体管理	・ライフサイクルのコントロール	・記憶媒体の購入記録や［ c ］を確認
文書管理サーバへのアクセス管理	・文書（VPN を介しての Y 社文書を含む）へのアクセスコントロール	・X 社 PT のメンバからランダムに選択して，［ d ］を確認 ・X 社 PT のメンバ以外の社員のアクセス拒否を確認 ・上記の結果のアクセスログを確認
ネットワーク利用に関するアカウント，パスワード管理	・X 社 PT のメンバのアカウント，パスワードのコントロール	X 社 PT のメンバからランダムに選択して， ・当該者のアカウントとログインの成功，失敗がアクセスログに記録されていることを確認 ・当該者が X 社 PT に異動してきたときの［ e ］を確認
	・パソコンからのアクセスコントロール	・パソコンからパスワードなしにネットワークにログインできないことを確認

監査チームは，表 1 を基にした現場立入調査で，入退室管理以外の項目についてコントロールが適切であることを確認した。

入退室管理については，D 課長に次のような説明を受けた。X 社では，入退室管理に IC カードを用いている。この IC カードは，身分証及び社員食堂での支払手段を兼ねており，写真，氏名，生年月日，会社名及び所属が印刷されている。表 2 は，D 課長が，入退室管理について監査チームに説明したときの資料である。

表２　入退室管理の概要

項目	内容
入退室管理規則	就業規則を適用
運用管理体制	IC カードでの無人管理とログによるチェック
入退室方法	IC カードをリーダに読ませ，社員番号を基に入室権限をチェックし，ドアを開閉
IC カードの記録項目	氏名，生年月日，社員番号，会社名，所属
IC カードのデータ書込手順	所属部長が承認 ネットワーク管理者による情報セキュリティ管理者の立会いの下での IC カードへのデータ書込み

〔ヒアリングと意見交換〕

監査チームは，X 社 PT のネットワーク管理者と情報セキュリティ管理者に対して，日常の業務内容と報告のフローについてヒアリングを行った。

監査チームは，その結果を基に，ネットワーク管理業務に関する仕事の引継ぎの容易さからネットワーク管理者の間でアカウントが共通に用いられていること，ネットワーク監視業務などでは情報セキュリティ管理者が立ち会わないときがあることについて，説明を求めた。D 課長は，後者について，操作結果がすべて該当サーバのログに記録され，定期的に情報セキュリティ管理者がチェックを行っているので問題はないと主張した。監査チームは，該当サーバのログをチェックするだけでも不正な行動を間接的に防止できることから，現状の管理体制でも十分であると結論づけた。

〔監査の結果報告〕

監査チームは,図 6 に示す監査報告書をまとめ,X 社の情報セキュリティ委員会で社長に報告し,監査を終えた。

監査報告書

監査チーム

1. 総合評価

特別プロジェクト棟内に設置されているネットワーク，システム及びデータベースに関する情報セキュリティ対策基準，実施規定はおおむね適切であり，実際の運用もこれを遵守していると判断する。

(途中省略)

3. 指摘事項

(1) 身分証とは別に入退室専用の IC カードを作成して携帯させる必要がある。さらに，特別プロジェクト棟への入退室管理を強化するための追加手段が必要である。
(2) ネットワーク管理者のアカウントを個人別にすべきである。
(3) 対策基準では，ランク A の情報資産が流出するリスクが残る。

以上

図６　監査報告書（抜粋）

〔監査のフォローアップ〕

X 社の社長は，情報セキュリティポリシの重要性を再認識した。そこで，監査報告書の指摘事項に基づいて X 社の情報セキュリティ対策を強化したいと考え，情報セキュリティ委員会に対して，“情報セキュリティ基本方針，対策基準”の見直しを指示した。

設問１　表 1 中の［ a ］～［ e ］に入れる適切な字句を答えよ。

(1) ［ a ］については，5 字以内で述べよ。

(2) ［ b ］，［ c ］については，それぞれ 9 字以内で述べよ。

(3) ［ d ］，［ e ］については，それぞれ 25 字以内で述べよ。

設問２　図 5 の X 社 PT に対する実施規定に関する次の問いに答えよ。

(1) 下線①の記録簿には，どのような項目を記録すればよいか。5 項目以上挙げ，45 字以内で述べよ。

(2) 図 5 中の［ ア ］に入れる適切な字句を，25 字以内で述べよ。

(3) 下線②で，“特別プロジェクト棟におけるインターネットの利用を禁ずる”理由を，“情報セキュリティ基本方針，対策基準”との関係から，50 字以内で述べよ。

設問３　図 6 中の指摘事項に関する次の問いに答えよ。

(1) 監査チームが指摘事項の(1)で想定している IC カードに関するリスクを，65 字以内で述べよ。また，指摘している追加手段を，25 字以内で述べよ。

(2) 監査チームが指摘事項の(2)で指摘しているように，複数のネットワーク管理者が同じアカウントを用いてネットワーク管理業務を行う場合，どのような問題が発生するか。50 字以内で述べよ。

設問４　図 6 中の指摘事項の(3)で指摘されていることが，X 社の情報の漏えいにつながったと考えられる。情報の漏えいに関連するリスクをもたらす規定上の不備は何か。30 字以内で述べよ。また，図 4 中の対策基準に追加すべき防止策を，65 字以内で述べよ。