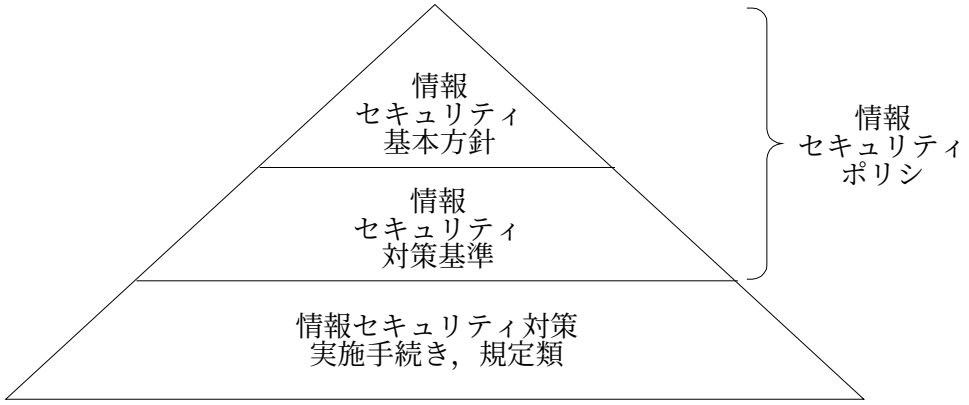
平成１５年度　秋期　情報セキュリティアドミニストレータ　午後Ⅰ問題

情報セキュリティポリシの位置づけ



問１　情報セキュリティポリシに基づくセキュリティ対策に関する次の記述を読んで，設問１～４に答えよ。

D 社は，自動車関連の部品や雑貨の販売，取付けや整備を行う中堅小売業者で，消費者向けに店頭販売と訪問販売を行っている。首都圏を中心に 10 支店があり，それぞれ管轄地域内の数か所の営業所と十数か所の店舗を統括している。営業所では配属された営業員が顧客リストに基づいて訪問販売を行い，店舗では従業員が店頭での接客，販売，整備などを行う。

D 社では，情報システム部が情報セキュリティポリシ及び具体的な取決めを定めた実施手順書の策定を終えたばかりであった。図１，２に，D 社の情報システム部が策定した情報セキュリティポリシの目次と実施手順書（利用者 ID とパスワードの項目の抜粋）を示す。

（1）対象情報システム及び対象情報資産
（2）情報システム装置への対策，ソフトウェアへの対策及びバックアップ対策
（3）ウイルス対策，不正アクセス対策及びソフトウェアの不正コピー対策
（4）情報システムのアクセス管理，ネットワーク管理及びリモートアクセス管理
（5）物理的及び環境的セキュリティ
（6）システム開発及び保守
（7）障害，トラブルへの対応及び法令などの遵守

図１　情報セキュリティポリシの目次

（1）利用者 ID は各人に配付され，初期パスワードを最初のログインと同時に変更する。
（2）パスワードは意味のない文字列にし，必ず 1 文字以上の特殊記号を入れる。利用者 ID は 6 けた，パスワードは 8 けた以上にする。
（3）パスワードは 1 か月ごとに変更するが，一度使用したパスワードは登録できない。

図２　実施手順書（利用者 ID とパスワードの項目の抜粋）

〔顧客情報システムの開発及び稼働〕

D 社では，新たに営業システムに顧客情報システムを追加して，顧客との関係を強化することになった。図１，２に基づいて開発された顧客情報システムでは，実施手順書で指定された利用者 ID とパスワードの基準に準拠した機能が実装されていたが，実際の運用においては，各自の利用者 ID とパスワードを書いたメモをパソコンの周りに残しているユーザが少なくなかった。

〔F 営業所での事件〕

ある朝，F 営業所の管轄支店の営業推進担当者が，F 営業所そばの駅のごみ箱から F 営業所の顧客リストがはみ出しているところを発見し，回収した。顧客リストには，顧客の氏名，住所のほかに推定年収，高額商品の購入履歴，現在の商談状況などが記載されていた。回収された顧客リスト

には細断などの処理が何もされていなかったので，顧客リストの出力を行った利用者 ID がすぐに特定された。しかし，この利用者 ID を利用する営業員は，この 1 週間入院しており，顧客リストが出力された日にはパソコンを操作していなかったことが判明した。この営業員がよく利用するパソコンは，外部の者も頻繁に出入りしている休息ラウンジのそばに置かれ，この営業員の利用者 ID とパスワードのメモがパソコンにはり付けてあった。

数日後，F 営業所での事件を知った情報システム部の G 部長は，情報セキュリティ担当者の E 氏とシステム運用担当者に，事件の調査と再発防止策の検討を指示した。検討の結果，①利用者 ID とパスワードのメモ類への記録及びはり付けの禁止が打ち出され，実施手順書に追加された。その後，各営業所の朝礼で各支店の営業推進担当者から営業員に再発防止策が繰り返し伝達されたので，各営業所では改善が見られた。

〔全社的な情報セキュリティ対策の検討〕

事件の数週間後，E 氏が，F 営業所で情報セキュリティ対策の遵守状況の調査を行ったところ，新たに，②システムから出力された帳票類が管理されずに営業所内で放置されていたり，社外に持ち出されていたりしていることが分かった。また，細断処理を行うと資源が再利用しにくくなるので，③すべての不要な帳票類は細断されずにそのままリサイクルゴミ箱に廃棄されていることも分かった。

E 氏は，問題が発生する前に，情報セキュリティを確保するための総合的な対策を実施することが必要であると感じ，G 部長に相談した。

次は，情報セキュリティ対策に関する G 部長と E 氏の会話である。

G 部長：情報システム部だけの情報セキュリティ対策ではだめだということだが。

E 氏：はい。対策を効果的に推進するためには，情報セキュリティに対して，全社的に取り組む必要があると思います。まず，各部署の情報セキュリティ責任者を集めた［ a ］を設置し，各部署や従業員の情報セキュリティに関する責任と権限を明確にして，全社的な取組として推進することが必要です。

G 部長：これまで，情報システム部としてとれる対策はとってきたのだからよいのではないか。効果が出なければ，人事部が［ b ］の罰則を強化して，営業所の朝礼でその徹底を図ればよい。

E 氏：いいえ。それだけでは十分とは思えません。［ b ］の罰則を強化しても，外部の者が自由に出入りしている現状の営業所内で，顧客リストなどが放置されていたのでは，対策としては不十分です。

G 部長：［ b ］の改定は人事部が行うことだし，文書管理規則は総務部が制定しているし，帳票自体の管理は各部署が行うことなので，それぞれに任せればよいのでは。

E 氏：情報セキュリティは，単に［ c ］化された情報や情報システム上のセキュリティを扱うだけでなく，全社で取り扱う情報資産すべてが対象です。

G 部長：すべての情報資産に対する管理方針は，JIS X 5080（ISO/IEC 17799）を参考に，情報セキュリティポリシ（図１）の中で定めたはずだ。また，自分の担当もままならないのに，

ほかの担当領域に口をだすのには抵抗がある。ところで，君からのメモに“物理的及び環境的セキュリティにも対策が必要”とあるが，何のことかね。

E 氏：営業所の現状に対応した対策として，営業所での入退室管理の実行など，物理的及び環境的セキュリティの対策を実施しなければ，今後，別の事件が起きる可能性があると思いメモに書きました。

G 部長：建物などは総務部の担当であるから，検討する場合には，総務部を交える必要がある。しかし，それだけでは，君が指摘する十分な対策にはならないのではないか。④従業員の管理やモラルも問題だと思うのだが。前回のトラブルのときも私の耳に入るまでに，随分時間がかかったようだが。

E 氏：そのとおりです。“人的セキュリティ”として，従業員の管理やモラルを向上させるための対策が必要です。しかし，現在の情報セキュリティポリシや規則には，何も明記されておりません。

G 部長：確かに明記はされていない。しかし，明記されていなくても，これまでに情報システム部として関連した対策をとってきたはずだ。

E 氏：はい。まず，情報システムとシステム上の情報に関する取扱ルールを作り，情報システム部が，画一的にすべての従業員に集合［　d　］を行ってきました。しかし，情報システム部員の説明では専門用語が多く，業務との関連がない説明のために分かりづらいとの声が多かったので，今後は，各部署の責任者にお願いして，業務の状況に応じた［　d　］を継続的に行って，情報セキュリティ意識を高める必要があると考えております。

G 部長：情報の取扱いといえば，情報の中には契約や法律が関係していて，取扱いに配慮を必要とするものもあるのではないか。

E 氏：そうですね。［　e　］契約に基づいて取引先から得た新車情報や部品情報などは，一般に，製品が発表されるまで［　e　］契約を遵守する必要があります。また，顧客情報はプライバシ保護にも関係するので，むやみに情報を取得したり，その情報を公表したりすることには問題があります。法務部や人事部と協力して，このことを従業員に意識させ，守らせる工夫が必要です。

G 部長：確かにそう言われると，全社的に取り組まないとうまく対策が取れないようだ。今後は，各部署にどう働きかけるべきか，検討してみよう。

設問１　本文中の［　a　］～［　e　］に入れる適切な字句を答えよ。［　a　］については，15 字以内で答えよ。［　b　］～［　e　］については，それぞれ 6 字以内で答えよ。

設問２　情報セキュリティポリシの目次（図１）の(1)～(7)の中で，本文中の下線①の再発防止策が関係しないと思われるものを二つ選び，番号で答えよ。

設問３　本文中の下線④のG部長の指摘に対する人的セキュリティの強化策として，本文中の問題点に基づき，［　d　］及び［　e　］以外の項目で，どのような対策を行うべきか。JIS X 5080（ISO/IEC 17799）の人的セキュリティに関する管理策に基づいて，25字以内で述べよ。

設問４　本文中の下線②，③に関する次の問いに答えよ。

(1) F営業所の帳票類の取扱いに関して，下線②を防止するためには，出力された帳票類をどのように管理すべきか。20字以内で述べよ。

(2) すべての情報資産に対する管理方針を踏まえて，資源の再利用を考慮した本文中の下線③の処置の代わりに採用すべき帳票類の処置方法を，50字以内で述べよ。

問２　物理的セキュリティの確保に関する次の記述を読んで，設問１～４に答えよ。

H 社は，5 年ほど前に設立されたソフトウェア会社である。設立後間もなくして発売したビジネスアプリケーションソフトウェアが評判になり，その後のバージョンアップ版も含めて売上は好調である。その結果，H 社は，順調に業績を伸ばし，設立当初は 10 名に満たなかった社員も，現在は 50 名を超えるほどになっている。

H 社では，社内情報システムが会社規模の急激な拡大に追いついていないことが懸案事項になっていた。また，情報セキュリティ上の事故の発生も懸念されていた。そのため，1 年ほど前に情報セキュリティポリシを策定し，そのポリシに基づいて，社内の情報セキュリティ対策の整備を進めてきた。

〔H 社のオフィス〕

H 社は，郊外の 10 階建てビルに本社オフィス（以下，現オフィスという）を構えている。社員が 20 名を超えた 3 年前に，現在のビルに移転した。入居当初は 5 階の 1 フロアだけであったが，オフィスが手狭になった 2 年前に，6 階の一部も借り，現在では 2 フロアを使用している。

H 社の現オフィスは，5 階，6 階ともに大部屋形式になっており，個室はない。5 階に三つある打合せスペースも，高さ 1.5m ほどのパーティションで区切られているだけである。5 階のオフィスの正面入り口を入ったところには，無人の受付があり，内線電話が設置されている。内線電話のあるところからは，執務スペースが直接見えないようにパーティションを立ててある。

H 社では，社員数の増加に伴って現オフィスが手狭になってきているので，より広いオフィススペースが必要になっている。そこで，適当な物件を探していたところ，都心にあるオフィスビルの 5 階の 1 フロアが 1 年後に空くとの情報を得たので，そこ（以下，新オフィスという）に入居することにした。新オフィスのレイアウトやネットワークの構成については，総務課と情報システム課のメンバを中心にしたプロジェクトチーム（以下，チームという）によって検討が進められている。

〔情報セキュリティポリシと現状の問題点〕

H 社の情報セキュリティポリシでは，オフィスのセキュリティ区画の分類について，図１のように規定されている。

第５章　物理環境セキュリティ
（セキュリティ区画の目的）
第１節　部外者のオフィスへの不正侵入を防ぎ，オフィス内の機密管理を確実にするために，セキュリティ区画を定義する。
（セキュリティ区画の分類）
第２節　オフィスを次の三つの区画に分類して管理する。
一般区画　社員以外の者であっても特別な制限なしに入室可能な区画。
業務区画　社員及び社員の許可を得た者だけが入室可能な区画。
アクセス制限区画　区画の管理責任者によって許可を得た者だけが入室可能で，入室者とその入室履歴を追跡できる区画。
（入退室管理）
（以下省略）

図１　H社の情報セキュリティポリシ（抜粋）

しかしながら，現オフィスでは，社員の執務スペース，サーバの設置スペース及び各種資料の保管場所を確保することが優先され，それぞれの部屋がどのセキュリティ区画に属するのか規定されていない。加えて，各セキュリティ区画の管理規定もないというのが実情である。その結果として，次のような問題が発生していることが，チームのメンバから指摘されている。

問題点(a) 事業に関する打合せ（販売戦略の検討や新製品の企画など）が行われている打合せスペースの隣の打合せスペースで，顧客に対する商品説明などが行われていることがある。
問題点(b) 受付と執務スペースの間に施錠されたドアがなく，社外の者が許可なく執務スペース内に入室してくることがある。
問題点(c) 独立したサーバ室がないので，サーバにアクセスする必要のない社員であっても，物理的にサーバにアクセスすることが可能な状態になっている。

〔セキュリティ区画の管理規定〕

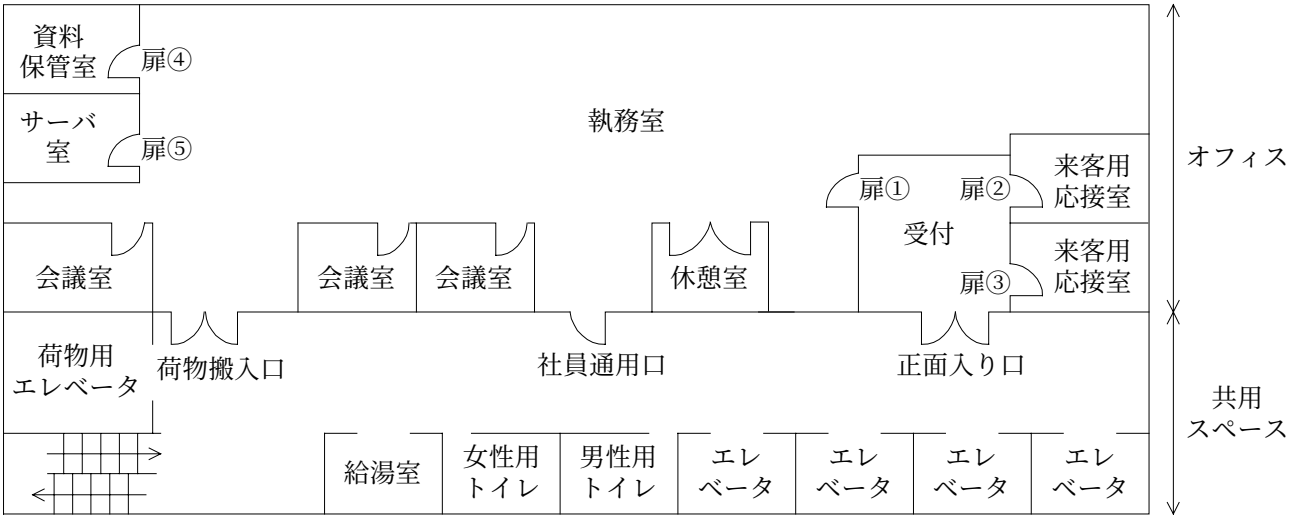
チームは，オフィスビルの移転を機に，図１の情報セキュリティポリシに基づいて，表１に示すセキュリティ区画の管理規定を策定した。新オフィスでは，この管理規定に基づいて各部屋を管理することによって，問題点(a)～(c)のような問題が発生しないようにすることを目指した。

表１　セキュリティ区画の管理規定

区画名	管理規定
一般区画	社員は，常に社員証を着用する。
業務区画	(1) 一般区画とは堅固な隔壁によって区切り，常に施錠する。 (2) 社員は，常に社員証を着用する。 (3) 社員以外の者が入室するためには，事前に入室の申請を行った上で，総務課長の承認を得る必要がある。
アクセス制限区画	(1) [a] とは隣接させない。 (2) [b] とは堅固な隔壁によって区切り，常に施錠する。 (3) 入室の履歴を自動的に記録する。 (4) 社員は，常に社員証を着用する。

〔新オフィスのレイアウト〕

次に，チームは，表１のセキュリティ区画の管理規定に基づいて，図２に示す新オフィスのレイアウトについて打合せを行った。新オフィスでは，各部屋が，すべて天井までを仕切るパーティションによって区切られる。また，表２に示すように，適切なセキュリティ区画に新オフィスの各部屋を区分し，管理することにした。



注　机，じゅう器の配置は省略。

図２　新オフィスのレイアウト（概略）

表２　新オフィスの各部屋の区分

区画名	部屋
一般区画	[c] ，[d]
業務区画	[e] ，[f] ，休憩室
アクセス制限区画	サーバ室，資料保管室

さらに，チームは，表 3 に示すように，主な扉の施錠要領を決定した。特に，社員通用口，荷物搬入口及び扉①のそれぞれについては，物理的セキュリティの強化のために，写真付きの社員証を兼ねた IC カードを導入し，この IC カードで開錠できる電気錠を設置することにした。この電気錠には“完全閉鎖”と“通常施錠”の二つのモードがあり，“完全閉鎖”モードでは IC カードによる開錠ができない。

ビルの 1 階には，ビル全体の保安管理を担当する管理室が設置され，希望するテナントは，かぎを預かってもらえることになっている。

表３　主な扉の施錠要領

扉	錠の種類	施錠要領
正面入り口	シリンダ錠	朝，最初に出社した社員が開錠し，最終退出者が施錠する。施錠中，かぎは，管理室に預ける。
社員通用口，荷物搬入口，扉①	電気錠	常に施錠しておく。入室時には IC カードで，退出時にはサムターンで開錠する。正面入り口の施錠時に“完全閉鎖”モードに移行し，開錠時に“通常施錠”モードに戻る。
扉②，扉③	シリンダ錠	平日の 9：00～17：30 の間，開錠する。
扉④，扉⑤	電気錠	常に施錠しておく。入室時には暗証番号の入力で，退出時にはサムターンで開錠する。扉ごとに暗証番号を決め，あらかじめ決められたそれぞれの部屋の入室許可者だけに通知する。

設問１　表 1，2 中の [a] ～ [f] に入れる適切な字句を答えよ。
[a] , [b] については，それぞれ表 1 中の区画名から答えよ。
[c] ～ [f] については，それぞれ図 2 中の部屋の名称から答えよ。

設問２　表 1 中には，アクセス制限区画として必要な管理規定が抜けている。二つ挙げ，それぞれ 25 字以内で述べよ。

設問３　管理室でかぎの受渡しを行う際に，記録とその内容の確認という観点から，H 社の社員と管理室の係員が実施すべきことを，それぞれ 30 字以内で述べよ。

設問４　表 3 中の扉④，扉⑤の施錠要領に関する次の問いに答えよ。

(1) この施錠要領は，表１のアクセス制限区画の管理規定(3)を満たすには不十分である。その理由と対策を，それぞれ 25 字以内で述べよ。

(2) 上記(1)の対策をとった場合，異動や退職などによって，ある社員のアクセス制限区画への入室許可を取り消す際に，管理責任者が実施すべき作業を，30 字以内で述べよ。

問３　企業グループ内の顧客情報の活用に関する次の記述を読んで，設問１～４に答えよ。

昨年, 百貨店X社の情報システム部門を分離して発足したZ社は, 情報サービス業を営んでおり, X 社の社内情報システムの運用を主な事業にしている。

X 社では，百貨店事業のほかに飲食事業及びホテル事業を長年展開してきたが，経営の機動力を高めるために，数年前から事業別の分社化を進めてきた。また，分社化に加えて，スポーツクラブ事業を運営する Y 社を買収して子会社化するなど，事業領域の拡大にも積極的に取り組んできた。X 社は, Z 社を分社化したことによって, グループ経営戦略のテーマの一つである企業グループ（以下，X 企業グループという）経営への移行を完了したと考えている。

X 社の経営企画部は，次の展開として，グループ情報化戦略の見直しを検討している。その一環として，X 企業グループ内の顧客の囲い込みを図るために，現在，自社単独でサービスを提供しているポイントカードサービス（以下，X サービスという）を X 企業グループ内で利用できるサービス（以下，新 X サービスという）に移行する計画である。図１に，新 X サービスの内容と運営方針（案）を示す。

(1) 利用者に，利用額に応じたサービスポイント（以下，S ポイントという）を付与する。
(2) S ポイントの合計が一定ポイントに達した利用者に，X 企業グループ内で利用できる商品券を郵送する。
(3) 利用者に対して，利用明細情報及び S ポイントの残高の照会サービスを行う。
(4) 希望する利用者に対して，イベントやキャンペーン案内などの情報提供を行う。
(5) 利用者の利用明細情報を分析して販売促進に活用する。
(6) 新 X サービスのカードシステムの運営は，ポイントカード（以下，カードという）の発行を含めて，すべて Z 社が行う。

図１　新Xサービスの内容と運営方針（案）

本件の企画立案に向けて，X 社の経営企画部の A 課長がリーダに任命された。また，顧客情報の取扱いに万全を期すために, 情報セキュリティアドミニストレータである Z 社の企画部の C 課長が補佐することになった。

次は，新 X サービスの内容と運営に関する A 課長と C 課長の会話である。

A 課長：システム企画の段階でどのような事項を検討しておくべきだろうか。

C 課長：カードの発行，利用明細情報の収集，照会方法などのほかに，カードを発行する際の申込情報や新たに加わる利用明細情報などの取扱いについて検討する必要があります。

A 課長：新 X サービスへの移行に当たって，顧客情報の取扱いについて検討が必要なのはどうしてなのか。

C 課長：X サービスと比べて新 X サービスでは，顧客情報の取扱いに関して，利用する［ a ］と利用する情報の［ b ］が異なるからです。

A 課長：新 X サービスでは，“X 企業グループの各社がイベントやキャンペーン案内などの情報提供や販売促進に活用する”ことが利用する［ a ］に加わり，“利用明細情報”が利用する情報の［ b ］に加わることになるのか。

C 課長：はい。同意を得ずにダイレクトメールを送付した企業がクレームを受けた事例がありますので，顧客情報の取扱いには注意が必要です。

A 課長：ところで，X 企業グループ内にカードシステムを導入しているサービスが，X 社以外にあるのだろうか。

C 課長：数年前から，Y 社がカードシステムを導入しています。

A 課長：これら既存のサービスのカード利用を中止して，新 X サービス用の新しいカードを発行したいと考えている。既存のサービスの申込情報については，Y 社が保有する情報を含めて新 X サービスに移行したい。

C 課長：新 X サービスのカード申込書の記載項目は，図２のとおりです。

・申込日
・個人基本情報：氏名，郵便番号，住所，電話番号，生年月日，性別，電子メールアドレス
・パスワード
・個人情報を利用して情報提供や販売促進活動を行うことに関する記載
（以下省略）

図２　新Ｘサービスのカード申込書の記載項目

〔新 X サービスの運営方法の概略〕

A 課長と C 課長は，新 X サービスの運営方法の案について，次のように取りまとめた。図３に，新 X サービスの運営方法（案）を示す。

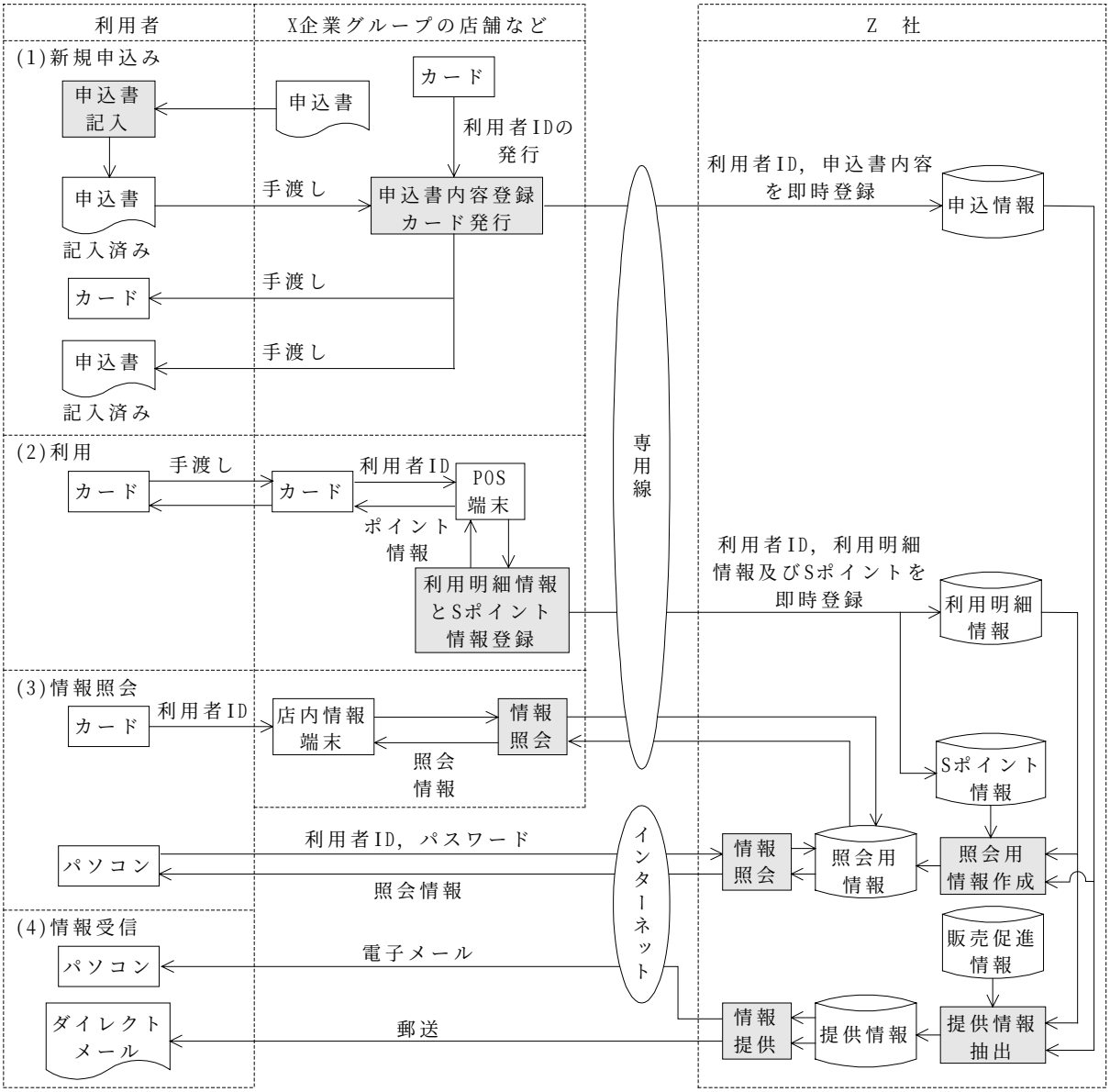


図３　新Ｘサービスの運営方法（案）

(1) 新規発行用の申込書を X 企業グループの店舗などに配置しておき，記入内容の確認と［　c　］を行った上でカードを発行して，申込書とともに手渡す。
(2) 利用時は，店員が POS 端末にカードを読み込ませて，S ポイントを加算する。
(3) 利用者は，店内情報端末にカードを読み込ませて，利用明細情報及び S ポイントの残高を照会することができる。また，インターネットからも照会することができる。
(4) 希望する利用者に対して，電子メールやダイレクトメールを用いてイベントやキャンペーン案内などの情報提供を行う。

A 課長と C 課長は，新 X サービスの運営方法に関して，更に検討を進めた。

C 課長：新 X サービスへの新規加入に加えて，既存のサービスから切り替える場合のカードの発行方法や，カードの紛失及び破損に際しての再発行方法についても検討が必要になります。

A 課長：カードの紛失の場合には再発行して郵送するが，カードの破損に限っては X 社のサービスカウンタで再発行して，破損したカードと引換えに持参した人にその場で手渡す方法にしたい。

C 課長：手渡す方法をとる場合，情報セキュリティの観点からは［　c　］を行うことが必要です。なぜならば，他人が［　d　］によってカードを入手できてしまうからです。

A 課長：個人情報の利用や管理に関して，利用者からクレームが出ないように，新 X サービスの導入と運営方法について引き続き検討していこう。

設問１　本文中の［　a　］～［　d　］に入れる適切な字句を答えよ。［　a　］，［　b　］については，それぞれ 2 字以内で答えよ。［　c　］，［　d　］については，それぞれ 5 字以内で答えよ。

設問２　既存のサービスの利用者を新 X サービスに移行するに当たって，個人情報の保護の観点から留意すべき内容を二つ挙げ，それぞれ 40 字以内で述べよ。

設問３　図３に示す新 X サービスの運営方法に関する次の問いに答えよ。

(1) この運営方法では，個人情報の保護に関して問題がある。発生すると考えられる事故を，50 字以内で具体的に述べよ。

(2) 上記(1)の事故の発生を回避するための対策を，15 字以内で述べよ。

設問４　図３に示す新 X サービスの運営方法では，個人情報の取扱業者として利用者に対応すべき事項に漏れがある。JIS Q 15001（個人情報保護に関するコンプライアンス・プログラムの要求事項）に基づいて，漏れている事項を，60 字以内で述べよ。

問４　営業支援システムの機能追加に関する次の記述を読んで，設問 1～4 に答えよ。

W 社は，社員 300 名の中堅の電子部品メーカであり，機器メーカに部品を供給している。都心の本社ビルに総務部，情報システム部，営業部などがあり，郊外の工場に設計部，製造部などがある。W 社のシステムは，全社統一的な視点で情報セキュリティポリシを遵守することが重要なので，情報システム部が企画段階から所管して，各部と共同のプロジェクトで検討を進めることにしている。

図１に，W 社の電子化情報に関する情報セキュリティポリシを示す。

〔電子化情報の区分〕
　電子化情報の区分は，文書区分に準じて，次のとおりとする。
(1) 極秘　：経営上の最高機密に属するもの。経営戦略情報など。
(2) 秘　　：業務上必要な社内関係者に使用を限定すべきもの。顧客情報など。
(3) 社外秘：社内だけでの使用を認めるもの。クレーム情報など。
(4) 公開　：社外に公開するもの。商品情報など。
（省略）
〔送信及び持ち出し〕
　電子化情報のインターネット経由での送信及び記録媒体による社外への持ち出しを行う際の要領は，電子化情報の区分によって，次のとおりとする。
(1) “極秘”情報　：インターネット経由での送信及び記録媒体による社外への持ち出しを禁止する。
(2) “秘”情報　　：秘匿化や改ざん防止措置などを講じる。原則として，インターネット経由での送信及び記録媒体による社外への持ち出しを禁止する。業務上必要がある場合には，情報セキュリティ責任者の了承を得る。
(3) “社外秘”情報：秘匿化や改ざん防止措置などを講じる。
〔廃棄〕
　記録媒体を廃棄する場合には，電子化情報の漏えいを完全に防ぐ措置を講じる。
（以下省略）

図１　W社の電子化情報に関する情報セキュリティポリシ

営業部では，データベース（以下，DB という）閲覧システム及び電子メールシステムからなる営業支援システムを運用してきた。DB 閲覧システムは，商品情報 DB，クレーム情報 DB 及び顧客情報 DB にアクセスするクライアントサーバ方式のシステムである。商品情報 DB は商品仕様情報など，クレーム情報 DB はクレームや対応策など，顧客情報 DB は顧客情報や購買履歴などからなる。これらは，営業部が管理するサーバで運用され，営業部員が随時，登録，更新及び閲覧を行うことができる。商品情報は，印刷して持参したり，電子メールに添付し送付したりすることによって顧客に提示していたが，社内に戻らないと利用できないので不便であった。そのため，社外から営業支援システムを利用できるようにしてほしいとの要望が寄せられていた。

このたび，営業部では，営業部員が外出先から営業支援システムへのアクセスをインターネット

経由で行うリモートアクセス機能と，Web サーバを通じて商品情報を一般ユーザに提供することができる商品情報 Web 機能を実現させることを企画し，情報システム部と営業部で構成される改善プロジェクトを発足させた。改善プロジェクトでは，情報システム部長を責任者として，情報システム部の SE である R 君と営業部の T 主任が要件定義を行い，情報セキュリティアドミニストレータの S 君が情報セキュリティの確保を担当することになった。

〔改善案の検討〕

R 君と T 主任は，図２に示す機器構成による改善案を提案した。

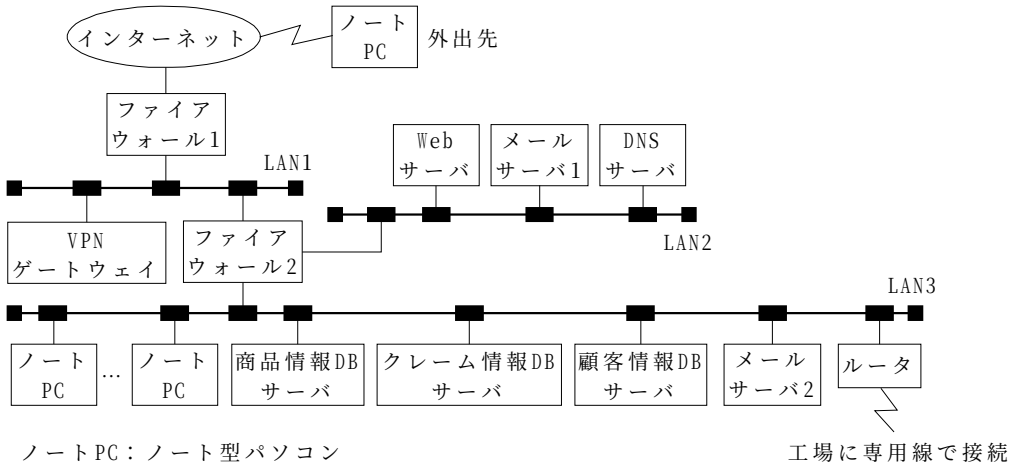


図２　改善案の機器構成

(1) ノート PC を新規に導入し，あらかじめ VPN ソフトウェアを組み込んで，所定のインターネットサービスプロバイダへのログインアカウントを設定した上で営業部員に配付する。外出先からノート PC を使って社内にアクセスする際は，VPN ソフトウェアを起動した後，LAN1 に新規に導入した VPN ゲートウェイに接続し，利用者 ID とパスワードで認証を受けた後，暗号化通信を行う。VPN ゲートウェイは，プロキシサーバとして動作させ，LAN3 の各 DB サーバ及びメールサーバ 2 に代理アクセスする。

これによって営業部員は，社内と同様に外出先からも営業支援システムを利用でき，いつでも顧客情報などをノート PC にダウンロードして，営業活動に利用することができる。

(2) 外出時以外は LAN3 にノート PC を接続して使用することにし，下取り業者に従来から使用していたデスクトップ PC を売却する。

(3) Web サーバに CGI プロセスを使ったソフトウェアを組み込み，営業部に設置されている商品情報 DB サーバから商品情報を検索できるようにして，インターネットに接続している一般ユーザに対して，W 社の商品情報を公開する。従来どおり，営業部員が商品情報の登録及び更新を随時行う。

(4) メールサーバ 1 にウイルスチェックソフトウェアを導入する。これまでも，外部からの電子メ

ールは，いったんメールサーバ 1 で受信された後，ファイアウォール 2 を通ってメールサーバ 2 に転送されている。また，社外へ送信される電子メールは，メールサーバ 2 からメールサーバ 1 に転送された後，社外に送信されている。

社員は，メールサーバ 2 にアクセスして電子メールを送受信している。ウイルスチェックソフトウェアを導入した後は，メールサーバ 1 において，社外と送受信するすべての電子メールのウイルスチェックを行う。さらに，ノート PC にもウイルスチェックソフトウェアを導入する。メールサーバ 1 とノート PC に導入したウイルスチェックソフトウェアのウイルス定義ファイルは，毎週定期的に更新する。

〔セキュリティ確保のための検討〕

S 君は，改善案の提示を受け，デスクトップ PC の下取り業者への売却に関して，①情報セキュリテイポリシに基づく指示を行った。また，R 君とともに検討を進め，運用面に関して次のような対策を提案した。

(1) ファイアウォールにおける通信制御

S 君は，ファイアウォール 2 に図 3 に示すような通信許可を追加した。

(1) [　ア　] と商品情報 DB サーバ，クレーム情報 DB サーバ及び顧客情報 DB サーバ間の DB 閲覧に関する通信
(2) Web サーバと [　イ　] 間の CGI プロセスによる通信
(3) [　　ウ　　]

図３　ファイアウォール２に追加した通信許可

(2) VPN ゲートウェイの利用者認証

VPN ゲートウェイの認証機能を用いて，正規のアカウント以外のユーザが社内に侵入することは阻止できる。しかし，[　a　] が [　b　] された場合には [　c　] を許すことになるので，同じ [　a　] を長期間使い続けないようにするなど，ノート PC の運用に関する実施手順を策定し，営業部員に徹底させることにした。

(3) ウイルス対策

ウイルス定義ファイルを②定期的に更新する運用には問題があったので，見直しを行った。

これらの対策の実施を条件に，改善案は，改善プロジェクトに承認された。

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　DoS 攻撃	イ　利用者 ID	ウ　ウイルス感染	エ　改ざん
オ　侵入	カ　認証	キ　盗み出	ク　パスワード

設問２　本文中の下線①に示したデスクトップ PC の売却に関して，S 君が指示した具体的な内容を，35 字以内で述べよ。

設問３　運用面の改善に関する次の問いに答えよ。

(1) 図３中の［　ア　］～［　ウ　］に入れる適切な字句を答えよ。［　ア　］，［　イ　］については，それぞれ 10 字以内で答えよ。［　ウ　］については，35 字以内で答えよ。

(2) 本文中の下線②の問題を，35 字以内で具体的に述べよ。

設問４　社外でのノート PC の利用に関する次の問いに答えよ。

(1) 〔改善案の検討〕の(1)に従って営業部員が運用を行う上で，遵守すべきことは何か。情報セキュリティポリシを踏まえて，50 字以内で述べよ。

(2) 上記(1)を遵守しても社外でのノート PC の利用には，ノート PC の盗難以外に幾つかのリスクが残る。特に留意すべきリスクを，30 字以内で述べよ。また，その技術的対策を，30 字以内で述べよ。