

**** 平成19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 ****
示現塾 プロジェクトマネージャ・テクニカルエンジニア（ネットワーク）など各種セミナーを開催中！！

開催日, 受講料, カリキュラム等, 詳しくは, <http://zigen.cosmoconsulting.co.jp> 今すぐアクセス！！

平成19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

問1 ワークスタイル改革におけるセキュリティに関する次の記述を読んで、設問1～5に答えよ。

Q社は、社員数2,000名の事務機器を取り扱う商社であり、多様な商品を全国の法人に販売している。本社には、経営企画部、総務部などの本部と、商品分野ごとに編成された10の事業部がある。事業部の社員の大半は営業員で、業務の根幹を支えている。Q社本社の勤務概要を表に示す。

表 Q社本社の勤務概要

部門名	状況	勤務状況 (1)	繁忙期 (2)	在席率 (%) (3)	社員数 (名) (4)	社員以外の状況
本部	経営企画部	所定勤務時間	決算月	90	20	—
	総務部	所定勤務時間で、8時半過ぎの出勤者が多い	不定	80	30	アルバイトを随時雇用し、社員をサポート
	人事部	所定勤務時間	年度初め	80	30	—
	情報システム部	休日出勤が多い。一部24時間シフトあり	不定	70	30	—
	経理部	所定勤務時間で、8時半過ぎの出勤者が多い	各月末及び決算月	100	40	派遣社員40名が社員に混じって業務
	法務部	所定勤務時間	不定	70	10	—
	研修部	所定勤務時間	4月	70	10	契約社員5名を雇用
事業部	A事業部	深夜勤務が多い	各月末	30	200	派遣社員30名が電話対応
	B事業部	午後出勤が多く、出勤時刻が不規則	各月末	30	250	パートタイム5名が封入・封かん
	C事業部	早朝出勤が多い	各月末	40	150	—
	D事業部	午後出勤が多く、出勤時刻が不規則	冬期	70	50	派遣社員を随時雇用し、アンケートのパンチ入力
	E事業部	8時半～9時に出勤	各月末	35	300	派遣社員10名、パートタイム10名が電話対応・来客対応
	F事業部	午後出勤が多く、出勤時刻が不規則	夏期	25	150	パートタイム10名が社員に混じって営業活動
	G事業部	所定勤務時間の勤務者が多い	各月末	70	100	派遣社員3名が経理事務
	H事業部	9時直前の出勤者が多い	通年	30	250	アルバイトを随時雇用し、展示会準備
	I事業部	早朝出勤者が多い	年度末	40	150	アルバイト5名が資料整理
	J事業部	所定勤務時間の勤務者が多い	各月末	35	200	パートタイム5名が来客対応

注(1) 所定勤務時間は、月曜～金曜日の9時～17時。事業部はフレックスタイム制を採用している。

(2) 決算月は、3月、6月、9月、12月、会計年度は4月～翌3月である。

(3) 平日の日中における執務室の平均在席率（概数）

(4) 通年平均の所属社員数（概数）

〔業務環境の課題〕

本社のオフィスビルは、開設後 20 年が経過しており、膨大な量の文書が執務空間を圧迫している。不要な文書を廃棄したり、利用頻度の低い資料を社外倉庫で保管したりしているが、それだけでは追いつかず、キャビネットに入りきれないままとっている。数年前から文書の電子化を推進しており、本部が作成した文書については、社内ホームページからダウンロードできるようにしたが、閲覧したい文書がどのホームページからダウンロードできるかの案内がなく、使い勝手が悪い。このような現状なので、必要な資料を印刷して、手元で管理する社員が少なくない。また、会議で紙媒体の資料を配布する習慣も改まらず、社内での紙の使用量は一向に減っていない。

営業員は、社外での商談が多く、執務室の在席率は低い。事務処理の締め日近くは在席率が高くなるが、それでも 50%を超えることはほとんどない。更なる業績向上のために、法人に対して様々な商品を組み合わせる営業の強化を図っているが、商品ごとに扱う部門が異なり、執務室が離れていることもあって、情報共有が進まない。その結果、提案内容が不十分であったり、提案に時間がかかったりして、商機を逸してしまうことがあった。

〔情報システムの概要と課題〕

情報システムは、会計管理、受発注、商品管理、人事の各サブシステムからなる基幹系システムと、企画や営業活動を支援する情報系システムとからなり、社内 LAN 上で稼働している。PC は、全社員に配布されており、ノート PC も多く利用されている。営業員は、ワープロ、表計算ソフトなどがインストールされているノート PC を携帯して外出する。外出中には、喫茶店などでインターネットに接続して Web サイトから情報を収集したり、ワープロを使って見積書や提案書を作成したりしている。

すべての PC とファイルサーバには、ネットワーク対応の OS（以下、ネット型 OS という）が導入され運用されている。Q 社が利用しているネット型 OS におけるネットワーク利用の仕組み（概要）を、図 1 に示す。

1. ネットワーク領域

- (1) ネット型 OS では、ファイルサーバ、ネットワークプリンタなどのネットワーク資源をネットワーク領域として管理する。ネットワークセグメントなどの物理的なネットワーク構成に依存せず、ネットワーク領域を設定することができる。
- (2) ユーザが、あるネットワーク領域にログインすると、そのネットワーク領域に登録されているネットワーク資源を一覧できるようになる。
- (3) 別のネットワーク領域に登録されているネットワーク資源を一覧する場合は、そのネットワーク領域にログインする方法と、異なるネットワーク領域を相互利用できるようにする機能を用いて両ネットワーク領域を相互利用できるようにする方法がある。なお、一つのネットワーク資源を二つ以上のネットワーク領域に登録することもできる。

2. ユーザ属性グループ

- (1) ネット型 OS では、ユーザをグループ化してユーザ属性グループとして管理でき、ユーザ属性グループ単位でネットワーク資源に対するアクセス権をきめ細かく設定することができる。
- (2) ユーザは、所属するユーザ属性グループに定義されたアクセス権で、ネットワーク資源にアクセスできる。なお、ユーザを複数のユーザ属性グループに所属させることもできる。

3. ネットワーク領域管理サーバ

- (1) ネットワーク領域には，ネットワーク領域管理サーバを設置する必要がある。
- (2) ネットワーク領域管理サーバは，ネットワーク領域のネットワーク資源を管理する機能に加え，Web の認証を統合する機能をもっている。
- (3) ネットワーク領域管理サーバとクライアント PC 間の認証情報のやり取りは，すべて暗号化されており，認証情報が されることはない。

図 1 ネット型 OS におけるネットワーク利用の仕組み（概要）

Q 社では，部門内で利用するファイルサーバやプリンタの管理は各部門に任されており，ネットワーク領域，ユーザ属性グループ及びユーザの管理は，部門ごとにネットワーク領域管理サーバを導入して行われている。一方，部門間で共用するアプリケーションは，Web アプリケーションとして構築されており，ベーシック認証を用いた個別のユーザ管理が行われている。このように，ユーザ管理が重複して行われているので無駄が多く，ユーザも利用対象ごとにログインし直す必要があり，不便である。

〔セキュリティ対策の状況〕

Q 社におけるセキュリティ対策の状況は，次のとおりである。

(1) セキュリティポリシーの運用

セキュリティポリシーを 7 年前に整備した。しかし，個人情報保護法の施行時や様々な法令の改正時など，新たなセキュリティ対策が必要とされるたびに変更を重ねてきたことから，社員が最新の内容を理解していない。セキュリティポリシーや関連する規程は社内のホームページに掲載されているが，規程によって所管部門及び掲載ホームページが異なるので，社員が業務を行う上で判断に迷った場合に，どのホームページを確認したらよいか分からない。

(2) ネットワークセキュリティ対策

インターネットと社内 LAN との境界にはファイアウォールを導入し，社外からの不正アクセスに対応している。また，DMZ に Web 用のプロキシサーバを設置し，社内 LAN からインターネットへのアクセスはすべてプロキシサーバを経由させるようにしている。このプロキシサーバでは，ブラックリスト方式によるフィルタリングソフトを稼働させており，一部のサイトへの接続を している。

(3) ウイルス対策

すべての PC とサーバにはウイルス対策ソフトを導入している。ウイルス対策ソフトは，インターネット上のソフトメーカのサイトに接続して，プログラム及び を常に最新状態に維持できるようにしている。

(4) セキュリティパッチ適用

OS やアプリケーションに対するセキュリティパッチの導入を，随時促している。ウイルス対策ソフトの更新が必要な場合や，OS のセキュリティパッチが発表された場合には，情報システム部が各部門に対応を依頼しているが，依頼が見逃ごされてしまうことがあり，問題視されている。

(5) ノート PC の社外持出し対策

社員が社外に持ち出すノート PC に，パーソナルファイアウォールを導入している。これによって，

ネットワークを介した攻撃によるインターネット接続中のノート PC からの情報漏えいは防止できるようになった。しかし、公共の場所でのぞき見られるリスクやノート PC の置忘れによる情報漏えいのリスクについては、対策が不十分である。社員に対しては、社外におけるノート PC の利用規程を設けて、対策の徹底を促しているが、社員に過失があっても情報漏えいが起こらないように、①更なる対策を検討している。

(6) 物理的セキュリティ対策

出入口に警備員を配置し、顔写真入りの社員証の提示を全社員に義務化している。来訪者には入場許可証を貸与している。来訪者が、商談コーナーと間違えて執務室に入ってしまうことがあるが、執務室には常に社員がおり、通常の勤務者以外が入室すればすぐに声をかけて退室させることができるので、セキュリティに関する問題が起きたことはない。パートタイム、アルバイト、派遣社員及び契約社員には、入場許可証を一定期間貸与する運用としている。

[ワークスタイル改革の検討]

業務の効率向上や情報共有の推進を目指して、ワークスタイル改革を行うことが経営決定され、これを実現するために、図 2 に示す活動方針によるオフィス改革プロジェクトが発足した。プロジェクトリーダーには K 常務が指名され、検討が進められた。

1. 目的

業務の効率向上と、情報共有の推進を目指した業務改革の一環として、次のような目的の下にプロジェクトを推進する。

- (1) フリーアドレス化を推進してオフィスの空席を減らし、その分のオフィススペースの削減や別用途への転用を図る。
- (2) 文書保管スペースの削減と、紙文書からの情報漏えいリスクの軽減を行うために、ペーパーレス化を更に推進する。
- (3) オフィスにおける情報活用の効率向上を図るために、社内業務用のワンストップ型情報システムを導入する。

2. プロジェクトの編成

(1) ワークスタイル検討グループ

業務ワンストップ化、フリーアドレス化、ペーパーレス化を実現するワークスタイルを検討し、情報システムへの要求事項を定義する。

(2) 新システム検討グループ

ワークスタイル検討グループから提示された情報システムへの要求事項を踏まえ、新システムを設計、評価、選定して構築する。

(3) セキュリティ検討チーム

ワークスタイル検討グループと共同で、セキュリティを確保したワークスタイルを検討する。また、新システム検討グループと共同で、セキュリティを確保した情報システムを構築する。

図 2 オフィス改革プロジェクトの活動方針

ワークスタイル検討グループは、空席を自由に利用できるフリーアドレスオフィスを実現するための検討を進めた。フリーアドレスオフィスでは、机上や引き出しを占有して業務に必要な荷物を格納することを禁止するので、施錠可能なキャビネットを一人 1 台割り当てることを提案することにした。すな

わち，外出時や帰宅時には，すべての荷物をキャビネットに入れ，キャビネットは所定のコーナに保管する。この施策は情報セキュリティ面でも効果があり， が実現しやすくなる。

一方，フリーアドレスオフィスでは，周囲の社員が顔見知りとは限らず，迷い込んだ来訪者と区別できないことが危惧されたので，全執務室の出入口に，IC カードと暗証番号による認証が必要な電子錠を設置する施策と，②社員であるかどうかを社内ですぐに判断できるような施策を提案することにした。

新システム検討グループは，情報システムへの要求事項を踏まえ，フリーアドレスオフィスにおけるコミュニケーションを確保するための携帯電話とノート PC の全社員への配布，ネットワーク対応型イメージスキャナの設置，及び文書管理システムとワークフローシステムの導入について具体化することにした。

〔ワンストップ型情報システムの検討〕

ワークスタイル検討グループは，業務のワンストップ化を検討した。その結果，ファイルサーバやプリンタを利用するためのネットワーク領域へのログインと，全社共用の様々な Web アプリケーションへのログインを一元化するシングルサインオン機能を，情報システムへの要求事項として提示した。

さらに，ユーザに重要事項をプッシュ型で通知する機能，様々な日常業務で利用するシステムの操作方法を分かりやすく示すプル型情報案内の機能，及び全社共用の Web アプリケーションの起動機能をもった社内ポータルシステムを，要求事項に含めた。特に，重要事項をプッシュ型で通知する機能は，毎日，出勤時にシステムにログインすると必ず表示され，内容を確認しないと次画面に進めないようにするよう求めた。

情報システムへの要求事項の提示を受けた新システム検討グループは，図 3 で示した段階的な整備計画を立案した。

(1) ネットワーク領域の再編

部門ごとに運用している部門ネットワーク領域に加えて，全社ネットワーク領域を新設し，全社共有ファイルサーバ，社内ポータルシステム，ワークフローシステム，及びネットワーク対応型イメージスキャナを新規に導入して登録する。プリンタについては，各部門で利用しているものをすべて全社ネットワーク領域にも登録し，自分の使いたいプリンタを手動で任意に選択できるようにする。

(2) シングルサインオン環境の構築

全社ネットワーク領域の新設と同時に，全社ネットワーク領域へのログインと，情報系システムの各業務アプリケーションへのログインをワンストップで行うために，認証の統合を行う。この際，③ネットワーク資源へのアクセス権の管理を効率よく行うために，Q 社が採用しているネット型 OS の機能を適切に活用する。

(3) 社内ポータルシステムの構築

ユーザが新システムにログインすると，自動的に図 4 で示した社内ポータルシステムが起動し，その日の重要事項の一覧をプッシュ型で通知するようにする。

図 3 段階的な整備計画

(1) ユーザが新システムにログインすると，プッシュ型で情報を通知するアプリケーションが，ログインスクリプトによって起動し，自動的に実行される。

(2) プッシュ型で情報を通知するアプリケーションは，各部門が随時更新する社内重要情報データベースか

ら，そのユーザに通知すべき重要情報を検索し，ユーザの画面に表示する。

- (3) 表示された重要情報の確認ボタンをユーザが押すと，プル型で情報を案内するリンクメニューと Web アプリケーションの起動ボタンを配置した画面を表示する。この際 Web アプリケーションの利用状況を正確に把握できるようにするため，Web アプリケーションの起動をこの画面経由に限定し，起動ボタンの押下をログに残す。

図 4 社内ポータルシステムの動作

[新システムへの移行案の検討]

検討が進んだところで，新システム検討グループは，図 5 で示した新システムへの移行案を検討した。

- (1) 人数が少ないので試行が容易な D 事業部をモデル部門に指定し，フリーアドレス化して，執務室を 20% 削減する。
- (2) 新システムを構築し，D 事業部に試験的に導入する。その際，社内ポータルシステムや社内重要情報データベースのサーバにおいて，④図 4 で示した社内ポータルシステムの動作を採用する場合に懸念される業務への重大な影響を考慮する。ただし，この段階では性能上の余裕をもたない最小限の機器構成とし，CPU 稼働率やディスク入出力時間を測定する。
- (3) D 事業部において，ネットワーク対応型イメージスキャナを稼働させ，紙文書を順次電子化して，ペーパーレス化を推進する。
- (4) D 事業部での試験導入で測定した CPU 稼働率やディスク入出力時間から人数比の計算を行い，社内ポータルシステムと社内重要情報データベースの全社展開時の機器構成を設計する。この設計に基づいてシステムを強化し，1 年後に全社展開する。

図 5 新システムへの移行案

新システムへの移行案が具体化したところで，情報システム部の Y 部長がセキュリティ検討チームの Z 君に新システムのセキュリティ対策などに関して確認した。次は，そのときの会話である。

Y 部長：セキュリティ対策の問題ではないが，⑤この移行案では，全社展開時に問題が起こる可能性が高い。修正が必要だ。

Z 君：分かりました。修正します。

Y 部長：ところで，紙文書はシステムで管理できないので情報漏えいリスクがあったが，ペーパーレス化を推進すれば回避できるのかね。

Z 君：紙文書の管理は残るので，情報漏えいリスクも残ります。また，電子化することで，電子化文書へのアクセス状況をシステムによって監視できるようになりますが，反面，セキュリティ上の欠陥があれば，一度に大量の情報が持ち出される危険が増大します。

Y 部長：電子化文書が一度に持ち出される危険性は，どのように減少させるつもりなのかね。

Z 君：アクセス制御などの設定を適切に行うことが重要ですが，社内での情報漏えい防止と，社外での情報漏えい防止とは考え方が異なります。

Y 部長：社外での情報漏えい防止は既に検討を行ってきたが，社内での情報漏えい防止はどう考えているのかね。

Z 君：社内での情報漏えい防止策を追加します。社員は，情報システムへのアクセス権をもっていますから，アクセス制御だけでは情報漏えいの防止は困難です。システムの利用状況をログに残

すことで，事後に行動を追跡できるようにします。その上で，懲罰規程があることと，ログを残すことを社員に告知すれば を働かせることもできます。

Y 部長：紙文書も残るということだが，紙文書からの情報漏えいについてはどう考えているのかね。

Z 君：紙文書は量が減りますから，従来どおりの規程で十分にリスクが低減されると考えています。さらに，セキュリティの全体的な向上のためにセキュリティパッチの導入情報やウイルス対策ソフトのアップデート情報とともに，社内ポータルシステムのプル型情報案内の機能で各種規程を分かりやすく提示し，ユーザがいつでもセキュリティ対策を正しく実施できるよう支援するつもりです。

Y 部長：⑥当社のセキュリティ対策の状況を改善するために，導入するワンストップ型情報システムの機能をもっと積極的に活用してほしい。また，会社の内部でも，他部門に知られてはならない情報がある。現在検討中の新システムでは，⑦プリンタの扱いで心配な点があるので，技術的なセキュリティ対策を検討してくれ。

Z 君：分かりました。

こうした議論を経て，オフィス改革プロジェクトの施策案は経営会議で承認され，実行に移された。

設問 1 次の (1)，(2) に答えよ。

- (1) 図 1 中の ，及び本文中の ～ に入れる適切な字句を答えよ。
- (2) 本文中の下線①で示した更なる対策として妥当なものは何か。のぞき見対策及び置忘れ対策の内容について，それぞれ 20 字以内で述べよ。

設問 2 「ワークスタイル改革の検討」における本文中の下線②で示した施策としてどのような事項が考えられるか。20 字以内で具体的に述べよ。

設問 3 新システムについて，(1)，(2) に答えよ。

- (1) 図 3 中の下線③で示したネット型 OS の機能の適切な活用方法を，40 字以内で具体的に述べよ。
- (2) 図 5 中の下線④で示した，社内ポータルシステムの動作を採用する場合に懸念される業務への重大な影響とはどのような事態か。60 字以内で具体的に述べよ。

設問 4 「新システムへの移行案の検討」について，(1)，(2) に答えよ。

- (1) 本文中の下線⑤で示した，起こる可能性が高い移行案の問題を，60 字以内で述べよ。
- (2) 本文中の下線⑦で示したプリンタの扱いについて，心配な点と，その技術的なセキュリティ対策を，それぞれ 40 字以内で述べよ。

設問 5 本文中の下線⑥で示した，ワンストップ型情報システムを使ってセキュリティ対策の状況を改善する方法を，60 字以内で述べよ。

問 2 システムの統合に伴う情報セキュリティの見直しに関する次の記述を読んで，設問 1～5 に答えよ。

R 社は，売上高 1,800 億円，社員数 500 名の玩具製造業者で，東京都に本社があり，全国主要都市には営業所，埼玉県には工場がある。本社には，技術部，営業部，総務部，情報システム部などがある。R 社の主力製品は，競争が激しい子供向けエレクトロニクス玩具であり，一般顧客からの問合せが多いことから，コールセンタを開設するとともに，ホームページ（以下，HP という）を設けて，商品情報を提供している。

R 社では，販売戦略として会員を募集しており，HP にメールアドレスを登録する会員（以下，Web 会員という）と，商品に添付した返信はがきで商品情報の郵送を申し込むダイレクトメール（以下，DM という）会員がいる。Web 会員の場合，HP で会員登録すると，ID とパスワードが発行され，専用の情報へのアクセスやメルマガジン（以下，メルマガという）購読などができる。一方，DM 会員には，定期的にニュースや案内が郵送される。

R 社では，コールセンタ及び HP の運用システム（以下，S システムという）と，本社情報システム（以下，T システムという）を利用している。

〔S システムの概要〕

S システム（図 1）は，2005 年に個人情報保護法の施行に合わせて，群馬県にある V 社データセンタ内部に構築された。S システムは，データベース（以下，DB という）サーバとそのほかの各種サーバを接続した内部 LAN，DMZ1 及びコールセンタの PC を接続した LAN（以下，コールセンタ LAN という）で構成されている。

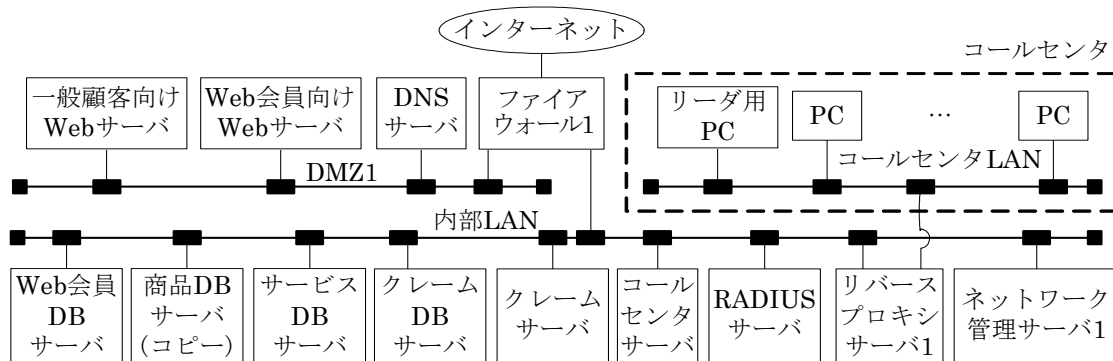


図 1 S システムの概要

商品 DB には商品情報，サービス DB にはメルマガなどのサービス情報，Web 会員 DB には Web 会員のメールアドレス，ID 及びパスワード，クレーム DB には製品種別及び苦情内容がそれぞれ記録されている。R 社では，コールセンタ業務及び S システムの運用業務（ハードウェアの死活監視，ウイルス感染や不正侵入の対策ログの採取，バックアップの取得と保管）を，データセンタを保有する V 社に委託している。

コールセンタでは，50 名の V 社社員と 5 名の R 社社員が，コールセンタ LAN の PC から，シングルサインオン機能をもつリバースプロキシサーバ 1 を介して，内部 LAN のサーバにアクセスする。V 社社員は，一次受付と商品への問合せに対応し，商品に対するクレームなどは R 社社員が対応して，ク

レーム DB に記録している。

また，V 社社員のリーダは，V 社社員の通話，PC の画面及び操作内容をネットワーク管理サーバ 1 経由で監視しており，対応が不適切なときには，指導している。

R 社の情報システム部は，V 社から連絡を受けた S システムの不具合への対応，V 社社員のアカウント管理業務に加えて，S システムの運用の適正性について点検している。また，情報システム部員は，毎日，Web 会員 DB やクレーム DB に追加されたり，更新されたレコードをテキスト形式で USB メモリに抽出して，本社に持ち帰っている。

〔T システムの概要〕

T システム（図 2）は，2001 年に本社内に設置され，2005 年に改造が加えられた。このシステムは，本社に勤務する社員 300 名を対象とした，グループウェア，電子メール，社外の Web の閲覧及び DM の発送に利用されている。DM の発送には，DM 会員 DB（DM 会員の個人情報を保存・管理）を利用している。R 社社員は，T システムのメールサーバ，DM 送付支援サーバ，グループウェアサーバなどに個別に認証を受けてアクセスし，また，プロキシサーバを経由して社外の Web を閲覧している。

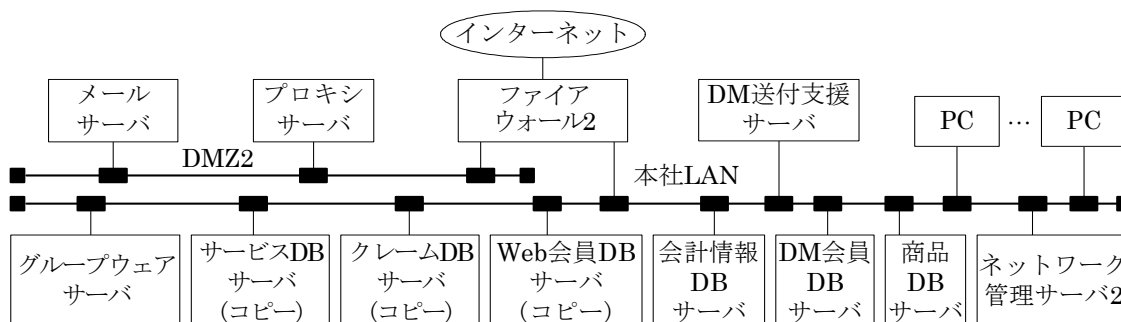


図 2 T システムの概要

主要な DB の可用性を高めるために，T システムは，S システムと相互に DB の内容のコピーを保有する冗長構成となっている。情報システム部は，T システムの運用（主要な DB のバックアップ，利用者のアカウント管理，サーバの停止・再開処理及び故障修理など），保守（ソフトウェアの変更管理など），及び管理権限の運用の適正性について自己点検を実施している。情報システム部員は，DB サーバを含む各種のサーバについて，あらゆる操作が可能な権限（以下，特権権限という）をもつアカウントを共用している。

〔システムの統合と情報セキュリティの見直し〕

R 社では，過去，外部による情報セキュリティ監査において，業務に無関係な Web 閲覧と①二つのシステムの DB 内容の同期に関するセキュリティポリシーへの違反が指摘されていた。DB 内容の同期に関しては運用上の制約から特例として認められていたが，DM 会員へのサービス向上の要望もあることから，関連部署は対応策を検討して，T システムのサーバなどを V 社データセンタに集約するシステム（以下，新システムという）の構築について合意した。新システムの概要を図 3 に示す。

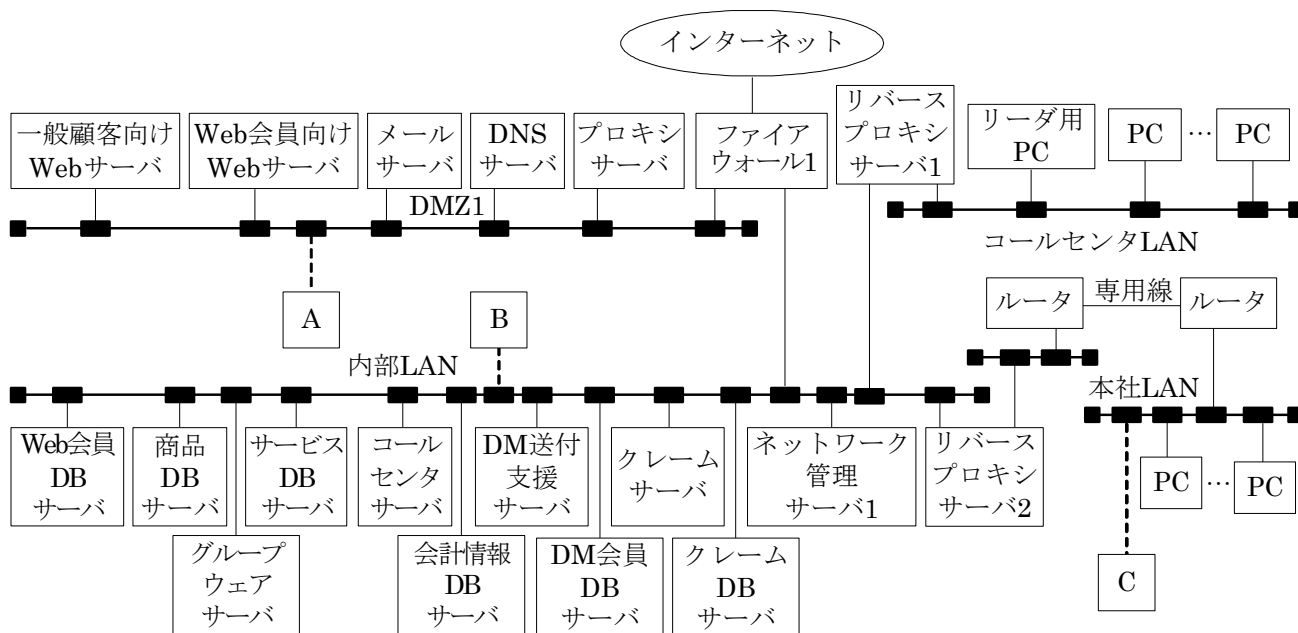


図 3 新システムの概要

R 社は、V 社データセンタへのシステムの集約をきっかけに、情報システム部の業務内容、外部委託、セキュリティポリシーなどを見直すことにした。この新システムへの集約案は経営会議で承認されて、情報システム部の X 部長を責任者とするプロジェクト（以下、改善 PJ という）が発足した。改善 PJ では、DM 会員 DB を利用して、コールセンタから DM 会員に電話をかけて情報を提供するサービス（以下、情報提供サービスという）の追加を決めた。これらの業務を V 社に委託する場合を想定して、新システムにおけるコールセンタ業務の概要を表 1 にまとめた。

表 1 新システムにおけるコールセンタ業務の概要

業務	内容	作業員
Web 会員管理	Web 会員のメールアドレス、ID、パスワードの再設定及び削除を行う。	V 社社員
DM 会員登録・変更・削除	DM 会員の個人情報（住所、氏名、家族構成、購入製品など）の変更・削除。	V 社社員
問合せ受付	Web 会員、DM 会員の識別を行い、商品問合せの場合は V 社社員に、クレームの場合は R 社社員に引き継ぐ。記録は行わない。	V 社社員
問合せ回答（商品）	商品情報の提供、使用方法などを回答する。記録は行わない。	V 社社員
問合せ回答（クレーム）	Web 会員 DB、DM 会員 DB、クレーム DB を参照して、問合せ回答結果をクレーム DB に記録する。	R 社社員
情報提供サービス	DM 会員 DB にアクセスし、DM 会員をランダムに選択し、電話をかけて情報を提供する。反応状況を DM 会員 DB に記録する。	V 社社員

〔新システムへの移行に伴う認証とアクセス権の見直し〕

入社 10 年目になる H 君は情報システム部の係長で、改善 PJ において情報セキュリティに関するリ

ーダを任されている。H 君は、まず、新システムのコールセンタ業務ごとに、現行 DB に対するアクセス権について要件を分析した。既存システムでは、DB へのアクセス権は、R 社社員と V 社社員による 2 種類となっている。一方、新システムでは、新しい情報提供サービスのために、V 社社員が新たに DM 会員 DB にアクセスする必要がある。そこで、H 君は、表 1 の業務の概要を基に、コールセンタ業務と DB へのアクセス権との関係を表 2 のように整理して、X 部長と検討した。

表 2 新システムのコールセンタ業務と DB へのアクセス権との関係

業務 DB	Web 会員管理	DM 会員登録・ 変更・削除	問合せ受付	問合せ回答 (商品)	問合せ回答 (クレーム)	情報提供 サービス
Web 会員 DB	RW	R	ア	R	R	—
商品 DB	—	—	—	イ	—	—
クレーム DB	—	—	—	—	ウ	—
DM 会員 DB	—	RW	R	R	R	RW

注 R：読出し，RW：読出しと書込み（削除を含む），—：該当しない

H 君：表 2 の分析結果に基づいてアクセス権を設定したいと思います。

X 部長：分かった。君の提案するように業務単位のアクセス権に変更しよう。新システムでの本社の PC の接続についてはどうなるだろう。

H 君：本社 LAN の PC は、新たに導入したリバースプロキシサーバ 2 に、専用線経由で接続されます。このリバースプロキシサーバ 2 は、利用者の認証情報とアクセス権情報を 1 台の②RADIUS サーバから得ます。内部 LAN へのアクセス権があるときには、内部 LAN のサーバにも接続できます。また、この構成をとることで、シングルサインオンに容易に移行できます。

X 部長：認証情報が一元化されるので、アカウントや権限の変更作業の効率が向上するね。

〔管理業務と特権権限の運用〕

X 部長：さて、新システムでは、外部委託について監査があった方がよいね。

H 君：はい。情報システム部は、今まで、運用や管理権限について自己点検を実施してきたノウハウがあるので、監査を実施できると思います。

X 部長：いや、監査を実施する場合は、ノウハウよりも a を考慮することがまず必要と思うが、少なくとも、新システムの運用関係者と兼務させないようにすべきだろう。ところで、情報システム部に新システムの特権権限を与えるのは権限過剰だという意見もあるが、新システムではどうするつもりなのか。

H 君：今まで、情報システム部では、DB のバックアップ作業やサーバ異常時の対処のために、特権権限を利用してきました。また、S システムの運用業務では、V 社も特権権限を利用しています。

X 部長：V 社が日常の運用業務に特権権限を利用するのはよくないな。何か、対策はないものだろうか。

H 君：そうですね。表 3 に示すように、例えば、DB サーバを含む各種サーバの操作に必要な管理権限を分解して、担当する業務ごとに必要な権限だけ付与することにはどうでしょうか。一例として、V 社や情報システム部は、運用権限で日常業務を運用します。アプリケーション開

発ベンダは，保守権限でサーバのアプリケーションプログラムの変更などを行います。監査人は，監査権限ではほかの管理権限による操作記録を監査します。

表 3 DBサーバを含む各種サーバの操作内容と管理権限の対応

DBサーバ を含む各種サーバの操作内容	管理権限	特権 権限	保守 権限	運用 権限	監査 権限
保守者，運用者，監査人への管理権限の付与		○			
アプリケーションプログラムの変更		○	○		
サーバの停止・再開処理		○		○	
DBのテーブルの作成・削除		○	○		
サーバの故障修理		○		○	
登録されているプログラムの実行		○		○	
サーバのバックアップ		○		○	
サーバの管理業務に関するログ読出し		○			○

注 ○印は，実行可能な操作権限を示す。

X 部長：DBサーバを含む各種サーバの操作について，特権権限以外に，管理権限を保守，運用，監査と分けるのは良い考えだね。ところで，表 3 によると，権限の付与には，特権権限を使うことになるのだね。

H 君：そのとおりです。権限の付与は日常的な作業ではありません。また，操作記録がログに記録されるので，事後にチェックできます。

X 部長：ログに記録が残っていても，個人情報漏えいしてからでは遅いのではないかと。V 社社員が単独でサーバ室に入室して特権権限を行使する場合には，例えば，媒体などによる個人情報の漏えいを防ぐための③物理的な管理策も必要になるね。早速，検討してもらえないだろうか。

改善 PJ は，検討した後，表 3 及び物理的な管理策を採用することにした。その後，V 社に対してコールセンタ業務，運用業務の追加分と変更点について説明し，了解を得た。

[セキュリティポリシーの改訂とアクセス監視]

X 部長と H 君は，セキュリティポリシーの改訂とアクセス監視について，次のように検討した。

H 君：新システムでは，災害発生時のリスクや④V 社への業務委託によって新たにリスクが生じます。

また，社員の業務に無関係な Web 閲覧に関する対策が必要です。

X 部長：まず，新しいリスクにも対応できるように，セキュリティポリシーの改訂案を作成してほしい。また，V 社への業務委託の内容も見直そう。ところで，社員の業務以外の Web 閲覧対策はどうすればよいのか。

H 君：まず，業務上必要のない Web 閲覧が違反であることを，セキュリティポリシーに追記します。

次に，内部 LAN にあるサーバへの不正アクセスなどを含む違反を検出するために，アクセスを監視し，記録します。定期的に，違反の記録を分析して，該当者に警告します。

X 部長：いや，アクセスを監視する前に⑤社員に周知すべきことがある。これは私が担当しよう。ところで，社員のアクセスを監視するには，新しいサーバが必要になるだろうか。

H 君：いいえ，既存のサーバなどを活用できます。社員が，本社 LAN の PC から内部 LAN にあるサーバへアクセスする場合には， の通過トラフィックを監視します。また，インターネットへの Web 閲覧などについては， の通過トラフィックを監視します。

X 部長：Web 閲覧の通信内容が暗号化されているときにはどうするつもりなのか。ブログなどへの書込みによる情報漏えいのリスクもあるね。

H 君：それについては，常習的な違反が疑われる社員の PC に対して，S システムで利用していた⑥対策を行います。

X 部長：分かった。セキュリティポリシーの改訂とアクセス監視の準備に入ってほしい。

H 君は X 部長と相談の上，図 4 に示すようにセキュリティポリシーにⅡ.3.(2)，Ⅱ.3.(3)，Ⅱ.4.の物理的管理，Ⅱ.5.の危機管理，及びⅡ.6.の違反行為への対応を追記して改訂することにした。このセキュリティポリシーの改訂は，情報セキュリティ委員会に諮って承認を受けた。

セキュリティポリシー

R 社社長

I. 基本方針

(省略)

II. 対策基準

1. 適用範囲

(1) 本基準は，社員及び派遣社員に適用する。

(2) 本基準は，R 社で利用するすべての情報資産（ハードウェア，ソフトウェア，ネットワーク，データベース，記録媒体及び書類）に適用する。

2. 情報管理

(1) R 社が守るべき情報を，その重要度に応じて A（機密情報），B（個人情報，非公開情報），C（公開情報）の三つのランクに分ける。

(2) 重要度 A，B の情報を記録した記録媒体は R 社外（委託先を含む）に持ち出してはならない。

(3) 情報資産の運用管理については，情報システム部が責任をもつ。ただし，管理業務は外部に委託することができる。

3. アクセス管理

(1) 重要度 A，B の情報資産へのアクセスは，必要の原則に基づいて定める権限者，又は権限を委譲された者に限る。

(2) 重要度 A，B の情報資産へのアクセスをリアルタイムに監視して，記録する。記録は，定期的に監査する。

(3) 社員及び派遣社員は，業務上必要のない Web 閲覧やメール送信を行ってはならない。

(省略)

4. 物理的管理

(1) 重要度 A，B の情報資産を扱うコールセンタやサーバ室への入退には，IC カードを用いる。

(2) コールセンタやサーバ室では，適切な箇所に監視カメラを設置する。

(省略)

5. 危機管理

(1) 情報システムの異常や故障を発見した社員及び派遣社員は，直ちに情報システム部に連絡する。

(2) ⑦災害に備えて，復旧時に必要な対策を行う。

(省略)

6. 違反行為への対応

(1) 不正アクセスや情報漏えいなどを行った社員は， に基づいて懲罰を受ける。

(省略)

7. 情報セキュリティ教育

(1) 情報セキュリティ教育を定期的実施する。

(2) 重要度 A，B の業務を新たに担当する社員及び派遣社員には，情報セキュリティ教育の受講を必須とする。

(以下，省略)

図 4 R社のセキュリティポリシー（改訂後）

R社では，新システムへの移行と情報セキュリティポリシーの改訂を終了し，経営会議に報告して，新システムの正式運用に入った。

設問 1 次の (1) ～ (3) に答えよ

(1) 表 2 中 ～ に入れる適切な略字又は記号を答えよ。

(2) 本文中の に入れる適切な字句を，10 字以内で答えよ。

(3) 図 4 中の に入れる適切な字句を，5 字以内で答えよ。

設問 2 表 3 中の管理権限の保守権限と運用権限を分離した場合，分離しない場合と比較して良くなる点を二つ挙げ，それぞれ 40 字以内で述べよ。

設問 3 新システムについて，(1) ～ (3) に答えよ。

(1) 本文中の下線②の RADIUS サーバは，図 3 中の A～C のどこに接続するのがよいか，最も適切な箇所を，A～Cの中から選び，記号で答えよ。

(2) 本文中の ， に入れる適切なサーバ名を答えよ。

(3) 本文中の下線⑥の対策を，40 字以内で述べよ。

設問 4 本文中の下線③の物理的な管理策を，30 字以内で述べよ。

設問 5 セキュリティポリシーについて，(1) ～ (4) に答えよ。

(1) 本文中の下線①の違反とは何か。該当する図 4 中の項目の番号を，例えば I.1.(1)のように答えよ。また，違反している R 社の業務内容を，40 字以内で述べよ。

(2) 図 4 中の下線⑦について，新システムへの移行によって必要となる災害復旧対策を，40 字以内で述べよ。

(3) 本文中の下線⑤の周知すべき内容を，30 字以内で述べよ。

(4) 本文中の下線④の新システムの業務委託で新たに生じるリスクを，40 字以内で述べよ。また，業務委託に付随して行うべき具体的な管理策を，60 字以内で述べよ。