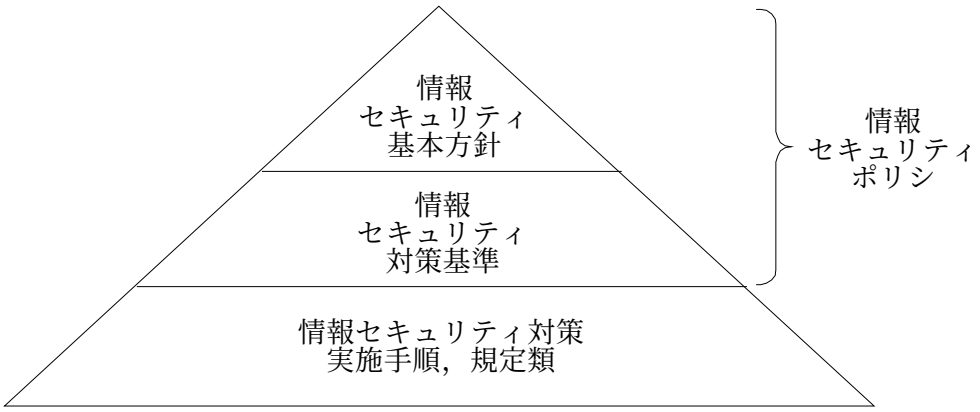
平成１６年度　秋期　情報セキュリティアドミニストレータ　午後Ⅱ問題

〔情報セキュリティポリシの位置付け〕

情報セキュリティポリシの位置付けは、次のとおりとする。



問１　個人情報の漏えい対策に関する次の記述を読んで，設問１～５に答えよ。

Ｖ社は, ホテルやスポーツクラブを経営している企業で, 従業員数 2,000 名, 年商は 500 億円である。Ｖ社は，ゴルフ場，テニスコートなどを運営する企業が合併することによって 10 年前に設立されホテルとスポーツクラブを全国 20 都市に展開してきた。ホテルやスポーツクラブの利用者向けに，磁気ストライプを用いた会員制ポイントカードを発行し，それが好評で売上を伸ばしている。本社には，営業企画部，総務部，情報システム部などがある。

〔情報システムの概要〕

Ｖ社は，ホテル業務とスポーツクラブ業務用の情報システム（以下，Ｖシステムという）を開発し，ポイントカード会員の氏名，住所，生年月日，性別，所属スポーツクラブなどのデータベース化された個人情報（以下，個人データという）の管理や，インターネットへのアクセスなどに利用している。図 1 に，Ｖシステムの構成を示す。

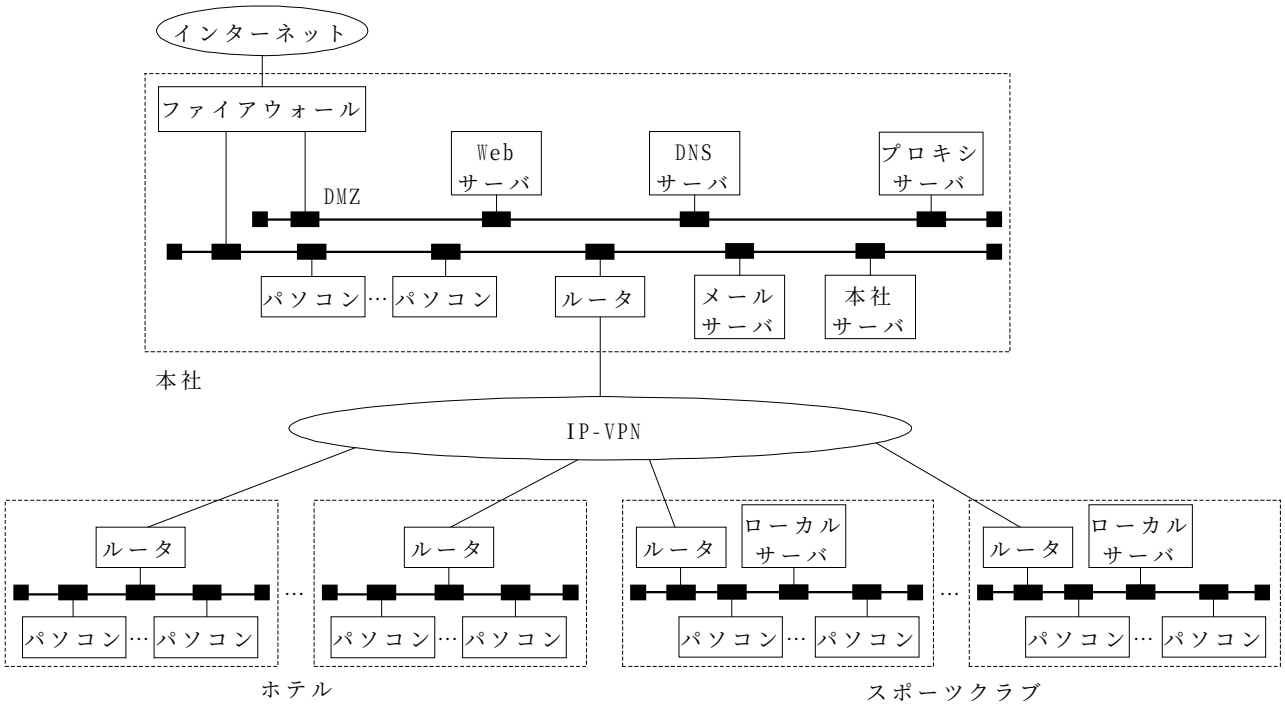


図１　Ｖシステムの構成

会員は，インターネットを経由して Web サーバにアクセスし，ポイントカードに記載されている会員番号でホテルやスポーツクラブを予約する。この予約データは，本社サーバに保存される。ただし，スポーツクラブの予約データは，本社サーバから該当するスポーツクラブのローカルサーバに転送される。

ホテルでは，本社サーバにアクセスして予約データを得て，宿泊客リストの印刷などの処理を行っている。また，会員がチェックアウトした際に，ポイントの利用状況を本社サーバに送信している。

スポーツクラブでは，インストラクタがパソコンのブラウザからローカルサーバにアクセスして，会員の予約データと個人データを基に，健康面からの制限事項を考慮したスポーツメニューを作成する。また，会員がスポーツを終えた後に，インストラクタが時間数，会員のポイントの利用状況や特記事項などを入力している。各スポーツクラブの事務所では，毎月 20 日締めで会員の施設利用状況をローカルサーバからパソコンにダウンロードして，会員への請求書と銀行への口座振替依頼書を作成している。

本社情報システム部は，Ｖシステムのネットワーク機器やすべてのサーバを運用管理し，ウイルス，不正侵入，情報漏えいなどの対策を行っている。

〔第 1 の事件〕

T スポーツクラブ（以下，T クラブという）では，会員が急増し，1 日当たりの利用会員が 400 名を超えることがある。T クラブには，クラブ長，管理部長，インストラクタ部長，及び従業員（事務員が 3 名，インストラクタが 30 名，派遣社員が 5 名）がいる。また，インストラクタのうち，20 名はアルバイトである。管理部長は T クラブの情報セキュリティ責任者であるが，多忙なこともあって，従業員に対する情報セキュリティ教育がおろそかになりがちで，利用者 ID とパスワードの付与については事務員任せになっている。事務員及び派遣社員は，利用者 ID を共用している。

請求処理で忙しい 9 月 21 日の未明に，T クラブで事件が起こった。T クラブの事務所が泥棒に侵入され，現金，預金通帳及びパソコン 1 台が盗まれた。21 日の朝に，出勤してきたインストラクタが盗難に気付いた。連絡を受けたクラブ長が，盗まれたパソコンを操作していた派遣社員に前日の作業内容をヒアリングしたところ，当該月の会員への請求データと銀行への口座振替データがパソコンに保存されたままであることが分かった。クラブ長は警察に盗難届を出したが，個人データ漏えいの可能性については言及しなかった。

その後，クラブ長が本社に対応の支援を依頼したところ，本社から，防犯対策担当者である総務部長と情報システム部の情報セキュリティ担当者である H 君が, 調査のために T クラブに派遣されてきた。H 君は，まず関係者にヒアリングし，次に T クラブのローカルサーバを調査した。調査を終えて，本社に戻った H 君は，上司の B 部長と相談して，図 2 の対応策をまとめた。

(1)“個人データ漏えいの可能性”について警察に届け出るとともに，マスコミに公表すること。また，該当する会員に対して，事件の概要とパソコン上の個人データ項目，今後起こる可能性のある事故とその場合の注意点について説明したおわびの文書を発送すること。
(2) T クラブの情報セキュリティ担当者を決めて，個人データへのアクセス履歴を定期的にチェックさせること。
(3) T クラブの従業員などに対して，個人データの取扱方法について教育すること。その場合，情報システム部が作成した Web ベースシステムを活用して，習得させること。
(4) パソコン上の個人データは，作業終了時には消去させること。
(5) 事務員及び派遣社員には，利用者 ID を共用させないこと。

図２　対応策

クラブ長は，対応策を受けて警察に届け出て，マスコミにも公表した。同時に，H 君の調査で個人データの漏えいが判明した 512 名の会員に対して，図 3 に示すおわびの文書を郵送した。

平成 16 年 9 月 25 日

会員各位

V社 T スポーツクラブ長△△○○

おわび

拝啓　秋冷の候，皆様にはますますご健勝のこととお慶び申し上げます。また，平素より T スポーツクラブをご利用いただきありがとうございます。

当クラブでは，皆様の個人情報管理には十分配慮してまいりましたが，［　ア　］。お客様には十分注意していただき，何か，ご不明な点，お気付きの点などがございましたら，下記までお問い合わせください。

このたびは，当クラブの不十分な管理によって，皆様に大変ご迷惑をおかけしましたことを心からおわび申し上げます。今後とも，皆様のご利用をお待ちしております。

敬具

お問合せ先：T スポーツクラブ管理部長××◇◇，電話：0#-1###-5###
受付時間：午前 9 時～午後 6 時（月～金），午前 10 時～午後 3 時（土，日，祝日）

図３　Ｔクラブからのおわびの文書

〔第 2 の事件〕

S ホテルは，部屋数が 200 室あり，きめ細かいサービスと料理で人気がある。S ホテルには，K 支配人のほか，従業員が 45 名（アルバイト 25 名を含む）いる。繁忙期には得意客で満室になるので，近隣のホテルに応援者を頼み，フロント業務を手伝ってもらっている。S ホテルの従業員や応援者は，必要の都度，S ホテルのフロントと事務所に設置されているパソコンからＶシステムにアクセスする。この際, 上司の許可を得てアクセスし, 宿泊客リストを印刷して, 部屋割りと食事のメニューを決めている。この宿泊客リストは，従業員や応援者が利用後，自らの判断によって廃棄している。ただし，宿泊者名簿は，旅館業法に従って別に紙で保管している。

ある日 G 氏が，宿泊とスポーツがセットになった，S ホテルの“ダイエットプラン”に申し込んだ。G 氏には，会員の登録情報どおり，禁煙室，L サイズの浴衣及び低カロリ食が用意された。ところが, 宿泊した日の 2 週間後から, ダイエット食品に関する不審なダイレクトメールが G 氏に郵送されるようになった。G 氏へのあて先が，ポイントカード登録時の記載誤りのある住所であったことから，G 氏はＶ社に問い合わせた。Ｖ社が調査したところ，G 氏が宿泊した日の宿泊客リストが盗まれていたことが分かり，Ｖ社は，当日利用した宿泊客に謝罪し，公表した。

〔リスク分析と情報セキュリティポリシの見直し〕

Ｖ社の A 社長は，二つの事件を受けて，Ｖ社としての対策が必要と判断し，個人情報の管理体制とＶシステムの改善を B 部長に指示した。B 部長は, H 君と個人データ漏えいに関するリスク分析を行った。次は，B 部長と H 君の会話である。

H 君：現在，ホテルとスポーツクラブで利用されている個人データの管理は不十分で，漏えいリスクは高いと思います。当社は，2005 年に全面的に施行される個人情報保護法に規定されている［　a　］に該当し，個人データの安全管理措置が義務付けられます。ですから，個人データ漏えいに対するリスク対策は必須です。

B 部長：そうか。リスクとリスク対策について詳しく説明してくれないか。

H 君：リスク対策には 4 種類あり，リスクの被害規模と発生頻度によって対策を選択するという考え方があります。例えば，被害規模が大きく，発生頻度が高いリスクの場合には，リスクを回避します。また，被害規模が大きいリスクの場合には，発生頻度が低くても，リスク保険などに［　b　］します。一方，被害規模が小さく，発生頻度が高いリスクの場合には，リスク対策の費用対効果が最適となるように，発生頻度の低減対策を行います。

B 部長：では，T クラブや S ホテルの場合には，どうすべきなのか。

H 君：どちらの場合も，大量の個人データを扱っています。現状のままでは，個人データ漏えいによる被害規模が大きく，発生頻度も高いので，リスクを回避すべきです。T クラブでは，個人データをパソコン内に保存しないようにするか，保存するときにはデータを暗号化して，漏えいしても読まれる可能性を減少させるべきです。また，S ホテルでは，宿泊客リストを印刷すべきではありません。個人データ漏えいの発生頻度を減少させるには，アクセスを厳しく制限する必要があります。

B 部長：分かった。まず，個人データへのアクセス制限の強化から始めよう。当社の情報セキュリティポリシの見直しと遵守させるための方策を検討してもらいたい。

〔Ｖ社の情報セキュリティポリシ〕

Ｖ社の情報セキュリティポリシは，情報システム部が中心となって 4 年前に作成されていた。しかし，ホテルやスポーツクラブの役員，管理職，従業員などへの周知や Web ベースシステムを活用した教育が十分に実施されておらず，必ずしも遵守されていない。そこで，H 君は B 部長の指示を受けて，ホテルやスポーツクラブの情報セキュリティ責任者で構成される情報セキュリティ委員会において，情報セキュリティポリシの問題点と改善策について検討した。その結果を図 4 に示す。

（i）ホテルやスポーツクラブでは，派遣社員やアルバイトが多く，しかも頻繁に入れ替わるので，利用者 ID とパスワードの発行，停止は，本社で迅速に行う。
（ii）従業員などが情報セキュリティポリシに違反した場合に備え，［　c　］規定が必要となる。
（iii）ホテルやスポーツクラブを対象に，情報セキュリティを定期的に評価する。
（iv）情報システム部による S ホテルの事故対策では，個人データ漏えいを防ぐために，事実上宿泊客リストの印刷を禁じている。これでは，ホテルのサービス低下を招くので，上司が宿泊客リストの中からサービス提供に必要な最小限の項目を抜き出して印刷した接客カードを，従業員や応援者に渡す。

図４　情報セキュリティ委員会で決定した改善項目

情報セキュリティ委員会は，図 4 の（i）～（iv）の改善項目を盛り込んだ情報セキュリティポリシの改訂案を作成した。この改訂案は，Ｖ社の経営会議で承認された（図 5）。

情報セキュリティポリシ

社長

Ⅰ．基本方針

Ｖ社は，ホテルとスポーツクラブの運営を通じて，お客様に満足していただけるサービスを提供する企業である。お客様サービスにとって重要な個人情報に関する情報セキュリティの確保を最優先に行動する。

Ⅱ．対策基準

1．適用範囲

（1）本基準は，役員，管理職及び従業員に適用する。

（2）本基準は，Ｖ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．情報セキュリティ委員会

（省略）

（3）情報セキュリティ委員会は，必要に応じて情報アクセス管理者を任命する。

（省略）

3．情報の管理

（1）Ｖ社が守るべき情報には，その重要度に応じてA（きわめて重要）～D（重要でない）のランクを付ける。

なお，個人情報は，A ランクとする。

（2）A ランクの情報をパソコンで取り扱う場合には，業務終了時に消去する。

（3）A ランクの情報の印刷，コピー及び破棄は上司の許可を得てから行い，管理記録を残す。

4．アクセス管理

（1）A ランクの情報を保存する機器は，物理的に［　d　］する。

（2）情報資産への適切なアクセス権限を設定する。

（3）従業員が個人データにアクセスする場合には，その都度，情報アクセス管理者の許可を得る。

（4）利用者 ID とパスワードの発行，停止は，本社で迅速に行う。

（5）利用者 ID は，共用しない。

（6）本社サーバと各スポーツクラブのローカルサーバへのアクセス記録は，すべて［　e　］に残し，その内容を定期的にチェックする。

5．インターネットアクセス

（省略）

6．事故対応

（省略）

7．Web ベースシステムによる教育

（省略）

8．情報セキュリティ監査

（省略）

9．［　c　］規定

（以下，省略）

図５　Ｖ社の情報セキュリティポリシ（改訂後）

〔情報セキュリティの支援と情報セキュリティ監査〕

H 君は，承認された情報セキュリティポリシを浸透させるために，表に示すような情報システム部による情報セキュリティの支援を提案し，B 部長の承認を得た。

表　情報システム部による情報セキュリティの支援

項目	支援内容
システムの運用支援	・利用者 ID とパスワードの迅速な発行，停止 ・Ｖシステムのログの定期的な監視 ・ヘルプデスクの設置
緊急対策の支援	・個人データ漏えい対策やウイルス対策など，緊急を要する情報セキュリティ対策に関する対応とアドバイス
教育の支援	・Web ベースシステムの教育コンテンツに［　イ　］を追加
情報セキュリティ評価などの支援	・情報セキュリティ対策の実施状況の定期的な評価 ・第三者による情報セキュリティ監査への対応 ・自己点検の支援

Ｖ社のスポーツクラブやホテルでは，情報セキュリティの支援体制が整ったことから，情報セキュリティポリシが浸透するようになり，情報セキュリティの改善が進んできた。しかし，情報セキュリティポリシに対する理解がまだ不十分なところもある。

そこで，A 社長は，個人情報保護を実現するための情報セキュリティポリシを更に徹底させるために，社外の情報セキュリティ監査チームに監査を依頼した。図 6 に，その報告書を示す。

情報セキュリティ監査報告書

1．全般事項

Ｖ社の本社では，個人情報に関するリスクマネジメントが実施され，個人情報保護法に準拠するための情報セキュリティ支援体制が整ったことは評価できる。ただし，バランスのとれたリスクマネジメント実現に向けた改善と，経営陣によるリーダシップが必要である。

2．指摘事項

（1）S ホテルの現在の運用では，個人データへのアクセス権限をもっているのは K 支配人だけであり，K 支配人の不在時に業務に支障を来している。情報セキュリティポリシのⅡ.4.(3)を踏まえ，アクセス権限の付与を含めてコントロールを見直す必要がある。

（以下，省略）

図６　情報セキュリティ監査報告書

情報セキュリティ監査報告書を受け取った A 社長は，B 部長に，早急に指摘事項を実施するよう指示した。また，A 社長は，個人情報に関する情報セキュリティ管理を徹底させるために，自ら，ホテルやスポーツクラブを訪れて，リスク分析の必要性とそれに基づいた個人情報に関する情報セキュリティのマネジメントについて説明することにした。

設問１　本文中の［　a　］～［　e　］に入れる適切な字句を答えよ。

（1）［　a　］については，10 字以内で答えよ。

（2）［　b　］～［　e　］については，解答群の中から選び，記号で答えよ。

解答群

ア　移転　　イ　移動　　ウ　隔離　　エ　採用　　オ　出力
カ　対応　　キ　入退室　　ク　罰則　　ケ　分離　　コ　ログ

設問２　第 1 の事件に関する次の問いに答えよ。

（1）本文中の下線で示した，H 君の調査の目的を，30 字以内で述べよ。

（2）図 2 中の(5)で指摘している利用者 ID の共用による問題点を二つ挙げ，それぞれ 20 字以内で述べよ。

（3）図 3 中の［　ア　］に入れる適切な字句を，100 字以内で述べよ。

設問３　第 2 の事件に関する解決策として，図 4 中の（iv）に示す改善項目が決定された。しかし，このままでは，第 2 の事件の抜本的な解決には至らない。上司が更に実施すべきことを，25 字以内で述べよ。

設問４　Web ベースシステムで提供する教育に関する次の問いに答えよ。

（1）第 1，2 の事件への対応策として，表中の［　イ　］に該当する教育項目を二つ挙げ，それぞれ 15 字以内で述べよ。

（2）Web ベースシステムを使って，ホテルやスポーツクラブの従業員などを教育するとき，教育効果を上げるために H 君が留意すべき点を二つ挙げ，それぞれ 30 字以内で述べよ。

設問５　情報セキュリティアドミニストレータであるあなたは，図 6 中の 2.(1)の指摘事項に基づいた運用改善策を求められている。図 5 中のⅡ.4.(3)に対応した改善策を，60 字以内で述べよ。

問２　事業継続計画の策定に関する次の記述を読んで，設問１～５に答えよ。

L 社は，土地，建物の売買仲介業や賃貸仲介業などを営む，社員数 820 名の不動産会社である。東京に本社を置き，全国 120 か所に営業所をもつ。L 社が扱っている土地，建物の物件数は，常時約 13 万件である。本社には，営業統括本部，経営企画部，総務部，人事部，財務部，情報システム部がある。営業統括本部は，全国の営業所を統括している。L 社では，5 年前から，表 1 に示すサブシステムで構成される情報システム（以下，L システムという）を運用してきた。

表１　Ｌシステムの概要

サブシステム	内容	サーバ
人事 サブシステム	人事部と営業所の人事担当者が社員情報を入力し，集計表作成，辞令作成，人事一覧表作成，人事考課データ管理などを行っている。	人事サーバ
会計 サブシステム	財務部と営業所の会計担当者が会計データを入力し，予算管理，資金管理，伝票処理などを行っている。	会計サーバ
営業管理 サブシステム	営業所の営業担当者が不動産情報を入力し，物件管理，契約書作成，顧客情報管理，営業履歴管理を行っている。営業管理サーバには，L 社の取り扱う不動産情報と顧客の個人情報が保管されている。個人情報保護の観点から，顧客の個人情報は，営業所では保管せずに，営業管理サーバ上で厳重に集中管理している。	営業管理サーバ
不動産 Web サブシステム	営業管理サーバから不動産情報だけを取り出して，インターネットで一般顧客に公開している。営業所の社員も不動産サーバにアクセスし，自社で取り扱う不動産情報を検索している。	不動産サーバ
広報 Web サブシステム	企業概要，事業内容，営業所情報などの企業情報を提供する。広報サーバ内のコンテンツは，総務部が各部署から収集し，社外に公開している。	広報サーバ
電子メール サブシステム	L システム内のネットワーク又はインターネットを通じて，電子メールを送受信している。	メールサーバ

L システムの各サーバは，本社から徒歩で 10 分ほどの所にある，外部委託先の M 社のデータセンタ（以下，M センタという）に設置され，ハウジングサービスを受けている。また，L 社本社や営業所と M センタ間は，IP-VPN で接続されている。各サーバは，本社の情報システム部で管理していて，トラブルが発生した場合，情報システム部のパソコンで状況を確認し，情報システム部の部員が M センタに直接赴いて，作業を行うことになっている。図 1 に，L システムの構成を示す。

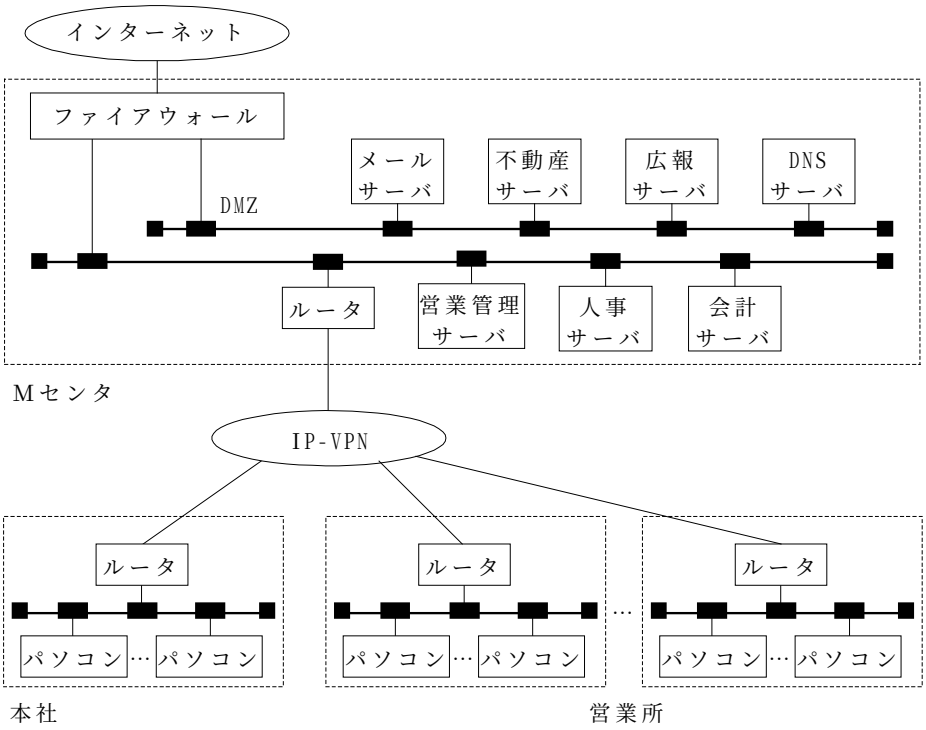


図１　Ｌシステムの構成

〔情報セキュリティポリシの策定〕

L 社では，L システムの導入後，業務の L システムへの依存度がきわめて高くなってきた。情報セキュリティに関する事故や事件が社会問題となり，情報セキュリティの確保が企業の経営課題と認識される中，L 社の経営会議でも L システムの情報セキュリティ対策について検討を重ねてきた。その一つとして，昨年，情報システム部が中心となって，ISMS 認証基準などを参考に情報セキュリティポリシを策定した。情報セキュリティポリシの策定後，順次，サブシステムの運用体制や運用手順を見直していて，今回，事業継続計画（Business Continuity Plan）を策定することになった。

情報セキュリティポリシでは，事業継続計画に関して図 2 のように定めている。

（1）重大な障害又は災害の影響から重要な情報を保護するために，全社的な［ a ］を行い，その結果に基づいた事業継続計画を事前に策定し，文書化する。
（2）業務への影響を考慮し，適切な時間内にシステムを復旧させるための計画を立てる。
（3）重大な障害又は災害を受けたときのバックアップシステムへの移行を含む計画を立てる。
（4）社員が事業継続計画を理解し，かつ，事業継続計画が有効であることを確認するために，少なくとも年 1 回の試験を行い，見直すことにする。

図２　情報セキュリティポリシ（事業継続計画に関する項目の抜粋）

〔事業継続計画の検討〕

事業継続計画の策定は，情報システム部の X 部長，Y 課長，情報セキュリティアドミニストレータの Z 主任を中心としたプロジェクトチームで行われた。X 部長，Y 課長と Z 主任は，図 2 を基に事業継続

計画を検討した。

X 部長：事業継続計画では，限られた時間内で，各サーバを順次復旧することを考えなければいけないな。適切な時間内にシステムを復旧させるためには，各サーバの許容停止時間を決めるべきだが，どうやって決定すればよいかな。

Z 主任：そうですね。情報セキュリティポリシにあるように［ a ］を行い，その結果を用いて，サーバ類が停止した場合の業務への影響を考えることが重要です。L システムでは，サーバの停止時間を，ほぼ業務が中断する時間と考えることができます。被災で業務が中断した場合，バックアップシステムに移行して業務を継続するか，又は，手作業などの代替手段によって業務を継続することによって対応できます。ですから，サーバの許容停止時間を検討するには，代替手段の調査も必要です。

Y 課長：まずは，L システムの各サーバについて，業務への影響度や代替手段を調査し，サーバの許容停止時間を決定します。

X 部長：それに加えて，L システムのバックアップシステムを具体的に検討するには，設置場所の選定やバックアップ方法の見直しが必要だろう。

Y 課長：分かりました。

〔サーバの許容停止時間の検討〕

Y 課長と Z 主任は，各サーバが停止した場合の業務への影響度と代替手段を調査した。調査は，各部署や営業所の社員に対するヒアリングによって実施された。その調査結果を基に，プロジェクトチーム内でサーバの許容停止時間を，表 2 のようにまとめた。

表２　サーバの許容停止時間

サーバ	業務への影響度	代替手段		許容停止時間
		有無	内容	
人事サーバ	中	有	各営業所で，紙媒体の帳票を用いて手作業で行う。	レベル 3
会計サーバ	大	有	各営業所で，紙媒体の帳票とパソコンの表計算ソフトを使って作業を行う。	レベル 2
営業管理サーバ	大	無	－	レベル 1
不動産サーバ	大	無	－	レベル 1
広報サーバ	中	無	－	レベル 2
メールサーバ	中	有	ほかの通信手段で対応する。	レベル 3
DNS サーバ	大	無	－	レベル 1

注　許容停止時間の目安　　レベル 1：24 時間以内に復旧する
レベル 2：3 日以内に復旧する
レベル 3：10 日以内に復旧する

〔バックアップシステムの具体的な検討〕

プロジェクトチームは，バックアップシステムの具体的な検討を行った。本社と M センタを含む広域災害が起こった場合を想定し，本社から電車で約 1 時間半の距離にある D 社のデータセンタ（以下，D センタという）にバックアップシステムを設置することにした。

Y 課長と Z 主任は，D センタの運用と新しい日常バックアップ方法の概要を，図 3 のようにまとめた。

（1）バックアップシステムの設置とネットワークの確保
　（a）レベル 1 のサーバと同一仕様のハードウェアを事前に設置し，L システムと同じ状態にするため，更に［　b　］しておく。
　（b）レベル 1 のサーバを管理するためのパソコンを事前に設置しておく。
　（c）L システムの IP-VPN を使用できるようにしておく。
（2）L システムのバックアップ方法
　（a）対象となるバックアップデータは，L システムのアプリケーションのデータファイルとする。
　（b）情報システム部の部員は，バックアップデータを取得し，DVD 媒体に保管する。
　　①　毎週火曜日の業務終了後，フルバックアップデータを取得する。
　　②　毎営業日（火曜日を除く）の業務終了後，差分バックアップデータを取得する。
　（c）バックアップデータは，保管委託先である C 社に宅配便で移送する。
　（d）バックアップデータは，3 世代分を保管する。

図３　Ｄセンタの運用と新しい日常バックアップ方法の概要

Y 課長は，D センタの運用と新しいバックアップ方法の概要を X 部長に報告した。

X 部長：D センタにレベル 1 のサーバと，そのサーバを管理するパソコンだけを設置するのだな。それ以外は，どうするのかね。

Y 課長：はい。レベル 2，3 のサーバを復旧するために必要なハードウェアやソフトウェアは，事前に必要機材一覧にまとめておきます。これらは，L システムの構築を依頼したシステムインテグレータの E 社に事前に連絡をとり，被災時に納入できるようにしておきます。また，バックアップデータには，我が社の営業情報や顧客の個人情報が多く含まれているので，バックアップデータの保管委託先としては，厳重な保管管理で有名な C 社を選定しました。C 社に保管するバックアップデータは，必要機材一覧に記載された機材とは別に管理します。

〔事業継続計画の策定〕

Y 課長と Z 主任は，事業継続計画の策定に当たって，盛り込むべき内容を調査し，その結果を図 4 のようにまとめた。

1．事前の準備
（1）被災時の非常時対応手順，被災時連絡先一覧，必要機材一覧などを整理して，文書化しておく。
（2）被災時連絡先一覧には，電子メール以外の複数の連絡手段による連絡先をまとめておく。
（省略）
2．非常時対応手順の主な内容
（1）非常時対応チームの設置
（a）平常システムの被災連絡を受けた者は，事前に決定しておいた統括者へ速やかに連絡する。
（b）統括者は，事前に決定してある非常時対応チームメンバに連絡し，非常時対応チームを編成する。
（c）非常時対応チームは，被災時連絡先一覧に従って連絡する。
（d）経営陣にも連絡して，適切な判断を下せる体制を整える。
（2）バックアップシステムへの移行の判断
（a）バックアップシステムへの移行を判断するために，非常時対応チームで平常システムの稼働状況及び被災状況を調査する。
（b）バックアップシステムに移行し，情報システムが復旧するまでの［　c　］を見積もる。
（c）平常システムの状況と［　c　］などを経営陣に報告し，バックアップシステムで情報システムを復旧すべきかどうかの判断を仰ぐ。
（d）バックアップシステムに移行しない場合は，(5)に従う。
（3）バックアップシステムへの移行準備
（a）非常時対応チームの適切な人員と応援要員で構成された移行チームを編成する。
（b）移行に必要な資源を検討し，準備する。
（c）バックアップシステム設置場所への，必要な資源の移送手段と移送経路を確認する。
（d）バックアップシステムの稼働開始時刻の見通しについて検討し，経営陣に報告する。
（e）業務に影響を受ける部署に［　c　］を連絡する。
（4）バックアップシステムでの復旧作業
（a）バックアップシステムで使用する資源を受け入れる。
（b）バックアップシステムの環境設定を行い，アプリケーションとデータファイルを復元する。複数のサーバ間で利用しているデータの整合性の検証を行う。
（c）バックアップシステムの正常稼働確認後，ネットワークの切替えを行う。
（5）平常システムでの復旧作業
（省略）

図４　事業継続計画に盛り込むべき内容

プロジェクトチームでは，図 4 に基づいて，事業継続計画案として非常時対応手順（案），被災時連絡先一覧（案），必要機材一覧（案）をまとめた。ここでは，非常時対応手順（案），被災時連絡先一覧（案）を図 5，6 に示す。

1．非常時対応チームの設置
（省略）
2．D センタのバックアップシステムへの移行の判断
（省略）
3．D センタのバックアップシステムへの移行準備
（1）情報システム部と他部署や近隣の営業所の社員で，移行チームを編成する。
（2）E 社に連絡し，必要機材一覧に示した機材を納入するように指示する。
（3）［ d ］。
（4）D センタまでの機材や移行チームの移送手段と移送経路を確認する。
（5）D センタでのバックアップシステムの①稼働開始時刻の見通しを，担当役員に報告する。
（6）営業統括本部，総務部，人事部，財務部に［ c ］を連絡する。
4．D センタのバックアップシステムでの復旧作業
（省略）
5．M センタでの L システムの復旧作業
（省略）

図５　非常時対応手順（案）

社名	部署名	一次連絡者	連絡先 （ e ） （ f ）	二次連絡者	連絡先 （ e ） （ f ）
L 社	営業統括本部	○○課長	×××××× ××××××	○○主任	×××××× ××××××
	⋮	⋮	⋮	⋮	⋮
	財務部	○○課長	×××××× ××××××	○○主任	×××××× ××××××
⋮	⋮	⋮	⋮	⋮	⋮
E 社	△△部	○○主任	×××××× ××××××	○○課長	×××××× ××××××

図６　被災時連絡先一覧（案）

〔事業継続計画案の評価試験の実施〕

事業継続計画案が一通り作成され，事業継続計画案が有効かどうかを評価するために評価試験を実施することにした。評価試験は，初めに小規模なテストデータを使う試験と，次に，事業継続計画の完成度を高めるために，C 社に保管してあるバックアップデータを使う試験の，2 段階で行うことにした。また，必要なハードウェアはレンタル会社から借りることにした。

最初の試験は，M センタの隣のビルから火災が発生し，M センタに延焼したので，すべてのサーバが

利用不可能になることを想定して行った。

最初の試験は予定どおり終了し，Y 課長と Z 主任は，試験の結果を X 部長に報告した。

Y 課長：最初の試験は，非常時対応チームの設置から，移行チームによる小規模なテストデータを使ったバックアップシステムの正常稼働の確認まで，予定どおり行うことができました。今回は，情報システム部だけで移行チームを編成したこともあり，バックアップシステムへの移行作業も順調に終わりました。次回の試験では，C 社に保管してあるバックアップデータを使う予定です。

X 部長：なるはど。C 社に保管してあるバックアップデータを使えば，より一層，実際の環境に近くなるな。次回の試験では，移行チームとして情報システム部以外の社員も参加させたいが，平常業務中では，協力を求めることは難しいだろうな。何かいいアイデアはないか。

Y 課長：そうですね。それでは，当社の社員の代わりに外部の人間に参加させることにして，E 社と新たに試験のための業務委託契約を結びたいと思います。

Z 主任：今回の試験で，非常時対応手順どおりに実施できることが確認できました。次回の試験で，C 社に保管してあるバックアップデータを使い，移行チームには情報システム部以外の者に参加してもらうことによって，事業継続計画の完成度も高まります。ただし，次回の試験方法では，情報漏えい防止の観点から不安な点があります。その対策も含めて，②次回の試験計画を立てたいと思います。

以上の議論を基に，次回の試験計画が策定され評価試験が実施された。評価試験は順調に終了し，事業継続計画案は正式に承認された。

設問１　本文中の［ a ］，［ c ］，［ e ］，［ f ］に入れる適切な字句を答えよ。

（1）［ a ］，［ c ］については，解答群の中から選び，記号で答えよ。

解答群

ア　運用体制構築　　イ　許容停止時間　　ウ　コスト

エ　コスト評価　　オ　システム停止時間　　カ　リスク評価

（2）［ e ］，［ f ］については，被災時における適切な連絡手段を，それぞれ 10 字以内で答えよ。

設問２　表 2 に関する次の問いに答えよ。

（1）被災時に遅延や混乱なく代替手段をとるために，帳票，表計算ソフト，ほかの通信手段の準備以外に，事前に行っておくべき運用面での対策を，20 字以内で述べよ。

（2）表 2 中で，営業管理サーバの代替手段を“無”と判断した理由を二つ挙げ，それぞれ 20 字以内で述べよ。

設問３　レベル 1 のサーバを，被災時に迅速に復旧できるようにするために行っておくべきこととして，図 3 中の［ b ］に入れる適切な字句を，40 字以内で述べよ。

設問４　図 5 に関する次の問いに答えよ。

（1）図 5 中の［　d　］に入れる適切な字句を，30 字以内で述べよ。

（2）下線①を検討する場合，考慮すべき重要な“時間”を三つ挙げ，それぞれ 20 字以内で具体的に述べよ。

設問５　情報漏えい防止の観点から，本文中の下線②に盛り込まれた対策を二つ挙げ，それぞれ 40 字以内で述べよ。