平成１８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

問１　認証機能に関する次の記述を読んで，設問 1～3 に答えよ。

V 社は，社員数 150 名の企業で，主に各地の名産品や各国から輸入した食料品の通信販売を行っている。従来，V 社は，雑誌に広告を掲載し，電話やファックスによる注文受付を行っていた。V 社には，商品企画や営業活動，顧客からの注文受付を行う営業部，商品の仕入れや在庫管理，営業部で受け付けた商品の発送などを行う商品管理部，一般事務を行う総務部，及び情報システムの管理を行う情報システム部がある。

今年，V 社では，ビジネスの拡大を目指して，インターネットによる注文受付を開始した。また，継続的に顧客を確保するために，キャンペーン商品や各地の名産品の情報，各国から輸入した食料品に関するコラムなどを掲載した無料のメールマガジン（以下，メルマガという）を毎週提供することにした。

〔V 社のシステム概要〕

V 社では，インターネットによる注文受付を開始する以前から，商品の管理に関して商品管理サーバを構築し，利用していた。社員は，商品管理サーバにアクセスすることによって，商品の在庫状況を確認できる。今回，注文受付 Web サーバ，注文受付サーバ及びメルマガサーバを構築した。構築後の V 社のシステム（以下，Q システムという）の概要を図 1 に，Q システムで使用する ID 種別を表に示す。

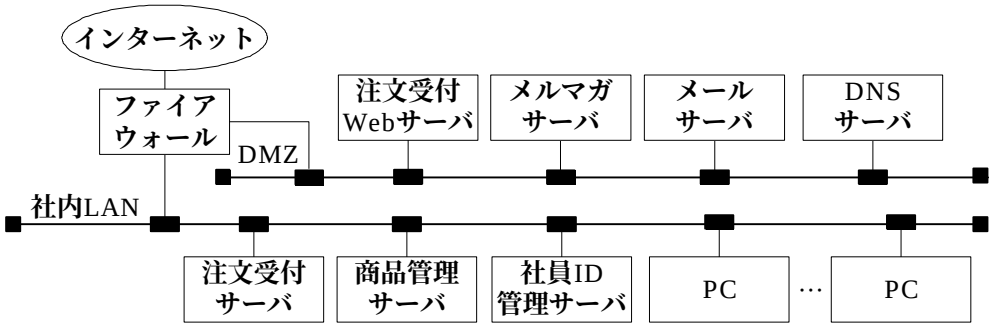

図１　Qシステムの概要

表　Qシステムで使用するＩＤ種別

ID 種別	概　要
会員 ID	・顧客がインターネット上で会員登録を行った際に発行される ID で，注文受付サーバで管理される。 ・顧客は，会員登録時にパスワード，氏名，住所，電話番号，生年月日，電子メールアドレス，クレジットカード情報を登録する。会員登録が完了すると，会員 ID が発行される。 ・顧客は会員登録後，会員 ID とパスワードを使って注文受付 Web サーバにアクセスし，注文受付サーバで管理するパスワードを変更することができる。パスワードを忘れた顧客のために，①パスワードリマインド機能（会員登録時に設定した電子メールアドレスを入力することで登録したパスワードが電子メールで送信される仕組み）が備えられている。

社員 ID	・すべての社員に割り当てられる ID で，社員 ID 管理サーバで管理される。 ・社員は，社員 ID とパスワードを利用して認証され，PC，メールサーバ，商品管理サーバ及び社員 ID 管理サーバにアクセスすることができる。 ・初期パスワードは，情報システム部でランダムな文字列を作成して保存するとともに，利用開始時に本人あてに書面で通知される。その後，社員は，社員 ID 管理サーバで，各自のパスワードを変更することができる。パスワードを忘れた場合，情報システム部は社員から連絡を受けて，新しい初期パスワードを設定し，利用開始時と同じ方法で通知する。 ・パスワードは，ハッシュ化した上で社員 ID 管理サーバに保存される。

〔メルマガの設定管理〕

メルマガサーバでは，メルマガ購読の申込みと解除の設定を行うことができ，会員 ID をもっていない利用者からの利用も広く可能としている。メルマガ購読の申込みと解除の設定方法を，図 2 に示す。

〔購読の申込み設定方法〕

1. メルマガ購読を希望する利用者は，設定画面の電子メールアドレスの入力欄に，各自の電子メールアドレスを入力する。
2. 設定画面の“申込み”ボタンを押して，メルマガ購読の申込み設定を行う。
3. メルマガ配信が既に行われている場合は，購読の申込み設定が行われたときに，“○○@○○.○○.○○（利用者の電子メールアドレス）様，既に当社のメルマガを購読されております。”というメッセージが設定画面に表示される。
4. メルマガ配信が行われていない場合は，購読の申込み設定が行われたときに，“○○@○○.○○.○○（利用者の電子メールアドレス）様，当社のメルマガ購読のお申込み，ありがとうございます。”というメッセージが設定画面に表示されるとともに，最新号のメルマガが送付され，配信が開始される。

〔購読の解除設定方法〕

1. メルマガ購読の解除を希望する利用者は，設定画面の電子メールアドレスの入力欄に，各自の電子メールアドレスを入力する。
2. 設定画面の“解除”ボタンを押して，メルマガ購読の解除設定を行う。
3. メルマガ配信が行われている場合は，購読の解除設定が行われたときに，“○○@○○○○.○○（利用者の電子メールアドレス）様，当社のメルマガのご購読ありがとうございました。またのご購読をお待ちしております。”というメッセージが設定画面に表示され，メルマガ配信が中止される。
4. メルマガ配信が行われていない場合は，購読の解除設定が行われたときに，“○○@○○○○.○○（利用者の電子メールアドレス）様の電子メールアドレスは，購読設定が行われておりません。”というメッセージが設定画面に表示される。

図２　メルマガ購読の申込みと解除の設定方法

〔情報セキュリティ監査〕

Q システムが構築され，サービスを開始するまでに，社会的にセキュリティ事故が多発していたので，Q システムの認証機能を中心に情報セキュリティ監査を専門会社に依頼した。情報セキュリティ監査の

結果，図 3 のような指摘事項が示された。

(ⅰ) メルマガサーバでは，他人が勝手に購読の申込みや解除の設定を行うことができる。②そのような設定ができない仕組み，又は③そのような設定が行われた場合に利用者が検知できる仕組みを導入すべきである。
(ⅱ) メルマガサーバでは，設定状況を他人が知り得ることから，設定画面に設定結果を表示することは問題である。設定画面には，設定結果を表示すべきではない。
(ⅲ) 会員 ID のパスワードがそのままの状態で，注文受付サーバのハードディスクに保存されている。パスワードは，ハッシュ化した上で保存しておくべきであり，顧客が入力したハッシュ化前のパスワードは削除すべきである。注文受付サーバの管理者であっても，顧客の登録したハッシュ化前のパスワードを直接確認できないようにすべきである。
(ⅳ) 注文受付 Web サーバに対しては，スクリプトなどによるブルートフォース攻撃（総当たり攻撃）によってログオンの試みを何回でも行うことができる。④同じ会員 ID で連続して複数回ログオンが試みられて失敗した場合に，システム側で防御する対策が必要である。また，⑤なりすましによってログオンされたことを，顧客が検知できる対策も実施すべきである。
(ⅴ) 初期パスワードを変更していない社員 ID が散見される。

図３　情報セキュリティ監査の指摘事項

情報セキュリティ監査の結果を受けて，情報システム部の R 部長と情報セキュリティアドミニストレータの S 君は，指摘事項への対応を検討した。次は，R 部長と S 君の会話である。

R 部長：指摘（i）と（ii）への対応は，具体的にどうするのか。
S 君：はい。利用者からメルマガ購読の申込みを受けた場合，電子メールアドレスの入力を確認しただけで，すぐにメルマガを配信するのではなく，仮設定が完了したことと，本設定用のホームページの URL 及び⑥照合用の文字列を記載したメッセージを，入力された電子メールアドレスあてに送信します。次に，利用者がその URL にアクセスし，電子メールアドレスと照合用の文字列を入力して，設定を完了するように変更します。この方法によって，設定画面に設定結果を表示しないようにできます。また，解除する場合は，申し込む場合と同様な方法を採ることもできますが，今回は，⑦利用者の購読解除を簡単にしたいので，現在のメルマガ購読の解除設定方法のままで，設定結果の表示だけを行わないように変更しようと思います。この変更に伴って，図 3 中の下線③の仕組みを追加します。
R 部長：なるほど。指摘（iii）では，会員 ID のパスワードをハッシュ化した上で保存しておくべきという指摘をされているが，パスワードをハッシュ化した上で保存しておく場合，どのようにパスワードを認証できるのか。
S 君：［ a ］と［ b ］を照合することによって顧客が入力したままのパスワード，つまりハッシュ化前のパスワードを削除してもパスワード認証ができます。しかし，ハッシュ化前のパスワードを削除する場合は，⑧パスワードを忘れた顧客への対応方法を変更する必要があります。

R 部長：そうか。指摘（v）では，社員 ID の初期パスワードが変更されていないことが指摘されている。この対策はどうするのかね。

S 君：はい。⑨パスワードの安全な運用管理の観点から，初期パスワードは 1 週間以内に変更させたいですね。また，その後も繰返し 3 か月以内にパスワードを変更させるようにすべきです。社員 ID 管理サーバでは，パスワードの再利用を禁止すること，パスワードの有効期限を 3 か月にすること，及び初回ログオン時に強制的にパスワードを変更させることはできます。しかし，初期パスワードを設定してから，社員が必ず 1 週間以内にログオンするとは限らないので，1 週間以内にログオンするように規則を定めたいと思います。

R 部長：なるほど。それでは，早速対応に取り掛かってくれ。

S 君は，対応をまとめ，Q システムの改良に着手した。

設問１　会員 ID について，(1)〜(3) に答えよ。

（1）本文中の［　a　］，［　b　］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　会員が最後に登録したパスワードのハッシュ化前のデータ
イ　会員が最後に登録したパスワードのハッシュ化後のデータ
ウ　ログオン時に入力したパスワードのハッシュ化前のデータ
エ　ログオン時に入力したパスワードのハッシュ化後のデータ

（2）図 3 中の下線④と下線⑤の対策を，それぞれ 20 字以内で具体的に述べよ。

（3）本文中の下線⑧の対応方法として，表中の下線①のパスワードリマインド機能に代わって，どのような仕組みを導入すべきか。40 字以内で具体的に述べよ。

設問２　本文中の下線⑨で，S 君は，初期パスワードを短期間で変更することを勧めている。現状の初期パスワードの配布方法では，社員が長期間ログオンしない場合，どのような問題が起こることを懸念しているのか。起こり得る問題を，30 字以内で具体的に述べよ。

設問３　メルマガの設定管理について，(1)〜(3) に答えよ。

(1)図 3 中の下線②の仕組みを導入しない場合，他人が勝手に設定を行うことができるだけでなく，V 社のメルマガサーバにも問題が起こる可能性がある。メルマガサーバに起こり得る問題を，20 字以内で具体的に述べよ。

（2）本文中の下線⑥の文字列に求められる要件を，20 字以内で述べよ。

（3）本文中の下線⑦の変更に伴って，追加すべき図 3 中の下線③の仕組みを，30 字以内で具体的に述べよ。

問２　PC の持出管理に関する次の記述を読んで，設問 1～4 に答えよ。

G 社は，主に中小企業向けに融資を行っている，社員数 300 名の金融機関であり，営業部，融資部，総務部，情報システム部などで構成されている。融資を希望する企業から問合せがあると，営業部員がその企業を訪問して経営診断を行った後，与信確認を経て，融資契約を結ぶ。

G 社では，競争の厳しい金融業界での生き残りをかけて，2 年前に営業支援情報システム（以下，J システムという）を再構築した。図 1 に，現在の J システムの構成を示す。営業部員は，融資を希望する企業を訪問した際に，その場で営業支援サーバにその企業の経営情報を直接入力し，分析して，融資条件を提示する。このように，J システムの導入によって，訪問先企業で迅速に融資条件を提示できるようになり，その結果，融資残高も順調に増えている。

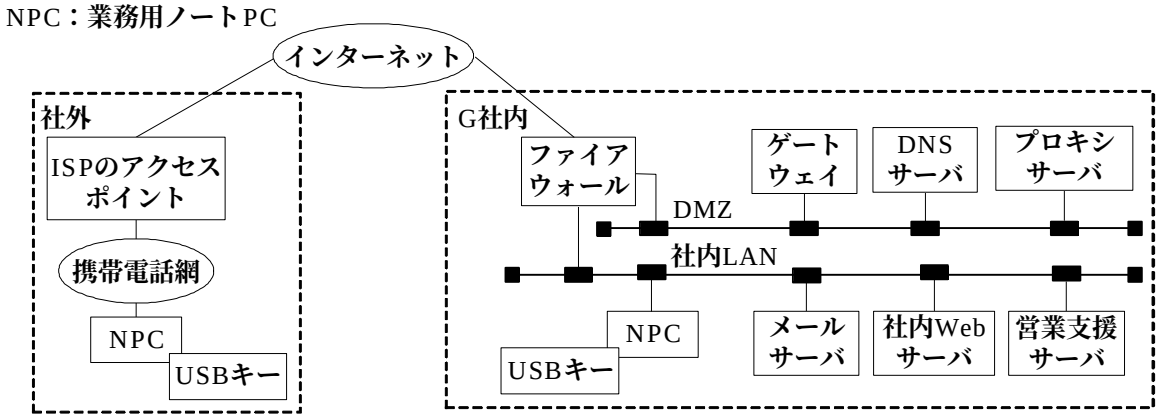

図１　Ｊシステムの構成

〔J システムの概要〕

営業部員には，NPC が 1 台ずつ配布されており，利用者認証のために，各自に割り当てられた USB キーを NPC に挿入し，更に USB キー内の秘密鍵を活性化するためのパスワードを入力する。営業部員が社外で NPC を利用するときは，G 社が契約している ISP のアクセスポイントに携帯電話網を経由してダイヤルアップ接続し，G 社内を経由しないインターネットの各種サービスの利用と，J システムのゲートウェイへの VPN 接続を行う。ゲートウェイでは利用者認証が行われ，各種サーバへのアクセス権に応じたアクセスが許可される。営業支援サーバは，NPC 上で稼働する Java アプレットを介して利用できる。J システムのメールサーバを用いた電子メールの送受信や，J システムのプロキシサーバを用いた Web サイトの閲覧については，各サーバでウイルス対策を実施している。

なお，社員が社外で J システムを利用する場合は，図 2 に示す利用規程に従う。

（1）社外に NPC を持ち出す際は，あらかじめ電子メールや口頭などで所属長の持出許可を得る。
（2）社外での NPC の利用終了後は，速やかに会社に持ち帰る。もし，速やかに持ち帰れない理由が生じた場合は，所属長の指示を仰ぐ。
（3）NPC の盗難や紛失に関しては，速やかに情報システム部に連絡する。
（4）社外で NPC を利用する場合は，第三者に［ a ］や画面を盗み見られないように注意する。
（5）社外での NPC の利用は，営業支援サーバへのアクセス，電子メールの送受信及び Web サイトの閲覧に限り許可する。
（6）NPC の持出しが複数日にわたる場合は，ウイルス定義ファイルを毎日 1 回は更新する。
（7）NPC 内のハードディスクには文書ファイルを保存してもよい。ただし，OS のポリシ設定機能による制限が施されており，一般利用者の権限ではプログラムのインストールはできない。

図２　社外での J システム利用規程

〔NPC の置忘れ事故〕

入社 5 年目の A 主任と，所属長の B 部長は，製造業者の H 社に対する融資案件を担当していた。ある日，業務多忙の B 部長に代わって，A 主任が 1 人で H 社を訪問して打合せを行うことになった。その際 A 主任は，所属長である B 部長の許可を得ずに NPC を持ち出してしまった。A 主任は，H 社で NPC から営業支援サーバにアクセスし，融資条件を算出して提示した。その結果，融資条件に関する H 社の同意が得られ，契約の内諾を得ることに成功した。A 主任は，既に終業時刻を過ぎていたので，B 部長には翌日報告することにして，会社には戻らず，NPC を所持したまま飲食店で友人と食事をした。その帰りの電車で，NPC と USB キーを入れたかばんを置き忘れてしまった。

A 主任は，帰宅してから NPC を置き忘れたことに気付き，慌てて駅に連絡したところ，遺失物として届けられていることが分かった。直ちに指定された駅に出向いて，NPC と USB キーが入ったかばんを受け取った。

置忘れ事故から数日後の営業部内会議で，A 主任は，NPC の置忘れについて B 部長に報告した。報告を受けた B 部長は，直ちに情報システム部に連絡した。この事故を重く見た情報システム部の C 課長が，H 社への訪問，飲食店への立寄り，食事，置忘れなどの一連の行動を A 主任から細かくヒアリングした。並行して，情報システム部では，A 主任の利用 ID を停止し営業支援サーバなどのサーバ類の［ b ］や，A 主任が持ち出した NPC の［ b ］などの内容を調査した。詳細な調査の結果，情報システム部では，J システムへの不正侵入はなかったと判断した。

〔NPC の置忘れ事故の事後対策〕

C 課長は，今回の事故を分析して報告書にまとめ，情報セキュリティ委員会で報告するとともに，B 部長にもその概要を次のように報告して議論した。

B 部長：今回は，大変迷惑を掛けてしまった。今後のこともあるので，問題点を教えてほしい。
C 課長：社外での J システム利用規程に照らし合わせると，A 主任の行動には，［ ア ］，［ イ ］及び①事故を速やかに情報システム部に報告しなかったという，三つの問題点があります。また，現在の規程では，口頭での持出許可を認めていることから，規程の運用がルーズになりがちであるという問題点も明らかになりました。

B 部長：分かった。今後は，持出許可の手続を厳正に行うように指導していきたい。ところで，そのほかに問題点はないだろうか。

C 課長：持出許可の手続を厳正に行っても，NPC のハードディスクにはデータが残ることによるリスクがあります。

B 部長：NPC を利用して，営業支援サーバや社内 Web サーバにアクセスする場合は，情報を閲覧するだけなので，NPC 内に残っているデータは消去すればよいと思っていたのだが，それだけでは不十分なのか。

C 課長：NPC の OS が提供するファイル削除機能は，ファイル名やファイルの格納場所に関する情報などを消去するだけであり，ファイル内のデータ自身はハードディスク内に残っています。また，NPC から営業支援サーバを利用したときに送られてくる Java アプレット，Web サイトを閲覧したときに送られてくる［　c　］，Web ブラウザの［　d　］やアクセスログの一部などがファイルとしてハードディスクに記録されることがあります。

B 部長：最近，専門誌やセミナなどでハードディスクを内蔵しない PC（以下，TC 端末という）がよく採り上げられているが，これを持出用の PC として，情報システム部が一括して貸し出すようにしてはどうだろう。

C 課長：はい。情報システム部では，ご指摘のような TC 端末を持出用に準備した上で，持出しは TC 端末だけに制限することを検討しています。つまり，従来の NPC と同様に USB キーによる利用者認証を経て，アプリケーションは，社内 LAN 上に設置する専用サーバ（以下，TC サーバという）上で動作させ，キーボードやマウスの操作情報と画面情報だけを TC 端末と TC サーバ間で通信し，Web ブラウザなどのアプリケーションは TC 端末単独では動作しない仕組みのシンクライアントシステムを導入する方向で検討しています。このシンクライアントシステムでは，TC サーバにウイルス対策を実施します。J システムのメールサーバを用いた，TC サーバからの電子メールの送受信と，J システムのプロキシサーバを用いた，TC サーバからの Web サイトの閲覧については，それぞれのサーバでウイルス対策を実施済です。

B 部長：ところで，営業部員が TC 端末の貸出しを受ける場合，利用記録を残す必要があるのではないか。

C 課長：はい。現在，TC 端末を持ち出す際に，持出者が記入して，情報システム部に提出する持出申請書（図 3）の導入を検討しています。

B 部長：なるほど。良い案だと思う。早急に進めてもらえると有り難い。

申請日	2006 年 10 月 13 日	持出者	A 主任	所属部署	営業部
利用場所	H 社	利用目的	訪問先での作業のため	同行者	B 部長
持出期間	2006 年 10 月 16 日 13:00 から　2006 年 10 月 16 日 17:00 まで			機器 ID	TC-001
持出確認欄	2006 年 10 月 16 日 13:15　　持出者　印，　　貸出管理者　印				
返却確認欄	年　月　日　：　　持出者　印，　　貸出管理者　印				

図３　持出申請書の様式と記入例

C 課長は，社外での J システム利用規程の改訂案を図 4 のように取りまとめた。

（1）社外で J システムを利用する際は，TC 端末の貸出しを受けるものとし，社内の NPC は持出しを禁止する。また，TC 端末の貸出しを受ける際は，持出申請書に必要事項を記入し，各部署で所属長の承認を得た後，情報システム部の貸出管理者から貸出しを受ける。
（2）社外での TC 端末の利用終了後は，速やかに会社に返却する。もし，速やかに返却できない理由が生じた場合は，所属長の指示を仰ぐ。
（3）TC 端末の盗難や紛失に関しては，速やかに情報システム部に連絡する。もし，届出の遅れ，虚偽報告などがあった場合は，就業規則に従って厳正に処分する。
（4）社外に TC 端末を持ち出した際は，万が一の TC 端末の紛失や盗難に備えて，［　ウ　］。
（5）社外で TC 端末を利用する場合は，第三者に［　a　］や画面を盗み見られないように注意する。
（6）社外での TC 端末の利用は，営業支援サーバへのアクセス，電子メールの送受信及び Web サイトの閲覧に限り許可する。
（7）TC サーバ内のハードディスクには，文書ファイルを保存してもよい。ただし，OS のポリシ設定機能による制限が施されており，一般利用者の権限ではプログラムのインストールはできない。

図４　社外でのＪシステム利用規程の改訂案

図 4 の改訂案は，経営会議で審議され，②承認手続に関する持出申請書の様式の不備を修正するという条件付きで承認され，直ちに様式を修正した後，社内に周知徹底することになった。

設問１　本文中の［　a　］～［　d　］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　キー操作	イ　キャッシュ	ウ　クッキー	エ　検索
オ　消去	カ　不正侵入	キ　メモリ	ク　ログ

設問２　本文中の下線②に関して，様式の不備を修正するために持出申請書に追加しなければならない項目を，10 字以内で答えよ。

設問３　置忘れ事故について，(1)～(3) に答えよ。
（1）本文中の［　ア　］，［　イ　］に入れる適切な文章を，それぞれ 30 字以内で答えよ。
（2）本文中の下線①のように，速やかに情報システム部に報告しなかった場合，NPC と USB キーを回収できたとしても，J システムに対してどのようなリスクが想定されるか。30 字以内で述べよ。
（3）図 4 中の［　ウ　］に入れる具体的な管理方法を，20 字以内で答えよ。

設問４　持出用の PC を NPC から TC 端末に変更することによって，G 社内へのウイルス感染の可能性を減らすことができる。それはどのような過程による感染か。NPC の利用場面を含め，本文中の字句を用いて，90 字以内で具体的に述べよ。

問３　ネットワークにおける PC 利用に関する次の記述を読んで，設問 1～4 に答えよ。

E 社は，社員数 150 名の文具・事務用品の商社で，社外向けにインターネットを利用した商品情報の提供や販売案内を，Web サイト上で行っている。一方，社内では，電子メールや PC のファイル共有機能を活用している。社内でやり取りするカタログなどのデータ量の増加とともに，社内ネットワークの通信トラフィックが増加したことから，昨年度，ネットワークを含めた情報システムを刷新した。

〔情報システムの運用状況〕

刷新した E 社の情報システムでは，図 1 のように，ポート VLAN 機能をもつレイヤ 3 スイッチ（以下，L3 スイッチという）をバックボーンとし，VLAN 非対応である標準的なスイッチングハブ（モニタポートなし）を各セグメント（DMZ，Seg_0～Seg_4）に配置して，ネットワークを構成している。セグメントのうち Seg_0～Seg_4 を社内セグメントと呼び，その中でも特に，Seg_1～Seg_4 を社員セグメントと呼ぶ。ネットワークに関する運用状況は，図 2 のとおりである。情報システムの設計と構築は外部業者に委託したが，日常的な運用はネットワーク機器の設定変更を含めて，社内情報システム担当の W 君が行っている。

FW：　ルータ兼ファイアウォール
　　(P1～P3はLANポート名)
Mail_1：SMTPサーバ
Mail_2：SMTP/POPサーバ
Web：　Webサーバ
Proxy：プロキシサーバ
FS_i：　ファイルサーバ_i
DNS_1，DNS_2：DNSサーバ
L3：　L3スイッチ
　　(P2～P7はLANポート名)
L2_j：　スイッチングハブ_j

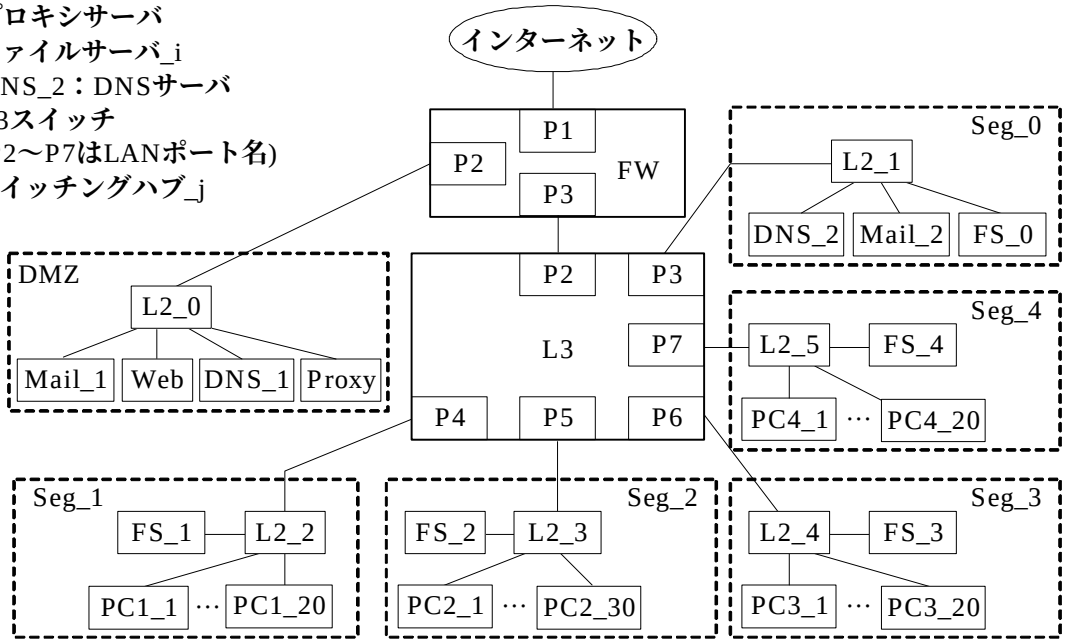

図１　Ｅ社の情報システム構成

（1）社内ネットワークのアドレス割当て
（a）プライベート IP アドレス 172.16.0.0 を利用する。
（b）ホスト部を 12 ビットとしてサブネット化する。
（c）ネットマスク：255.255. [a] .0
（2）FW の設定
（a）インターネットと DMZ との間のフィルタリングルール
・HTTP/HTTPS/SMTP/DNS 相互通信を許可する（通過時のログを採取しない）。
・上記プロトコル以外のすべてのパケットは破棄する（破棄時のログを採取する）。
（b）DMZ と社員セグメントとの間のフィルタリングルール
・HTTP/HTTPS 相互通信を許可する（通過時のログを採取しない）。
・SSH 相互通信を許可する（通過時のログを採取する）。
・上記プロトコル以外のすべてのパケットは破棄する（破棄時のログを採取する）。
（c）DMZ と Seg_0 との間のフィルタリングルール
・HTTP/HTTPS/SMTP/DNS/SSH 相互通信を許可する（通過時のログを採取しない）。
・上記プロトコル以外のすべてのパケットは破棄する（破棄時のログを採取する）。
（d）インターネットと社内セグメントとの間のフィルタリングルール
・あて先がインターネット側のパケットは破棄する（①破棄時のログを採取しない）。
（運用管理上で必要なときに，インターネット側への通信を許可する。）
・あて先が社内セグメント側のパケットは破棄する（破棄時のログを採取しない）。
（3）L3 スイッチの設定
（a）各 VLAN の設定（ポート VLAN 機能を利用）

VLAN（セグメント）	LAN ポート名（IP アドレス）	ネットワークアドレス
VLAN4（Seg_1）	P4（172.16.79.254）	172.16. [b] .0
VLAN5（Seg_2）	P5（172.16.95.254）	172.16.80.0
VLAN6（Seg_3）	P6（172.16.111.254）	172.16.96.0
VLAN7（Seg_4）	P7（172.16.127.254）	172.16.112.0
VLAN3（Seg_0）	P3（172.16.239.254）	172.16.224.0

（b）パケット転送の設定
・FW 側と社内セグメントとの間では，パケット転送を相互に行う。
・異なる社員セグメント間では，パケット転送を相互に行わない。
・社員セグメントと Seg_0 との間では，パケット転送を相互に行う。

図２　ネットワークに関する運用状況

〔盗聴の可能性〕

E 社では，顧客や社員などの様々な個人情報を取り扱っており，最近では，その管理を含めたセキュリティの強化が要求されていた。その点，刷新したネットワークでは，すべての通信がスイッチ経由で行われるので，W 君は通信セキュリティに関しては特に向上したと考えていた。ところが，ある日，社

内の友人である M 君から,スイッチングハブを用いた通信でも盗聴の可能性があることを指摘された。M 君はネットワーク技術に精通しているので,W 君は盗聴の可能性について質問してみることにした。次は，そのときの 2 人の会話である。

W 君：以前，利用していたリピータハブでは，接続する複数のホストに対して，［ c ］ドメインが一つなので盗聴できるが，スイッチングハブでは，［ c ］ドメインが分割されるので盗聴できないと聞いているよ。
M 君：スイッチングハブを用いると，本来，二つのホストの［ d ］間だけで直接通信されるので盗聴は難しくなるが，不可能ではない。［ e ］アドレスの偽造や ARP テーブルの書換えによって，②同じスイッチングハブに接続しているほかのホストの通信を盗聴できるよ。
W 君：当社でもその可能性を考慮しないといけないね。どうすればよいかな。
M 君：セキュリティプロトコルを用いて，通信経路を守るのが最も良い方法だろうけど，容易ではない場合もあるだろうね。その場合には，③盗聴者のホストが接続されないように，ネットワーク機器や LAN ケーブルに対する物理的なアクセス制限をすべきだろうね。特に，社内への入退管理を強化し，定期的に機器やケーブルの監視を行うことも重要だろうね。

W 君は，セキュリティプロトコルの導入は今後の課題とし，まず，M 君にアドバイスされた物理的なアクセス制限の導入について具体的に検討し，実施することにした。

〔ワーム F の感染〕

ある日，W 君が出社すると，社内から相次いで“PC が再起動を繰り返して利用できない”という連絡があった。調査したところ，OS の脆弱性を悪用したワーム F がまん延していることが原因と判明した。数週間前に公表されたセキュリティパッチを適用していれば，その感染を防ぐことができたが，E 社では適用していなかった。社員の多くが，PC は FW で守られているので安全であると誤解していたこともあって，事態の悪化を招いた。実際に，ログを調べたところ，ワーム F の感染過程は図 3 に示すとおりであることが分かった。営業部員が社外でも利用しているモバイル PC を媒介にして，社内にワーム F が持ち込まれ，その感染が広まったものと推定された。

(i) ある社員セグメントのホストがワーム F に感染し，発症
(ii) そのホストのワーム F が，アクセス可能なホストの TCP ポート 135 番へアクセス開始
(iii) 別セグメントのファイルサーバ（IP アドレス：172.16.［ f ］.254）がワーム F に感染し，発症
(iv) そのファイルサーバのワーム F が，（ii）と同様に，アクセス可能なホストへアクセス開始
(v) E 社内のほぼすべてのホストがワーム F に感染し，発症

図３　ワーム F の感染過程

さらに，他社のネットワーク管理者から,“御社からワーム F と思われるアクセスを受けた”との報告を受けた。調査したところ，社内セグメントの感染ホストから，FW を通過して，外部へアクセスが行われていたことが分かった。早期に対処したので，それ以降，感染の拡大は確認されず，大事には至

らなかった。

念のため，更に詳しく調べたところ，社内セグメントからインターネット側への通信が可能な状態のままであったことが判明した。先日，新たなネットワークアプリケーションを実験的に導入した際，フィルタリングルールの一つを変更した。最終的に，そのルール変更を元に戻したつもりであったが，戻すべき設定を“有効化”し忘れていた。FW の設定の変更後に，確認が不十分であったことが問題視された。

〔事態の収拾と対策〕

W 君は，ウイルス対策ソフトによるワーム F の駆除と，該当するセキュリティパッチの適用で，事態を収拾させた。その後，最新のセキュリティパッチの適用とウイルス対策ソフトの定期的なアップデートを PC 利用規約に加えた。当初，社員の間で多少の混乱もあったが，操作手順の詳細を掲載した社内向けホームページを作成し，周知徹底させた効果もあって，すべての社員が操作できるようになった。

一方，W 君は，④前述の FW における設定を“有効化”し忘れた件について，再発防止策として，あらかじめ，図 2 中の下線①を変更しておき，それに関連するフィルタリングルールを変更する際に，ICMP を用いた検査を導入することを，上司に報告した。

設問１　本文中の［ a ］～［ f ］に入れる適切な字句を答えよ。

(1)［ a ］，［ b ］については，適切な数値を答えよ。

(2)［ c ］～［ 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　ASIC　　イ　HMAC　　ウ　IX　　エ　MAC

オ　NIC　　カ　コリジョン　　キ　ネットワーク　　ク　ブロードキャスト

ケ　ランダム

(3)［ f ］については適切な最大値を答えよ。

設問２　本文中の下線②の可能性があるとき，PC1_1 の POP 通信におけるパスワードを盗聴できるのは，盗聴者のホストがどのセグメントにあるときか。図 1 のセグメント名（DMZ，Seg_0～Seg_4）の中からすべて選べ。

設問３　本文中の下線③の物理的なアクセス制限を行っても起こり得る盗聴リスクを，具体的な手段を含めて，50 字以内で述べよ。

設問４　本文中の下線④の検査について，(1)，(2) に答えよ。

(1) この検査における ICMP パケットは，例えば，PC2_1 で行う場合，図 1 中のどの機器のどの LAN ポートをあて先とすべきか。図 1 の中から機器名と LAN ポート名を選べ。

(2) W 君は，検査を行うために，図 2 中の下線①の設定を変更した。W 君の考えた検査方法を，その変更内容を含めて，60 字以内で述べよ。

問４　テレワークの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。

K 社は，社員数 1,500 名の印刷・出版業者で，雑誌，書籍の出版のほか，社員名簿や決算報告書などの情報管理が必要な冊子の制作も行っている。

K 社は，執筆者，デザイナなどの個人や企業（以下，委託先という）に業務の一部を委託しているので，情報セキュリティに配慮し，次のような運用を行ってきた。

（i） K 社の情報システムの利用は，社員に限定する。

（ii） 委託先との電子データの受渡しは，フロッピーディスクや USB メモリなどの媒体による受渡しだけに限定し，受け取った際には必ずウイルス検査を実施する。

（iii）データセンタ事業者の L 社と契約を結び，表 1 に示す L 社データセンタが提供する K 社向けサービスを利用する。Web サーバを，ハウジングサービスを利用して設置し，ファイアウォール，メールサーバ及びウイルス対策ソフト管理サーバを，運用サービスを利用して運用する。

（iv）K 社の所有するすべてのサーバと PC に，Z 社製ウイルス対策ソフトを導入して，ウイルス対策ソフト管理サーバと毎日通信し，ウイルスの検出と駆除を行う。

表１　Ｌ社データセンタが提供するＫ社向けサービス

サービス名		K 社向けサービスの内容
ハウジングサービス		（1）K 社所有の Web サーバを設置し，インターネット接続を提供 （2）別途締結する委託契約に基づいて運用を実施
運用サービス	ファイアウォール運用サービス	（3）L 社所有のファイアウォールを貸与 （4）パケットフィルタリングによる不正アクセス対策を実施。フィルタリングルールは，IP アドレス，プロトコル（ポート番号）を条件としてパケットの通過を許可又は拒否することができ，K 社が適時，変更可能
	メールサーバ運用サービス	（5）L 社所有のメールサーバを貸与 （6）メールサーバは，SMTP による電子メール（以下，メールという）の送受信，POP によるメールボックスへのアクセスを提供。メールアカウントは，K 社が指定 （7）Z 社製ウイルス対策ソフトによるメールセキュリティサービスを提供。送受信メールの本文と添付ファイルを検査し，感染している場合は駆除 （8）ウイルス対策ソフトで内容を判別できないバイナリファイルが添付されている場合には，送信者にかかわらず添付ファイルを削除 （9）迷惑メール防止サービスを提供。迷惑メールは，送信者メールアドレス又は件名を，指定した迷惑メールリストと照合して判定し，該当した場合にメールを削除。迷惑メールリストは，K 社による更新も可能
	ウイルス対策ソフト管理サーバ運用サービス	（10）L 社所有のウイルス対策ソフト管理サーバを貸与 （11）Z 社製ウイルス対策ソフトのプログラム本体及びウイルス定義ファイルの最新版を保持し，K 社のサーバや PC に配布

		(12) 随時 Z 社サイトと通信することで，ウイルス対策ソフトのプログラム本体及びウイルス定義ファイルを最新版に維持

〔テレワークにおける情報セキュリティ対策〕

K 社の制作部門は，出張や外出が頻繁であり，また，就業時刻が不規則になりがちであったので，昨年，社内ルールと業務運用を見直し，インターネット経由でファイルを送受信して外出先や自宅における執務を行うテレワーク制度を導入した。この際，情報セキュリティを確保するために，インターネット経由でファイルを送受信する場合は，すべて暗号化することを義務付けることにし，情報セキュリティポリシに追記した。

こうした方針を受け，図のようなネットワーク構成を検討した。

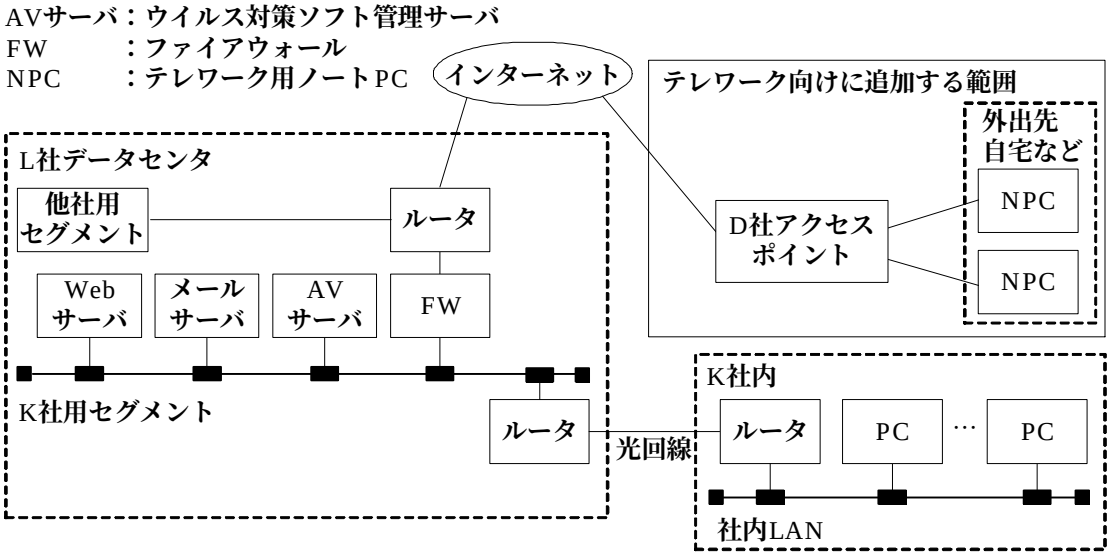

図　テレワークにおける情報セキュリティ対策後のK社のネットワーク構成

K 社では，NPC を導入し，テレワークを行うことを許可された社員（以下，許可社員という）に貸与し，ISP を運営する D 社と許可社員ごとの契約を行い，インターネットに接続させた。NPC は，インターネットに直接接続されるので，K 社の社内用 PC 向けセキュリティ対策に加えて，新たな対策が必要となった。この新たな対策として，インターネットを経由して送受信するファイルを暗号化するための，ファイル暗号化ツールを導入した。また，NPC のオープンポートへの不正アクセスを遮断するために［　a　］を導入した。さらに，NPC を携帯中に盗難に遭った場合や，紛失して第三者に使われた場合でも，ハードディスクの内容が読み出されることを防ぐために［　b　］を導入した。

インターネットを経由して，暗号化したファイルを K 社内と送受信する仕組みとして，次の 3 案を比較し，検討した。

第 1 案は，NPC が直接メールサーバと SMTP 及び POP で通信を行い，メールにファイルを添付して送受信する方法である。第 2 案は，D 社と契約する際に確保した許可社員ごとのメールアカウントを使い，D 社アクセスポイントで運用されているメールサービス用メールサーバと L 社データセンタで運

用されているメールサーバとの間で SMTP 通信する方法である。この方法では，①表 1 のサービス内容を変更して対応する。第 3 案は，Web サーバに表 2 の仕様の Web メールを構築する方法である。

K 社では，総合的に判断して，第 3 案を選んだ。

表２　Web メールの仕様

項目	概要
機能	メールサーバとのメール送受信の提供
利用者認証	ID 及びパスワード
通信暗号化	サーバ認証モードでの SSL
ウイルスチェック	Z 社製ウイルス対策ソフトによる検出，駆除

〔リモートアクセス利用者の拡大〕

テレワークの導入は好評で，許可社員以外の社員から，“ 個人契約のインターネット環境と個人所有の PC の業務への使用を許可してほしい ”との要望が寄せられた。また，現場から，“ 業務改善のために，メールを使ったファイルの送受信を，委託先との間でも認めてほしい ” という要望があった。

このような要望を踏まえ，リモートアクセス利用者の拡大を検討する過程で，公的機関や民間企業から情報セキュリティに関する情報を収集した。これらの情報に基づいて K 社で整理した，最近の情報セキュリティに関する情報と対応措置を，表 3 に示す。ここで，ファイル交換ソフト T は，公開用ディレクトリに格納されているファイルを，PC 間で相互に，自由に交換できるファイル交換用のソフトウェアである。表 3 を踏まえて K 社の状況を調査したところ，社員や委託先の中に，ファイル交換ソフト T を個人的に利用している者が少なくないことが判明した。

検討の結果，委託先には，②許可社員と同じように NPC を貸与し，D 社アクセスポイントのアカウントを割り当てる運用を認めた。また，許可社員以外の社員に対しては，個人契約のインターネット環境と個人所有の PC の使用を許可することとした。

表３　最近の情報セキュリティに関する情報と対応措置

リスク	情報セキュリティに関する情報	対応措置
ウイルス U による情報漏えい	ウイルス U が，ファイル交換ソフト T を利用している PC に感染すると，PC 内の任意のファイルを，T のファイル公開用ディレクトリにコピーする。ウイルス U は，T で交換するファイルに潜んでいて感染することが多い。	亜種の発生が頻繁で，Z 社製ウイルス対策ソフトの対応と③ほかの対策との併用を検討
ウイルス Y による情報漏えい	ウイルス Y が PC に感染すると，その PC を Web サーバ化し，ハードディスクの内容をすべて公開し，URL を公開掲示板などに書き込む。ウイルス Y は，実行形式のファイルで，メールに添付されて送りつけられる。	Z 社製を含め，ウイルス対策ソフトの対応版は迅速に提供されているので，④その適切な運用を実施

スパイウェアによる情報漏えい	無償で提供される有用なソフトウェア一式に含まれていて，利用者に気付かれないように，利用者のインターネット利用状況などをスパイウェア開発元に送付する。	Z 社製を含め，ウイルス対策ソフトの対応版は迅速に提供されているので，④その適切な運用を実施

K 社内とファイルの送受信を行う NPC と，個人所有の PC のいずれに対しても，表 3 の対応措置に則して対処することなどの十分なセキュリティ対策を義務付け，就業規則を適用して違反者を罰することを周知し，実行に移した。

設問１　本文中の［ a ］，［ b ］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　USB 無効化ツール　　イ　検疫ネットワーク
ウ　コンテンツフィルタリングソフト　　エ　ディスク暗号化ツール
オ　盗み見防止フィルタ　　カ　パーソナルファイアウォール

設問２　本文中の下線①におけるサービス内容の変更に該当する項目の番号を，表 1 中の（1）～（12）の中から選び，セキュリティ対策上，必要最小限の変更内容を，45 字以内で述べよ。

設問３　リモートアクセス利用者の拡大について，(1)，(2) に答えよ。

（1）表 3 中の下線③のほかの対策とは何か。NPC を貸与すること以外の対策を，25 字以内で具体的に述べよ。

（2）表 3 中の下線④の適切な運用とは何か。45 字以内で具体的に述べよ。

設問４　本文中の下線②のように，委託先に許可社員と同じような運用を認める場合，違反させないようにするためには，本文に明記されている対策だけでは不十分である。追加すべき対策を，45 字以内で具体的に述べよ。