平成20年度　春期
テクニカルエンジニア（情報セキュリティ）
午後Ⅰ　問題

試験時間	12:10 ～ 13:40（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. この注意事項は，問題冊子の**裏表紙**に続きます。必ず読んでください。
4. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
5. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問4
選択方法	3問選択

6. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に，**受験番号**を記入してください。正しく記入されていない場合は，採点されません。
   (3) **生年月日欄**に，受験票に印字されているとおりの**生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。
   (4) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を○印で囲んでください。
   なお，○印がない場合は，採点の対象になりません。4問とも○印で囲んだ場合は，はじめの3問について採点します。
   (5) 解答は，問題番号ごとに指定された枠内に記入してください。
   (6) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問1，問3，問4を選択した場合の例〕

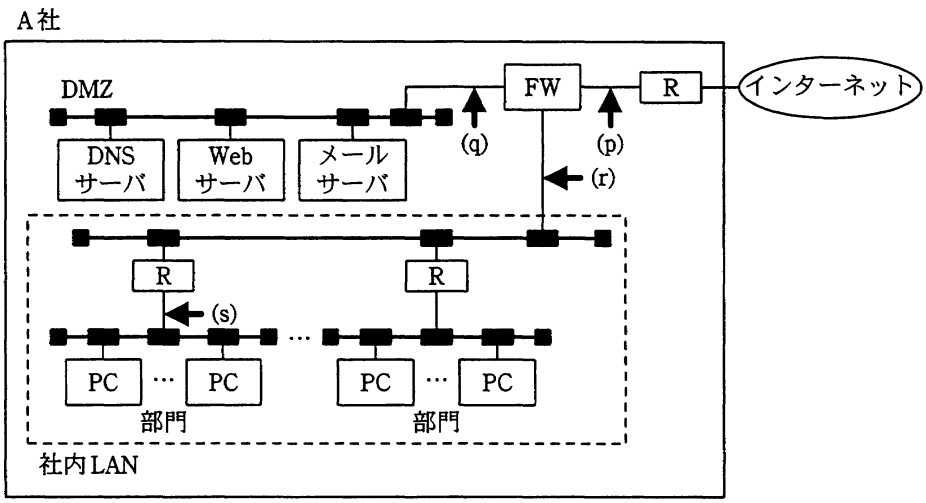
選択欄
○問1
問2
○問3
○問4

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

問1　ボット感染とその対策に関する次の記述を読んで，設問1～3に答えよ。

A社は，従業員数300名の電子機器製造販売会社である。A社では，IPアドレスとドメイン名を取得して，業務用ネットワークを自社で管理している。

ある日，A社から迷惑メールが送信されているとの指摘を複数社から受けた。そこで，システム管理部門のY主任とX君がA社の業務用ネットワークの調査を進めることになった。A社の業務用ネットワークの構成を図1に示す。



FW：ファイアウォール
（社内LANからインターネットに向けたすべての通信はNAT変換される）
R　：ルータ

図1　A社の業務用ネットワークの構成

〔迷惑メールの解析と送信防止策〕

Y主任とX君は，迷惑メールを受け取った各社から該当する迷惑メールのコピーをファックスで受け取り，解析を始めることにした。

X君　：V社からファックスで受け取った迷惑メールのヘッダ情報は図2のとおりです。Return-Pathに示される送信者は当社とは関係ありませんが，なぜV社は，当社から送信されていると指摘してきたのでしょうか。

Y主任：メールのヘッダ情報は送信者によって詐称できます。Return-Path以外にも，

[a]の箇所が詐称されている可能性があります。

X君　：なるほど。それ以外のヘッダ情報から，当社が管理するNAT変換用に割り当てられたグローバルアドレスから迷惑メールが送信されたと確認できます。

Y主任：ほかの会社から送られてきたヘッダ情報にも，共通した特徴がありますね。

```
（省略）
Return-Path: <naisho-address@○○.jp>
Received: from smtp01.v-sya.co.jp (smtp01.v-sya.co.jp [△△.166.48.140])
        by pop01.v-sya.co.jp (smtp) with ESMTP id □□
        for <tanto@v-sya.co.jp>; Wed, 25 Jul 2007 18:14:05 +0900
Received: from (ⅰ) v-sya.co.jp (unknown [(ⅱ) ▲▲.144.99.188])
        by (ⅲ) smtp01.v-sya.co.jp (Postfix) with SMTP id ■■
        for <tanto@v-sya.co.jp>; Wed, 25 Jul 2007 18:13:59 +0900 (JST)
To: <tanto@v-sya.co.jp>
From: (ⅳ) "Himitsu" <naisho-address@○○.jp>
Date: Wed, 25 Jul 2007 18:05:00 +0900
Subject: RE:
（省略）
```

注　図中の○○，△△，▲▲，□□及び■■は，特定の数字又は文字列を表す。

図2　V社が受け取った迷惑メールのヘッダ情報

X君　：各社に送信された迷惑メールを確認すると，メールごとに本文やあて先が変化していますが，当社の従業員が故意に迷惑メールを送信しているのでしょうか。

Y主任：そのようにも考えられますが，社内PCがボットに感染して，外部から制御されている可能性もありますね。

X君　：しかし，当社のFWはインターネットから社内LANに向けた通信を制限しており，ボットに感染した社内PCを外部から制御することはできないはずです。

Y主任：確か，社内LANからインターネットに向けた通信はすべて許可されていましたね。ボットは，自身から外部の指令サーバに向けた通信を行い，制御を受けることがあります。

X君　：なるほど，分かりました。

Y主任 ：まず，当社から送信される迷惑メールを止めなければなりません。迷惑メールの送信には，ボット自身がメール送信機能をもっていて，直接外部のメールサーバに送信する場合と，DMZ 上のメールサーバを利用して送信する場合とがあります。

X君　：前者に対しては，FW の制御ルールに，①図 3 に示す新たな制御ルールを追加することにします。後者に対しては，メールサーバに［ b ］又は［ c ］のいずれかの方式を適用します。これらの対策は，PC に保存されているメールサーバのアカウント情報を盗用しないボットには有効です。

Y主任 ：［ b ］方式には社内 PC のメールソフトが対応していません。PC のメールソフトが対応していなくても利用できる［ c ］方式を適用してください。

送信元	あて先	プロトコル	制御
Ⅰ	Ⅱ	α	Ⅲ

図 3　社内 LAN からの迷惑メール送信を防止する FW の新たな制御ルール

〔ボットに感染した PC の追跡〕

Y主任と X君は，迷惑メールの送信防止策の実施を完了した。

X君　：これで安心ですね。

Y主任 ：いいえ。ボットを放置しておくと，ほかの PC への感染活動や［ d ］攻撃を行うボットネットに加担し続けることになり，他者に迷惑をかけてしまいます。社内 LAN 上のボットを早急に追跡しなければなりません。

X君　：それでは，ボットが外部から指令を受けるときの通信に注目して追跡することにします。ボットが利用する通信プロトコルは何でしょうか。

Y主任 ：多くの場合，Internet Relay Chat（IRC）を使って通信が行われているようです。大抵の IRC 通信は，TCP ポート 6667 を使っています。当社には，パケットの収集と解析を行うネットワークアナライザが 1 台ありますので，②図 1 中の適切な箇所に設置して IRC 通信の監視を始めてください。

X 君は Y 主任の指示に従い，まず，ネットワークアナライザの設置箇所を通過するすべてのパケットを 3 日分収集した。

X君　：収集したパケットを解析した結果，TCP ポート 6667 を使ったパケットを発見できましたが，指令を含む IRC 通信は見つかりませんでした。

Y主任：ボットには，指令を含む通信の発見を逃れるために，通信を暗号化するものや通信ポートを変えるものもあります。後者については，③社内 LAN からインターネットに向けた通信ポートの制限を FW に適用できれば，指令を含む通信を遮断できるのですが，適用できない場合があります。

X君　：ところで，当社のすべての PC にはウイルス対策ソフトがインストールされています。指令を含む通信を発見できないのは，既に駆除されているからではないでしょうか。

Y主任：それはありません。当社のウイルス対策ソフトの稼働状態とウイルス検知状況はシステム管理部門によって管理されています。現時点で，すべてのウイルス対策ソフトは定期的にパターンファイルが更新された状態で稼働しているということが分かっていますが，ボットを検知したという報告はありません。

X君　：それではなぜ，ウイルス対策ソフトで発見できないのでしょうか。

Y主任：最近のボットには，自身の発見を逃れるために迷惑メールの送信頻度を抑える機能や，④パターンマッチング方式のウイルス対策ソフトによる検知を難しくする仕組みをもつものがあります。また，⑤ rootkit のように，関連するファイルやプロセス情報を OS から見えなくする仕組みをもつものもあります。

その後，Y 主任と X 君はパケット解析を更に進めた結果，ボットに感染した PC を特定することができた。その PC は，従業員によって OS の自動更新機能が無効になっていたことが判明したので，A 社では，社内 PC の OS の自動更新機能は必ず有効にするよう徹底した。

設問1　迷惑メールの解析，ボットの脅威，ネットワーク監視について，(1)～(3)に答えよ。

(1) 本文中の［　a　］に入れる該当箇所を図2中の下線(ⅰ)～(ⅳ)からすべて選び，記号で答えよ。

(2) 本文中の［　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　DDoS　　イ　DNSスプーフィング

ウ　Land　　エ　バッファオーバフロー

(3) 本文中の下線②で，ネットワークアナライザを設置するのに適切な箇所を，図1の(p)～(s)から一つ選び，記号で答えよ。

設問2　迷惑メールの送信防止策について，(1)，(2)に答えよ。

(1) 本文中の下線①の新たな制御ルールとして，図3中の［　Ⅰ　］～［　Ⅲ　］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。また，図3中の［　α　］に入れる適切なプロトコル名を，英文字6字以内で答えよ。

Ⅰ，Ⅱに関する解答群

ア　DMZ　　イ　インターネット

ウ　社内LAN　　エ　任意

Ⅲに関する解答群

ア　許可　　イ　拒否

(2) 本文中の［　b　］，［　c　］に入れる適切な方式を解答群の中から選び，記号で答えよ。また，それぞれの方式の仕組みを，35字以内で述べよ。

解答群

ア　DomainKeys　　イ　POP before SMTP

ウ　Sender Policy Framework　　エ　SMTP AUTH

設問3　ボットに感染したPCによる被害の抑止と追跡について，(1)～(3)に答えよ。

(1) 本文中の下線③について，Y主任が，FWに適用できない場合があるとしている理由を，50字以内で述べよ。

(2) 本文中の下線④について，ウイルス対策ソフトによる検知を難しくする仕組みを，20字以内で述べよ。

(3) 本文中の下線⑤について，rootkitがファイルやプロセスを見えなくする仕組みを，30字以内で述べよ。

問2　ネットワークセキュリティに関する次の記述を読んで，設問1～3に答えよ。

B社は，従業員数200名の日用雑貨販売会社である。B社では，10年前の創業時から，無料カタログ冊子を配布し，電話受付によって日用雑貨の通信販売を行ってきた。また，4年前には，インターネットを利用した注文受付を開始した。現在では注文の約7割がインターネットからとなっており，売上も毎年順調に伸びてきている。

インターネットを利用した注文受付システム（以下，Xシステムという）は，Webを使用したシステムで，システム開発会社のS社が構築した。Xシステムのネットワーク構成は，図のとおりである。

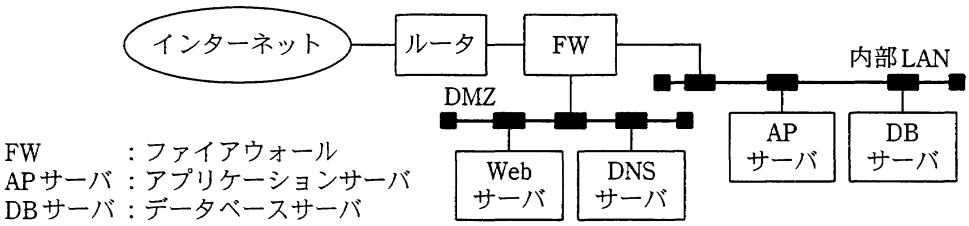


図　Xシステムのネットワーク構成

〔セキュリティインシデントの発生〕

ある朝，B社のシステム部門のF主任が出社すると，電話受付部門のK主任から，前夜の電話受付について次のとおり報告があった。

・前夜の電話受付数は，通常の約1.5倍であった。

・Xシステムが利用できない，という苦情が数件あった。

この報告を受けてF主任は，Xシステムの動作確認を行ったが，異常は発見できなかった。インターネット回線の障害について，通信事業者に確認したが，障害は発生していないとのことであった。気になったF主任は，上司であるG課長に相談することにした。次は，F主任とG課長の会話である。

F主任：昨夜，Xシステムが利用できないという苦情があったので，先ほど動作確認を行ったのですが，現時点では特に異常は見られません。利用者側の問題の可能性もありますが，苦情が複数届いていることから，Xシステムに何らか

の障害が発生した可能性が高いと思います。

G課長：そのようだな。Web サーバのアクセスログや FW のログなどを詳細に調べる必要がある。苦情のあった時間帯を K 主任に確認した上で，その前後の時間帯を含めてログを調べてみてくれ。

F主任：はい，分かりました。

F 主任は Web サーバのアクセスログと FW のログ，それぞれの資源（CPU，メモリ）及びパケット量の監視ログを調査したところ，Web サーバと FW の資源使用率が約 2 時間にわたって高くなっていること，及びこの間の Web サーバへのパケット量が増えていることが分かった。

F主任：この時間帯の Web サーバのアクセスログを見ましたが，アクセス数は特に増えていないようです。

G課長：ということは，Web サーバへの HTTP 接続以外のパケットということになるな。もしかすると，不正アクセスが行われている可能性がある。すぐに S 社に調査してもらおう。

早速，S 社でセキュリティに詳しい J 氏に連絡を取り，解析を依頼した。その結果，SYN Flood 攻撃を受けていたことが判明した。

〔ネットワークセキュリティ対策の検討と実施〕

次は，SYN Flood 攻撃について，J 氏が G 課長と F 主任に説明を行ったときの会話である。

J氏　：SYN Flood 攻撃は，TCP の接続開始処理をねらった攻撃です。一般に，TCP の接続開始処理は，［ a ］ハンドシェイクと呼ばれる手順を経ることで行われます。ホスト A からホスト B への接続開始処理を例に挙げると，まず，ホスト A から［ b ］パケットがホスト B に送られます。次に，［ b ］パケットを受け取ったホスト B から［ c ］パケットが返されます。最後に，ホスト A から［ d ］パケットが送られることによっ

て，接続開始処理が完了します。SYN Flood 攻撃は，何らかの方法で，最後の［ d ］パケットがホスト B に届かないようにすることで，ホスト B に未完了の接続開始処理（以下，ハーフオープンという）を大量に発生させる攻撃です。この結果，①正当な利用者がホスト B に接続できなくなったり，接続に時間がかかるようになったりします。

なお，多くの場合，［ d ］パケットがホスト B に届かないようにするために，［ b ］パケットの［ e ］IP アドレスを詐称する方法が使われています。

G 課長：なるほど，それで②パケット量が増えても，Web サーバのアクセスログに記録されているアクセス数が増えないわけですね。

J 氏　：そうです。

F 主任：それで，この攻撃への対策は，どのようにしたらよいのでしょうか。

J 氏　：正当な TCP の接続開始処理かどうかを判断し，不正な接続開始処理であれば破棄するという方法が考えられます。しかし，正当な接続開始処理と判断するためには，［ d ］パケットを受け取るまで待たなければならず，［ b ］パケットを受け取った時点で判断することは困難です。また，ハーフオープン状態になっている接続開始処理と同じ［ e ］IP アドレスからの接続要求を拒否するという方法も考えられますが，③効果が得られないことが多いのです。そのため，最近の FW は，ハーフオープン状態の接続がある数に達すると，それ以上の接続開始処理はいったん FW で保留することで，あて先のサーバに接続要求が到達しないようにできます。これによって，SYN Flood 攻撃の対象サーバに対して，不正な接続開始処理を抑制することができます。

F 主任：X システムで使用している FW でも，その対策は可能ですか。

J 氏　：はい，ソフトウェアを最新版に更新することで可能です。

G 課長：それでは，早速，その手配をお願いします。

J 氏　：分かりました。まずは，作業計画を立案した上で，できるだけ早く対応します。ただ，今回の攻撃で，FW の資源使用率が，通常に比べてかなり高くなっていましたので，今回のような攻撃を受けると，FW 自体のパフォーマンスを維持できなくなる可能性があります。上位機種に交換した方がよいと思

います。

G課長：なるほど。今のFWは正常時のアクセス予想数から選定された機種だから，不正アクセスを想定するとパフォーマンスに問題が発生する可能性が高くなるのですね。さらに，インターネットを利用した注文が伸びてきていることを考慮すると，上位機種への交換も必要ですね。ソフトウェアの更新はすぐに実行することにして，上位機種の手配もお願いします。それから，しばらくの間，SYN Flood攻撃の有無や，FWとWebサーバの資源使用率について監視をお願いします。

J氏　：承知しました。

FWのソフトウェアの最新版への更新は翌日のメンテナンス時間帯に，上位機種への交換は3日後のメンテナンス時間帯に行われ，当面のSYN Flood攻撃対策は完了した。

〔ネットワークセキュリティ対策の強化〕

2週間後，J氏は，監視結果の報告のために，B社を再度訪問した。

J氏　：ここ2週間ほど監視した結果，SYN Flood攻撃を何回か受けてはいますが，そのときでも，Webサーバの資源使用率は，最初にSYN Flood攻撃を受けたときと比べるとかなり改善されています。FWの資源使用率についても，上位機種への交換後，問題ない範囲になりました。また，インターネット回線の使用率も問題ありませんでした。

G課長：それはよかった。ところで，今後，更に強力なSYN Flood攻撃を受けた場合に備えて，今の機器構成でできる対策はないでしょうか。

J氏　：そうですね，攻撃を受けた場合には，インターネットに接続されているルータで［　b　］パケットの帯域制限を行う対策と，④Webサーバで行う対策を併用するのがよいと思います。

G課長：なるほど。F主任，J氏とともに早急に対策手順を作成してくれ。

F主任：はい，分かりました。

F主任は，J氏とともに対策手順を作成し，XシステムのSYN Flood攻撃対策の強化を図った。

設問1　本文中の［　a　］～［　e　］に入れる適切な字句を，それぞれ8字以内で答えよ。

設問2　SYN Flood攻撃とその対策について，(1)～(3)に答えよ。

(1)　本文中の下線①について，正当な接続要求に応答できなくなったり，接続に時間がかかるようになったりする理由を，“資源”という字句を用いて35字以内で述べよ。

(2)　本文中の下線②について，その理由を50字以内で述べよ。

(3)　本文中の下線③について，その理由を35字以内で述べよ。

設問3　SYN Flood攻撃対策の強化について，本文中の下線④に示す対策の内容を，“タイムアウト”という字句を用いて40字以内で述べよ。

問3　通信データの保護に関する次の記述を読んで，設問1，2に答えよ。

C 社は，従業員数 2,000 名の小売業者である。業界団体から個人情報保護に関するガイドライン（以下，ガイドラインという）が公開されたのを契機に，C 社は，個人情報を取り扱っているインターネット販売システム（以下，Y システムという）を対象に，ガイドラインの遵守状況の調査と，遵守できていない項目への対応計画案の検討を始めた。

ガイドラインの遵守状況の調査，対応計画案の検討作業はおおむね順調に進んでいたが，通信データの保護に関する項目については，担当者のスキル不足から，作業が遅れ気味であった。C 社は，作業の遅れを取り戻すために，Y システムの運用管理を委託している SI ベンダの T 社に調査，検討作業を依頼した。T 社の情報セキュリティエンジニアである Q 氏は，ガイドラインの内容から，Y システムに適用すべき通信データの保護に関する要件を抽出し，C 社情報システム部門の P 部長に対して，遵守状況の調査結果の報告と対応計画案の提示を行った。次は，そのときの P 部長と Q 氏の会話である。

〔通信データの保護に関する要件〕

Q 氏　：Y システムにおける通信データの保護に関する要件案を図 1 に示します。

1. 通信回線又は LAN を介して個人データを送受信する場合は，盗聴されても通信データの内容が分からないようにするために，暗号化を行わなければならない。
2. データセンタ内の LAN においては，未登録機器の LAN への接続を拒否する技術的対策を実装することで暗号化の代替策としてもよい。

図 1　Y システムにおける通信データの保護に関する要件案

Q 氏　：図 1 を基に，Y システムに対して，通信データの保護に関する要件の遵守状況を調査したところ，一部の要件は遵守されておらず，対応計画を検討すべき箇所があることが判明しました。Y システムにおいて，通信データの保護を検討すべき箇所を図 2 に示します。

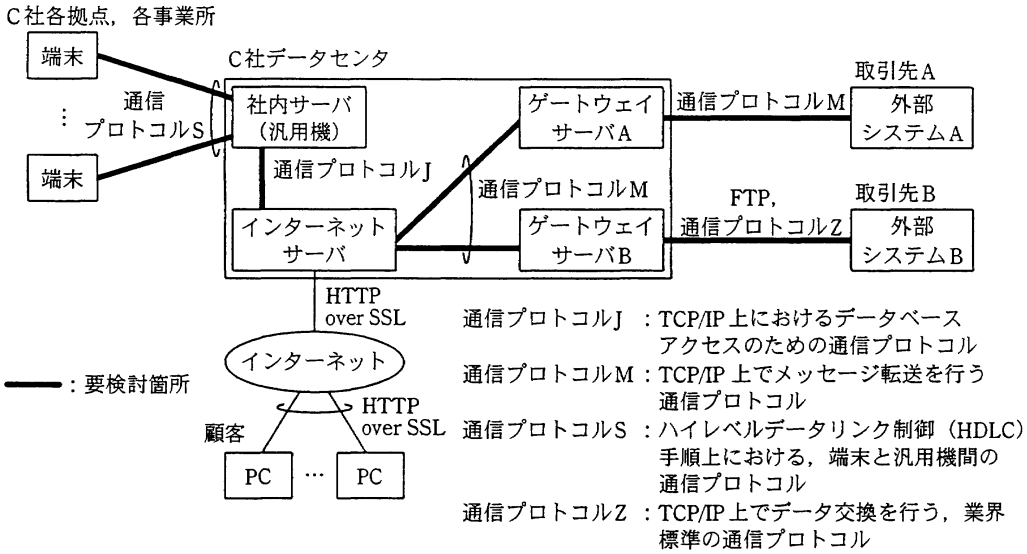


図２　Ｙシステムにおいて通信データの保護を検討すべき箇所

Ｑ氏　：図 2 において，業務アプリケーションは，社内サーバとインターネットサーバの上で稼働しています。各拠点，各事業所に配置されている端末は，画面表示とキーボード入力の機能だけを提供する汎用機専用の端末であり，端末上では業務アプリケーションは稼働していません。また，端末と社内サーバは，IP とは異なる通信プロトコル S で通信しており，専用の通信機器が使われているので，IP への変更は困難な状況です。インターネットサーバ上で稼働している業務アプリケーションは，各外部システムとデータの送受信を行っており，各ゲートウェイサーバは，送信データから送信電文への変換，及び受信電文から受信データへの変換を行っています。

Ｐ部長：図 1 について質問があります。通信データの保護には，暗号化の代わりに光ファイバの通信回線（以下，光回線という）を利用することも有効であると聞いたことがあります。この方法は採用できないのでしょうか。

Ｑ氏　：採用できません。通信回線における盗聴のリスクには 2 種類あります。一つは，第三者が①ネットワークアナライザをネットワーク機器や通信回線に接続して通信データを盗聴するリスクです。分配器などの機器が不正に接続されていない光回線の場合は，光回線の状態を監視することで，リスクをもたらす脅威の発生を検知できます。もう一つは，第三者が②ネットワークアナ

ライザをネットワーク機器や通信回線に接続することなく，通信データを盗聴するリスクです。光回線の場合は，このような盗聴は困難であると考えられています。Yシステムの場合は，各取引先の構内ネットワークにおいて，C社データセンタと同程度のセキュリティ対策の実施を求めることができないので，光回線の終端と外部システム間のネットワークに，ネットワークアナライザを接続されるリスクが残ります。また，C社データセンタと各拠点，各事業所を結ぶ通信回線は，様々な用途で使われており，光回線への変更は困難です。したがって，光回線は有効な対策とはなりません。

P部長：了解しました。

〔対応策の検討〕

Q氏　：通信データの保護に関する要件に基づいて，具体的な対応策を検討したいと思います。まず，データセンタ内のLAN（以下，構内LANという）についてですが，追加投資を抑えることを考慮し，現行のネットワーク機器の設定変更によって，通信データの保護を実現するとよいでしょう。具体的には，ネットワーク機器のMACアドレス認証と呼ばれる機能を利用し，ネットワーク機器に登録されていないMACアドレスをもつ機器は未登録機器とみなし，構内LANへの接続を拒否します。ただし，③未登録機器の設定によっては構内LANに接続できてしまう可能性がありますので，残存リスクを評価し，許容できるか否かを判断する必要があります。

P部長：データセンタの物理的セキュリティは良好な状況にあるから，この残存リスクは小さく，許容できると判断します。構内LANについてはこの方法でよいでしょう。

Q氏　：次に，通信回線を介して送受信される通信データの保護について，具体的な製品選択を行う前に，暗号化方式の候補を選択したいと思います。通信データの暗号化方式の一覧を表1に示します。さらに，各通信回線における通信データの暗号化方式の候補として，表1に挙げた暗号化方式から選択したものを，表2に示します。

P部長：候補としては，表2の暗号化方式でよさそうですね。今後は，表2に基づいて，具体的な製品選択の検討に入ることにします。

表1　通信データの暗号化方式の一覧

方式1	業務アプリケーションによる業務データの暗号化
方式2	SSL による通信の暗号化
方式3	通信を行うホストの IPsec 機能による，通信の暗号化
方式4	ネットワーク機器（ルータ，VPN 装置など）の機能による，IP 通信の暗号化
方式5	回線暗号化装置の機能による，データリンク層における通信の暗号化

表2　各通信回線における通信データの暗号化方式の候補

番号	対象となる通信回線	通信プロトコル	暗号化方式の候補	候補以外の暗号化方式を除外する理由
1	端末～社内サーバ間	通信プロトコル S	・方式 [a]	・[ア] ・[イ]
2	ゲートウェイサーバ A ～外部システム A 間	通信プロトコル M	・方式 [b] ・方式 [c] ・方式 [d]	・[ウ]
3	ゲートウェイサーバ B ～外部システム B 間	FTP，通信プロトコル Z	・方式 [c] ・方式 [d]	・通信プロトコル Z では，SSL が使用できないから ・外部システム B では，FTP と SSL を組み合わせて使用できないから ・[ウ]

C 社情報システム部門は，当初の予定どおりに Y システムのガイドライン対応計画案をまとめ，経営者の承認を得ることができた。

設問1　通信データの盗聴に関する対策について，(1)，(2) に答えよ。

(1) 本文中の下線①について，ネットワークアナライザを光回線に接続する方法を，40 字以内で述べよ。

(2) 本文中の下線②において，Q 氏が想定している具体的な盗聴方法を，25 字以内で述べよ。

設問2　〔対応策の検討〕について，(1) ～ (3) に答えよ。

(1) 本文中の下線③において想定される設定方法を，30 字以内で述べよ。

(2) 表 2 中の [a] ～ [d] に入れる適切な数字を答えよ。

(3) 表 2 中の [ア] ～ [ウ] に該当する理由を，[ア]，[イ] はそれぞれ 35 字以内，[ウ] は 70 字以内で述べよ。

問4　ISMS構築時のリスクマネジメントに関する次の記述を読んで，設問1～4に答えよ。

D社は，従業員数400名の通信販売会社であり，ISMSの認証取得を目指して，マネジメントシステムを構築中である。

D社の情報システムには，全社共用サーバと部門サーバがある。全社共用サーバは情報システム部が運用管理しており，部門サーバは各部門が運用管理している。従業員は，各自のデスクトップPC又はノートPCを利用して社内業務を行っている。

D社では，マネジメントシステムの構築に伴い，リスクマネジメントを実施することになり，技術的な検討を要する部分は，情報システム部のH主任とM君が担当することになった。次は，H主任とM君の会話である。

〔リスクマネジメントの実施手順〕

H主任：当社では，リスクマネジメントを実施する手順として，最初にリスクアセスメントを行い，次にリスク対応を行うことにしている。リスクアセスメントでは，まず，リスク分析を行い，次にリスク評価を行う。リスク分析では，情報資産の重要度，脅威及び脆弱性をレベルで表し，それぞれのレベルの積をリスク値として算定する。リスク評価では，リスク値が一定値を超えたものを対応すべきリスクとして決定する。

M君　：対応すべきリスクとして決定されたものについては，どうするのですか。

H主任：対応すべきリスクに対して，個々に対応を検討していく。リスク対応には，四つの選択肢がある。第一に，適切な管理策を採用して，リスクを低減するという選択肢がある。第二に，リスクが組織の方針及びリスク［　a　］基準を満たす場合には，そのリスクを［　a　］するという選択肢がある。第三に，リスクの存在する状況から撤退することによって，リスクを［　b　］するという選択肢がある。第四に，関連する事業上のリスクを保険会社や供給者などの他者に［　c　］するという選択肢がある。

現時点でリスク評価までは完了しているので，次の段階では，リスクを低減する選択肢の中で，技術的な管理策を検討していこう。

〔技術的な管理策の検討〕

M 君　：対応すべきリスクとして，ノート PC を社外に持ち出す際の，紛失時，盗難時の情報漏えいが挙げられています。ノート PC には，ログインパスワードを設定していますが，それだけでは不十分なのでしょうか。

H 主任：①ノート PC にログインしなくても，ハードディスクの内容を読み出す方法があるから，このままでは十分ではないね。ノート PC が紛失，盗難に遭った場合に情報が読まれてしまう可能性を低くするために，②技術的な管理策を採用すべきだろう。予算に余裕があれば，持出しが必要な情報だけを格納した，持出し専用のノート PC も導入したいね。

M 君　：対応すべきリスクとして，次に，外部記憶媒体への不正書出しが挙げられています。これはなぜでしょうか。社内規程では，外部記憶媒体への書出しを禁止しているので，リスクはないと思いますが。

H 主任：実態としては，必ずしも社内規程が守られているとはいえないね。社内教育と内部監査で徹底する方法もあるが，強制的な方法も併せて考えた方がいい。強制的な方法として，外部記憶媒体を物理的に使えなくする方法もあるが，読込みができなくなると業務に支障が出る場合もあるので，ソフトウェアによって書出しだけを禁止する方法がいいだろう。

M 君　：対応すべきリスクとして，さらに，全社共用サーバに対する不正ログインが挙げられています。不正ログインのリスクに対しては，パスワードによる管理策を採用しています。全社共用サーバの OS では，最短パスワード長を 7 文字に設定しているのですが。

H 主任：それだけでは，不正ログインのリスクに対して不十分だ。パスワードに関して OS に設定すべき項目は，ほかにもある。リスクを低減するために設定項目を追加しよう。

M 君　：対応すべきリスクとして，部門サーバに対する不正ログインも挙げられています。部門サーバに対しても，全社共用サーバと同様に考えればいいのですね。

H主任：それだけでは十分とはいえない。全社共用サーバはサーバ室に設置してあり，物理的なアクセスは制限されているが，部門サーバは各部門の執務室に設置してあり，従業員ならだれでも物理的にアクセスできる。したがって，CD から起動されて，パスワードファイルにアクセスされてしまうリスクがあるね。

M君　：しかし，部門サーバの OS では，パスワードはハッシュ化されています。ハッシュ値からパスワードを復元することは，困難なのではないでしょうか。

H主任：パスワード候補のハッシュ値をあらかじめ計算し蓄えておいたテーブルを利用して，ハッシュ値からパスワードを特定する方法もある。例えば，小文字のアルファベットと数字で作成される 7 文字のパスワードの候補数は，［　d　］で表されるから，約 780 億通りになる。1 秒間にパスワードを 1 万回試すことができるとすると，すべてのパスワードを試すには，約 91 日必要だ。ところが，テーブルがソート済みで 2 分探索法を利用できるとすると，テーブルのデータ数を N として，最大比較回数は［　e　］+1 を超えない整数値になる。1 回の比較に 100 ミリ秒かかるとしても，最大 3.7 秒で探索できることになる。

M君　：なるほど。ただし，約 780 億通りだとすると，テーブルのサイズはかなり大きくなりそうですね。

H主任：そのとおりだ。パスワードとハッシュ値の一組当たりのサイズを 30 バイトとすると，全体で約 2.4 T（10^{12}）バイトのテーブルになる。しかし，レインボーテーブルというテーブルを用いた攻撃では，ハッシュ値の計算を併用することによって，テーブルのサイズを抑えつつ，数秒から数分でほとんどのパスワードを解読できたという報告がある。

M君　：それは危険ですね。では，どうしたらいいのでしょうか。

H主任：パスワードの情報だけでなく，ソルトという情報を付加してハッシュ値を計算することによって，ハッシュ値からパスワードを特定しにくくする方法を採用した OS を導入するのがいいだろう。しかし，すぐには OS を変更できないので，当面は，鍵のかかる専用ラックに格納して，部門サーバへの物理的なアクセスを制限することにしよう。

D 社は，技術的な検討結果を踏まえて技術的な管理策を決定し，社内規程に反映させ，社内教育，内部監査などを実施した。その後，審査を受け，ISMS の認証を取得することができた。

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　移転	イ　回避	ウ　管理	エ　拒否
オ　根絶	カ　受容	キ　譲渡	ク　売却

設問 2　ノート PC の紛失時や盗難時の情報漏えいについて，(1)，(2) に答えよ。

(1)　本文中の下線①の具体的な内容を，35 字以内で述べよ。

(2)　本文中の下線②の管理策による対応方法を，30 字以内で述べよ。

設問 3　外部記憶媒体への不正書出しについて，アプリケーションプログラムには変更を加えないで，外部記憶媒体への不正書出しをソフトウェアによって防ぐ方法を，40 字以内で具体的に述べよ。

設問 4　サーバに対する不正ログインについて，(1) ～ (3) に答えよ。

(1)　本文中の［ d ］，［ e ］に入れる適切な数式を解答群の中から選び，記号で答えよ。

解答群

ア　7^{36}	イ　36^{7}	ウ　${}_{36}C_{7}$	エ　${}_{36}P_{7}$
オ　$\log_2 N$	カ　$\log_{10} N$	キ　$N \log_2 N$	ク　$N \log_{10} N$

(2)　全社共用サーバのパスワードに関する設定において，不正ログイン対策として OS に設定できる項目を，本文中に記載された最短パスワード長以外に三つ挙げ，それぞれ 15 字以内で答えよ。

(3)　ソルトを使用するとハッシュ値からパスワードを特定しにくくなるのはなぜか。その理由を，40 字以内で具体的に述べよ。

7. 途中で退室する場合には，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	12:50 ～ 13:30

8. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
9. 問題冊子の余白などは，適宜利用して構いません。
10. 試験中，机上に置けるもの及び使用できるものは，次のものに限ります。
なお，会場での貸出しは行っていません。
受験票，黒鉛筆又はシャープペンシル，鉛筆削り，消しゴム，定規，時計（アラームなど時計以外の機能が付いているものは不可），ハンカチ，ティッシュ
これら以外は机上に置けません。使用もできません。
11. 試験終了後，この問題冊子は持ち帰ることができます。
12. 答案用紙は，いかなる場合でも，すべて提出してください。回収時に提出しない場合は，採点されません。
13. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。
14. 午後Ⅱの試験開始は 14:10 ですので，13:50 までに着席してください。