SC

平成25年度　春期
情報セキュリティスペシャリスト試験
午後Ⅰ　問題

試験時間	12:30 ～ 14:00（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. **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。**
4. 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	2問選択

5. 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，**生年月日欄**に**受験票の生年月日**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。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **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。○印がない場合は，採点されません。3問以上○印で囲んだ場合は，はじめの2問について採点します。
   (4) 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。
   (5) 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を選択した場合の例〕

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。

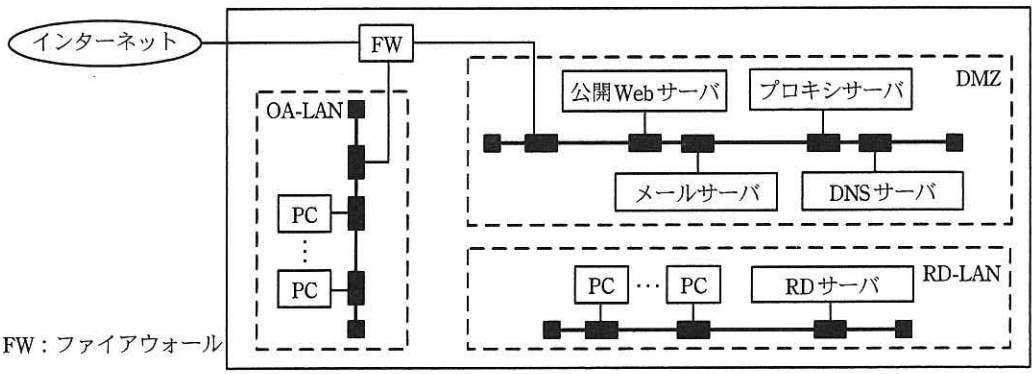
問1　マルウェア解析に関する次の記述を読んで，設問1～3に答えよ。

J社は，新薬の研究開発を行っている従業員数100名の研究所であり，ある特殊な分野の研究開発で世界的に高い評価を受けている。J社のネットワークは，研究開発事業で利用するネットワーク（以下，RD-LANという），外部との情報交換に利用するネットワーク（以下，OA-LANという）及びDMZの三つで構成されている。J社のネットワーク構成を図1に示す。

(1) RD-LANはRDサーバと十数台のPCで構成されている。RDサーバには，J社において最も機密度が高い情報である新薬の研究報告書が，電子ファイルとして保管されている。機密保護の観点から，RD-LANは，他のネットワークと物理的に隔離されている。RD-LANと他のネットワーク間のデータの受渡しは，J社の情報セキュリティポリシに従ってJ社所有のUSBメモリを介して行われ，必要最小限にとどめられている。

(2) OA-LANは100台のPCで構成されている。PCは業務に必要な電子メールの送受信及びインターネット上のWebの閲覧に利用されている。

(3) DMZは，公開Webサーバ，プロキシサーバなどで構成されている。プロキシサーバは，ブラックリストに登録したURLへのWebアクセスを遮断するフィルタリング機能をもっているが，J社では何も登録していない。



注記　OA-LANとRD-LANのネットワークアドレスは異なる。

図1　J社のネットワーク構成

全ての PC，RD サーバ，DMZ の各サーバ及びネットワーク機器には固定の IP アドレスが設定されており，RD-LAN の PC と RD サーバを除いて，デフォルトゲートウェイが設定されている。また，全ての PC，RD サーバ及び DMZ の各サーバにはウイルス対策ソフトがインストールされており，OA-LAN の PC には，Web を閲覧する際に利用する Z ブラウザがインストールされている。現在，最新の Z ブラウザはバージョン 3 であるが，従業員の中には，操作しやすいという理由で，古いバージョン 2 の Z ブラウザを利用している者もいる。また，各サーバではサーバへのアクセスのログを取得している。FW では許可及び拒否する全ての通信のログを取得している。J 社の FW のフィルタリングルールを表 1 に示す。

表 1　FW のフィルタリングルール

項番	送信元	宛先	サービス	動作
1	プロキシサーバ	インターネット	HTTP，HTTPS	許可
2	メールサーバ	インターネット	SMTP	許可
3	DNS サーバ	インターネット	DNS	許可
4	インターネット	公開 Web サーバ	HTTP，HTTPS	許可
5	インターネット	メールサーバ	SMTP	許可
6	インターネット	DNS サーバ	DNS	許可
7	PC	プロキシサーバ	代替 HTTP	許可
8	PC	メールサーバ	SMTP，POP3	許可
9	PC	DNS サーバ	DNS	許可
10	全て	全て	全て	拒否

注記 1　J 社で利用する主要なサービスのポート番号は，次のとおりである。
HTTP：80，HTTPS：443，代替 HTTP：8080，DNS：53，SMTP：25，POP3：110
注記 2　項番が小さいものから順に，最初に一致したルールが適用される。
注記 3　項番 7～9 の送信元の PC には，RD-LAN 上の PC は含まない。

〔過去のウイルス感染事例〕

J 社では数年前に，公開 Web サーバの情報が愉快犯と思われる攻撃者によって改ざんされるという事件があった。原因は，公開 Web サーバに利用していたミドルウェアが脆弱(ぜい)性のあるバージョンのままとなっていたことにあった。しかも，それだけでなく，公開 Web サーバのウイルス定義ファイルが古かったことから，ウイルスにも感染していた。この時には，J 社のセキュリティ管理者である Y 主任が，セキュリティベンダ X 社の S 氏に協力を仰ぎ，公開 Web サーバのミドルウェアのバージョンを更新するとともにウイルスを駆除した上で，念のため DMZ の全サーバと OA-LAN の全 PC

について最新のウイルス定義ファイルでフルスキャンを行い，ウイルスに感染していないことを確認している。

〔マルウェアの検出〕

今年になって，マルウェアの攻撃による情報漏えい事件の発生が相次いで報道されていることから，S 氏は Y 主任に，マルウェアの感染の有無を確認する検査サービスを提案した。S 氏によると，検査サービスは，専門のアナリストが専用ツールで PC を調査し，疑わしい検体が発見された場合，解析を行うことで，ウイルス対策ソフトでは検出できないマルウェアを検出できるという。Y 主任は，RD-LAN は重要度の高い機密情報が保管されているが，インターネットとは接続されていないので，検査サービスを受けるまでもないと考えた。一方，OA-LAN はインターネットと接続されていることから，念のため OA-LAN の PC のうち 50 台について，検査サービスを受けることにした。検査の結果，5 種類のマルウェアが発見された。Y 主任はマルウェアの影響などを明らかにするために，S 氏にマルウェアの詳細な解析を依頼した。

〔マルウェアの解析結果〕

S 氏は，発見したマルウェア ML1～ML5 の検体を X 社の解析センタに持ち帰り，詳細に解析した。その解析結果の概要を表 2 に示す。

表 2　マルウェアの解析結果の概要

マルウェア名	特徴
ML1	・電子メールに添付された，ML1 が埋め込まれているファイルを PDF 閲覧ソフトで開くと，電子メールの本文の内容に関連する PDF ファイルを表示するとともに，PDF 閲覧ソフトの脆弱性を利用して OS の管理者権限を獲得し，ML2，ML3 を OS のシステムフォルダに配置する。
ML2	・利用者が Z ブラウザのバージョン 2 を利用している場合，Z ブラウザを起動するとその脆弱性を利用して，Z ブラウザのプロセスで動作する。Z ブラウザを終了すると動作を停止する。Z ブラウザがバージョン 3 の場合は，ML2 は動作しない。 ・Z ブラウザで設定されているプロキシサーバの IP アドレス，ポート番号，及びプロキシサーバでの認証の際に利用者が入力した認証情報を窃取し，OS のシステム情報格納領域に保持する。 ・攻撃者が用意しておいた数十の Web サーバ（以下，攻撃者のサーバという）に対して，プロキシサーバ経由で HTTP 通信を試みる。通信に成功すると，ML4 をダウンロードして OS のシステムフォルダに配置する。
ML3	・OS のシステムフォルダに配置されると，攻撃者のサーバに対して，HTTP 通信を試みる。通信に成功すると，ML4 をダウンロードして OS のシステムフォルダに配置する。

表２　マルウェアの解析結果の概要（続き）

マルウェア名	特徴
ML4	・OS のシステムフォルダに配置されると，攻撃者のサーバに，自身をダウンロードしたマルウェアと同じ方法で HTTP 通信を行い，OS の全てのコマンドを，攻撃者のサーバから HTTP 通信を介して遠隔操作可能な状態にする。 ・ML4 に感染した PC と同じネットワークセグメント（以下，セグメントという）内の他の PC，サーバ，ネットワーク機器の存在，空きポート，アプリケーションのバージョンなどの情報を収集し，結果を攻撃者のサーバに送信する。 ・様々なミドルウェアの脆弱性を利用した数百の攻撃用コードをもち，攻撃者の指示によって，ネットワーク上の他の PC，サーバ及びネットワーク機器を攻撃する。攻撃が成功すると，攻撃対象に ML4 自身を感染させる。それと同時に，ML5 を感染させることもできる。
ML5	・ML5 に感染した PC に USB メモリが接続されると，ML5 が自身を USB メモリに感染させる。 ・感染した USB メモリを，未感染の PC に接続したとき，ML5 が自身を感染させ，新たに感染した PC が接続されているセグメント内の PC，サーバ，ネットワーク機器の存在，空きポート，アプリケーションのバージョンなどの情報を収集し，保持する。 ・新たに感染した PC が接続されているセグメント内の PC，サーバなどに ML4 が存在していた場合は，保持している情報を ML4 経由で攻撃者のサーバに送信する。
共通	・ML1～ML5 はパック処理されている。パック処理とは，マルウェア本体をエンコードし，それをデコードするための展開コードを付加して一つのファイルにすることである。ファイル実行時に，展開コードがマルウェア本体をデコードし，実行する。 ・ML3～ML5 は，OS 起動時に自身を自動的に起動するように設定する。 ・ML2～ML5 は，OS のシステムフォルダに配置される際に，ファイルのタイムスタンプを特定のシステムファイルと同じものに書き換える。 ・ML2～ML5 は，感染した PC のパーソナルファイアウォール及び J 社が利用するウイルス対策ソフトのファイアウォール機能を無効にする。

引き続き，S 氏は，OA-LAN の構成機器の情報を調査した。その結果，次の見解に達した。

・4 か月前，複数の従業員に届いた，ML1 が埋め込まれているファイルを，一部の従業員が開いたことで PC がマルウェアに感染した。

・ML1～ML5 は，パック処理に共通した固有の特徴が見られることから，同一の攻撃者によって作られた。

・サーバ，PC がマルウェアに感染すると，その後，攻撃者がマルウェアを削除しても，感染の痕跡が残る。

・痕跡及び①ML3 の活動を示すログが残っていることから，攻撃者が ML3 の活動を隠蔽するために，J 社のある機器のログの改ざんを試みたが，成功しなかった。

・ML4 経由で J 社のネットワーク環境を知った攻撃者によって，ML5 がここ数日の間に送り込まれた。

〔マルウェア解析後の暫定対策〕

解析結果から，S 氏は直ちに対処が必要である旨を，Y 主任に報告した。Y 主任は S 氏の助言を受けて，ML2～ML4 と外部との通信を遮断する設定変更をプロキシサーバで行った。あわせて，②ML2 の活動を阻止するための対策も実施した。Y 主任は，過去のウイルス感染時の対策を参考に，DMZ の全サーバと，OA-LAN の PC のうち検査未実施の 50 台について，マルウェアの検査サービスを依頼したが，S 氏は，“今回はその他に，FW，RD-LAN の PC と RD サーバ及び［ a ］についても検査すべきである”と助言した。

J 社は S 氏の助言に従ってマルウェアの検査サービスを受けた。その結果，OA-LAN の PC にだけ ML1～ML5 の存在又は感染の痕跡が確認された。

次は，検査の結果に関する Y 主任と S 氏の会話である。

Y 主任：数年前のウイルス感染と同じ攻撃者なのでしょうか。

S 氏　：それは分かりませんが，今回の攻撃は，近年増えている攻撃と特徴がよく似ています。例えば，攻撃者が目的を達成するために，③マルウェアを発見されにくくする工夫をしている点や，侵入先の企業のセキュリティ対策に合わせて攻撃方法を変更している点などです。

Y 主任：侵入先のセキュリティ対策に合わせて攻撃方法を変更するというのは，具体的にはどういうことでしょうか。

S 氏　：ML5 がその代表例と言えます。攻撃者は，ML1～ML4 によって得た情報を基に④J 社のネットワーク構成上のセキュリティ対策を知り，それを突破できるように ML5 を送り込んだのではないかと考えています。仮に今回の攻撃者が，数年前のウイルス感染のような愉快犯であれば，ML5 を送り込まなかったと思います。しかし，今回の攻撃者は目的を達成するために，時間を掛けてでも攻撃を継続するのではないかと考えられます。

Y 主任：当社にとって，どんな被害が想定されるのでしょうか。

S 氏　：過去の同様の攻撃事例，J 社で実施されているリスク評価の結果を踏まえた情報資産の価値，ML5 が送り込まれたことを総合的に考えると，［ b ］されることが想定されます。

S 氏は更にマルウェアの解析を進め，マルウェアの駆除手順を J 社に提供した。それによって，J 社では OA-LAN の PC からマルウェアを駆除することができた。その後，Y 主任は S 氏の協力を得て，今回のマルウェア感染の根本原因を分析した。その分析結果を基に，PDF 閲覧ソフトのセキュリティパッチ適用，USB メモリへの書出し制限ソフトウェアの導入，従業員教育など，予防的な対策を実施した。

設問 1　〔マルウェアの解析結果〕について，(1)，(2)に答えよ。

(1)　ML4 をダウンロードしたマルウェア名を答えよ。

(2)　攻撃者が ML3 の活動を隠蔽するためにログの改ざんを試みた機器はどれか。マルウェアの特徴と J 社のネットワーク環境を基に答えよ。また，本文中の下線①について，どのような内容のログか。25 字以内で具体的に述べよ。

設問 2　〔マルウェア解析後の暫定対策〕について，(1)～(3)に答えよ。

(1)　本文中の［　a　］に入れる適切な字句を，本文中の用語を用いて 10 字以内で答えよ。

(2)　ML2～ML4 と外部との通信を遮断するために，Y 主任が行った設定変更を，40 字以内で具体的に述べよ。

(3)　本文中の下線②の対策とはどのようなものか。本文中の記載内容を基に 25 字以内で述べよ。

設問 3　攻撃者の目的について，(1)～(3)に答えよ。

(1)　本文中の下線③の工夫を，マルウェアの機能の観点から二つ挙げ，それぞれ 20 字以内で具体的に述べよ。

(2)　本文中の下線④について，攻撃者が突破を試みた J 社のセキュリティ対策とは何か。30 字以内で具体的に述べよ。

(3)　本文中の［　b　］に入れる，想定される J 社の被害を 15 字以内で答えよ。

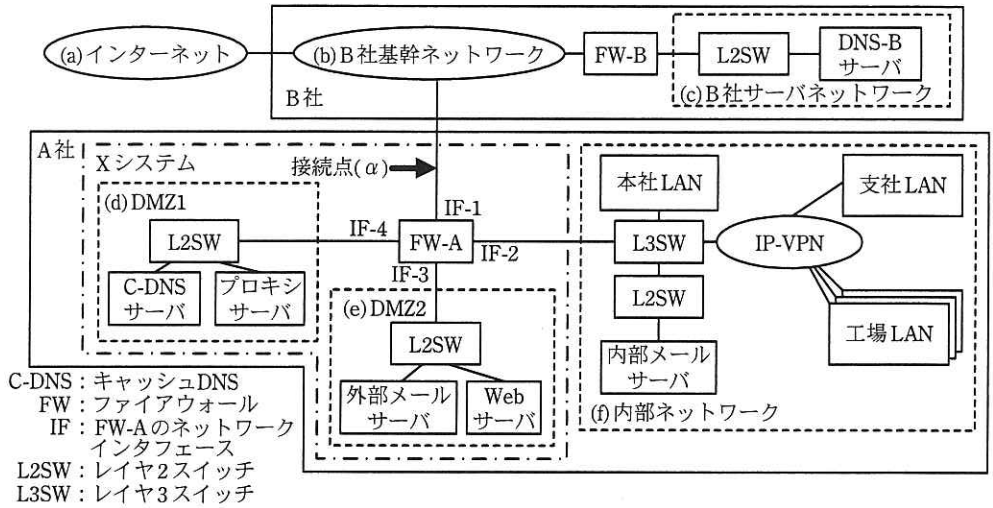
問2　IP アドレス詐称対策に関する次の記述を読んで，設問 1，2 に答えよ。

A 社は，従業員数 4,000 名の化学メーカである。東京に本社，大阪に支社，国内の 3 か所に工場がある。A 社では，電子メール（以下，メールという）の利用などのために，インターネット接続システム（以下，X システムという）を導入している。X システムは本社に設置され，B 社のインターネット接続サービス（以下，B 社サービスという）を利用している。また，本社，支社及び工場の LAN は IP-VPN で接続されている。

X システムの運用は，責任者である情報システム部の D 部長の下で，E 主任と F さんが担当している。X システムの各サーバでは，サーバへのアクセス及びプログラムの動作状況のログを記録している。

A 社のドメイン名は，B 社の DNS-B サーバで管理している。DNS-B サーバは DNS コンテンツサーバであり，リゾルバ機能（インターネット上のサーバ名の名前解決を行う機能）及び DNS キャッシュ機能（名前解決結果を一時的に保持する機能）をもたない。

現在の A 社及び B 社サービスのネットワーク構成を図 1 に，X システムの主な機器と機能を表 1 に示す。



注記 1　A 社の PC は全て本社 LAN，支社 LAN 又は工場 LAN に接続されている。
注記 2　PC の記載は省略している。

図 1　A 社及び B 社サービスのネットワーク構成

表1　Xシステムの主な機器と機能

機器名称	機能
FW-A	ステートフルパケットフィルタリング型FWであり，IPアドレス詐称対策機能及びパケットフィルタリング機能がある。IPアドレス詐称対策機能，パケットフィルタリング機能の順に処理する。また，通信の許可及び拒否のログを記録する機能がある。
C-DNSサーバ	リゾルバ機能及びDNSキャッシュ機能がある。
プロキシサーバ	プロキシ機能，Webコンテンツキャッシュ機能及びウイルススキャン機能がある。
外部メールサーバ	インターネットとの間及び内部メールサーバとの間のメール転送機能，SPF（Sender Policy Framework）検証機能並びにウイルススキャン機能がある。
Webサーバ	コンテンツ公開機能及びコンテンツ更新機能がある。

〔攻撃の検出〕

ある週の月曜日，Fさんが前週のFW-Aのログを分析したところ，C-DNSサーバを宛先とするDNSパケットが約10万件も通過を拒否されており，その全てが名前解決応答パケット（以下，応答PTという）であった。しかし，これらの拒否された応答PTに対応する名前解決問合せパケット（以下，問合せPTという）をC-DNSサーバから送信した記録は，FW-Aのログになかった。報告を受けたE主任は，次のことをFさんに説明した。

・DNSの名前解決通信は，主に［　a　］を用いる。［　a　］は，［　b　］ハンドシェイクを用いてコネクションを確立するTCPと比べて，送信元IPアドレスの詐称の検知が困難である。

・大量のDNSパケットは，応答PTの送信元IPアドレスや宛先ポート番号を細工した，キャッシュポイズニング攻撃（以下，CP攻撃という）のためのものだったと考えられる。

・CP攻撃への根本的な対策は，公開鍵暗号によるディジタル署名の仕組みを応用した［　c　］というDNSセキュリティ拡張方式を導入することだが，鍵の管理など，今までにない運用手順が必要になる。根本的な対策をするかどうか決める前に，なぜCP攻撃が発生したかを調査する必要がある。

そこで，E主任とFさんが，C-DNSサーバの設定を調べたところ，CP攻撃を成功しにくくする設定がなされていることを確認した。さらに，再帰的な名前解決の問合せPTの送信元を限定する設定が行われていることも確認した。

しかし，なおも拒否される応答 PT が多い状況が続いていることから，E 主任は，F さんに対し，図 1 中の接続点(α)にパケットモニタを接続した上で，FW-A 及び C-DNS サーバを調査するよう指示した。F さんが行った調査の結果を図 2 に示す。

(1) 送信元を詐称した問合せ PT
・C-DNS サーバは次のような問合せ PT を 10 分ごとに 1 個受信していた。
送信元が外部メールサーバであり，かつ，宛先が C-DNS サーバであり，かつ，FW-A が通過を許可した問合せ PT。内容は，国内の取引先の G 社が取得したドメイン名の TXT レコードの問合せであった。
(2) C-DNS サーバに向けた応答 PT
・(1)の問合せ PT が届いた直後の 1 秒間に，送信元が G 社の DNS サーバであり，かつ，宛先が C-DNS サーバである応答 PT が 100 個届き，FW-A が通過を拒否した。
・100 個の応答 PT の宛先ポート番号は，到着順に連番であった。
・応答内容は G 社のドメイン名の TXT レコードであった。
・TXT レコードには，SPF レコードが設定されていた。SPF レコードに設定されていた IP アドレスは，G 社に割り当てられたものではなかった。
・C-DNS サーバが(1)の問合せ PT の名前解決を行うための問合せ PT は，インターネット上の DNS サーバに送信されてはいなかった。
(3) C-DNS サーバのキャッシュ
・C-DNS サーバのキャッシュには，G 社のドメイン名の TXT レコードが保存されていた。
・TXT レコードには，SPF レコードが設定されており，G 社に割り当てられた IP アドレスのうち，G 社がメールを送信するサーバの IP アドレスが設定されていた。

図 2　F さんが行った調査の結果

この結果から，E 主任は，図 2 の(2)は G 社のドメイン名の TXT レコードに対する CP 攻撃であると判断した。

そこで，E 主任と F さんは，FW-A の設定を更に調べることにした。まず，送信元，宛先及びサービスの組合せによってパケットの許可又は拒否の動作を指定するフィルタリングルールを確認し，誤りがないことを確認した。

続いて，表 2 に示す IP アドレス詐称対策ルールを確認したところ，①表 2 の項番 1 の送信元に誤りがあることに気が付き，直ちに設定を修正した。

表2　IPアドレス詐称対策ルール

項番	FW-A の IF	送信元	動作
1	IF-1	DMZ1，内部ネットワーク	拒否
2	IF-1	全て	許可
3	IF-2	内部ネットワーク	許可
4	IF-2	全て	拒否
5	IF-3	DMZ2	許可
6	IF-3	全て	拒否
7	IF-4	DMZ1	許可
8	IF-4	全て	拒否

注記1　パケットが受信された“FW-A の IF”，及びパケットの“送信元”の組合せで，パケットの通過を許可するか又は拒否するかの“動作”を指定する。
注記2　項番が小さいものから順に，最初に一致したルールが適用される。

E 主任は，図 2 の(2)の攻撃は偶然に成功する可能性があることを F さんに説明した。E 主任は，②図 2 の(2)の攻撃に続いて行われる可能性が高い，TXT レコードを利用する機能への攻撃が発生していると考えた。そこで，X システムの各サーバのログを，過去 1 か月分にわたって調査するよう F さんに指示した。調査の結果，攻撃はあったものの，各サーバの設定が正しく行われていたので失敗に終わっていたことが確認された。

〔支社システムの検討と導入〕

A 社では，インターネット及び IP-VPN のトラフィックの増加に対処するために，支社に新たなインターネット接続システム（以下，支社システムという）の導入を計画していた。E 主任と F さんは，支社システムとして，支社に新たな FW を導入し，インターネット，新たな DMZ 及び支社 LAN を接続することにした。新たな DMZ には X システムのプロキシサーバと同じ機能の支社プロキシサーバを導入し，インターネットとの接続には，B 社サービスを利用することにした。

続いて，支社プロキシサーバでの名前解決に C-DNS サーバを利用し，支社プロキシサーバと C-DNS サーバとの間の通信を B 社サービス経由にする前提で，FW-A と C-DNS サーバの設定の見直しを検討した。検討の結果，送信元が支社プロキシサーバに詐称された問合せ PT を拒否する設定は不可能であり，FW-A の IP アドレス詐称対策機能が有効に機能しないことが分かった。そこで再検討した結果，③支社システムに

機能を追加することで対応することにした。この対応策によって，支社プロキシサーバと C-DNS サーバ間の通信が不要になることも確認した。支社システムへの［ c ］の導入は，X システムも併せて支社システムの完成後に検討することとし，今回は見送ることとした。

E 主任と F さんは，検討結果を支社システム導入計画としてまとめ，D 部長に報告した。D 部長は，支社システム導入計画を経営陣に説明し，了承を得た。E 主任と F さんは，支社システム導入計画の遂行に着手した。

設問 1　〔攻撃の検出〕について，(1)～(5)に答えよ。

(1) 本文中の［ a ］～［ c ］に入れる適切な字句を，［ a ］については英字 5 字以内，［ b ］については 6 字以内，［ c ］については英字 8 字以内で答えよ。

(2) E 主任と F さんが確認した，C-DNS サーバにおいて CP 攻撃を成功しにくくする対策とは何か。“ポート番号”という字句を用いて，対策の内容を 30 字以内で述べよ。

(3) C-DNS サーバにおいて，図 2 中の(1)の問合せ PT を拒否しない設定にしている理由を，40 字以内で述べよ。

(4) 本文中の下線①について，表 2 の項番 1 の送信元として設定すべき全てのネットワークを，図 1 中の(a)～(f)から選び，記号で答えよ。

(5) 本文中の下線②の攻撃の内容を，40 字以内で述べよ。

設問 2　〔支社システムの検討と導入〕について，(1)，(2)に答えよ。

(1) 送信元を支社プロキシサーバに詐称した問合せ PT に対し，FW-A の IP アドレス詐称対策機能が有効に機能しない理由を，60 字以内で述べよ。

(2) 本文中の下線③について，支社システムに追加する機能を，20 字以内で述べよ。

問3　リモートアクセス環境の情報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。

H社は，従業員数600名の産業用機械製造・販売会社であり，本社と8か所の支店がある。H社では，全従業員に1台ずつデスクトップPCを貸与している。他拠点への出張が多い従業員と，外出が多い営業部員には，社外持出し用PCも貸与している。社外持出し用PCは，出張先で業務システムから業務データを取り出せるように，拠点の社内LANに接続して業務システムを使うことが許可されている。

また，営業部員にはリモートアクセス環境が提供されている。H社には20の業務システムがあり，全てデータセンタ（以下，DCという）に設置されているが，現在リモートアクセス環境で利用できる業務システムは，営業支援システムだけである。

現在H社では，PC管理の効率化，及び従業員の利便性向上を目的として，デスクトップ仮想化によるシンクライアント環境（以下，VDIという）の導入の準備をしており，社内で利用しているデスクトップPCをVDIに置き換えることが，既に決定している。H社のVDIの概要を図1に示す。

(a) 仮想化ソフトウェアが動作するサーバ（以下，VDIサーバという）がDCに設置されており，その上で最大50台まで稼働する仮想化されたPC（以下，V-PCという）に，利用者がクライアント端末から接続する。
(b) 社内で利用しているデスクトップPCは全て回収し，デスクトップPC型のシンクライアント端末（以下，DTという）を全従業員に貸与する。また，①本社及び支店に，共用端末として数台のDTを設置し，他拠点から出張中の従業員が利用できるようにするとともに，出張時のPC利用に関するルールを設ける。
(c) DTからV-PCにキーボード及びマウスの入力が送信され，V-PCからDTに画面情報が送信される。
(d) 管理者は，ウイルス対策ソフトがインストールされ，ウイルス定義ファイルの自動更新が有効にされたマスタイメージを作成する。
(e) 利用者は，管理者が最新のマスタイメージから複製するV-PCを利用する。
(f) V-PCを利用するには，DTからV-PC接続ソフトを使って，VDI接続サーバに接続する。VDI接続サーバは利用者を認証した後で，DTとV-PCを接続する。
(g) VDI接続サーバでの利用者認証後，シングルサインオンによって，利用者は自動的にV-PCにログオンするとともに，追加の利用者認証なしで全ての業務システムを利用できる。
(h) 利用者がV-PCをログオフすると，そのV-PCは解放され，複製時の状態に初期化される。次回のログオン時には初期化されたV-PCに接続される。
(i) 利用者がV-PCをログオフせずに，V-PC接続ソフトを終了するか，又はDTの電源を切ると，V-PCの状態は維持され，次回の接続時にはそのV-PCに接続される。
（以下，省略）

図1　VDIの概要

〔リモートアクセス環境改善の要望〕

営業部では以前から，リモートアクセス環境で利用できる業務システムが限られていることに対する不満が挙がっていた。VDI 導入の決定を受けて，営業部長は情報システム部の K 部長に対して，“VDI の導入に合わせてリモートアクセス環境も強化し，勤怠管理・経費精算を行う業務管理システムと，電子メール（以下，メールという）も社外から利用できるようにしてほしい”という要望を出した。

K 部長は，営業部の要望を受け入れて，情報システム部の N 主任に，リモートアクセス環境の改善を検討するように指示した。改善案には，リモートアクセス特有のセキュリティ上のリスクへの対策も含めるように指示した。

〔リモートアクセス環境改善の検討〕

N 主任は，改善案として，VPN を利用してリモートアクセスを行う案（以下，案 1 という）と，VDI を利用してリモートアクセスを行う案（以下，案 2 という）を検討した。それぞれの案の概要を図 2 及び図 3 に示す。

- 社外持出し用 PC に VPN 接続ソフトをインストールし，DC に設置した VPN 装置に接続する。
- VPN 装置での ID とパスワードによる利用者認証後，社外持出し用 PC から直接業務システムにアクセスする。
- 社外持出し用 PC から VPN を利用して，営業支援システムのほか，業務管理システムとメールサーバにアクセスできる。
- VPN 接続後，業務システムごとの利用者認証に成功すると，業務システムを利用できる。
- 社外持出し用 PC では，修正パッチの自動適用と，ウイルス対策ソフトのウイルス定義ファイルの自動更新を有効にする。

図 2　案 1 の概要

- 社外持出し用 PC の代わりに，ノート型のシンクライアント端末（以下，NT という）を使用し，DC に設置したゲートウェイサーバ（以下，GW サーバという）に接続する。
- GW サーバでの ID とパスワードによる利用者認証後，シングルサインオンによって VDI 接続サーバの利用者認証が自動的に行われ，NT から V-PC に接続する。
- NT から，V-PC を使って間接的に業務システムを利用する。
- NT と GW サーバの間の通信は暗号化する。

図 3　案 2 の概要

N 主任はさらに，案 1 と案 2 について，リモートアクセス特有のリスクに対するリスク評価を行い，対策案を検討した。リスク評価の結果を表 1 に，リスクへの対策案を表 2 に示す。

表1　案1と案2それぞれのリスク評価の結果

リスク		リスク評価	
		案1	案2
(ア)	リモートアクセス通信経路での盗聴による情報漏えい	社外持出し用 PC と VPN 装置との間の通信が暗号化されているので，リスクは小さい。	NT と GW サーバとの間の通信が暗号化されているので，リスクは小さい。
(イ)	なりすましによるリモートアクセス環境への不正接続	VPN 装置がインターネットに公開されるので，リスクが大きい。	GW サーバがインターネットに公開されるので，リスクが大きい。
(ウ)	社外持出し用 PC 又は NT の盗難・紛失による情報漏えい	[a] が社外持出し用 PC に保存される可能性があるので，リスクが大きい。	V-PC 利用時は [a] が NT に残らないが，V-PC 以外の利用によって保存される可能性があるので，リスクが大きい。
(エ)	ウイルスの感染	社外持出し用 PC が長期間使用されていない場合，リスクが大きい。	図 1 の(e)の運用が確実でない場合，リスクが大きい。

表2　リスクへの対策案

リスク	リスクへの対策案	
	案1	案2
(ア)	−	−
(イ)	VPN 装置での利用者認証を強化する。	GW サーバでの利用者認証を強化する。
(ウ)	社外持出し用 PC で [b] の対策を行う。	NT で案 1 と同様の対策を行う，又は，[a] の保存を制限できる機能をもつ NT を利用する。
(エ)	利用者が，社外持出し用 PC 起動時に未適用の修正パッチがないことを確認する。	管理者が修正パッチの公開を確認した後で，②直ちに実施すべき作業を定める。

注記　リスク（ア）は，リスクが小さいので対策しない。

〔検討結果に対する指摘〕

N 主任はこれらの検討結果とシステム構成図を K 部長に提出した。K 部長は案 1 と案 2 とを比較して，次の 2 点を理由に案 2 を採用すべきであると N 主任に伝えた。

・リモートアクセス特有のリスクへの対策に，VDI の仕組みを生かせる。

・現在進めている VDI 導入の投資を生かせる。

N 主任が作成した，案 2 のシステム構成図を図 4 に示す。

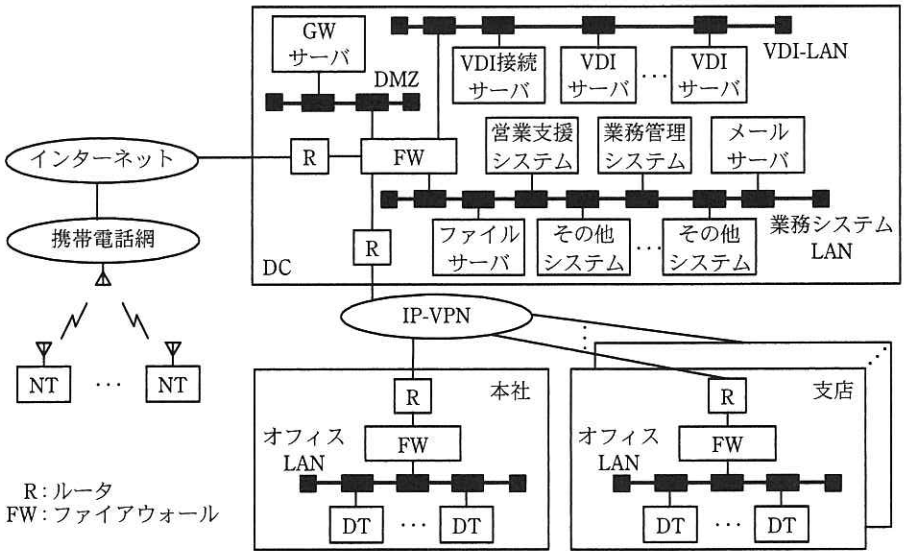


図４　案２のシステム構成図

また，K 部長は N 主任に，案 2 のリスクへの対策案は，次の点で不十分であると指摘した。

(1)　リスク(イ)が顕在化した場合，③案 1 よりも影響範囲が大きいと考えられる。より確実な対策を検討する必要がある。

(2)　リスク(ウ)への対策を確定させるために，NT の仕様を確認する必要がある。また，リスク(エ)について，NT 上のリスクと対策が考慮されていないので，対策を検討する必要がある。

(3)　VDI 導入の検討では，ネットワークのアクセス制御を変更していない。リモートアクセスの検討を行うこの機会に，VDI の仕組みをセキュリティリスクの低減に生かせるように，ネットワークのアクセス制御を変更する必要がある。

〔指摘への対応〕

N 主任は，指摘(1)への対応として，様々な利用者認証の手法を調査した結果，GW サーバの利用者認証に，ワンタイムパスワードの導入を提案することにした。次に，指摘(2)への対応に先立って NT の製品選定を行うために，市場シェアの高い V 社製の NT の仕様を確認した。V 社製の NT の仕様の抜粋を図 5 に示す。

(i) H社が現在のPCで使用しているものと同じOSが稼働し，V-PC接続ソフトがインストールされている。
(ii) ファイルシステムをもっており，データの保存ができるが，書込み制限機能を有効にすることによって，NTの電源を切ったときに，NTは初期状態に戻る。
(iii) 管理者が設定することによって，修正パッチの適用及びファイルの配信を自動で行うことができる。利用者がNTをオフィスLANに接続すると，自動的に書込み制限機能が解除され，修正パッチの適用及びファイルの配信が行われる。管理者による設定は，修正パッチの適用及びファイルの配信ごとに行う必要がある。
(iv) 管理者が設定することによって，利用者によるアプリケーションのインストールを禁止できる。

図5　V社製のNTの仕様（抜粋）

図5の仕様を調べたN主任は，V社製のNTを採用候補とした。その上で，指摘(2)への対応を検討した。

仕様(ii)の機能が，リスク(ウ)への対策として効果があると考えたN主任は，この機能を有効にするとともに，NTの利用終了時に必ずNTの電源を切ることをルール化することにした。

リスク(エ)については，NTがウイルスに感染するリスクに対する考慮が漏れていたので，このリスクに対して次の四つの対策を考えた。

(A) NTへの修正パッチの適用を，仕様(iii)の機能を使って行う。そのためにNTの管理サーバが必要になるので，VDI-LAN上に設置する。

(B) ウイルス対策ソフトをNTにインストールする。

(C) 仕様(iv)の機能を使って，V-PCへの接続に必要なアプリケーション以外はインストールさせない。

(D) NTは，V-PCの利用だけに用いる。

このうち，対策(B)については，リスク(ウ)への対策として仕様(ii)の機能を利用することを前提とした場合，高い頻度で行われるウイルス定義ファイルの更新のたびに，④管理者の作業と利用者の操作が発生してしまうので，現実的には難しいと考えた。そこで，対策(A)，対策(C)及び対策(D)をリスク(エ)への対策とすることにした。

最後にN主任は，指摘(3)への対応として，⑤図4中の各FWの設定を変更し，オフィスLANからアクセスできるネットワークをVDI-LANに限定することにした。

N主任は，以上の検討結果をまとめ，K部長に報告した。

〔改善案の承認〕

報告を受けたK部長は，N主任の案は，十分なセキュリティを確保し，かつリモートアクセス環境に対する営業部の要望を満たしていると判断し，採用を決定した。その後H社は，VDI導入と合わせてリモートアクセス環境の強化を行うことを決定した。

設問1　図1中の下線①によって得られるセキュリティ上の効果を，40字以内で具体的に述べよ。

設問2　〔リモートアクセス環境改善の検討〕について，(1)～(3)に答えよ。

(1)　表1中及び表2中の［　a　］に入れる適切な字句を10字以内で答えよ。

(2)　表2中の［　b　］に入れる適切な字句を15字以内で答えよ。

(3)　表2中の下線②について，管理者が実施すべき作業を三つ，それぞれ20字以内で述べよ。

設問3　本文中の下線③について，K部長が指摘した理由を，35字以内で述べよ。

設問4　〔指摘への対応〕について，(1)，(2)に答えよ。

(1)　本文中の下線④について，ウイルス定義ファイルの更新のたびに発生する管理者の作業と利用者の操作を，それぞれ25字以内で述べよ。

(2)　本文中の下線⑤について，N主任が考えたセキュリティリスク低減の効果を，30字以内で具体的に述べよ。また，そのような効果がある理由を30字以内で述べよ。

問4　情報漏えい対策に関する次の記述を読んで，設問1～4に答えよ。

L社は，従業員数200名のソフトウェアパッケージ開発会社である。L社では，自社で開発したソフトウェアパッケージを，顧客ごとの要件に合わせてカスタマイズする業務を行っている。商談の早い段階から，開発部門，営業部門など各部門の関係するメンバ（以下，プロジェクトメンバという）でプロジェクトを編成し，プロジェクトマネージャの下で業務を行っている。

〔L社の情報システムの構成〕

L社の情報システムの構成を図1に示す。

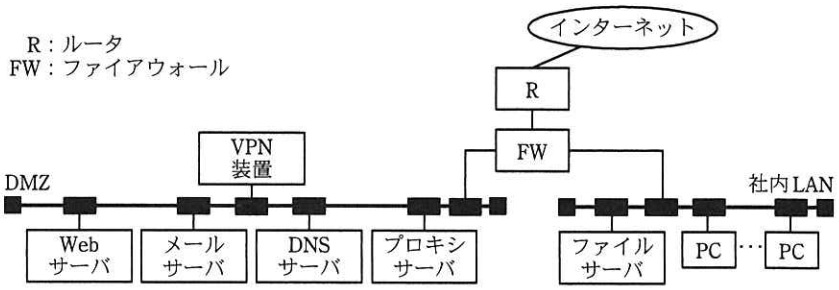


図1　L社の情報システムの構成

社内LAN上のPCからのインターネットの利用は，DMZ上のプロキシサーバ経由でのWebへのアクセスと，DMZ上のメールサーバ経由での電子メール（以下，メールという）の送受信の二つだけが許可されている。社内業務の多くは，社内LAN上のファイルサーバでファイルを共有して行われている。

〔機密情報の管理〕

L社内で扱う情報は，企業戦略上極めて重要で，かつ，ごく一部の関係者だけに開示される“厳秘”情報，関係者だけに開示される“秘”情報（以下，“厳秘”情報と“秘”情報を合わせて，機密情報という），通常の業務で使用する社内情報及び公知の情報に分類される。

L社では，①不正競争防止法に定められた営業秘密の3要件を文書管理規程に明示して，これを踏まえた分類と管理を従業員に求めている。また，機密情報にアクセス

できる者を制限するとともに，客観的認識可能性に配慮して，アクセスした情報が機密情報であるということを認識できるように管理することを求めている。

電子媒体の機密情報は，アクセス権を付与して管理している。紙媒体の機密情報は，表紙に“厳秘”又は“秘”の秘密区分を明記し，鍵が掛かるキャビネットで管理するという運用ルールを定めている。

〔情報システムのセキュリティ対策〕

L 社の情報システムでは，社内情報の保護のために図 2 に示す技術的セキュリティ対策が実施されている。人的セキュリティ対策としては，特に機密情報の管理に関して，入社時及び定期的な教育で周知徹底している。また，入社時に，セキュリティポリシ遵守の誓約書を提出させている。

1. 不正アクセス対策
   （省略）
2. アクセス制御
   (1) VPN 装置などの利用者 ID の管理　（省略）
   (2) ファイルサーバのアクセス権管理　（省略）
3. マルウェア対策
   （省略）
4. ログ管理
   （省略）
5. メールセキュリティ
   (1) 送受信メールのログ記録　（省略）
   (2) 送受信メールのマルウェア検査　（省略）
   (3) 送信メールの情報漏えい対策と誤送信対策　（省略）
6. Web フィルタリング
   (1) プロキシサーバ上でのフィルタリング
   インターネット上の Web メール，Web ストレージサービス，SNS などの Web サイトへの情報の書込みを全て遮断

（以下，省略）

図 2　L 社の情報システムの技術的セキュリティ対策

〔アクセス制御とログ管理〕

図 2 の 2.(1)及び 2.(2)は，情報システム部の社内情報基盤の運用担当者（以下，運用担当者という）が行う。機密情報を含むプロジェクトの全ての情報は，一つの専用フォルダで管理する。専用フォルダの使用開始・終了及びアクセス権の付与・解除は，

プロジェクトマネージャが運用担当者に申請する。運用担当者は，プロジェクト開始時に専用フォルダを作成し，申請されたプロジェクトメンバにアクセス権を付与する。プロジェクトメンバは，専用フォルダ内にサブフォルダを作成することができる。

プロジェクト終了時は，運用担当者が専用フォルダ内のファイルのバックアップを保管し，専用フォルダを削除する。また，従業員の退職時の運用ルールを図 3 に示す。従業員の退職時を含め，専用フォルダ内のファイルへのアクセスが不要になったときは，退職時の運用ルールなどに従って利用者 ID，アクセス権の管理を行う。

1. 退職する従業員は，所定の退職届用紙に記入・署名・押印した後，所属部門長が確認・押印して人事部に提出する。（人事規程から転載）
2. 所属部門長は，人事部から退職届受理の通知を受けると，退職する従業員のプロジェクト参画状況を確認した上で，該当する各プロジェクトマネージャに通知する。
3. 各プロジェクトマネージャは，速やかに“利用者 ID 停止・アクセス権解除申請書”を作成・押印し，運用担当者に送付する。
4. 運用担当者は，“利用者 ID 停止・アクセス権解除申請書”に従って，退職日終業時刻以降に，利用者 ID を停止し，アクセス権を解除する。

図 3　退職時の運用ルール

ファイルサーバの各フォルダへのアクセスログは，情報システム部の P 君が週 1 回分析している。例えば，短時間に大量のデータにアクセスするような不審なアクセスが見つかった場合には，上司の Q 主任，又は必要に応じて情報セキュリティ責任者である R 部長に報告し，指示を仰いでいる。

〔社外作業におけるセキュリティ対策〕

専用フォルダ内の情報は，顧客先でも必要になるので，社外持出し用 PC で社外からもアクセスできるようにしている。また，社外持出し用 PC でインターネットにアクセスして情報を収集できるようにしている。

社外からファイルサーバにアクセスする場合は，社外持出し用 PC を携帯電話網経由で L 社の VPN 装置に接続する。VPN 装置は利用者 ID とパスワードで認証を行い，社内 LAN への接続に対してリバースプロキシサーバとして動作する。

従業員が専用フォルダ内の情報をファイルサーバから社外持出し用 PC にダウンロードして使用する場合の情報漏えい対策としては，USB メモリなどの外部記録媒体へ

の書込みを禁止し，無線 LAN 機能を停止している。さらに，PC の管理権限を与えていない。また，社外持出し用 PC には，ウイルス対策ソフトを導入している。

〔インシデントの発生〕

ある日 P 君は，あるプロジェクトの専用フォルダが，その 4 日前の夜間に，外部から大量にアクセスされていたことに気付き，Q 主任に連絡した。Q 主任が確認したところ，1 週間前に退職した元従業員の利用者 ID が用いられていたことが分かった。

その利用者 ID はまだ有効であったので，Q 主任は，即座にその利用者 ID を停止することで VPN 接続ができないようにした上，②証拠を保存するために必要な措置を取り，調査を行った。当該プロジェクトのプロジェクトマネージャは 1 か月間の海外出張中で，利用者 ID の停止申請処理をしていなかった。

〔社内情報の保護対策〕

今回のインシデントの調査としてアクセスログを分析したが，機密情報への不正なアクセスは発見されなかった。しかし，事態を重く見た経営陣は，以前からセキュリティ上の懸念があった社外持出し用 PC も含め，機密情報保護の観点で，情報セキュリティ対策を見直し，速やかに改善するよう R 部長に指示し，Q 主任が対策をまとめることになった。Q 主任の検討結果の抜粋を図 4 に示す。

1. 退職者の利用者 ID の停止及びアクセス権の解除漏れ対策
   退職者などの人事情報を情報システムと連動させることで，確実に利用者 ID の停止とアクセス権の解除は可能になるが，情報システムの改修に時間が掛かるので，当面は運用改善による次の緊急対策を行うこととする。
   対策：［ a ］からの連絡を受け，運用担当者が利用者 ID の停止とアクセス権の解除を，［ b ］後，速やかに行う。
2. インターネットアクセスの情報漏えい対策
   社内からのインターネットアクセスと比較して，社外での社外持出し用 PC からのインターネットアクセスはセキュリティ上のリスクが大きいので，社内からのインターネットアクセスと同様の制限を課すために，次の対策を追加する。
   対策：社外での社外持出し用 PC からのインターネットへのアクセスは，［ c ］。

図 4　Q 主任の検討結果（抜粋）

Q 主任の検討結果をレビューした R 部長は，検討結果の対策を速やかに実施するよう指示した。さらに，R 部長は，これまでの L 社の電子媒体の機密情報に対する管理は，客観的認識可能性の点から不十分であると考え，Q 主任に，③運用上のルールを策定し，全従業員に周知徹底するよう指示した。

設問 1　本文中の下線①の営業秘密の 3 要件を，それぞれ 15 字以内で答えよ。

設問 2　本文中の下線②で利用する手法や技術のことを何というか。適切な用語を 15 字以内で答えよ。

設問 3　図 4 に示した Q 主任の検討結果について，(1)，(2)に答えよ。

(1)　1.の対策について，［ a ］，［ b ］に入れる適切な字句を，それぞれ答えよ。

(2)　2.の対策で想定しているセキュリティ上のリスクを，40 字以内で述べよ。また，［ c ］に入れる具体的な対策を，20 字以内で述べよ。

設問 4　本文中の下線③の運用上のルールの内容を，40 字以内で述べよ。

6. 退室可能時間に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	13:10 ～ 13:50

7. **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。
8. 問題冊子の余白などは，適宜利用して構いません。
9. 試験時間中，机上に置けるものは，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，黒鉛筆及びシャープペンシル（B 又は HB），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は使用不可），ハンカチ，ポケットティッシュ，目薬
   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 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。
13. 午後Ⅱの試験開始は 14:30 ですので，14:10 までに着席してください。

試験問題に記載されている会社名又は製品名は，それぞれ各社の商標又は登録商標です。
なお，試験問題では，™ 及び ® を明記していません。

©2013　独立行政法人情報処理推進機構