SG

平成28年度　秋期
情報セキュリティマネジメント試験
午前　問題

試験時間	9:30 ～ 11:00（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50
選択方法	全問必須

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) 答案用紙は光学式読取り装置で読み取った上で採点しますので，B又はHBの黒鉛筆で答案用紙の**マークの記入方法**のとおりマークしてください。マークの濃度がうすいなど，**マークの記入方法**のとおり正しくマークされていない場合は，読み取れません。特にシャープペンシルを使用する際には，マークの濃度に十分ご注意ください。訂正の場合は，あとが残らないように消しゴムできれいに消し，消しくずを残さないでください。
   (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**を記入及びマークしてください。答案用紙の**マークの記入方法**のとおり記入及びマーク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及びマークしてください。
   (3) **解答**は，次の例題にならって，**解答欄**に一つだけマークしてください。答案用紙の**マークの記入方法**のとおりマークされていない場合は，採点されません。

〔例題〕　秋の情報処理技術者試験が実施される月はどれか。

ア　8　　イ　9　　ウ　10　　エ　11

正しい答えは“ウ　10”ですから，次のようにマークしてください。

例題	㋐ ㋑ ● ㋓

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。

問題文中で共通に使用される表記ルール

各問題文中に注記がない限り，次の表記ルールが適用されているものとする。

試験問題での表記	規格・標準の名称
JIS Q 9001	JIS Q 9001:2015
JIS Q 14001	JIS Q 14001:2015
JIS Q 15001	JIS Q 15001:2006
JIS Q 20000-1	JIS Q 20000-1:2012
JIS Q 20000-2	JIS Q 20000-2:2013
JIS Q 27000	JIS Q 27000:2014
JIS Q 27001	JIS Q 27001:2014
JIS Q 27002	JIS Q 27002:2014
JIS X 0160	JIS X 0160:2012
ISO 21500	ISO 21500:2012
ITIL	ITIL 2011 edition
PMBOK	PMBOK ガイド 第5版
共通フレーム	共通フレーム 2013

問1　IC カードと PIN を用いた利用者認証における適切な運用はどれか。

ア　IC カードによって個々の利用者が識別できるので，管理負荷を軽減するために全利用者に共通の PIN を設定する。

イ　IC カード紛失時には，新たな IC カードを発行し，PIN を再設定した後で，紛失した IC カードの失効処理を行う。

ウ　PIN には，IC カードの表面に刻印してある数字情報を組み合わせたものを設定する。

エ　PIN は，IC カードの配送には同封せず，別経路で利用者に知らせる。

問2　リスクの顕在化に備えて地震保険に加入するという対応は，JIS Q 31000:2010 に示されているリスク対応のうち，どれに分類されるか。

ア　ある機会を追求するために，そのリスクを取る又は増加させる。

イ　一つ以上の他者とそのリスクを共有する。

ウ　リスク源を除去する。

エ　リスクを生じさせる活動を開始又は継続しないと決定することによって，リスクを回避する。

問３　JPCERT/CC の説明はどれか。

ア　工業標準化法に基づいて経済産業省に設置されている審議会であり，工業標準化全般に関する調査・審議を行っている。

イ　電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクトであり，総務省及び経済産業省が共同で運営する暗号技術検討会などで構成される。

ウ　特定の政府機関や企業から独立した組織であり，国内のコンピュータセキュリティインシデントに関する報告の受付，対応の支援，発生状況の把握，手口の分析，再発防止策の検討や助言を行っている。

エ　内閣官房に設置され，我が国をサイバー攻撃から防衛するための司令塔機能を担う組織である。

問４　JVN（Japan Vulnerability Notes）はどれか。

ア　情報システムに存在する脆弱性の深刻度を評価する手法

イ　製品に存在する脆弱性に対して採番された識別子

ウ　脆弱性対策情報などを提供するポータルサイト

エ　組織内の情報セキュリティ問題を専門に扱うインシデント対応チーム

問５　ファイルサーバについて，情報セキュリティにおける“可用性”を高めるための管理策として，適切なものはどれか。

ア　ストレージを二重化し，耐障害性を向上させる。

イ　ディジタル証明書を利用し，利用者の本人確認を可能にする。

ウ　ファイルを暗号化し，情報漏えいを防ぐ。

エ　フォルダにアクセス権を設定し，部外者の不正アクセスを防止する。

問6　情報セキュリティ対策を検討する際の手法の一つであるベースラインアプローチの特徴はどれか。

ア　基準とする望ましい対策と組織の現状における対策とのギャップを分析する。
イ　現場担当者の経験や考え方によって検討結果が左右されやすい。
ウ　情報資産ごとにリスクを分析する。
エ　複数のアプローチを併用して分析作業の効率化や分析精度の向上を図る。

問7　組織の所属者全員に利用者 ID が発行されるシステムがある。利用者 ID の発行・削除は申請に基づき行われているが，申請漏れや申請内容のシステムへの反映漏れがある。資料 A，B の組合せのうち，資料 A と資料 B を突き合わせて確認することによって，退職者に発行されていた利用者 ID の削除漏れが最も確実に発見できるものはどれか。

	資料 A	資料 B
ア	組織の現在の所属者の名簿	退職に伴う利用者 ID の削除申請書
イ	退職者の一覧	組織の現在の所属者の名簿
ウ	利用者 ID とそれが発行されている者の一覧	組織の現在の所属者の名簿
エ	利用者 ID とそれが発行されている者の一覧	退職に伴う利用者 ID の削除申請書

問８　JIS Q 27000 におけるリスク評価はどれか。

ア　対策を講じることによって，リスクを修正するプロセス
イ　リスクが受容可能か否かを決定するために，リスク分析の結果をリスク基準と比較するプロセス
ウ　リスクの特質を理解し，リスクレベルを決定するプロセス
エ　リスクの発見，認識及び記述を行うプロセス

問９　JIS Q 31000:2010 における残留リスクの定義はどれか。

ア　監査手続を実施しても監査人が重要な不備を発見できないリスク
イ　業務の性質や本来有する特性から生じるリスク
ウ　利益を生む可能性に内在する損失発生の可能性として存在するリスク
エ　リスク対応後に残るリスク

問10　情報セキュリティ意識向上のための教育の実施状況を JIS Q 27002 に従ってレビューした。情報セキュリティを強化する観点から，改善が必要な状況はどれか。

ア　従業員の受講記録を分析し，教育計画を見直していた。
イ　従業員の職務内容や職制に応じた内容の教育を実施していた。
ウ　出張中で受講できなかった従業員を対象に，追加の教育を実施していた。
エ　正規従業員と同様の業務に従事している派遣従業員を除いて，教育を実施していた。

問11　システム管理者に対する施策のうち，IPA“組織における内部不正防止ガイドライン”に照らして，内部不正防止の観点から適切なものはどれか。

ア　システム管理者間の会話・情報交換を制限する。
イ　システム管理者の操作履歴を本人以外が閲覧することを制限する。
ウ　システム管理者の長期休暇取得を制限する。
エ　夜間・休日のシステム管理者の単独作業を制限する。

問12　ボットネットにおける C&C サーバの役割はどれか。

ア　Web サイトのコンテンツをキャッシュし，本来のサーバに代わってコンテンツを利用者に配信することによって，ネットワークやサーバの負荷を軽減する。
イ　遠隔地からインターネットを経由して社内ネットワークにアクセスする際に，CHAP などのプロトコルを用いることによって，利用者認証時のパスワードの盗聴を防止する。
ウ　遠隔地からインターネットを経由して社内ネットワークにアクセスする際に，チャレンジレスポンス方式を採用したワンタイムパスワードを用いることによって，利用者認証時のパスワードの盗聴を防止する。
エ　侵入して乗っ取ったコンピュータに対して，他のコンピュータへの攻撃などの不正な操作をするよう，外部から命令を出したり応答を受け取ったりする。

問13　会社や団体が，自組織の従業員に貸与するスマートフォンに対して，情報セキュリティポリシに従った一元的な設定をしたり，業務アプリケーションを配信したりして，スマートフォンの利用状況などを一元管理する仕組みはどれか。

ア　BYOD（Bring Your Own Device）
イ　ECM（Enterprise Content Management）
ウ　LTE（Long Term Evolution）
エ　MDM（Mobile Device Management）

問14　サーバにバックドアを作り，サーバ内での侵入の痕跡を隠蔽するなどの機能をもつ不正なプログラムやツールのパッケージはどれか。

ア　RFID　　イ　rootkit　　ウ　TKIP　　エ　web beacon

問15　SIEM（Security Information and Event Management）の機能として，最も適切なものはどれか。

ア　機密情報を自動的に特定し，機密情報の送信や出力など，社外への持出しに関連する操作を検知しブロックする。
イ　サーバやネットワーク機器などのログデータを一括管理，分析して，セキュリティ上の脅威を発見し，通知する。
ウ　情報システムの利用を妨げる事象を管理者が登録し，各事象の解決・復旧までを管理する。
エ　ネットワークへの侵入を試みるパケットを検知し，通知する。

問16　SPF（Sender Policy Framework）を利用する目的はどれか。

ア　HTTP 通信の経路上での中間者攻撃を検知する。

イ　LAN への PC の不正接続を検知する。

ウ　内部ネットワークへの侵入を検知する。

エ　メール送信元のなりすましを検知する。

問17　次の電子メールの環境を用いて，秘密情報を含むファイルを電子メールに添付して社外の宛先の利用者に送信したい。その際のファイルの添付方法，及びその添付方法を使う理由として，適切なものはどれか。

〔電子メールの環境〕

・電子メールは，Web ブラウザから利用できる電子メールシステム（Web メール）を用いて送信する。

・Web ブラウザと Web メールのサーバとの通信は HTTP over TLS（HTTPS）で行う。

・社外の宛先ドメインのメールサーバは SMTP と POP3 を使用している。

・IP 層以下は暗号化していない。

ア　Web ブラウザから Web メールのサーバまでの通信が暗号化されているので，ファイルは平文のままでメールに添付する。

イ　Web ブラウザから Web メールのサーバまでの通信は暗号化されるが，その後の通信が暗号化されないこともあるので，ファイルを暗号化してメールに添付する。

ウ　Web ブラウザから宛先の利用者がメールを受信する PC まで，全ての通信は暗号化されるので，ファイルは平文のままでメールに添付する。

エ　Web メールのサーバから宛先ドメインのメールサーバまでの通信は暗号化されないが，サーバ間の通信は Base64 形式でエンコードすれば盗聴できないので，ファイルは Base64 形式でエンコードしてメールに添付する。

問18　ウイルス検出におけるビヘイビア法に分類されるものはどれか。

ア　あらかじめ検査対象に付加された，ウイルスに感染していないことを保証する情報と，検査対象から算出した情報とを比較する。

イ　検査対象と安全な場所に保管してあるその原本とを比較する。

ウ　検査対象のハッシュ値と既知のウイルスファイルのハッシュ値とを比較する。

エ　検査対象をメモリ上の仮想環境下で実行して，その挙動を監視する。

問19　インターネットと社内サーバの間にファイアウォールが設置されている環境で，時刻同期の通信プロトコルを用いて社内サーバがもつ時計をインターネット上の時刻サーバの正確な時刻に同期させる。このとき，ファイアウォールで許可すべき時刻サーバとの間の通信プロトコルはどれか。

ア　FTP（TCP，ポート番号 21）

イ　NTP（UDP，ポート番号 123）

ウ　SMTP（TCP，ポート番号 25）

エ　SNMP（TCP 及び UDP，ポート番号 161 及び 162）

問20　人間には読み取ることが可能でも，プログラムでは読み取ることが難しいという差異を利用して，ゆがめたり一部を隠したりした画像から文字を判読して入力させることによって，プログラムによる自動入力を排除するための技術はどれか。

ア　CAPTCHA　　イ　QR コード

ウ　短縮 URL　　エ　トラックバック ping

問21　情報の“完全性”を脅かす攻撃はどれか。

ア　Web ページの改ざん
イ　システム内に保管されているデータの不正コピー
ウ　システムを過負荷状態にする DoS 攻撃
エ　通信内容の盗聴

問22　クロスサイトスクリプティングの手口はどれか。

ア　Web アプリケーションに用意された入力フィールドに，悪意のある JavaScript コードを含んだデータを入力する。
イ　インターネットなどのネットワークを通じてサーバに不正にアクセスしたり，データの改ざんや破壊を行ったりする。
ウ　大量のデータを Web アプリケーションに送ることによって，用意されたバッファ領域をあふれさせる。
エ　パス名を推定することによって，本来は認証された後にしかアクセスが許可されないページに直接ジャンプする。

問23　内閣は，2015 年 9 月にサイバーセキュリティ戦略を定め，その目的達成のための施策の立案及び実施に当たって，五つの基本原則に従うべきとした。その基本原則に含まれるものはどれか。

ア　サイバー空間が一部の主体に占有されることがあってはならず，常に参加を求める者に開かれたものでなければならない。

イ　サイバー空間上の脅威は，国を挙げて対処すべき課題であり，サイバー空間における秩序維持は国家が全て代替することが適切である。

ウ　サイバー空間においては，安全確保のために，発信された情報を全て検閲すべきである。

エ　サイバー空間においては，情報の自由な流通を尊重し，法令を含むルールや規範を適用してはならない。

問24　スクリプトキディの典型的な行為に該当するものはどれか。

ア　PC の利用者が Web サイトにアクセスし，利用者 ID とパスワードを入力するところを後ろから盗み見して，メモをとる。

イ　技術不足なので新しい攻撃手法を考え出すことはできないが，公開された方法に従って不正アクセスを行う。

ウ　顧客になりすまして電話でシステム管理者にパスワードの再発行を依頼し，新しいパスワードを聞き出すための台本を作成する。

エ　スクリプト言語を利用してプログラムを作成し，広告や勧誘などの迷惑メールを不特定多数に送信する。

問25　緊急事態を装って組織内部の人間からパスワードや機密情報を入手する不正な行為は，どれに分類されるか。

ア　ソーシャルエンジニアリング　　イ　トロイの木馬
ウ　踏み台攻撃　　エ　ブルートフォース攻撃

問26　パスワードリスト攻撃に該当するものはどれか。

ア　一般的な単語や人名からパスワードのリストを作成し，インターネットバンキングへのログインを試行する。
イ　想定し得るパスワードとそのハッシュ値との対のリストを用いて，入手したハッシュ値からパスワードを効率的に解析する。
ウ　どこかの Web サイトから流出した利用者 ID とパスワードのリストを用いて，他の Web サイトに対してログインを試行する。
エ　ピクチャパスワードの入力を録画してリスト化しておき，それを利用することによってタブレット端末へのログインを試行する。

問27　ランサムウェアに分類されるものはどれか。

ア　感染した PC が外部と通信できるようプログラムを起動し，遠隔操作を可能にするマルウェア
イ　感染した PC に保存されているパスワード情報を盗み出すマルウェア
ウ　感染した PC のキー操作を記録し，ネットバンキングの暗証番号を盗むマルウェア
エ　感染した PC のファイルを暗号化し，ファイルの復号と引換えに金銭を要求するマルウェア

問28　なりすましメールでなく，EC（電子商取引）サイトから届いたものであることを確認できる電子メールはどれか。

ア　送信元メールアドレスがECサイトで利用されているアドレスである。
イ　送信元メールアドレスのドメインがECサイトのものである。
ウ　ディジタル署名の署名者のメールアドレスのドメインがECサイトのものであり，署名者のディジタル証明書の発行元が信頼できる組織のものである。
エ　電子メール本文の末尾にテキスト形式で書かれた送信元の連絡先に関する署名のうち，送信元の組織を表す組織名がECサイトのものである。

問29　PKI（公開鍵基盤）における認証局が果たす役割はどれか。

ア　共通鍵を生成する。
イ　公開鍵を利用してデータを暗号化する。
ウ　失効したディジタル証明書の一覧を発行する。
エ　データが改ざんされていないことを検証する。

問30　情報技術セキュリティ評価のための国際標準であり，コモンクライテリア（CC）と呼ばれるものはどれか。

ア　ISO 9001　　イ　ISO 14004
ウ　ISO/IEC 15408　　エ　ISO/IEC 27005

問31　プロバイダ責任制限法において，損害賠償責任が制限されるプロバイダの行為に該当するものはどれか。ここで，“利用者”とはプロバイダに加入してサービスを利用している者とする。

ア　契約書に記載した利用者の個人情報を，本人の同意を得ずに関連会社に渡した。
イ　他のプロバイダに移転する利用者に対して，不当に高い違約金を請求した。
ウ　利用者の送信メールの内容を盗聴し，それを興味本位で他人に伝えた。
エ　利用者の電子掲示板への書込みが，他人の権利を侵害しているとは知らずに放置した。

問32　刑法の電子計算機使用詐欺罪が適用される違法行為はどれか。

ア　いわゆるねずみ講方式による取引形態の Web ページを開設する。
イ　インターネット上に，実際よりも良品と誤認させる商品カタログを掲載し，粗悪な商品を販売する。
ウ　インターネットを経由して銀行のシステムに虚偽の情報を与え，不正な振込や送金をさせる。
エ　企業の Web ページを不正な手段によって改変し，その企業の信用を傷つける情報を流す。

問33　“特定個人情報ファイル”の取扱いのうち，国の個人情報保護委員会が制定した“特定個人情報の適正な取扱いに関するガイドライン（事業者編）”で，認められているものはどれか。

ア　個人番号関係事務を行う必要がなくなり，かつ，法令による保存期間を経過した場合は，暗号化した上で保管する。

イ　事業者内の誰でも容易に参照できるよう，事務取扱担当者を限定せず従業員全員にアクセス権を設定する。

ウ　従業員の個人番号を含む源泉徴収票を，業務委託先の税理士に作成させる。

エ　従業員の個人番号を利用して営業成績を管理する。

問34　広告宣伝の電子メールを送信する場合，特定電子メール法に照らして適切なものはどれか。

ア　送信の許諾を通知する手段を電子メールに表示していれば，同意を得ていない不特定多数の人に電子メールを送信することができる。

イ　送信の同意を得ていない不特定多数の人に電子メールを送信する場合は，電子メールの表題部分に未承諾広告であることを明示する。

ウ　取引関係にあるなどの一定の場合を除き，あらかじめ送信に同意した者だけに対して送信するオプトイン方式をとる。

エ　メールアドレスを自動的に生成するプログラムを利用して電子メールを送信する場合は，送信者の氏名・連絡先を電子メールに明示する。

問35　不正アクセス禁止法による処罰の対象となる行為はどれか。

ア　推測が容易であるために，悪意のある攻撃者に侵入される原因となった，パスワードの実例を，情報セキュリティに関するセミナの資料に掲載した。

イ　ネットサーフィンを行ったところ，意図せずに他人の利用者 ID とパスワードをダウンロードしてしまい，PC 上に保管してしまった。

ウ　標的とする人物の親族になりすまし，不正に現金を振り込ませる目的で，振込先の口座番号を指定した電子メールを送付した。

エ　不正アクセスを行う目的で他人の利用者 ID，パスワードを取得したが，これまでに不正アクセスは行っていない。

問36　準委任契約の説明はどれか。

ア　成果物の対価として報酬を得る契約

イ　成果物を完成させる義務を負う契約

ウ　善管注意義務を負って作業を受託する契約

エ　発注者の指揮命令下で作業を行う契約

問37　JIS Q 27001 に準拠して ISMS を運用している場合，内部監査について順守すべき要求事項はどれか。

ア　監査員には ISMS 認証機関が認定する研修の修了者を含まなければならない。

イ　監査責任者は代表取締役が任命しなければならない。

ウ　監査範囲は JIS Q 27001 に規定された管理策に限定しなければならない。

エ　監査プログラムには前回までの監査結果を考慮しなければならない。

問38　インシデントの調査やシステム監査にも利用できる，証拠を収集し保全する技法はどれか。

ア　コンティンジェンシープラン　　イ　サンプリング
ウ　ディジタルフォレンジックス　　エ　ベンチマーキング

問39　事業継続計画（BCP）について監査を実施した結果，適切な状況と判断されるものはどれか。

ア　従業員の緊急連絡先リストを作成し，最新版に更新している。
イ　重要書類は複製せずに１か所で集中保管している。
ウ　全ての業務について，優先順位なしに同一水準のBCPを策定している。
エ　平時にはBCPを従業員に非公開としている。

問40　“情報セキュリティ監査基準”に関する記述のうち，最も適切なものはどれか。

ア　“情報セキュリティ監査基準”は情報セキュリティマネジメントシステムの国際規格と同一の内容で策定され，更新されている。
イ　情報セキュリティ監査人は，他の専門家の支援を受けてはならないとしている。
ウ　情報セキュリティ監査の判断の尺度には，原則として，“情報セキュリティ管理基準”を用いることとしている。
エ　情報セキュリティ監査は高度な技術的専門性が求められるので，監査人に独立性は不要としている。

問41　システムの移行テストを実施する主要な目的はどれか。

ア　確実性や効率性の観点で，既存システムから新システムへの切替え手順や切替えに伴う問題点を確認する。

イ　既存システムの実データのコピーを利用して，新システムでも十分な性能が得られることを確認する。

ウ　既存の他システムのプログラムと新たに開発したプログラムとのインタフェースの整合性を確認する。

エ　新システムが，要求された全ての機能を満たしていることを確認する。

問42　あるデータセンタでは，受発注管理システムの運用サービスを提供している。次の“受発注管理システムの運用中の事象”において，インシデントに該当するものはどれか。

〔受発注管理システムの運用中の事象〕

夜間バッチ処理において，注文トランザクションデータから注文書を出力するプログラムが異常終了した。異常終了を検知した運用担当者から連絡を受けた保守担当者は，緊急出社してサービスを回復し，後日，異常終了の原因となったプログラムの誤りを修正した。

ア　異常終了の検知　　イ　プログラムの誤り

ウ　プログラムの異常終了　　エ　保守担当者の緊急出社

問43　メールサーバのディスクに障害が発生して多数の電子メールが消失した。消失した電子メールの復旧を試みたが，2 週間ごとに行っている磁気テープへのフルバックアップしかなかったので，最後のフルバックアップ以降 1 週間分の電子メールが回復できなかった。そこで，今後は前日の状態までには復旧できるようにしたい。対応策として，適切なものはどれか。

ア　2 週間ごとの磁気テープへのフルバックアップに加え，毎日，磁気テープへの差分バックアップを行う。
イ　電子メールを複数のディスクに分散して蓄積する。
ウ　バックアップ方法は今のままとして，メールサーバのディスクをミラーリングするようにし，信頼性を高める。
エ　毎日，メールサーバのディスクにフルバックアップを行い，2 週間ごとに，バックアップしたデータを磁気テープにコピーして保管する。

問44　プロジェクトに関わるステークホルダの説明のうち，適切なものはどれか。

ア　組織の外部にいることはなく，組織の内部に属している。
イ　プロジェクトの成果が，自らの利益になる者と不利益になる者がいる。
ウ　プロジェクトへの関与が間接的なものにとどまることはなく，プロジェクトには直接参加する。
エ　プロジェクトマネージャのように，個人として特定できることが必要である。

問45　クライアントサーバシステムを構築する。Web ブラウザによってクライアント処理を行う場合，専用のアプリケーションによって行う場合と比較して，最も軽減される作業はどれか。

ア　クライアント環境の保守　　イ　サーバが故障したときの復旧
ウ　データベースの構築　　エ　ログインアカウントの作成と削除

問46　E-R 図に関する記述のうち，適切なものはどれか。

ア　関係データベースの表として実装することを前提に表現する。

イ　管理の対象をエンティティ及びエンティティ間のリレーションシップとして表現する。

ウ　データの生成から消滅に至るデータ操作を表現する。

エ　リレーションシップは，業務上の手順を表現する。

問47　IP アドレスの自動設定をするために DHCP サーバが設置された LAN 環境の説明のうち，適切なものはどれか。

ア　DHCP による自動設定を行う PC では，IP アドレスは自動設定できるが，サブネットマスクやデフォルトゲートウェイアドレスは自動設定できない。

イ　DHCP による自動設定を行う PC と，IP アドレスが固定の PC を混在させることはできない。

ウ　DHCP による自動設定を行う PC に，DHCP サーバのアドレスを設定しておく必要はない。

エ　一度 IP アドレスを割り当てられた PC は，その後電源が切られた期間があっても必ず同じ IP アドレスを割り当てられる。

問48　BPOの説明はどれか。

ア　災害や事故で被害を受けても，重要事業を中断させない，又は可能な限り中断期間を短くする仕組みを構築すること

イ　社内業務のうちコアビジネスでない事業に関わる業務の一部又は全部を，外部の専門的な企業に委託すること

ウ　製品を生産しようとするときに必要となる部品の数量や，調達する資材の所要量，時期を計算する生産管理手法のこと

エ　プロジェクトを，戦略との適合性や費用対効果，リスクといった観点から評価を行い，情報化投資のバランスを管理し，最適化を図ること

問49　共通フレームによれば，企画プロセスにおいて明確にするものはどれか。

ア　新しい業務の在り方や手順，入出力情報，業務上の責任と権限，業務上のルールや制約などの事項

イ　業務要件を実現するために必要なシステムの機能，システムの開発方式，システムの運用手順，障害復旧時間などの事項

ウ　経営・事業の目的及び目標を達成するために必要なシステムに関係する経営上のニーズ，システム化又はシステム改善を必要とする業務上の課題などの事項

エ　システムを構成するソフトウェアの機能及び能力，動作のための環境条件，外部インタフェース，運用及び保守の方法などの事項

問50　マトリックス組織を説明したものはどれか。

ア　業務遂行に必要な機能と利益責任を，製品別，顧客別又は地域別にもつことによって，自己完結的な経営活動が展開できる組織である。

イ　構成員が，自己の専門とする職能部門と特定の事業を遂行する部門の両方に所属する組織である。

ウ　購買・生産・販売・財務など，仕事の専門性によって機能分化された部門をもつ組織である。

エ　特定の課題の下に各部門から専門家を集めて編成し，期間と目標を定めて活動する一時的かつ柔軟な組織である。

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	10:30 ～ 10:50

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。ただし，問題冊子を切り離して利用することはできません。
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（時計型ウェアラブル端末は除く。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. 午後の試験開始は **12:30** ですので，**12:10** までに着席してください。