問 1 正解 完璧 直前チェック

PKIを構成するOCSPを利用する目的はどれか。

ア　誤って破棄してしまった秘密鍵の再発行処理の進捗状況を問い合わせる。
イ　ディジタル証明書から生成した鍵情報の交換がOCSPクライアントとレスポンダの間で失敗した際，認証状態を確認する。
ウ　ディジタル証明書の失効情報を問い合わせる。
エ　有効期限の切れたディジタル証明書の更新処理の進捗状況を確認する。

問 2 正解 完璧 直前チェック

ハッシュ関数の性質の一つである衝突発見困難性に関する記述のうち，適切なものはどれか。

ア　SHA-256の衝突発見困難性を示す，ハッシュ値が一致する二つのメッセージの探索に要する最大の計算量は，256の2乗である。
イ　SHA-256の衝突発見困難性を示す，ハッシュ値の元のメッセージの探索に要する最大の計算量は，2の256乗である。
ウ　ハッシュ値が与えられたときに，元のメッセージの探索に要する計算量の大きさによる，探索の困難性のことである。
エ　ハッシュ値が一致する二つのメッセージの探索に要する計算量の大きさによる，探索の困難性のことである。

問 3 正解 完璧 直前チェック

経済産業省が公表した“クラウドサービス利用のための情報セキュリティマネジメントガイドライン”が策定された目的について述べたものはどれか。

ア　JIS Q 27002の管理策を補完し，クラウドサービス利用者が情報セキュリティ対策を円滑に行えるようにする。
イ　クラウドサービス提供事業者に対して情報セキュリティ監査を実施する方法を利用者に提示する。
ウ　クラウドサービスの利用がもたらすセキュリティリスクをサービス提供事業者の視点で提示する。
エ　セキュリティリスクの懸念が少ないクラウドサービス提供事業者を利用者が選択できるような格付け基準を提供する。

問1　ウ

解説　**OCSP**（Online Certificate Status Protocol）は，ディジタル証明書の失効情報をリアルタイムで確認するためのプロトコルである。OCSPはCRL（証明書失効リスト）の代替として策定され，CRLをもたなくてもリアルタイムで失効情報を確認することが可能である。RFC 2560によって規定されている。

問2　エ

解説　**衝突発見困難性**は，ハッシュ値が一致する二つのメッセージを探索するための計算量が大きいことによって，探索が困難となり解読されにくいことを意味する。ハッシュ値はあらかじめわかっていない状態から解析を行う。

問3　ア

解説　「クラウドサービス利用のための情報セキュリティマネジメントガイドライン 序文 0.1 一般」には，「クラウド利用者の観点からJIS Q 27002（実践のための規範）の各管理策を考慮し，クラウドコンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として，このガイドを作成した」と記載されている。
イ，ウ，エ：このガイドラインは，組織がクラウドコンピューティングを全面的に利用する状態を想定して記載されているといえる。

問 4 正解 完璧 直前チェック

ディジタル証明書に関する記述のうち，適切なものはどれか。

ア　S/MIMEやTLSで利用するディジタル証明書の規格は，ITU-T X.400で規定されている。
イ　ディジタル証明書は，SSL/TLSプロトコルにおいて通信データの暗号化のための鍵交換や通信相手の認証に利用されている。
ウ　認証局が発行するディジタル証明書は，申請者の秘密鍵に対して認証局がディジタル署名したものである。
エ　ルート認証局は，下位の認証局の公開鍵にルート認証局の公開鍵でディジタル署名したディジタル証明書を発行する。

問 5 正解 完璧 直前チェック

FIPS 140-2を説明したものはどれか。

ア　暗号モジュールのセキュリティ要求事項
イ　情報セキュリティマネジメントシステムに関する認証基準
ウ　ディジタル証明書や証明書失効リストの標準仕様
エ　無線LANセキュリティ技術

問 6 正解 完璧 直前チェック

CSIRTの説明として，適切なものはどれか。

ア　IPアドレスの割当て方針の決定，DNSルートサーバの運用監視，DNS管理に関する調整などを世界規模で行う組織である。
イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。
ウ　企業・組織内や政府機関に設置され，コンピュータセキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。
エ　情報技術を利用し，宗教的又は政治的な目標を達成するという目的をもった人や組織の総称である。

問4 イ

解説 **ディジタル証明書**は，ITU-Tで公開鍵証明書の標準として**X.509**が策定され，そのX.509v3をもとにインターネット利用を目的とした公開鍵証明書をIETFでRFCとして標準化したものである。ディジタル証明書には，シリアル番号，発行者名，有効期間，所有者名，所有者の公開鍵等の情報が含まれており，認証局の秘密鍵で電子署名が付与されている。

ア：S/MIMEやTLSで利用するディジタル証明書の規格は，ITU-TのX.500ディレクトリシリーズのX.509で規定されている。
ウ：ディジタル証明書には，申請者の公開鍵に認証局の電子署名が付与されている。
エ：下位認証局の証明書は，ルート認証局の秘密鍵で電子署名されている。

問5 ア

解説 **FIPS 140-2**：暗号モジュールに関するセキュリティ要件仕様を規定する米国連邦標準規格。

イ：**BS 7799-2**や国内規格の**ISMS認証基準Ver.2.0**の後継として開発された国際規格および国内規格として，**ISO 27001**，**JIS Q 27001**がある。
ウ：インターネットのための**X.509公開鍵基盤**（PKI）に対する標準がある。
エ：**IEEE 802.11**無線LANの国際規格のなかでは，セキュリティ技術として**SSID**（Service Set Identifier），**MACアドレスフィルタリング**，**WEP**（Wired Equivalent Privacy），**WPA2**（Wi-Fi Protected Access 2）などがある。

問6 ウ

解説 **CSIRT**（Computer Security Incident Response Team：コンピュータ・セキュリティ・インシデント・レスポンス・チーム）は，セキュリティに関する様々な事象について活動を行う組織の総称である。企業の場合では，CSIRTを立ち上げることで，事象（インシデント）の問合せ窓口の設置や，セキュリティ教育，技術情報の提供などを実施することでセキュリティ対応を継続的に高度に対応していくことが可能となる。

問 7 正解 完璧 直前チェック

基本評価基準，現状評価基準，環境評価基準の三つの基準でIT製品のセキュリティ脆弱性の深刻さを評価するものはどれか。

ア CVSS　　イ ISMS　　ウ PCI DSS　　エ PMS

問 8 正解 完璧 直前チェック

CRYPTRECの活動内容はどれか。

ア 暗号技術の安全性，実装性及び利用実績の評価・検討を行う。
イ 情報セキュリティ政策に係る基本戦略の立案，官民における統一的，横断的な情報セキュリティ対策の推進に係る企画などを行う。
ウ 組織の情報セキュリティマネジメントシステムについて評価し認証する制度を運用する。
エ 認証機関から貸与された暗号モジュール試験報告書作成支援ツールを用いて暗号モジュールの安全性についての評価試験を行う。

問 9 正解 完璧 直前チェック

DNSキャッシュサーバに対して外部から行われるキャッシュポイズニング攻撃への対策のうち，適切なものはどれか。

ア 外部ネットワークからの再帰的な問合せに応答できるように，コンテンツサーバにキャッシュサーバを兼ねさせる。
イ 再帰的な問合せに対しては，内部ネットワークからのものだけに応答するように設定する。
ウ 再帰的な問合せを行う際の送信元のポート番号を固定する。
エ 再帰的な問合せを行う際のトランザクションIDを固定する。

問7　ア

解説

CVSS（Common Vulnerability Scoring System）：情報システムの脆弱性に対する汎用的な評価手法である。CVSSでは，基本評価基準，現状評価基準，環境評価基準といった三つの基準で脆弱性を評価する。

基本評価基準（Base Metrics）：情報システムのセキュリティの考え方である。機密性，完全性，可用性に対する影響を評価する。

現状評価基準（Temporal Metrics）：脆弱性について現在の深刻度を調査する。

環境評価基準（Environmental Metrics）：製品利用者の利用環境も含めた脆弱性について調査する。

ISMS（Information Security Management System）：情報セキュリティマネジメントシステム。企業が情報を適切に管理し，機密情報を守るための仕組みである。計画（Plan），実行（Do），確認（Check），改善（Action）の各フェーズを繰り返しながら，セキュリティレベルを改善していく。

PCI DSS（Payment Card Industry Data Security Standard）：クレジット業界の世界的なセキュリティ基準である。

PMS（Personal information protection Management Systems）：日本語では個人情報保護マネジメントシステムのことで，プライバシマーク（Pマーク）の認証取得のために必要となる管理ルールである。

問8　ア

解説 **CRYPTREC**（CRYPtography Research and Evaluation Committees）は，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る。公募された暗号技術や，一般的に広く利用されている暗号技術を評価・検討し，安全性や実装性能がともに優れたものを選択する役割がある。

問9　イ

解説 **DNSキャッシュポイズニング**とは，URLといったDNSを利用したIPアドレス検索を行う際に，正しいIPアドレスを検索できないようにすること。攻撃者が不正なIPアドレスを返すようDNSのキャッシュ（一定期間IPアドレス情報を記憶している仕組み）を汚染させることである。そのため，汚染されたキャッシュ上のWebサーバにアクセスしようとすると本来とは異なるサーバに誘導される。

キャッシュを汚染されないようにするためには，再帰的な問合せを外部から行わないようにし，内部ネットワークからだけに応答するよう設定するのがよい。

問 10 正解 完璧 直前チェック

標準化団体OASISが，Webサイト間で認証，属性及び認可の情報を安全に交換するために策定したフレームワークはどれか。

ア　SAML　　イ　SOAP　　ウ　XKMS　　エ　XML Signature

問 11 正解 完璧 直前チェック

暗号化や認証機能をもち，遠隔にあるコンピュータを操作する機能をもったものはどれか。

ア　IPsec　　イ　L2TP　　ウ　RADIUS　　エ　SSH

問 12 正解 完璧 直前チェック

DoS攻撃の一つであるSmurf攻撃の特徴はどれか。

ア　ICMPの応答パケットを大量に送り付ける。
イ　TCP接続要求であるSYNパケットを大量に送り付ける。
ウ　サイズが大きいUDPパケットを大量に送り付ける。
エ　サイズが大きい電子メールや大量の電子メールを送り付ける。

問10　ア

解説

SAML（Security Assertion Markup Language）：標準化団体OASISによって策定された，IDやパスワードなどの認証情報を安全に交換するための仕様。SAMLを用いることで，一度の認証で複数のWebサイトやサービスの利用が可能となる**シングルサインオン**（SSO：Single Sign-On）を実現できる。WebサイトがSAMLに対応していれば，異なるドメインのサイトへ移動したときに，移動元のサイトと移動先のサイトがSAMLプロトコルで通信し，自動的に認証情報を引き継ぐことができる。

SOAP（Simple Object Access Protocol）：SOAPによる通信では，XML文書にエンベロープと呼ばれる付帯情報がついたメッセージをHTTPなどでやり取りする。

XKMS（XML Key Management Specification）：XMLを利用して公開鍵基盤（PKI）の鍵情報を効率よく管理するためのプロトコルである。

XML Signature：W3C（World Wide Web Consortium）によって勧告された規格。XMLにおいてディジタル署名を利用するための規格である。

問11　エ

解説

IPsec（Security Architecture for the Internet Protocol）：IPパケットのデータ暗号化と改ざん検出を行うプロトコルである。

L2TP（Layer2 Tunneling Protocol）：仮想的にデータリンク層のトンネルを構築するプロトコルである。ダイヤルアップ接続によるインターネットを介したリモートアクセスにおいて利用される。

RADIUS（Remote Authentication Dial In User Service）：認証サーバがネットワーク上のサーバ認証とアカウントのサービスを提供するプロトコル。

SSH（Secure Shell）：リモートからホストのシェルを操作する際に，通信路を暗号化技術を用いて保護する仕組み。

問12　ア

解説　**Smurf攻撃**とはネットワークに大量のパケットを発生させてサービス不能状態を作り出す攻撃手法である。攻撃の手法は次の通り。

ICMPではICMP Echo Requestが送信されるとEcho Replayが返信される。攻撃者は送信元を攻撃対象のサイトに偽造して，Echo Requestをブロードキャストアドレス宛に送信する。Echo Replyがネットワークの全てのコンピュータから返信され，この大量のReplyによりサービス不能となる。

問 13 正解 完璧 直前チェック

サイドチャネル攻撃を説明したものはどれか。

ア　暗号化装置における暗号化処理時の消費電力などの測定や統計処理によって，当該装置内部の機密情報を推定する攻撃
イ　攻撃者が任意に選択した平文とその平文に対応した暗号文から数学的手法を用いて暗号鍵を推測し，同じ暗号鍵を用いて作成された暗号文を解読する攻撃
ウ　操作中の人の横から，入力操作の内容を観察することによって，IDとパスワードを盗み取る攻撃
エ　無線LANのアクセスポイントを不正に設置し，チャネル間の干渉を発生させることによって，通信を妨害する攻撃

問 14 正解 完璧 直前チェック

ディジタルフォレンジックスを説明したものはどれか。

ア　画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む。
イ　コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり，システムを実際に攻撃して侵入を試みる。
ウ　ネットワークの管理者や利用者などから，巧みな話術や盗み聞き，盗み見などの手段によって，パスワードなどのセキュリティ上重要な情報を入手する。
エ　犯罪に対する証拠となり得るデータを保全し，その後の訴訟などに備える。

問 15 正解 完璧 直前チェック

スパムメールへの対策であるDKIM（DomainKeys Identified Mail）の説明はどれか。

ア　送信側メールサーバでディジタル署名を電子メールのヘッダに付加して，受信側メールサーバで検証する。
イ　送信側メールサーバで利用者が認証されたとき，電子メールの送信が許可される。
ウ　電子メールのヘッダや配送経路の情報から得られる送信元情報を用いて，メール送信元のIPアドレスを検証する。
エ　ネットワーク機器で，内部ネットワークから外部メールサーバのTCPポート番号25への直接の通信を禁止する。

問13　ア

解説　**サイドチャネル攻撃**は，暗号を解読するための攻撃手法の一つである。暗号化や復号の際に発生する電磁波，熱，演算処理時間など暗号を直接解読するのではなく，外部からの観測といった二次的要素から解読を行う手法である。
イ：選択平文攻撃の説明である。
ウ：ショルダーハッキングの説明である。
エ：ジャミングの説明である。

問14　エ

解説　**ディジタルフォレンジックス**は，パソコンやサーバなどのコンピュータ機器が犯罪や裁判での証拠となりえるときに，データを保全し賠償などに備えることや，内容を分析，鑑定するための手段や技術を指す。
ア：**電子透かし**の説明である。
イ：**擬似アタックテスト**の説明である。
ウ：**ソーシャルエンジニアリング**の説明である。

問15　ア

解説　**DKIM**は，送信者が正当な団体であるかどうかを認証する送信者認証技術である。メールを送信するときに自分がもっている秘密鍵でディジタル署名を行い，メールを受け取る受信側では送信情報を元にDNSを管理しているサーバに問い合わせて公開鍵を取得し，メールが正当であるかを検証する。

問 16 正解 完璧 直前チェック

認証にクライアント証明書を用いるプロトコルはどれか。

ア　EAP-MD5　　イ　EAP-PEAP　　ウ　EAP-TLS　　エ　EAP-TTLS

問 17 正解 完璧 直前チェック

サンドボックスの仕組みについて述べたものはどれか。

ア　Webアプリケーションの脆弱(ぜい)性を悪用する攻撃に含まれる可能性が高い文字列を定義し，攻撃であると判定した場合には，その通信を遮断する。
イ　侵入者をおびき寄せるために本物そっくりのシステムを設置し，侵入者の挙動などを監視する。
ウ　プログラムの影響がシステム全体に及ばないように，プログラムが実行できる機能やアクセスできるリソースを制限して動作させる。
エ　プログラムのソースコードでSQL文の雛(ひな)形の中に変数の場所を示す記号を置いた後，実際の値を割り当てる。

問 18 正解 完璧 直前チェック

DNSSECに関する記述として，適切なものはどれか。

ア　DNSサーバへのDoS攻撃を防止できる。
イ　IPsecによる暗号化通信が前提となっている。
ウ　代表的なDNSサーバの実装であるBINDの代替として使用する。
エ　ディジタル署名によってDNS応答の正当性を確認できる。

問 19 正解 完璧 直前チェック

リモートアクセス環境において，認証情報やアカウンティング情報をやり取りするプロトコルはどれか。

ア　CHAP　　イ　PAP　　ウ　PPTP　　エ　RADIUS

春 秋

問16　ウ

解説　**EAP**（Extensible Authentication Protocol）は，PPP（Point to Point Protocol）用の認証プロトコルであり，各種の拡張認証方式を利用することができる。無線LANでは，Ether（データリンク層）のユーザ認証の規格であるIEEE 802.1xが採用されている。
ア：認証にIDとパスワードを用いる方式である。証明書は利用しない。
イ，エ：認証に証明書を用いるが，サーバ側でのみ証明書を用いる。
ウ：認証にクライアント証明書を用いる方式である。

問17　ウ

解説　**サンドボックス**は，外部から受け取ったプログラムをシステム全体に影響が及ばないよう，リソースを制限して実行する動作環境である。
ア：WAF（Web Application Firewall）の説明である。
イ：ハニーポットの説明である。
エ：バインド機構の説明である。

問18　エ

解説　**DNSSEC**（DNS Security Extensions）は，DNSサーバから送られてくるIPアドレスとホスト名の対応情報の信頼性を証明するセキュリティ拡張機能のことである。応答を送信するDNSサーバが秘密鍵を使って応答に署名し，受信する側が公開鍵で検証する。秘密鍵で正しい署名を付けるので，署名の検証によって偽の応答を検知できる。そのためDNSキャッシュポイズニングを防ぐことができる。

問19　エ

解説
CHAP（Challenge Handshake Authentication Protocol）：PPP（Point to Point Protocol）接続において利用者認証に用いられるプロトコル。
PAP（Password Authentication Protocol）：PPPによるダイヤルアップ接続の際に利用されるユーザ認証のためのプロトコル。
PPTP（Point to Point Tunneling Protocol）：2台のコンピュータ間で情報を暗号化して送受信するためのプロトコル。
RADIUS（Remote Authentication Dial In User Service）：アクセスサーバと認証サーバ間でアカウンティング情報によって通信を可能とする認証プロトコル。クライアントが認証を求める際に，認証を必要とするサーバ（アクセスサーバ）と認証機能を分離し，アカウンティング情報の一元管理，アクセスログの記録が可能となる。

問 20 正解 完璧 直前チェック

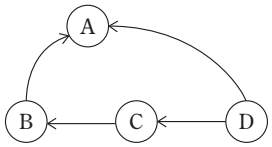
インターネット標準RFC 5322（旧RFC 822）に準拠した電子メールにおいて，ヘッダと本体を区別する方法はどれか。

ア <header>と</header>で囲まれた部分をヘッダ，<body>と</body>で囲まれた部分を本体とする。
イ 1個のピリオドだけから成る行の前後でヘッダと本体を分ける。
ウ Subjectフィールドがヘッダの最後であり，それ以降を本体とする。
エ 最初に現れる空行の前後でヘッダと本体を分ける。

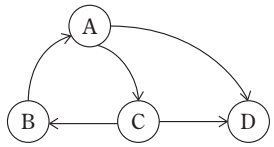
問 21 正解 完璧 直前チェック

トランザクションA～Dに関する待ちグラフのうち，デッドロックが発生しているものはどれか。ここで，待ちグラフの矢印は，$X \rightarrow Y$のとき，トランザクションXはトランザクションYがロックしている資源のアンロックを待っていることを表す。

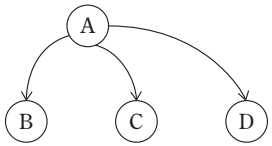
ア



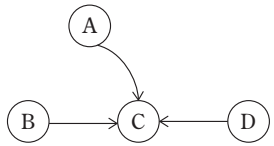
イ



ウ



エ



問 22 正解 完璧 直前チェック

テストで使用されるスタブ又はドライバの説明のうち，適切なものはどれか。

ア スタブは，テスト対象モジュールからの戻り値を表示・印刷する。
イ スタブは，テスト対象モジュールを呼び出すモジュールである。
ウ ドライバは，テスト対象モジュールから呼び出されるモジュールである。
エ ドライバは，引数を渡してテスト対象モジュールを呼び出す。

問20 エ

解説 **RFC 5322**（Request For Comments 5322）は，インターネットメッセージフォーマット（Internet Message Format）の，コンピュータユーザ間で送信される電子メールの文法使用を定めたものである。

電子メールのヘッダと本文の区切りは，最初に現れる空行の前後でヘッダと本文を分ける仕様となっている。

問21 イ

解説 **デットロック**とは，各トランザクションの占有している（ロックしている）状態と，開放（アンロック）を待つ状態が同時に発生し，処理が停止してしまうことである。
ア，ウ，エ：ロック状態と，開放待ちが同時に発生していないため，デットロックではない。
イ：A，B，Cがお互いにロックと，アンロック状態となるためデットロック状態といえる。

問22 エ

解説 ボトムアップテストは，モジュールの下位から上位へと順次結合してテストしていく方法である。テストにおいて，上位モジュールの代わりの**ドライバ**が必要となる。

トップダウンテストは，逆に上位から下位モジュールへと順次結合してテストしていく方法である。テストにおいて，下位モジュールの代わりとなる**スタブ**が必要となる。
ア，イ：ドライバに関する記述である。
ウ：スタブに関する記述である。

問 23 正解 完璧 直前チェック

コンテンツの不正な複製を防止する方式の一つであるDTCP-IPの説明として，適切なものはどれか。

ア　BSデジタル放送や地上デジタル放送に採用され，コピーワンスの番組を録画するときに使われる方式
イ　DLNAとともに用いられ，接続する機器間で相互認証し，コンテンツ保護が行えると認識して初めて録画再生を可能にする方式
ウ　DVDに採用され，映像コンテンツを暗号化して，複製できないエリアにその暗号化鍵を記録する方式
エ　HDMI端子が搭載されたディジタルAV機器に採用され，HDMI端子から表示機器にディジタル信号を送るときに受信する経路を暗号化する方式

問 24 正解 完璧 直前チェック

JIS Q 20000-1で定義されるインシデントに該当するものはどれか。

ア　ITサービスの新人向け教育の依頼
イ　ITサービスやシステムの機能，使い方に対する問合せ
ウ　アプリケーションの応答の大幅な遅延
エ　新設営業所へのITサービス提供要求

問 25 正解 完璧 直前チェック

情報セキュリティに関する従業員の責任について，“情報セキュリティ管理基準”に基づいて監査を行った。指摘事項に該当するものはどれか。

ア　雇用の終了をもって守秘責任が解消されることが，雇用契約に定められている。
イ　定められた勤務時間以外においても守秘責任を負うことが，雇用契約に定められている。
ウ　定められた守秘責任を果たさなかった場合，相応の措置がとられることが，雇用契約に定められている。
エ　定められた内容の守秘義務契約書に署名することが，雇用契約に定められている。

問23　イ

解説　**DTCP-IP**（Digital Transmission Content Protection over Internet Protocol）は，著作権保護されたディジタル映像を家庭内LANなどのIPネットワークで送信するためのプロトコルである。

DLNA（Digital Living Network Alliance）は，DVDレコーダといったAV家電や，パソコン，モバイル機器を各種メーカが販売する機器の相互接続性を確立するためのガイドラインとなる。

ア：**CPRM**（Content Protection for Recordable Media）の説明である。
ウ：**CPPM**（Content Protection for Prerecorded Media）の説明である。
エ：**HDCP**（High-bandwidth Digital Content Protection system）の説明である。

問24　ウ

解説　**JIS Q 20000**は，ITサービスマネジメントに関する国際規格である。ITILと同意語となるプロセスによって定義されている。インシデントとは，正常に稼動しているサービスを阻害するイベントや，状態をいう。

ア，イ，エ：依頼，問合せ，要求は，サービスを阻害する要因ではないため，インシデントではない。
ウ：システムの可用性に影響がある状態といえるため，インシデントとなる。

問25　ア

解説　**情報セキュリティ管理基準**：経済産業省が策定する。組織体が効率的な情報セキュリティマネジメント体制を構築し，適切なコントロールを整備，運用するための実践規範である。

ア：守秘義務は，雇用の終了（退職）後も必要である。退職後に秘密事項を外部に発信しないよう契約で明確にする必要がある。
イ，ウ，エ：雇用契約の記載内容として正しいといえる。