## 問 1

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　企業内・組織内や政府機関に設置され，情報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 2

正解 □ 完璧 □ 直前チェック □

情報セキュリティ対策のクリアデスクに該当するものはどれか。

ア　PCのデスクトップ上のフォルダなどを整理する。
イ　PCを使用中に離席した場合，一定時間経過すると，パスワードで画面ロックされたスクリーンセーバに切り替わる設定にしておく。
ウ　帰宅時，書類やノートPCを机の上に出したままにせず，施錠できる机の引出しなどに保管する。
エ　机の上に置いたノートPCを，セキュリティワイヤで机に固定する。

## 問 3

正解 □ 完璧 □ 直前チェック □

情報セキュリティに係るリスクマネジメントが効果的に実施されるよう，リスクアセスメントに基づいた適切なコントロールの整備，運用状況を検証又は評価し，保証又は助言を与えるものであり，実施者に独立かつ専門的な立場が求められるものはどれか。

ア　コントロールセルフアセスメント（CSA）
イ　情報セキュリティ監査
ウ　情報セキュリティ対策ベンチマーク
エ　ディジタルフォレンジックス



春

### 問1　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。
ア：**ICANN**（The Internet Corporation for Assigned Names and Numbers）の説明である。
イ：**IETF**（Internet Engineering Task Force）の説明である。
エ：**ハクティビスト**の説明である。

### 問2　ウ

**解説**　**クリアデスク**は，帰宅時に，書類やノートPCなどの機密情報を扱っている機器を，物理的な盗難に備えて施錠できるキャビネットや引出しに保管することである。
ア，イ：PC内部データの整理や，設定ではない。
エ：ノートPCをセキュリティワイヤで固定することは，物理的なセキュリティとして有効な施策であるが，クリアデスクではない。

### 問3　イ

**解説**
**コントロールセルフアセスメント**（CSA）：リスクマネジメントまたは内部統制などに関する統制活動の有効性を，運用業務を実施する部門内で主観的に検証・評価することである。
**情報セキュリティ監査**：情報セキュリティに係るリスクマネジメントが効果的に実施されるよう，リスクアセスメントに基づいた適切なコントロールの整備，運用状況を検証又は評価し，保証又は助言を与えるものである。
**情報セキュリティ対策ベンチマーク**：質問形式の企業情報セキュリティ自己診断システム。いくつかの設問に答えることで，自社のセキュリティレベルが他社と比較してどの程度なのか指針を得ることができる。
**ディジタルフォレンジックス**：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得るときに，データを保全して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。

## 問 4

正解 □ 完璧 □ 直前チェック □

ノートPCやスマートフォンなどのモバイル機器に重要情報を格納して持ち出すとき，機器の紛失による情報漏えい対策として有効なものはどれか。

ア　モバイル機器でのSNSの使用を制限する。
イ　モバイル機器内の情報をリモートから消去できるツールを導入する。
ウ　モバイル機器に通信を暗号化するツールを導入する。
エ　モバイル機器にのぞき見防止フィルムを貼付する。

## 問 5

正解 □ 完璧 □ 直前チェック □

JIS Q 27001において，リスクを受容するプロセスに求められるものはどれか。

ア　受容するリスクについては，リスク所有者が承認すること
イ　受容するリスクをモニタリングやレビューの対象外とすること
ウ　リスクの受容は，リスク分析前に行うこと
エ　リスクを受容するかどうかは，リスク対応後に決定すること

## 問 6

正解 □ 完璧 □ 直前チェック □

JIS Q 27001に基づく情報セキュリティ方針の取扱いとして，適切なものはどれか。

ア　機密情報として厳格な管理を行う。
イ　従業員及び関連する外部関係者に通知する。
ウ　情報セキュリティ担当者各人が作成する。
エ　制定後はレビューできないので，見直しの必要がない内容で作成する。



春

### 問4　イ

**解説**　ノートPCやスマートフォンなどのモバイル機器に重要情報を格納して持ち出す場合は，機器の紛失時に情報が漏洩しないための対策が必要である。主な対策としては，モバイル機器内の情報をリモートから消去できるツールの導入である。ノートPCの場合は，HDDの暗号化対策も一つであるが，暗号化は解除されないとは限らないため，リモートで消去できるツールのほうがよい。

ア：SNSの使用を制限しても，紛失したモバイル機器のデータは漏えいする。
ウ：暗号化ツールを導入しても，解除される可能性がある。
エ：のぞき見防止フィルムを貼っても，紛失時の情報漏えい対策とはならない。

### 問5　ア

**解説**　リスクへの対応方法としては，リスク受容，リスク回避，リスク移転がある。

**リスク受容**：リスクがあることがわかっていても，対策を行わないこと。被害の影響がきわめて小さい場合や，リスクの発生頻度がきわめて低い場合の対応方法である。リスク受容プロセスでは，受容するリスクについてリスク所有者が承認することが必要である。

**リスク回避**：リスクが発生しないように事前に対策を行うことである。

**リスク移転**：保険に入るなどにより，第三者へ資金的なリスクを移すことである。

### 問6　イ

**解説**　**情報セキュリティ方針**とは，組織としての情報セキュリティに対する取組み姿勢を示した文書のことである。組織のトップにより承認されて公開される。一般に，行動方針，体制，管理の取組みについても記載する。

ア：情報セキュリティ方針は，外部に公開する資料である。
ウ：情報セキュリティ方針は，組織として作成し，トップが承認する。
エ：情報セキュリティ方針は，適時見直しを行う。

## 問 7

正解 □ 完璧 □ 直前チェック □

IPA“組織における内部不正防止ガイドライン”にも記載されている，組織の適切な情報セキュリティ対策はどれか。

ア　インターネット上のWebサイトへのアクセスに関しては，コンテンツフィルタ（URLフィルタ）を導入して，SNS，オンラインストレージ，掲示板などへのアクセスを制限する。
イ　業務の電子メールを，システム障害に備えて，私用のメールアドレスに転送するよう設定させる。
ウ　従業員がファイル共有ソフトを利用する際は，ウイルス対策ソフトの誤検知によってファイル共有ソフトの利用が妨げられないよう，ウイルス対策ソフトの機能を一時的に無効にする。
エ　組織が使用を許可していないソフトウェアに関しては，業務効率が向上するものに限定して，従業員の判断でインストールさせる。

## 問 8

正解 □ 完璧 □ 直前チェック □

情報システムに対するアクセスのうち，JIS Q 27002でいう特権的アクセス権を利用した行為はどれか。

ア　許可を受けた営業担当者が，社外から社内の営業システムにアクセスし，業務を行う。
イ　経営者が，機密性の高い経営情報にアクセスし，経営の意思決定に生かす。
ウ　システム管理者が，業務システムのプログラムのバージョンアップを行う。
エ　来訪者が，デモシステムにアクセスし，システムの機能の確認を行う。

## 問 9

正解 □ 完璧 □ 直前チェック □

“不正のトライアングル”理論において，全てそろったときに不正が発生すると考えられている3要素はどれか。

ア　機会，動機，正当化　　イ　機密性，完全性，可用性
ウ　顧客，競合，自社　　エ　認証，認可，アカウンティング



春

### 問7　ア

**解説**　**「組織における内部不正防止ガイドライン」**は，企業やその他の組織において必要な内部不正対策を効果的に実施可能とすることを目的として作成されたものである。内部不正防止の重要性や対策の体制，関連する法律などの概要を平易な文体で説明しているほか，組織における内部不正の在り方については，基本方針から，資産管理，技術的管理，証拠確保，コンプライアンス，職場環境，事後管理など10の観点のもと，合計30項目からなる具体的な対策を示している。

ア：正しい。不要なWebサイトへのアクセス制限は，内部不正防止となる。
イ：業務のメールを，私用のメールアドレスに転送することは，内部情報の漏えいにつながる。
ウ：ウイルス対策ソフトの機能を一時的に無効にすると，ウイルス感染リスクが高まるため，必要性の確認をした上で無効の判断を行う必要がある。
エ：組織が許可していないソフトの使用は，ライセンス違反やウイルス感染リスクがある。

### 問8　ウ

**解説**　**特権的アクセス権**は，システム全体に対する読込み，変更，削除が可能な権限である。

ア：許可を受けた営業担当者は，特権的アクセスではなく利用者でのアクセスといえる。社外から社内の営業システムにアクセスすることと，特権的アクセスは関連しない。
イ：経営者は，機密情報にアクセスする権限があるので，特権的アクセス権は利用しない。
ウ：システム管理者がプログラムのバージョンアップ時に利用するアカウントは，特権的アクセス権のあるアカウントを利用する。
エ：デモシステムでは，特権的アカウントを利用することはない。

### 問9　ア

**解説**　**不正のトライアングル**とは，米国の犯罪学者D.R.クレッシーが提唱した，人が不正行為を実現化するときの理論である。不正行為は，①機会，②動機，③正当化が揃ったときに実行され，逆に，この三つが揃わないと不正は発生しない。

**機会**：不正行為の実行が可能となる環境。
**動機**：不正行為を実行しなければならない事情。
**正当化**：不正行為を肯定する理由付けがされるとき。

## 問 10 正解 完璧 直前チェック

利用者アクセスログの取扱いのうち，IPA“組織における内部不正防止ガイドライン”にも記載されており，内部不正の早期発見及び事後対策の観点で適切なものはどれか。

ア　コストにかかわらずログを永久保存する。
イ　利用者にログの管理権限を付与する。
ウ　利用者にログの保存期間を周知する。
エ　ログを定期的に確認する。

## 問 11 正解 完璧 直前チェック

BYODの説明，及びその情報セキュリティリスクに関する記述のうち，適切なものはどれか。

ア　従業員が企業から貸与された情報端末を，客先などへの移動中に業務に利用することであり，ショルダハッキングなどの情報セキュリティリスクが増大する。
イ　従業員が企業から貸与された情報端末を，自宅に持ち帰って私的に利用することであり，機密情報の漏えいなどの情報セキュリティリスクが増大する。
ウ　従業員が私的に保有する情報端末を，職場での休憩時間などに私的に利用することであり，セキュリティ意識の低下などに起因する情報セキュリティリスクが増大する。
エ　従業員が私的に保有する情報端末を業務に利用することであり，セキュリティ設定の不備に起因するウイルス感染などの情報セキュリティリスクが増大する。

## 問 12 正解 完璧 直前チェック

IDSの機能はどれか。

ア　PCにインストールされているソフトウェア製品が最新のバージョンであるかどうかを確認する。
イ　検査対象の製品にテストデータを送り，製品の応答や挙動から脆弱(ぜい)性を検出する。
ウ　サーバやネットワークを監視し，セキュリティポリシを侵害するような挙動を検知した場合に管理者へ通知する。
エ　情報システムの運用管理状況などの情報セキュリティ対策状況と企業情報を入力し，組織の情報セキュリティへの取組状況を自己診断する。



春

### 問10　エ

**解説**　情報システムにおけるログの記録と保存では，内部不正の早期発見及び事後対策の観点から，重要情報へのアクセス履歴及び利用者の操作履歴などのログを記録し，定めた期間に安全に保存する必要がある。

ア：ログの保存期間は，リスクとコストのバランスによって決定する。
イ：ログの確認には，改ざん及び削除防止並びに特定のシステム管理者からのみアクセス可能などの措置が取られる方がよい。確認をする際には，総括責任者またはシステム管理者から許可を得る管理体制が必要である。
ウ：ログの保存期間は，内部不正の抑止の観点から内部者に知らせない方がよい。
エ：ログは定期的に確認する必要がある。多量なファイルへのアクセスや業務範囲外のファイルへのアクセスなど通常の業務と異なる事象が発見された者に対して，事象確認または監視強化などの対策が必要である。

### 問11　エ

**解説**　**BYOD**（Bring Your Own Device）は，個人所有の端末を業務利用することである。企業は，社員用に端末を用意するコストが低減されるメリットがあり，個人は，携帯電話やスマートフォンを個人用・会社用と複数台持ち歩く必要がなくなるなどの管理面のメリットがある。

ア，イ：BYODは，会社から貸与された情報端末ではない。
ウ：個人の情報端末を休憩中に使用することは問題ない。
エ：個人の情報端末を業務で利用する場合，セキュリティ設定の不備などでセキュリティリスクが増大する。

### 問12　ウ

**解説**　**IDS**（Intrusion Detection System）は，ネットワークやホストにウイルスなどが侵入した際に検知する仕組みである。ネットワークを検知する仕組みをNIDS，ホストを検知する仕組みをHIDSと呼ぶ。

**NIDS**（ネットワーク型IDS）：保護する機器のネットワーク経路上に設置して，外部からの不審なアクセスやデータがないか検知するシステムである。
**HIDS**（ホスト型IDS）：サーバ上のファイルが改ざんされたかどうかを検出する。

ア：ソフトウェア製品が最新のバージョンであるかどうかは，IDSで検知するものではない。
イ：**セキュリティ監査ツール**の説明である。
エ：**情報セキュリティ対策ベンチマーク**の説明である。

## 問 13 正解 完璧 直前チェック

クライアントとWebサーバの間において，クライアントからWebサーバに送信されたデータを検査して，SQLインジェクションなどの攻撃を遮断するためのものはどれか。

ア　SSL-VPN機能　　イ　WAF
ウ　クラスタ構成　　エ　ロードバランシング機能

## 問 14 正解 完璧 直前チェック

PCで行うマルウェア対策のうち，適切なものはどれか。

ア　PCにおけるウイルスの定期的な手動検査では，ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。
イ　PCの脆弱(ぜいじゃく)性を突いたウイルス感染が起きないように，OS及びアプリケーションの修正パッチを適切に適用する。
ウ　電子メールに添付されたウイルスに感染しないように，使用しないTCPポート宛ての通信を禁止する。
エ　ワームが侵入しないように，PCに動的グローバルIPアドレスを付与する。

## 問 15 正解 完璧 直前チェック

システム管理者による内部不正を防止する対策として，適切なものはどれか。

ア　システム管理者が複数の場合にも，一つの管理者IDでログインして作業を行わせる。
イ　システム管理者には，特権が付与された管理者IDでログインして，特権を必要としない作業を含む全ての作業を行わせる。
ウ　システム管理者の作業を本人以外の者に監視させる。
エ　システム管理者の操作ログには，本人にだけアクセス権を与える。



春

### 問13　イ

**解説**

**WAF**（Web Application Firewall）：外部ネットワークとLANの中間に設置し，外部からの不正アクセスを防ぐファイアウォールの一種である。Webアプリケーションの通信を管理することにより，Webページのセキュリティホールを悪用するSQLインジェクションなどの攻撃を遮断できる。

**SSL-VPN機能**：暗号化にSSL（Secure Socket Layer）を用いたVPN（Virtual Private Network）である。

**クラスタ構成**：複数のコンピュータをネットワークで連結し，全体で一つのコンピュータであるかのように動作するシステムである。

**ロードバランシング機能**：同一処理を行う複数のサーバに付加を分散させる機能である。

### 問14　イ

**解説**　**マルウェア**は，外部からPCに進入するコンピュータウイルスである。PCの破壊や，情報の漏えいなどを行う有害ソフトウェアで，コンピュータウイルス，ワーム，スパイウェア，ランサムウェアなどの「悪意のこもった」ソフトウェアの総称である。

ア：ウイルス対策ソフトの定義ファイルは，過去にあったウイルスの情報を更新する場合もあるので，最新化した日付以降だけでなく，全ファイルを対象にスキャンする必要がある。
ウ：TCPポート宛ての通信を禁止しても，電子メールの添付ファイルのウイルスを開くと感染する。
エ：動的グローバルIPアドレスの付与は，コンピュータウイルスのワームの侵入とは関連していない。

### 問15　ウ

**解説**　**システム管理者による内部不正を防止する対策**では，管理者権限をもっている人が作業する際，必ず本人以外の者に監視される必要がある。複数人による作業実施や，ログの監視などが対策として有効である。

ア：複数人で一つの管理者IDを利用する場合はあるが，誰が作業したのかはログからも追跡することが困難であるため，不正防止対策とはならない。
イ：特権を必要としない作業は，特権の付与されていないIDで作業する。
エ：操作ログは，本人にアクセス権を与えると改ざんできるため，ほかの人にアクセス権を与える。

## 問 16

正解 □ 完璧 □ 直前チェック □

ディジタルフォレンジックスでハッシュ値を利用する目的として，適切なものはどれか。

ア　一方向性関数によってパスワードを復元できないように変換して保存する。
イ　改変されたデータを，証拠となり得るように復元する。
ウ　証拠となり得るデータについて，原本と複製の同一性を証明する。
エ　パスワードの盗聴の有無を検証する。

## 問 17

正解 □ 完璧 □ 直前チェック □

機密ファイルが格納されていて，正常に動作するPCの磁気ディスクを産業廃棄物処理業者に引き渡して廃棄する場合の情報漏えい対策のうち，適切なものはどれか。

ア　異なる圧縮方式で，機密ファイルを複数回圧縮する。
イ　専用の消去ツールで，磁気ディスクのマスタブートレコードを複数回消去する。
ウ　ランダムなビット列で，磁気ディスクの全領域を複数回上書きする。
エ　ランダムな文字列で，機密ファイルのファイル名を複数回変更する。

## 問 18

正解 □ 完璧 □ 直前チェック □

2要素認証に該当する組はどれか。

ア　ICカード認証，指紋認証
イ　ICカード認証，ワンタイムパスワードを生成するハードウェアトークン
ウ　虹彩認証，静脈認証
エ　パスワード認証，パスワードリマインダ



春

### 問16　ウ

**解説**　**ディジタルフォレンジックス**とは，不正アクセスなどの不正行為の法的な証拠を明らかにするための「ディジタル鑑識」のことである。ログファイルの記録や，改変や破壊されたファイルの復元だけでなく，データが捏造されたものかどうかを検証したり，ディジタル署名やハッシュ値などを用いて記録の同一性を保全したりする。

### 問17　ウ

**解説**　機密ファイルが格納されていて，正常に動作するPCの磁気ディスクを産業廃棄物処理業者に引き渡して廃棄する場合の情報漏えい対策では，**物理破壊**もしくは，**データの全領域を複数回上書き消去**する。

ア：機密ファイルを複数回圧縮しても，データは残っているため対策とはならない。
イ：PCの磁気ディスクのマスタブートレコードは，OSが起動するときに利用する領域であるため，データは残る。
エ：ランダムな文字列でファイル名を変更しても，ファイルは残っているため対策とはならない。

### 問18　ア

**解説**　**2要素認証**は，ICカード情報と生体情報といった異なる二つの情報を組み合わせて認証することで，認証の安全性を高める考え方である。一般的に認証に用いられる情報は，本人のみが知っている情報（例えばパスワード）や，所有しているワンタイムパスワードのトークン，指紋などの生体情報である。

ア：ICカード認証は所有している情報，指紋認証は生体情報となり，2要素である。
イ：ICカード認証と，ワンタイムパスワードはどちらも所有している情報となるため，1要素である。
ウ：虹彩認証，静脈認証は，どちらも本人の生体情報であるため1要素である。
エ：パスワード認証と，パスワードリマインダは，どちらも本人のみが知っている情報となるため1要素である。

## 問 19

正解 □ 完璧 □ 直前チェック □

APTの説明はどれか。

ア　攻撃者はDoS攻撃及びDDoS攻撃を繰り返し組み合わせて，長期間にわたり特定組織の業務を妨害する。

イ　攻撃者は興味本位で場当たり的に，公開されている攻撃ツールや脆弱性検査ツールを悪用した攻撃を繰り返す。

ウ　攻撃者は特定の目的をもち，標的となる組織の防御策に応じて複数の手法を組み合わせ，気付かれないよう執拗に攻撃を繰り返す。

エ　攻撃者は不特定多数への感染を目的として，複数の攻撃方法を組み合わせたマルウェアを継続的にばらまく。

## 問 20

正解 □ 完璧 □ 直前チェック □

利用者PCのHDDが暗号化されていないとき，攻撃者が利用者PCからHDDを抜き取り，攻撃者が用意したPCに接続してHDD内の情報を盗む攻撃によって発生する情報漏えいのリスクの低減策のうち，適切なものはどれか。

ア　HDDにインストールしたOSの利用者アカウントに対して，ログインパスワードを設定する。

イ　HDDに保存したファイルの読取り権限を，ファイルの所有者だけに付与する。

ウ　利用者PC上でHDDパスワードを設定する。

エ　利用者PCにBIOSパスワードを設定する。





### 問19　ウ

**解説**　APT（Advanced Persistent Threats：標的型諜報攻撃）の一番の特徴は，特定組織を標的とした目的をもった攻撃である。攻撃手法は，攻撃対象者へメールでウイルスを送付し，ウイルスを実行させることでバックドアを開通するリモートコントロールによる情報の搾取である。APTは，複数の攻撃を組み合わせることや特定システムへの継続的なハッキングなど複雑であるため，危険かつ対策が困難な攻撃である。

ア：複数の手法を組み合わせて高度化されていない攻撃は，APTとはならない。

イ，エ：攻撃対象を特定しない場合は，APTとはならない。

### 問20　ウ

**解説**　利用者PCのHDDが暗号化されていないとき，攻撃者が利用者PCからHDDを抜き取り，攻撃者が用意したPCに接続してHDD内の情報を盗むことが可能となる。この攻撃によって発生する情報漏えいのリスクを低減するためには，**HDDパスワードの設定**や，**データの暗号化**が必要である。

ア：ログインパスワードを設定しても，HDDを参照されると内容を読み取られてしまう。

イ：攻撃者が用意したPCにHDDを接続すればファイルのアクセス権を変更して読み取られてしまう。

エ：BIOSパスワードは，HDDの内容の参照とは関連しないため，対策にはならない。

## 問 21 正解 完璧 直前チェック

クロスサイトスクリプティングに該当するものはどれか。

ア　Webアプリケーションのデータ操作言語の呼出し方に不備がある場合に，攻撃者が悪意をもって構成した文字列を入力することによって，データベースのデータの不正な取得，改ざん及び削除を可能とする。

イ　Webサイトに対して，他のサイトを介して大量のパケットを送り付け，そのネットワークトラフィックを異常に高めてサービスを提供不能にする。

ウ　確保されているメモリ空間の下限又は上限を超えてデータの書込みと読出しを行うことによって，プログラムを異常終了させたりデータエリアに挿入された不正なコードを実行させたりする。

エ　攻撃者が罠を仕掛けたWebページを利用者が閲覧し，当該ページ内のリンクをクリックしたときに，不正スクリプトを含む文字列が脆弱なWebサーバに送り込まれ，レスポンスに埋め込まれた不正スクリプトの実行によって，情報漏えいをもたらす。

## 問 22 正解 完璧 直前チェック

クリックジャッキング攻撃に該当するものはどれか。

ア　Webアプリケーションの脆弱性を悪用し，Webサーバに不正なリクエストを送ってWebサーバからのレスポンスを二つに分割させることによって，利用者のWebブラウザのキャッシュを偽造する。

イ　WebサイトAのコンテンツ上に透明化した標的サイトBのコンテンツを配置し，WebサイトA上の操作に見せかけて標的サイトB上で操作させる。

ウ　Webブラウザのタブ表示機能を利用し，Webブラウザの非活性なタブの中身を，利用者が気付かないうちに偽ログインページに書き換えて，それを操作させる。

エ　利用者のWebブラウザの設定を変更することによって，利用者のWebページの閲覧履歴やパスワードなどの機密情報を盗み出す。



春

### 問21　エ

**解説**　**クロスサイトスクリプティング**は，動的にWebページを生成するアプリケーションの脆弱性を利用した攻撃である。例えば，攻撃者によって掲示板に悪意のスクリプトコードが書き込まれた場合に，スクリプトコードをチェックせずに掲示板に載せることで，その掲示板にアクセスしたブラウザが悪意のスクリプトを実行する。対策としては，入力されたデータをチェックして，スクリプトの文字列を置き換えて無効化する**サニタイジング**が有効である。

ア：**SQLインジェクション**の説明である。

イ：**DoS**（Denial of Service）攻撃の説明である。

ウ：**バッファオーバフロー**攻撃の説明である。

### 問22　イ

**解説**　**クリックジャッキング攻撃**とは，Webページのコンテンツ上に透明化した不正コンテンツを配置し，あたかも正しいサイトを操作しているように見えるが実際は不正コンテンツ上で操作させるようにWebページを偽装することである。PCのマウスクリックを乗っ取る（jack）攻撃である。

2009年にJPCERTからクリックジャッキングに関する技術メモが公開され，そのなかで対策や注意喚起が行われている。

ア：**HTTPレスポンス分割攻撃**（HTTP Response Splitting Attack）の説明である。

ウ：**タブナビング**（Tabnabbing）の説明である。

エ：**ブラウザハイジャッカー**（Browser Hijacker）の説明である。

## 問 23

正解 □ 完璧 □ 直前チェック □

送信者Aが文書ファイルと，その文書ファイルのディジタル署名を受信者Bに送信したとき，受信者Bができることはどれか。ここで，受信者Bは送信者Aの署名検証鍵Xを保有しており，受信者Bと第三者は送信者Aの署名生成鍵Yを知らないものとする。

ア　ディジタル署名，文書ファイル及び署名検証鍵Xを比較することによって，文書ファイルに改ざんがあった場合，その部分を判別できる。
イ　文書ファイルがウイルスに感染していないことを認証局に問い合わせて確認できる。
ウ　文書ファイルが改ざんされていないこと，及びディジタル署名が署名生成鍵Yによって生成されたことを確認できる。
エ　文書ファイルとディジタル署名のどちらかが改ざんされた場合，どちらが改ざんされたかを判別できる。

## 問 24

正解 □ 完璧 □ 直前チェック □

公開鍵暗号を利用した電子商取引において，認証局（CA）の役割はどれか。

ア　取引当事者間で共有する秘密鍵を管理する。
イ　取引当事者の公開鍵に対するディジタル証明書を発行する。
ウ　取引当事者のディジタル署名を管理する。
エ　取引当事者のパスワードを管理する。

## 問 25

正解 □ 完璧 □ 直前チェック □

ドライブバイダウンロード攻撃の説明はどれか。

ア　PCにUSBメモリが接続されたとき，USBメモリに保存されているプログラムを自動的に実行する機能を用いてウイルスを実行し，PCをウイルスに感染させる。
イ　PCに格納されているファイルを勝手に暗号化して，戻すためのパスワードを教えることと引換えに金銭を要求する。
ウ　Webサイトを閲覧したとき，利用者が気付かないうちに，利用者の意図にかかわらず，利用者のPCに不正プログラムが転送される。
エ　不正にアクセスする目的で，建物の外部に漏れた無線LANの電波を傍受して，セキュリティの設定が脆弱（ぜい）な無線LANのアクセスポイントを見つけ出す。



春

### 問23　ウ

**解説**　**ディジタル署名**とは，電子文書の発信者の正当性を保証するために付加される暗号化された署名情報である。第三者によって電子文書が改ざんされていないか，偽造されたものでないかを確認することができる。

ア，エ：ディジタル署名では情報の改ざんの有無を検知できるが，改ざんされた内容までは確認できない。

イ：認証局は，ディジタル署名の正当性を認証する機関であるため，ウイルス感染の問合せは関係ない。

ウ：送信者Aの署名生成鍵Yで署名された文書は，検証鍵Xでのみ検証することができる。

### 問24　イ

**解説**　**認証局**（CA：Certification Authority）は，取引当事者の公開鍵証明のためのディジタル証明書を発行している。公開鍵暗号方式を用いたディジタル書名では，送信者の公開鍵が正しいものであるかの証明が必要になる。この公開鍵の証明を行うためには，信頼できる認証局が認証局の秘密鍵で，送信者の公開鍵を暗号化したディジタル証明書を発行する。

### 問25　ウ

**解説**　**ドライブバイダウンロード攻撃**は，Webサイトを閲覧したとき，利用者が気付かないうちに，利用者の意図にかかわらず，利用者のPCに不正プログラムが転送される攻撃である。

ア：**autorun.infファイル**を悪用したウイルス感染の攻撃手法である。autorun.infはPCにデバイスが接続されたときに，自動起動するファイル名を記載するファイルである。USB，CD-ROM，DVDなどの外部媒体で利用される。

イ：**ランサムウェア**の説明である。

エ：**ウォードライビング**の説明である。

## 問 26 正解 完璧 直前チェック

パスワードリスト攻撃の手口に該当するものはどれか。

ア　辞書にある単語をパスワードに設定している利用者がいる状況に着目して，攻撃対象とする利用者IDを定め，英語の辞書にある単語をパスワードとして，ログインを試行する。
イ　数字4桁のパスワードだけしか設定できないWebサイトに対して，パスワードを定め，文字を組み合わせた利用者IDを総当たりに，ログインを試行する。
ウ　パスワードの総文字数の上限が小さいWebサイトに対して，攻撃対象とする利用者IDを一つ定め，文字を組み合わせたパスワードを総当たりに，ログインを試行する。
エ　複数サイトで同一の利用者IDとパスワードを使っている利用者がいる状況に着目して，不正に取得した他サイトの利用者IDとパスワードの一覧表を用いて，ログインを試行する。

## 問 27 正解 完璧 直前チェック

バックドアに該当するものはどれか。

ア　攻撃を受けた結果，ロックアウトされた利用者アカウント
イ　システム内に攻撃者が秘密裏に作成した利用者アカウント
ウ　退職などの理由で，システム管理者が無効にした利用者アカウント
エ　パスワードの有効期限が切れた利用者アカウント

## 問 28 正解 完璧 直前チェック

PCとサーバとの間でIPsecによる暗号化通信を行う。ブロック暗号の暗号化アルゴリズムとしてAESを使うとき，用いるべき鍵はどれか。

ア　PCだけが所有する秘密鍵　　イ　PCとサーバで共有された共通鍵
ウ　PCの公開鍵　　エ　サーバの公開鍵





### 問26　エ

**解説**　**パスワードリスト攻撃**は，複数サイトで同一のIDとパスワードを使っている利用者がいることを前提とした攻撃手法である。不正に入手したサイトのIDとパスワードの一覧表を用いてログインを不正に行う。
ア：**辞書攻撃**（Dictionary Attack）の説明である。
イ：**総当たり攻撃**（Brute force Attack）の一種である。
ウ：**総当たり攻撃**の説明である。

### 問27　イ

**解説**　**バックドア**は，その名の通り裏口を表す。侵入者がコンピュータへの侵入に成功したときに，管理者に気付かれて侵入路が塞がれても，次回の不正行為に利用できるように別の新たな侵入経路としてバックドアを作る。また，バックドアが設置されたコンピュータは，別のコンピュータへの攻撃の踏み台として利用されることも多い。
ア，ウ，エ：ロックされたアカウント，無効アカウント，有効期限切れアカウントは，バックドアではない。

### 問28　イ

**解説**　**AES**（Advanced Encryption Standard）とは，米国商務省標準技術局（NIST）によって制定された**標準暗号化方式**である。共通鍵暗号方式のブロック暗号であり，DESの後継規格となった米国政府標準暗号である。鍵長は128ビット，192ビット，256ビットの3種から選択できる。
ア：AESは共通鍵暗号方式であるため，PCとサーバ両方で同一の鍵を保有する必要がある。
ウ，エ：AESは共通鍵暗号方式であるため，公開鍵は利用しない。

## 問 29 正解 完璧 直前チェック

攻撃者がシステムに侵入するときにポートスキャンを行う目的はどれか。

ア　事前調査の段階で，攻撃できそうなサービスがあるかどうかを調査する。
イ　権限取得の段階で，権限を奪取できそうなアカウントがあるかどうかを調査する。
ウ　不正実行の段階で，攻撃者にとって有益な利用者情報があるかどうかを調査する。
エ　後処理の段階で，システムログに攻撃の痕跡が残っていないかどうかを調査する。

## 問 30 正解 完璧 直前チェック

AさんがBさんの公開鍵で暗号化した電子メールを，BさんとCさんに送信した結果のうち，適切なものはどれか。ここで，Aさん，Bさん，Cさんのそれぞれの公開鍵は3人全員がもち，それぞれの秘密鍵は本人だけがもっているものとする。

ア　暗号化された電子メールを，Bさん，Cさんともに，Bさんの公開鍵で復号できる。
イ　暗号化された電子メールを，Bさん，Cさんともに，自身の秘密鍵で復号できる。
ウ　暗号化された電子メールを，Bさんだけが，Aさんの公開鍵で復号できる。
エ　暗号化された電子メールを，Bさんだけが，自身の秘密鍵で復号できる。

### 問29　ア

**解説**　**ポートスキャン**は，コンピュータなどのアクセス可能なサービス（通信ポート）を外部から調査することである。攻撃者は，侵入できそうなサービスがあるかどうか確認するために実行する。

ポートスキャンでは，PCやサーバのTCP，UDPの受け待ちポート番号を調べてどのようなサービスが起動されているかどうかを判断することができる。例えば，TCP80番ポートであれば，Webサービス（HTTP）である。一般的に，1023番以下のポート番号は，どのサービスで利用されているかが決まっている。

### 問30　エ

**解説**　**公開鍵暗号方式**の，公開鍵を利用する場合の考え方は，次のとおりである。

① 秘密鍵，公開鍵をペアで所有する。
② 秘密鍵は本人のみ知っている鍵で，公開鍵は誰でも参照可能な鍵である。
③ 秘密鍵で暗号化したものは，公開鍵でしか複合できない。逆に公開鍵で暗号化したものは秘密鍵でしか複合できない。

設問の「AさんがBさんの公開鍵で暗号化した電子メール」は，Bさんの秘密鍵でのみ複合でき，メールを読めるのはBさんのみとなる。

## 問 31 正解 完璧 直前チェック

“OECDプライバシーガイドライン”には8原則が定められている。その中の四つの原則についての説明のうち，適切なものはどれか。

| | 原則 | 説明 |
|---|---|---|
| ア | 安全保護の原則 | 個人データの収集には制限を設け，いかなる個人データも，適法かつ公正な手段によって，及び必要に応じてデータ主体に通知し，又は同意を得た上で収集すべきである。 |
| イ | 個人参加の原則 | 個人データの活用，取扱い，及びその方針については，公開された一般的な方針に基づかなければならない。 |
| ウ | 収集制限の原則 | 個人データの収集目的は収集時点よりも前に特定し，利用はその利用目的に矛盾しない方法で行い，利用目的を変更するに当たっては毎回その利用目的を特定すべきである。 |
| エ | データ内容の原則 | 個人データは，利用目的に沿ったもので，かつ利用目的の達成に必要な範囲内で正確，完全，最新の内容に保つべきである。 |

## 問 32 正解 完璧 直前チェック

個人情報に関する記述のうち，個人情報保護法に照らして適切なものはどれか。

ア　構成する文字列やドメイン名によって特定の個人を識別できるメールアドレスは，個人情報である。

イ　個人に対する業績評価は，特定の個人を識別できる情報が含まれていても，個人情報ではない。

ウ　新聞やインターネットなどで既に公表されている個人の氏名，性別及び生年月日は，個人情報ではない。

エ　法人の本店所在地，支店名，支店所在地，従業員数及び代表電話番号は，個人情報である。



春

## 問31 エ

**解説** **OECDプライバシーガイドライン**は，OECD（経済協力開発機構）の理事会で採択された「プライバシー保護と個人データの国際流通についての勧告」の中に記述されている八つの原則である。

| | 原　則 | 説　明 |
|---|---|---|
| 1 | 収集制限の原則 | 個人データの収集には制限を設ける必要があり，データ主体に知らしめ又は同意を得た上で，収集されるべきである。 |
| 2 | データ内容の原則 | 個人データは，その利用目的に沿い，利用目的に必要な範囲内で正確，完全であり最新に保たれなければならない。 |
| 3 | 目的明確化の原則 | 個人データの収集目的は明確化されなければならない。その後のデータの利用は，当該収集目的に矛盾せず，目的の変更毎に明確化されるべきである。 |
| 4 | 利用制限の原則 | 個人データは，明確化された目的以外の目的のために開示利用その他の使用に供されるべきではない。ただし，データ主体の同意がある場合や，法律の規定による場合は例外となる。 |
| 5 | 安全保護の原則 | 個人データは，紛失もしくは不当なアクセス，破壊，使用，修正，開示等の危険に対し，合理的な安全保護措置により保護されなければならない。 |
| 6 | 公開の原則 | データ収集の実施，方針などを明確にする。データの利用目的や，データ管理者を明示する。 |
| 7 | 個人参加の原則 | 個人は，データ主体に対して自己のデータに関する内容や，所在を確認することができる。データ管理者は，異議申し立てを保証する必要がある。 |
| 8 | 責任の原則 | データ管理者は，上記の諸原則を実施するための措置に従う責任を有する。 |

ア：収集制限の原則の説明である。

イ：公開の原則の説明である。

ウ：目的明確化の原則の説明である。

## 問32 ア

**解説** **個人情報保護法**（個人情報の保護に関する法律）第二条より引用すると，以下である。

「個人情報」とは，生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより特定の個人を識別することができることとなるものを含む。）をいう。

イ：業績評価に個人を識別できる情報がある場合は，個人情報となる。

ウ：新聞やインターネットで公表されている個人の情報も個人情報となる。

エ：法人は，個人情報に該当しない。

## 問 33

正解 □ 完璧 □ 直前チェック □

刑法における“電子計算機損壊等業務妨害”に該当する行為はどれか。

ア　企業が運営するWebサイトに接続し，Webページを改ざんした。
イ　他社の商標に酷似したドメイン名を使用し，不正に利益を得た。
ウ　他人のWebサイトを無断で複製して，全く同じWebサイトを公開した。
エ　他人のキャッシュカードでATMを操作し，自分の口座に振り込んだ。

## 問 34

正解 □ 完璧 □ 直前チェック □

特定電子メール送信適正化法で規制される，いわゆる迷惑メール（スパムメール）はどれか。

ア　ウイルスに感染していることを知らずに，職場全員に送信した業務連絡メール
イ　書籍に掲載された著者のメールアドレスへ，匿名で送信した批判メール
ウ　接客マナーへの不満から，その企業のお客様窓口に繰返し送信したクレームメール
エ　送信することの承諾を得ていない不特定多数の人に送った広告メール

## 問 35

正解 □ 完璧 □ 直前チェック □

不正競争防止法によって保護される対象として規定されているものはどれか。

ア　自然法則を利用した技術的思想の創作のうち高度なものであって，プログラム等を含む物と物を生産する方法
イ　著作物を翻訳し，編曲し，若しくは変形し，又は脚色し，映画化し，その他翻案することによって創作した著作物
ウ　秘密として管理されている事業活動に有用な技術上又は営業上の情報であって，公然と知られていないもの
エ　法人等の発意に基づきその法人等の業務に従事する者が職務上作成するプログラム著作物



春

### 問33　ア

**解説**　**電子計算機損壊等業務妨害罪**とは，刑法　第二百三十四条の二より引用すると，「人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し，若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え，又はその他の方法により，電子計算機に使用目的に沿うべき動作をさせず，又は使用目的に反する動作をさせて，人の業務を妨害した者。」とされている。
イ：**不正競争防止法違反**に該当する。
ウ：**著作権法違反**に該当する。
エ：刑法　第二百四十六条の二　**電子計算機使用詐欺**に該当する。

### 問34　エ

**解説**
**特定電子メール送信適正化法**：特定電子メールの送信の適正化のための措置等を定めることにより，電子メールの利用についての良好な環境の整備を図り，高度情報通信社会の健全な発展に寄与することを目的としている。
**スパムメール**：受信者に断りもなく，勝手に広告や詐欺内容メールを送り付ける行為である。
ア：ウイルス感染はスパムメールに該当しない。
イ：書籍に掲載されているメールアドレスは，批判なども受け付けるためのものであるため，スパムメールとはならない。
ウ：企業のお客様窓口は，クレームを受け付けるためのものでもあるため，スパムメールとはならない。

### 問35　ウ

**解説**
**不正競争防止法**：市場における競争が公正に行われるように，営業秘密の保護，信用の保護などを定めている。また，公正な競争を阻害する不正な行為や不法行為を禁止している。不正競争防止法で営業秘密として認められるには，次の三つの要件を満たすことが求められる。
**秘密管理性**：営業秘密を秘密として管理されていること。
**有用性**：生産や販売の方法など事業活動に有用な技術，または営業上の情報であること。
**非公知性**：一般的には知られておらず，又は容易に知ることができないこと。
ア：特許法にて保護される内容である。
イ，エ：著作権法にて保護される内容である。

## 問 36

正解 □ 完璧 □ 直前チェック □

請負契約の下で，自己の雇用する労働者を契約先の事業所などで働かせる場合，適切なものはどれか。

ア　勤務時間，出退勤時刻などの労働条件は，契約先が定めて管理する。
イ　雇用主が自らの指揮命令の下に当該労働者を業務に従事させる。
ウ　当該労働者は，契約先で働く期間は，契約先との間にも雇用関係が生じる。
エ　当該労働者は，契約先の指揮命令によって業務に従事するが，雇用関係の変更はない。

## 問 37

正解 □ 完璧 □ 直前チェック □

スプレッドシートの利用に係るコントロールの監査において把握した，利用者による行為のうち，指摘事項に該当するものはどれか。

ア　スプレッドシートに組み込まれたロジックの正確性を，検算によって確認していた。
イ　スプレッドシートに組み込まれたロジックを，業務上の必要に応じて，随時，変更し上書き保存していた。
ウ　スプレッドシートにパスワードを付した上で，アクセスコントロールが施されたサーバに保管していた。
エ　スプレッドシートを所定のルールに従ってバックアップしていた。



春

### 問36　イ

**解説**　**請負契約**では，自己の雇用する労働者を契約先で働かせる場合の条件は以下となる。

**勤務管理**：自己の会社で管理し，契約先は勤務管理しない。契約先が勤務管理すると違法となる。

**雇用関係**：労働者は，自己の会社のみ雇用関係となる。契約先との雇用関係はない。

**指揮命令**：労働者に対して，自己の会社からの指揮命令権がある。契約先から指揮命令された場合は違法となる。

ア：勤務時間，出退勤時間などの労働条件は当該労働者を雇用している請負元の労働条件で，当該労働者は働くことになる。

ウ：契約先との雇用関係はない。

エ：契約先の指揮命令はない。

### 問37　イ

**解説**

**スプレッドシート**：表計算ソフトなどで作成した表や数式を含むシートである。企業では，実務で数多く利用されており，一般的に利用されているツールであるともいえる。

**コントロールの監査**：ロジックの正しさでは，変更する際の手続きやアクセス権，バックアップの方式などを確認する。

ア：正確性を検算でチェックしている点は，監査において指摘事項にはならない。

イ：ロジックを，必要に応じて随時変更し上書きした場合，ロジックの誤りがあったときに，いつから誤っていたか確認ができないため指摘事項となる。

ウ：パスワードでの保護によってアクセスコントロールすることは，監査において指摘事項にはならない。

エ：所定のルールに従ったバックアップは，監査において指摘事項にはならない。

## 問 38

正解 □ 完璧 □ 直前チェック □

従業員の守秘義務について，“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義務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義務を負うことが，雇用契約に定められている。
ウ　定められた守秘義務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 39

正解 □ 完璧 □ 直前チェック □

“情報セキュリティ監査基準”に基づいて情報セキュリティ監査を実施する場合，監査の対象，及びコンピュータを導入していない部署における監査実施の要否の組合せのうち，最も適切なものはどれか。

| | 監査の対象 | コンピュータを導入していない部署における監査実施の要否 |
|---|---|---|
| ア | 情報資産 | 必要 |
| イ | 情報資産 | 不要 |
| ウ | 情報システム | 必要 |
| エ | 情報システム | 不要 |



春

### 問38　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。

### 問39　ア

**解説**　**情報セキュリティ監査基準**とは，情報セキュリティ監査業務の品質を確保し，有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。情報セキュリティに係るリスクのマネジメントが効果的に実施されるように，リスクアセスメントに基づく適切なコントロールの整備，運用状況を，情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して，もって保証を与えあるいは助言を行う。

**情報資産**の監査：コンピュータの有無にかかわらず，情報として存在しているため監査対象となる。

**情報システムの監査**：コンピュータシステムを指すため，コンピュータを導入していない場合は監査不要となる。そのため，コンピュータを導入していない部署における監査は，情報資産の監査を実施することが妥当だといえる。

## 問 40

正解 □ 完璧 □ 直前チェック □

SLAに記載する内容として，適切なものはどれか。

ア　サービス及びサービス目標を特定した，サービス提供者と顧客との間の合意事項
イ　サービス提供者が提供する全てのサービスの特徴，構成要素，料金
ウ　サービスデスクなどの内部グループとサービス提供者との間の合意事項
エ　利用者から出されたITサービスに対する業務要件

## 問 41

正解 □ 完璧 □ 直前チェック □

事業継続計画で用いられる用語であり，インシデントの発生後，次のいずれかの事項までに要する時間を表すものはどれか。

(1)　製品又はサービスが再開される。
(2)　事業活動が再開される。
(3)　資源が復旧される。

ア　MTBF　　イ　MTTR　　ウ　RPO　　エ　RTO

## 問 42

正解 □ 完璧 □ 直前チェック □

過去5年間のシステム障害について，年ごとの種類別件数と総件数の推移を一つの図で表すのに最も適したものはどれか。

ア　積上げ棒グラフ　　イ　二重円グラフ
ウ　ポートフォリオ図　　エ　レーダチャート



春

### 問40　ア

**解説**

**SLA**（Service Level Agreement）：サービス提供者と委託者（顧客）の間で，サービスの品質に関して結ぶ契約のことである。サービスの品目と水準，及び水準を達成できなかった場合のペナルティ事項などを合意する。

イ：**サービスカタログ**の説明である。

ウ：**OLA**（Operational Level Agreement）の説明である。

エ：**SLR**（Service Level Requirement）の説明である。

### 問41　エ

**解説**

**MTBF**（Mean Time Between Failures：平均故障間隔）：コンピュータシステムが故障してから次に故障するまでの間隔の平均である。

**MTTR**（Mean Time To Repair：平均修理時間）：コンピュータシステムが故障してから，修理が完了して使用可能になるまでの時間の平均である。

**RPO**（Recovery Point Objective：目標復旧時点）：再開時に事業活動が実施できるようにするために，事業活動で使用される情報がどの状態まで復旧されなければならないかを示す時点。

**RTO**（Recovery Time Objective：目標復旧時間）：インシデントの発生後，製品又はサービスが再開される時間，事業活動が再開される時間，資源が復旧される時間のいずれかのこと。

解答は，事業継続計画での用語である点と，(1)，(2)，(3)の内容から，RTOとなる。

### 問42　ア

**解説**

**積み上げ棒グラフ**：複数の項目とその合計を示し，大小比較をするときに用いる。

**二重円グラフ**：360度の円を100分比に応じて中心点から扇状に区切ったグラフを円グラフという。この円グラフの大小二つを重ね，内側の円と外側の円で異なる項目の構成比率を表すときに用いる。

**ポートフォリオ図**：独立した二つの軸上に，拡充事象を配置しどの位置にあるかによって比較する図である。

**レーダチャート**：放射線状に伸びた数値軸上の値を線で結んだ多角形のグラフ。クモの巣チャートとも呼ばれる。複数項目の比較や傾向の分析に用いられる。

## 問 43

正解 □ 完璧 □ 直前チェック □

コンピュータシステムに対して問合せの終わり又は要求の終わりを指示してから，利用者端末に最初の処理結果のメッセージが出始めるまでの経過時間を何というか。

ア　アクセスタイム　　イ　サイクルタイム
ウ　ターンアラウンドタイム　　エ　レスポンスタイム

## 問 44

正解 □ 完璧 □ 直前チェック □

企業の様々な活動を介して得られた大量のデータを整理・統合して蓄積しておき，意思決定支援などに利用するものはどれか。

ア　データアドミニストレーション　　イ　データウェアハウス
ウ　データディクショナリ　　エ　データマッピング

## 問 45

正解 □ 完璧 □ 直前チェック □

ルータの機能に関する記述として，適切なものはどれか。

ア　LAN同士やLANとWANを接続して，ネットワーク層での中継処理を行う。
イ　データ伝送媒体上の信号を物理層で増幅して中継する。
ウ　データリンク層でネットワーク同士を接続する。
エ　二つ以上のLANを接続し，LAN上のMACアドレスを参照して，その参照結果を基にデータフレームを他のLANに流すかどうかの判断を行う。



春

### 問43　エ

**解説**

**アクセスタイム**：CPUやメモリに対して読出しや書込みを行うときの時間を表す。
**サイクルタイム**：繰り返し行われる作業において，1回の作業にかかる時間である。
**ターンアラウンドタイム**：利用者がシステムに処理のリクエストを入力して，そのリクエストの結果が出力されるまでの時間。秒や分の単位で表現される。
**レスポンスタイム**：コンピュータへの入力が終了してからその結果の応答出力が開始されるまでの時間のことである。

### 問44　イ

**解説**

**データウェアハウス**：情報の倉庫と呼ばれ，データベースとして大量のデータを整理・分類して蓄積し，経営に役立つ情報としてビジネスで活用するための手段を提供するシステムである。企業の様々な活動を介して得られた大量のデータを目的別に整理・統合して蓄積し，意思決定支援などに利用する。
**データアドミニストレーション**：データ管理を行うことである。
**データディクショナリ**：データの名称，意味などを定義し管理するものである。
**データマッピング**：異なるデータ間の関連付けを表すものである。

### 問45　ア

**解説**　**ルータ**とは，パケットを伝送するときの機器で，二つ以上のネットワークの間に中継するための機器として設置される。
イ：**リピータ**の説明である。
ウ：**ブリッジ**の説明である。
エ：**スイッチングハブ**（レイヤ2スイッチ）の説明である。

## 問 46

正解 □ 完璧 □ 直前チェック □

社内ネットワークからインターネットへのアクセスを中継し，Webコンテンツをキャッシュすることによってアクセスを高速にする仕組みで，セキュリティ確保にも利用されるものはどれか。

ア　DMZ　　イ　IPマスカレード(NAPT)
ウ　ファイアウォール　　ウ　プロキシサーバ

## 問 47

正解 □ 完璧 □ 直前チェック □

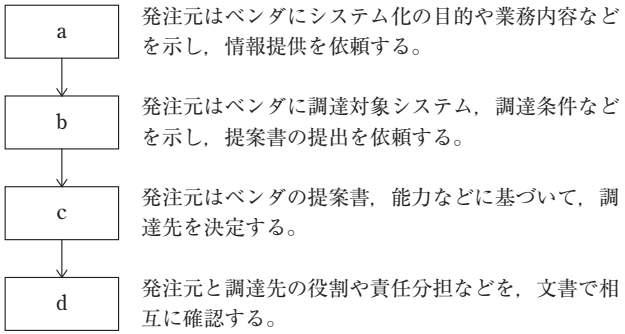
利用者が，インターネットを経由してサービスプロバイダのシステムに接続し，サービスプロバイダが提供するアプリケーションの必要な機能だけを必要なときにオンラインで利用するものはどれか。

ア　ERP　　イ　SaaS　　ウ　SCM　　エ　XBRL

## 問 48

正解 □ 完璧 □ 直前チェック □

図に示す手順で情報システムを調達するとき，bに入るものはどれか。




ア　RFI　　イ　RFP　　ウ　供給者の選定　　エ　契約の締結



春

### 問46　エ

**解説**

**DMZ**(DeMilitarized Zone)：ファイアウォールによってネットワーク上に隔離された区画を作り，外部とのアクセスの中継となるサーバ(リバースプロキシサーバ)を配置する。

**IPマスカレード**(NAPT：Network Address Port Translation)：グローバルIPアドレスからプライベートIPアドレスに変換するための機能である。アドレス変換時にポート番号も用いる。

**ファイアウォール**：信頼できないネットワークと，信頼できるネットワークの境界におかれ，通信を制御するために用いられる。

**プロキシサーバ**：内部ネットワークから外部ネットワークへのアクセスを中継するサーバである。

### 問47　イ

**解説**

**ERP**(Enterprise Resource Planning)：企業全体の経営資源を総合的に計画・管理し，経営の効率化を図るための手法。

**SaaS**(Software as a Service)：ソフトウェアの機能(サービス)をネットワーク経由で利用する形態である。

**SCM**(Supply Chain Management)：調達，製造，物流，販売，サービスといった，生産から販売のプロセス(サプライチェーン)における情報の流れを整理統合し，サプライチェーン全体で共有することを通じて全体の効率化を図る。

**XBRL**(eXtensible Business Reporting Language)：各種事業報告用の情報(財務・経営・投資などの様々な情報)を作成・流通・利用できるように標準化されたXMLベースのコンピュータ言語である。

### 問48　イ

**解説**　図のa～dは，RFI，RFP，供給者の選定，契約の締結という順序になる。

**RFI**(Request for Information：情報提供依頼書)：発注元からベンダに対して，システム化の目的や業務内容を示し，情報提供を依頼する。

**RFP**(Request for Proposal：提案依頼書)：発注元からベンダに対して，各種条件を記載し具体的な提案を依頼する文書である。

## 問 49 正解 □ 完璧 □ 直前チェック □

事業継続計画の策定に際し，リスクへの対応として適切なものはどれか。

ア　全リスクを網羅的に洗い出し，リスクがゼロとなるように策定する。
イ　想定するリスクのうち，許容できる損失を超えるものを優先的に対処する。
ウ　想定するリスクの全てについて，発生時の対応策をとることを目的とする。
エ　想定するリスクの優先度に差をつけずに検討する。

## 問 50 正解 □ 完璧 □ 直前チェック □

企業経営の透明性を確保するために，企業は誰のために経営を行っているか，トップマネジメントの構造はどうなっているか，組織内部に自浄能力をもっているかなどの視点で，企業活動を監督・監視する仕組みはどれか。

ア　コアコンピタンス　　イ　コーポレートアイデンティティ
ウ　コーポレートガバナンス　　エ　ステークホルダアナリシス

春

## 問49 イ

**解説** **事業継続計画**（BCP：Business Continuity Plan）は，災害や事故などが発生したときに重要事業を継続させ，万一中断しても可能な限り短時間で再開するための計画である。事業が中断した場合は，最も緊急度の高い業務から再開させる。そのため，代替設備の手配，復旧作業の推進などに経営資源を投入する。

ア，ウ：全リスクを網羅的に実施し，リスクがゼロになるような計画は，コストがかかりすぎる危険性がある。コストバランスよく対応するのがよい。

エ：想定するリスクは多数になるため，優先度をつけて対応する。

## 問50 ウ

**解説**

**コアコンピタンス**：他社がまねのできない，独自のノウハウや技術のこと。

**コーポレートアイデンティティ**：企業の特性や個性を明示し，共通のイメージで顧客が認識できるようにすること。

**コーポレートガバナンス**：株主に対して企業活動の正当性を保持するために，経営管理が適切に行われているかどうかを監視し，点検すること。

**ステークホルダアナリシス**：プロジェクトの利害関係者であるステークホルダが，プロジェクトに対して与える影響を分析する。ステークホルダの識別を行い，その要求と影響を明確にし，マネジメントする。