

2.2 ネットワーク (6)

<知識レベル問題>

問1 Check ☐ ☐ ☐

難易度：☆

インターネットへの接続サービスを提供する回線事業者はどれか。

- ア ISP イ NIC ウ SI エ W3C

P.060

問2 Check ☐ ☐ ☐

難易度：☆

パケット通信に関する記述のうち、適切なものはどれか。

- ア 一般的な課金方式としては、定額制が使用される。
イ 送信したデータは、送信した順序で相手先に届けられる。
ウ データの送信には、すべて同じ伝送経路が利用される。
エ 伝送するデータは、一定の長さに分割して送信する。

P.060

問3 Check ☐ ☐ ☐

難易度：☆

収容局から家庭までの加入者線が光ファイバケーブルであるものはどれか。

- ア ADSL イ FTTH ウ HDSL エ ISDN

P.061

問4 Check ☐ ☐ ☐

難易度：☆

携帯電話回線に接続された携帯電話やスマートフォンを利用して、ノート型PCなどをインターネットに接続する方法はどれか。

- ア anonymous FTP イ PIAFS
ウ テザリング エ ルーティング

P.061

問5 Check ☐ ☐ ☐

難易度：☆

公衆回線を専用線のように利用できるサービスはどれか。

- ア IP電話 イ VPNサービス
ウ Webサービス エ モバイル通信

P.061

通信サービス

<実践レベル問題>

問6 Check ☐ ☐ ☐

難易度：☆☆

ADSL回線に関する記述のうち、適切なものはどれか。

- ア ADSLモデムから収容局までの一部区間で、光ファイバ回線を使用してもよい。
イ ADSLモデムから収容局までの距離に関係なく、常に一定の通信速度を維持する。
ウ アナログ電話とPCを同時に利用すると、単独利用に比べて通信速度が低下する。
エ ダウンロード時の通信速度はアップロード時の通信速度に比べて速い。

P.061

問7 Check ☐ ☐ ☐

難易度：☆☆

VoIPの説明として、適切なものはどれか。

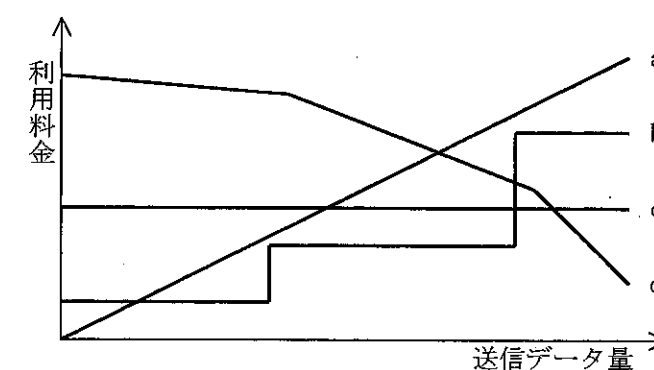
- ア インターネット上にあるアプリケーションやデータを、PCから利用する方式
イ 音声データをパケット化し、リアルタイムに送受信する技術
ウ ネットワークで接続された拠点間の通信において、認証及び暗号化と復号によってセキュリティを確保する技術
エ ネットワークに接続されたコンピュータのホスト名とIPアドレスを対応付けて管理するシステム

P.062

問8 Check ☐ ☐ ☐

難易度：☆☆☆

次の図中のa～dのうち、従量制の課金方式を表しているものはどれか。



- ア a イ b ウ c エ d

P.062

2.3 情報セキュリティ(1)

<知識レベル問題>

問1 Check ☐ ☐ ☐

難易度: ☆

“情報セキュリティの脅威”における分類に関する説明のうち、適切でないものはどれか。

- ア 機器自体や機器が設置された建物などに関する脅威を、物理的脅威と呼ぶ。
- イ コンピュータ技術を利用して攻撃してくる脅威を、技術的脅威と呼ぶ。
- ウ 組織に対して経済的な損失を与える脅威を、経済的脅威と呼ぶ。
- エ 人間の行為が原因となる脅威を、人的脅威と呼ぶ。

P.062

問2 Check ☐ ☐ ☐

難易度: ☆

システムの正当な利用者が処理をうっかり間違えた結果として、重要なデータが消去されてしまった。このような脅威を何というか。

- ア 誤操作
- イ 破壊
- ウ 破損
- エ 紛失

P.063

問3 Check ☐ ☐ ☐

難易度: ☆

悪意をもって他人のPCに侵入し、データを盗み見たり、破壊したりする行為を何というか。

- ア クラッキング
- イ ショルダハッキング
- ウ トラッシング
- エ 標的型攻撃

P.063

問4 Check ☐ ☐ ☐

難易度: ☆

セキュリティ事故の例のうち、原因が物理的脅威に分類されるものはどれか。

- ア 大雨によってサーバ室が浸水し、機器が停止した。
- イ 外部から公開サーバに大量のデータを送られて、公開サーバが停止した。
- ウ 攻撃者がネットワークを介して社内のサーバに侵入し、ファイルを破壊した。
- エ 社員が電子メールの宛先を間違えて、重要なデータが流出した。

P.063

情報セキュリティの脅威(1)

<実践レベル問題>

問5 Check ☐ ☐ ☐

難易度: ☆☆

情報システムの安定稼働を妨げるさまざまな脅威への事前対策に関する記述のうち、適切なものはどれか。

- ア 外部からの不正侵入を完全に阻止できれば、不正アクセスへの事前対策としては問題ない。
- イ 自然災害に対しては予測が困難なので、人的災害に絞って事前対策を講じる。
- ウ すべてのデータをバックアップしておけば、ほかの事前対策は不要となる。
- エ 予想損失額や対策コストとのトレードオフを考慮して、必要な事前対策を講じる。

P.063

問6 Check ☐ ☐ ☐

難易度: ☆☆

ソーシャルエンジニアリングによる被害に結びつきやすい状況はどれか。

- ア 運用担当者のセキュリティ意識が低い。
- イ サーバ室の天井の防水対策が行われていない。
- ウ サーバへのアクセス制御が行われていない。
- エ 通信経路が暗号化されていない。

P.064

問7 Check ☐ ☐ ☐

難易度: ☆☆☆

PCやハードディスクを譲渡したり返却したりする前に実施しておくこととして、ハードディスクからの情報漏えいを防ぐ最も確実な方法はどれか。

- ア ハードディスク全体を16進数の00やFF、または乱数で複数回上書きしておく。
- イ ハードディスク全体を論理フォーマットしておく。
- ウ ハードディスク内のすべてのファイルやフォルダをごみ箱に捨て、最後にごみ箱を空にしておく。
- エ ハードディスクにパスワードロックをかけておく。

P.064

2.3 情報セキュリティ(2)

<知識レベル問題>

問1 Check ☐ ☐ ☐

難易度: ☆

悪意をもって作成されたソフトウェアの総称はどれか。

- ア アドウェア イ シェアウェア
ウ マルウェア エ ミドルウェア

P.064

問2 Check ☐ ☐ ☐

難易度: ☆

マクロウイルスに関する説明として、適切なものはどれか。

- ア インターネットなどのネットワークを通じて、感染したコンピュータを外部から不正に遠隔操作できるようにする。
イ 個人情報などを盗み出して、第三者に自動的に送信する。
ウ 便利なソフトウェアに見せかけてインストールさせた後、不正な動作をする。
エ ワープロソフトや表計算ソフトのデータファイルに感染する。

P.064

問3 Check ☐ ☐ ☐

難易度: ☆

銀行やクレジットカード会社などを装った偽のWebページを開設し、金融機関や公的機関などを装った偽の電子メールなどで、利用者を巧みに誘導して、暗証番号やクレジットカード番号などの個人情報を盗み取る行為を何と呼ぶか。

- ア キーロガー イ ゼロデイ攻撃
ウ バッファオーバーフロー攻撃 エ フィッシング

P.065

問4 Check ☐ ☐ ☐

難易度: ☆

スパムメールの説明として、適切なものはどれか。

- ア あらかじめ登録した参加者全員に配信される、同じ内容の電子メールのこと
イ 受信者の承諾なしに無差別に送付される電子メールのこと
ウ 受信を承諾した相手にだけ送信される電子メールのこと
エ 電子メールの受信者が複数の相手に同一内容の電子メールの送信や転送を行い、受信者が増加し続ける電子メールのこと

P.065

情報セキュリティの脅威(2)

<実践レベル問題>

問5 Check ☐ ☐ ☐

難易度: ☆☆

ランサムウェアの説明として、適切なものはどれか。

- ア ウイルスなどを検知して、コンピュータを脅威から守り、安全性を高めるソフトウェアの総称
イ 感染すると勝手にファイルやデータの暗号化などを行って、正常にデータにアクセスできないようにし、元に戻すための代金を利用者に要求するソフトウェア
ウ キーボード入力や画面出力といった入出力機能や、ディスクやメモリの管理などコンピュータシステム全体を管理するソフトウェア
エ ローマ字から平仮名や片仮名へ変換したり、仮名から漢字へ変換するなどコンピュータでの利用者の文字入力を補助するソフトウェア

P.065

問6 Check ☐ ☐ ☐

難易度: ☆☆

DoS攻撃によってサーバが受ける直接的な被害はどれか。

- ア 暗号化してあるデータが解読される。
イ 管理者用パスワードが変更される。
ウ コンピュータウイルスに感染する。
エ サービスの提供が阻害される。

P.065

問7 Check ☐ ☐ ☐

難易度: ☆☆☆

クロスサイトスクリプティングに関する記述として、適切なものはどれか。

- ア Webサイトの運営者が意図しないスクリプトを含むデータであっても、利用者のブラウザに送ってしまう脆弱性を利用する。
イ Webページの入力項目にOSの操作コマンドを埋め込んでWebサーバに送信し、サーバを不正に操作する。
ウ 複数のWebサイトに対して、ログインIDとパスワードを同じものに設定するという利用者の習性を悪用する。
エ 利用者を罠のあるWebサイトに誘導する目的などのために、偽の送信元IPアドレスをもったパケットを送る。

P.065

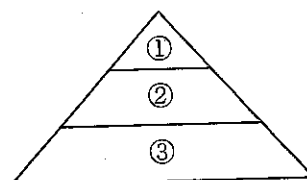
2.3 情報セキュリティ(3)

<知識レベル問題>

問1 Check ☐ ☐ ☐

難易度：☆

情報セキュリティの文書を詳細化の順に、右の図のように上から並べた場合、①～③に当てはまる用語の組合せとして、適切なものはどれか。



	①	②	③
ア	基本方針	対策基準	対策実施手順
イ	基本方針	対策実施手順	対策基準
ウ	対策基準	基本方針	対策実施手順
エ	対策基準	対策実施手順	基本方針

P.066

問2 Check ☐ ☐ ☐

難易度：☆

情報セキュリティにおける“可用性”の説明として、適切なものはどれか。

- ア システムの動作と出力結果が意図したものであること
- イ 情報が正確であり、改ざんされたり破壊されたりしていないこと
- ウ 認可された利用者が、必要なときに情報にアクセスできること
- エ 認可されていないプロセスに対して、情報を非公開にすること

P.066

問3 Check ☐ ☐ ☐

難易度：☆

ISMSの運用において、監査結果をインプットとし、ISMSを継続的に改善するための是正処置及び予防処置を行うプロセスはPDCAサイクルのどれにあたるか。

- ア P
- イ D
- ウ C
- エ A

P.066

問4 Check ☐ ☐ ☐

難易度：☆

リスクマネジメントにおいて、リスクを資産ごとに洗い出すものはどれか。

- ア リスク対策
- イ リスク特定
- ウ リスク評価
- エ リスク分析

P.066

情報セキュリティ管理

<実践レベル問題>

問5 Check ☐ ☐ ☐

難易度：☆☆

組織で策定する情報セキュリティポリシーに関する記述のうち、最も適切なものはどれか。

- ア 情報セキュリティ基本方針だけでなく、情報セキュリティに関する規則や手順の策定も経営者が行うべきである。
- イ 情報セキュリティ基本方針だけでなく、情報セキュリティに関する規則や手順も社外に公開することが求められている。
- ウ 情報セキュリティに関する規則や手順は組織の状況にあったものにすべきであるが、最上位の情報セキュリティ基本方針は業界標準の雛形をそのまま採用することが求められている。
- エ 組織内の複数の部門で異なる情報セキュリティ対策を実施する場合でも、情報セキュリティ基本方針は組織全体で統一させるべきである。

P.067

問6 Check ☐ ☐ ☐

難易度：☆☆

組織の活動に関する記述a～dのうち、ISMSの特徴として、適切なものを全て挙げたものはどれか。

- a 一過性の活動でなく改善と活動を継続する。
- b 現場が主導するボトムアップ活動である。
- c 導入及び活動は経営層を頂点とした組織的な取り組みである。
- d 目標と期限を定めて活動し、目標達成によって終了する。

- ア a, b
- イ a, c
- ウ b, d
- エ c, d

P.067

問7 Check ☐ ☐ ☐

難易度：☆☆

ISMSにおけるセキュリティリスクへの対応には、リスク移転、リスク回避、リスク受容及びリスク低減がある。リスク回避に該当する事例はどれか。

- ア セキュリティ対策を行って、問題発生の可能性を下げた。
- イ 問題発生時の損害に備えて、保険に入った。
- ウ リスクが小さいことを確認し、問題発生時は損害を負担することにした。
- エ リスクの大きいサービスから撤退した。

P.067

2.3 情報セキュリティ(4)

<知識レベル問題>

問1 Check ☐ ☐ ☐

難易度: ☆

社内の情報セキュリティ教育に関する記述のうち、適切なものはどれか。

- ア 再教育は、情報システムを入れ替えたときだけ実施する。
- イ 新入社員へは、業務に慣れた後に実施する。
- ウ 対象は、情報資産にアクセスする社員だけにする。
- エ 内容は、社員の担当業務、役割及び責任に応じて変更する。

P.067

問2 Check ☐ ☐ ☐

難易度: ☆

バイオメトリクス認証の例として、適切なものはどれか。

- ア 本人だけが知っているパスワードで認証する。
- イ 本人だけがもっている身分証明書で認証する。
- ウ 本人の指紋で認証する。
- エ ワンタイムパスワードを用いて認証する。

P.067

問3 Check ☐ ☐ ☐

難易度: ☆

ウイルス対策ソフトの適切な運用方法はどれか。

- ア インストールした時に一度だけ、ハードディスク全体を検査する。
- イ ウイルス対策ソフトは、ウイルス検査を行うときにだけ起動する。
- ウ 導入後もウイルス定義ファイルの更新を継続して行う。
- エ プロバイダ側でウイルスチェックが行われている場合は、PCへのウイルス対策ソフトの導入は不要である。

P.068

問4 Check ☐ ☐ ☐

難易度: ☆

プログラムによる自動投稿を防止するために、画面に表示された歪んだ文字や数字を入力させる仕組みはどれか。

- ア 画像認証 (CAPTCHA)
- イ コンテンツフィルタ
- ウ 電子透かし
- エ バイオメトリクス認証

P.068

情報セキュリティ対策

<実践レベル問題>

問5 Check ☐ ☐ ☐

難易度: ☆☆

セキュリティ対策の目的①～④のうち、適切なアクセス権を設定することによって効果があるものだけを全て挙げたものはどれか。

- ① DoS攻撃から守る。
- ② 情報漏えいを防ぐ。
- ③ ショルダハッキングを防ぐ。
- ④ 不正利用者による改ざんを防ぐ。

ア ①, ② イ ①, ③ ウ ②, ④ エ ③, ④

P.068

問6 Check ☐ ☐ ☐

難易度: ☆☆

生体認証による入退室管理システムに全社員を登録し、社内の各部屋に入室を許可する社員を設定した。退室は管理していない。a～dの記述のうち、この入退室管理システムで実現できることだけを全て挙げたものはどれか。

- a 権限のある社員だけに入室を許可する。
- b 入室者が部屋にいた時間を記録する。
- c 入室を試みて、拒否された社員を記録する。
- d 部屋にいる人数を把握する。

ア a, b, c イ a, c ウ a, d エ b, c, d

P.068

問7 Check ☐ ☐ ☐

難易度: ☆☆☆

インターネットでショッピングサイトに接続したとき、ブラウザにSSL鍵マークが表示された。さらに、サーバ証明書が、目的のショッピングサイトの運営者のものであることを確認した。このときに判断できることはどれか。

- ア このショッピングサイト運営者の財務状況は、安定している。
- イ このショッピングサイトで注文した商品は、納品日に必ず手元に届く。
- ウ 利用者が入力した個人情報などが改ざんされても、サーバ側で修正できる。
- エ 利用者が入力した個人情報などは、途中経路で漏えいすることはない。

P.069

2.3 情報セキュリティ(5)

<知識レベル問題>

問1 Check ☐ ☐ ☐

難易度: ☆

パスワードに関する記述のうち、適切なものはどれか。

- ア パスワードには、英単語など意味のある言葉を使用する。
- イ パスワードは必ずメモしておき、誰からも見やすい場所に貼っておく。
- ウ パスワード漏えいの事実が発覚した場合、速やかに管理者に報告する。
- エ 忘れないようにするために、できるだけ短いパスワードを設定する。

P.069

問2 Check ☐ ☐ ☐

難易度: ☆

一度の認証で、許可されている複数のサーバやアプリケーションなどを利用できる仕組みを何というか。

- ア シングルサインオン
- イ デジタルフォレンジックス
- ウ バイオメトリクス認証
- エ ワンタイムパスワード

P.069

問3 Check ☐ ☐ ☐

難易度: ☆

ネットワークにおいて、外部からの不正アクセスを防ぐために内部ネットワークと外部ネットワークの間に置かれるものはどれか。

- ア DNSサーバ
- イ サーチエンジン
- ウ スイッチングハブ
- エ ファイアウォール

P.070

問4 Check ☐ ☐ ☐

難易度: ☆

セキュリティに問題があるPCを社内ネットワークなどに接続させないことを目的とした仕組みであり、外出先で使用したPCを会社に持ち帰った際に、ウイルスに感染していないことなどを確認するために利用するものはどれか。

- ア DMZ
- イ IDS
- ウ 検疫ネットワーク
- エ ファイアウォール

P.070

アクセス制御

<実践レベル問題>

問5 Check ☐ ☐ ☐

難易度: ☆☆

システムの利用者認証技術に関する記述のうち、適切なものはどれか。

- ア 一度の認証で、許可されている複数のサーバやアプリケーションなどを利用できる仕組みをチャレンジレスポンス認証という。
- イ 指紋や声紋など、身体的な特徴を利用して本人認証を行う仕組みをシングルサインオンという。
- ウ 特定の数字や文字の並びではなく、位置についての情報を覚え、認証時には画面に表示された表の中で、自分が覚えている位置に並んでいる数字や文字をパスワードとして入力する方式をバイオメトリクス認証という。
- エ 認証のために一度しか使えないパスワードのことを、ワンタイムパスワードという。

P.070

問6 Check ☐ ☐ ☐

難易度: ☆☆

企業内ネットワークからも、外部ネットワークからも論理的に隔離されたネットワーク領域であり、そこに設置されたサーバが外部から不正アクセスを受けたとしても、企業内ネットワークには被害が及ばないようにするためのものはどれか。

- ア DMZ
- イ DNS
- ウ DoS
- エ SSL

P.071

問7 Check ☐ ☐ ☐

難易度: ☆☆

無線LANのセキュリティにおいて、アクセスポイントが接続要求を受け取ったときに、端末固有の情報を基にアクセス制御を行う仕組みはどれか。

- ア ESSID
- イ MACアドレスフィルタリング
- ウ WEP
- エ WPA

P.071

2.3 情報セキュリティ (6)

<知識レベル問題>

問1 Check ☐ ☐ ☐

難易度: ☆

共通鍵暗号方式に関する記述のうち、適切なものはどれか。

- ア 暗号化に用いる鍵を第三者に公開しても、第三者は暗号文を復号できない。
 イ 公開鍵暗号方式よりも、暗号化処理と復号処理の計算量は少ない。
 ウ 通信経路で改ざんされた暗号文を復号処理で訂正し、元の暗号文に復元する機能をもつ。
 エ 複数の相手ごとに通信内容を秘密にしたい場合でも、暗号化に用いる鍵は一つである。

P.071

問2 Check ☐ ☐ ☐

難易度: ☆

無線LANで利用される暗号方式の規格はどれか。

- ア AES イ DES ウ RSA エ WPA2

P.072

問3 Check ☐ ☐ ☐

難易度: ☆

Xさんは、Yさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容を秘密にする必要があるので、公開鍵暗号方式を用いて暗号化して送信したい。電子メールの内容を暗号化するのに使用する鍵はどれか。

- ア Xさんの公開鍵 イ Xさんの秘密鍵
 ウ Yさんの公開鍵 エ Yさんの秘密鍵

P.072

問4 Check ☐ ☐ ☐

難易度: ☆

公開鍵基盤 (PKI) において認証局 (CA) が果たす役割はどれか。

- ア SSLを利用した暗号化通信で使用する認証プログラムを提供する。
 イ Webサーバに不正な仕組みがないことを示す証明書を発行する。
 ウ 公開鍵が被認証者のものであることを示す証明書を発行する。
 エ 被認証者のデジタル署名を安全に送信する。

P.072

暗号化/デジタル署名

<実践レベル問題>

問5 Check ☐ ☐ ☐

難易度: ☆☆

セッション鍵暗号方式で用いられるハイブリッド方式に関する記述のうち、適切なものはどれか。

- ア 共通鍵と公開鍵で二重に暗号化するので、改ざんが難しい。
 イ 共通鍵と公開鍵を併用するので、高速な暗号通信には向かない。
 ウ 公開鍵暗号方式を使って、共通鍵を暗号化して通信相手に送信する。
 エ 使用する鍵の数は、全体で単独方式の2乗倍必要となる。

P.072

問6 Check ☐ ☐ ☐

難易度: ☆☆

受信した電子メールにPKI (公開鍵基盤) を利用したデジタル署名を付与した場合に関する記述 a ~ d のうち、判断可能な記述だけをすべて挙げたものはどれか。

- a 電子メールの添付ファイルはウイルスに感染していない。
 b 電子メールの内容は通信途中において、他の誰にも盗み見られていない。
 c 電子メールの発信者は、なりすましされていない。
 d 電子メールは通信途中で改ざんされていない。

- ア a, b イ a, c ウ b, d エ c, d

P.073

問7 Check ☐ ☐ ☐

難易度: ☆☆☆

小文字の英字からなる文字列の暗号化を考える。次表で英字を文字番号に変換し、変換後の文字番号について1文字目には1を、2文字目には2を、…、n文字目にはnを加える。それぞれの数を26で割った余りを新たに文字番号とみなし、表から対応する英字に変換する。

例 fax → 6, 1, 24 → 6+1, 1+2, 24+3 → 7, 3, 27 → 7, 3, 1 → gca
 この手続きで暗号化した結果が“tmb”であるとき、元の文字列はどれか。

文字番号	1	2	3	4	5	6	7	8	9	10	11	12	13
英字	a	b	c	d	e	f	g	h	i	j	k	l	m
文字番号	14	15	16	17	18	19	20	21	22	23	24	25	26
英字	n	o	p	q	r	s	t	u	v	w	x	y	z

- ア she イ shy ウ ski エ sky

P.073