



シラバス 6.3 対応

令和
07
年度

でぶどりと学ぶ

15歳からの

ITパスポート

田中 健



このPDFは、CQ出版社発売の書籍「でぶどりと学ぶ15歳からのITパスポート」の一部見本です。内容・購入方法については、下記のWebサイトをご覧ください。内容：<https://shop.cqpub.co.jp/hanbai/books/51/51081.html>

これ1冊で
ゼロから
合格!

必須の
過去問
300問
以上!

オリジナル
缶バッジ
プレゼント!



CQ出版社

見本

まえがき

はじめにお断りしておきたいのです。この本はIT パスポートで出題される用語の数々が詳しく丁寧に解説されている本ではありません。言ってしまうとネットを検索したら出てくる正しい解説はおまけ的な存在。その用語をどのように捉えればよいかという解釈がメインの本です。

高校の授業を思い出してみてください。この先生の授業はおもしろいと思えるポイントはどこにあるでしょうか。淡々と正しい解説が展開されるのが良いという人も一定数は居ると思います。しかし、多くは教科書本文の行間を埋める先生独自の解釈、何気なく放たれる一言の圧倒的存在感にあるのではないのでしょうか。文字の羅列だけではどうも頭に入ってこない内容に先生の解釈が乗っかることで急に理解できて納得できる。納得できると楽しくなってもっと理解したくなり、結果としてその教科を好きになり、先生の授業をおもしろいと思う。こんな好循環があるはず。だからこそ、普段から情報の先生として教壇に立っている時と同じように、本の中でも行間を埋める解釈を心がけました。

さらに、授業をおもしろいと思えるもう一つのポイント、下世話なネタにも一切手を抜いていません。筆者は高校生のみなさんが実際に使っている『情報I』の教科書の著者でもあるのですが、教科書には到底書けない、というか書いてはいけない内容にもがっかり踏み込んでみました。高校あるある、日常あるある、恋愛あるある、共感できそうなものを手当たり次第詰め込んであります。IT パスポートの勉強をするついでにニヤニヤしてもらえれば、筆者としては至上の喜びです。

この本の中では、でぶどり君もIT パスポート合格のためにがんばっているようです。「情報ようわからん」から「情報って意外とおもしろい」に、そして「なんか情報好きかも」に、そして「IT パスポート合格してしまった」に。でぶどり君ともども、そんな好循環にみなさんを巻き込みますよう。

2024年10月 田中 健

追伸：共感できないネタがあったらぜひ教えてください。



目次

テクノロジー系

第1章	セキュリティ	1
1-1	情報セキュリティ	2
1-2	情報セキュリティ管理	24
1-3	情報セキュリティ対策・実装技術	38
第2章	ネットワーク	71
2-1	ネットワーク方式	72
2-2	通信プロトコル	88
2-3	ネットワーク応用	96
第3章	アルゴリズムとプログラミング	113
3-1	アルゴリズムとプログラミング	114
3-2	プログラム言語	130
3-3	離散数学	136
3-4	応用数学	146
3-5	情報に関する理論	152
第4章	情報デザインと情報メディア	163
4-1	情報デザイン	164
4-2	インタフェース設計	172
4-3	マルチメディア技術	178
4-4	マルチメディア応用	188
第5章	データベース	193
5-1	データベース方式	194
5-2	データベース設計	198
5-3	データ操作	208
5-4	トランザクション処理	214
第6章	システム	223
6-1	システムの構成	224
6-2	システムの評価指標	234
第7章	ハードウェア	243
7-1	コンピュータ・入出力装置	244
第8章	ソフトウェア	261
8-1	ソフトウェアの構成	262
8-2	ファイルシステム	266
8-3	オフィスソフト	274

ストラテジ系

第 9 章	企業活動と法務	285
9-1	経営・組織論	286
9-2	業務分析・データ利活用	298
9-3	会計・財務	306
9-4	知的財産権	320
9-5	セキュリティ関連法規	328
9-6	労働関連・取引関連法規	338
9-7	コンプライアンスと情報倫理	344
9-8	標準化	352
第 10 章	経営戦略マネジメント	361
10-1	経営戦略手法	362
10-2	マーケティング	374
10-3	ビジネス戦略と経営管理	384
第 11 章	技術戦略マネジメント	395
11-1	技術開発戦略の立案・技術開発計画	396
11-2	ビジネスシステム	404
11-3	エンジニアリングシステム	416
11-4	e- ビジネス	422
第 12 章	システム戦略マネジメント	431
12-1	情報システム戦略	432
12-2	業務プロセス	438
12-3	ソリューションビジネス	446
12-4	システム活用促進・評価	454

マネジメント系

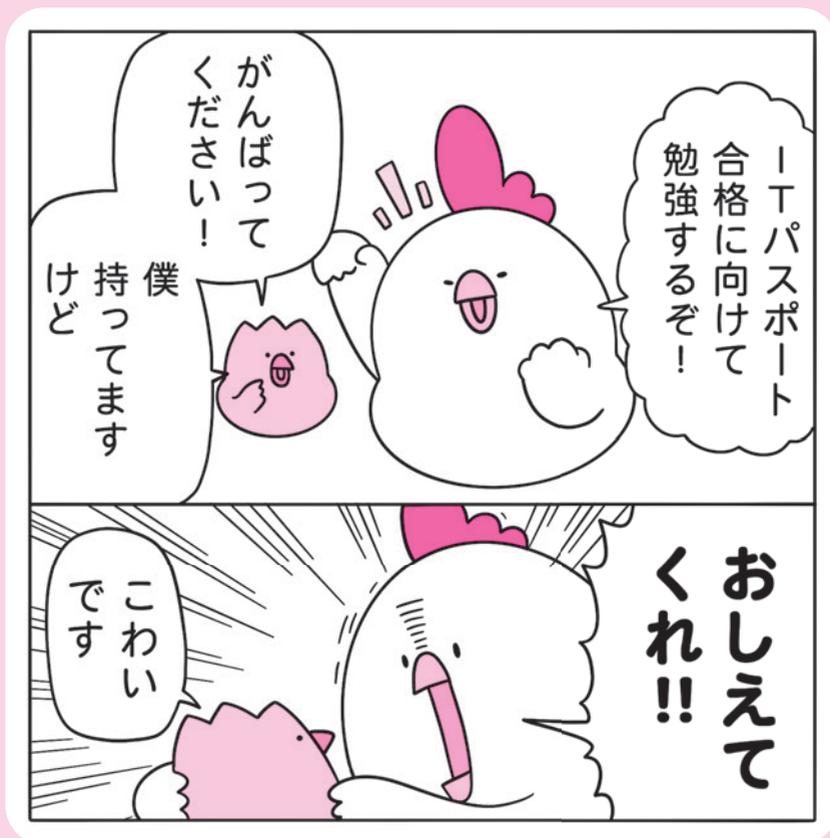
第 13 章	システム開発技術	461
13-1	システムの企画と要件定義	462
13-2	システムの開発・運用・保守	472
13-3	ソフトウェア開発手法	480
第 14 章	プロジェクトマネジメント	491
14-1	プロジェクトマネジメント	492
14-2	サービスマネジメント	500
14-3	ファシリティマネジメント	512
14-4	監査と内部統制	518
	本書のサポートについて	528

テクノロジー系

第1章

セキュリティ

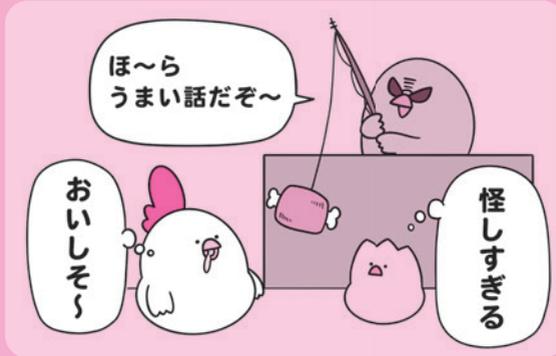
出題頻度 ★★★★★



テクノロジー系

第1章 セキュリティ

1-1 情報セキュリティ



情報セキュリティの概念

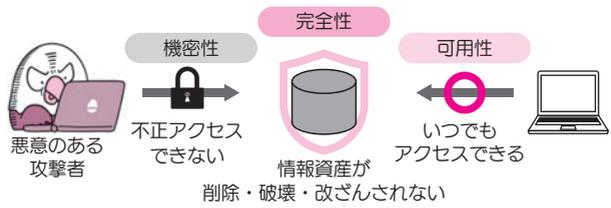
現代ではインターネットに代表されるサイバー空間を通じたコミュニケーションは日々の生活に欠かせない便利なものになっている。SNS アプリを通じたダイレクト・メールやビデオ通話もこれに含まれる。

しかし、その裏側では、アカウント乗っ取りなどのサイバー攻撃に起因する様々な事件もニュースになっている。こうした攻撃から個人情報などのデータ、スマートフォンなどの情報機器を守り、安全にコミュニケーションできる状態を保つこと、また、そのための対策を総称して**情報セキュリティ**という。

情報セキュリティの要素は次のように分類される。

要素の名称	要素の概要とその対策の例
機密性	限られた人だけが情報に接触できるようにすること (例) フォローを許可した人にしか投稿を見られないような鍵アカウント
完全性	情報が欠けていたり改ざんされたりしていない状態にすること (例) 破損した動画データを正確に復元できるようなバックアップ
可用性	情報が壊れて使えない状態にならないようにすること (例) 学校 PC ルーム内の情報機器・通信環境の定期メンテナンス

情報セキュリティの3大要素

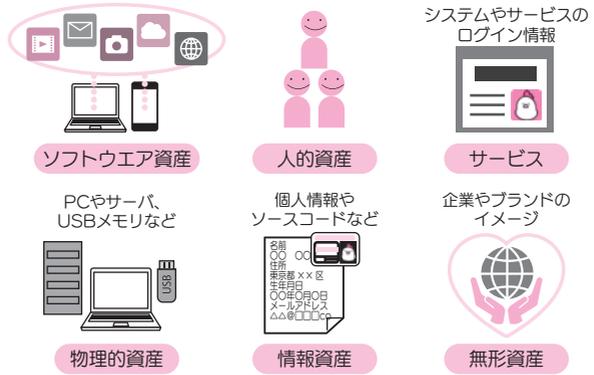


情報資産

運営のために学校がもつ情報を資産として扱う考え方のことをいい、在籍する生徒の成績、住所、家族構成、部活の活動実績や卒業生の進路先などが相当する。有形無形の区別なく、書類など紙に印刷されたもの、各種記憶装置にデジタルデータとして記録されたもの、オンラインストレージなど組織外部に保存されたものも含まれる。

特に重要とされる**個人情報**が学校外に漏れると、自宅に電話がかかってくるなど迷惑行為の被害に繋がるおそれがあり、学校は情報資産を適切な方法で管理し、知るべきではない者の手に渡らないような環境を整えることが重要になる。連絡先の記載された名簿が配付されなくなった大きな理由といえる。

さまざまな情報資産



クイズ

Q 卒業アルバムは情報資産に含まれる？

A 情報資産はコンピュータやネットワーク上にあるものだけでなく、紙に印刷されたものも含まれる。
卒業アルバムには顔写真や名前など、個人を特定できる情報しかないため、究極の情報資産と言える。



ぜいじゃくせい

脆弱性と脅威

スマートフォンやアプリなどに存在するセキュリティ上の弱点を**脆弱性**といい、脆弱性を突いて損害を与えるような物事を総称して**脅威**という。

例えば、SNSのパスワード再設定にかかる手続きのセキュリティが甘いという脆弱性があることで、アカウントが乗っ取られるような攻撃を受ける、という脅威が発生することになる。



脆弱性の種類

脆弱性には次のような種類がある。

種類	説明	例
ソフトウェアの脆弱性	ソフトウェアの設計や実装上の不具合やエラーによって生じる脆弱性	バグ、セキュリティホール
ネットワークの脆弱性	ネットワークや通信プロトコルに存在するセキュリティ上の弱点	ファイアウォールの設定ミス、偽の攻撃用アクセスポイント
人的脆弱性	ユーザーの誤操作やセキュリティポリシーの無視など、人間の行動に起因するセキュリティ上の脆弱性	パスワードの共有、機密情報の誤送信

Point

脅威と脆弱性は何が違う？



脅威……コンピュータやネットワークに害をもたらすもの

例：ウイルス、ハッキング

脆弱性…攻撃を受けやすい弱点のこと

例：バグやセキュリティホール



人的脅威とは

脅威のうち、**人間が起こす行動がきっかけになるもの**をいい、情報漏洩の原因の大多数を占めるともいわれる。例として、USBメモリの置き忘れ、不注意から起きる誤操作、意図的な個人情報を持ち出しなどが挙げられる。



check

盗聴 (Sniffing)

通信途中のデータを送信者の知らないところでコピーすること。暗号化通信されたものでなければ、IDやパスワード、DM内容など全て読み取ることができる。当然のことながら壁に耳をつけて隣の部屋の音を聴くがごとくデジタルデータは盗み聴きできないので、「盗読」の方がイメージしやすいかもしれない。



check

なりすまし (Spoofing)

自分以外の人物がもつ情報を利用して自分を騙る全ての行為。だまし取ったIDとパスワードを使ってネットバンクにアクセスし預金を引き出すような金銭的な被害があるもの、同じ高校生だと思ってDMを送り合っていたら実はかなり年上の社会人だったというような精神的に来る被害があるものなど、その内容は多岐に亘る。





check!

クラッキング (Cracking)

ありとあらゆる破壊活動・不正活動の総称。ドアを蹴り破って突入するという意味のある英単語「crack」から想像できるとおり、侵入に成功したコンピュータ内部のデータの削除、自分の成績データを1から5に変えるような改竄のほか、正規購入者であることを示すライセンス認証を突破するゲームソフトの不正コピーも含まれる。



check!

ソーシャルエンジニアリング (Social Engineering)

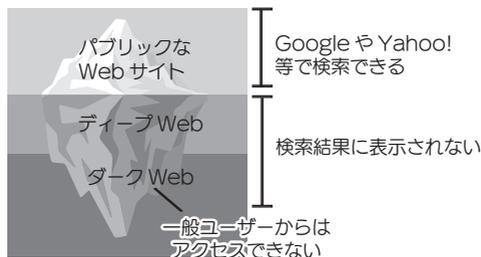
情報機器を悪用する方法ではなく、人の不注意につけこんで情報を取得する方法の総称。このご時世でも意外と個人情報を書かれた書類がそのまま捨てられているゴミ箱を漁るトラッシング、通りすがりに他人の画面を盗み見るショルダーハッキングなど、さまざまな手口が「情報」の教科書でも多数紹介されている。

他にも、関係者が機密情報を外部に持ち出す**内部不正**や、社長を騙ってヒラの従業員に「極秘案件」のようなメールを送信し、それを信用した従業員を操る手口を用いた**ビジネスメール詐欺**などがある。

コラム

ダークウェブ

特定のブラウザのみでアクセスできるウェブサイト。スマートフォンにはじめから入っているブラウザからの通信は遮断するような設定になっており、検索エンジンで見つかることもない。そのアンダーグラウンドな背景に乗じて、違法な取引が日々行われているとされる。インターネット上には一般庶民にはほぼほぼ辿りつけない闇が多い。



クイズ



ソーシャルエンジニアリング攻撃から企業を守るために最も効果的な対策はどれ？

- 1 定期的なパスワードの変更
- 2 従業員へのセキュリティ教育とトレーニング
- 3 最新のウイルス対策ソフトウェアのインストール



正解 2. 従業員へのセキュリティ教育とトレーニング

他の選択肢も重要だが、人の心理や行動を利用するソーシャルエンジニアリングに特化した対策としては、人への教育が最も有効といえる。

技術的脅威とは

脅威のうち、**プログラムを使って行われるもの**をいい、**機械的に同じ攻撃を繰り返せること**が特徴。被害を及ぼすようなプログラムは**マルウェア**と総称され、主に次のような型がある。

ボット型	多数の感染したコンピュータ（ボット）を使って、一つのネットワークを形成するマルウェアのこと。感染したコンピュータは、外部からの命令によって制御され、スパムメールの送信、分散型サービス拒否攻撃（DDoS 攻撃）、クリック詐欺、個人情報の盗み出し、さらなるマルウェアの拡散などに使われる。
ワーム型	ネットワークを介して自動的にコピーし、他のシステムに感染を広げるウイルス。独立して動作し、人間の介入なしに広がることができるため、短時間で大規模なネットワークに影響を及ぼす。
トロイの木馬型	有用なソフトウェアに見せかけて悪意のある機能を隠して配布されるウイルス。不用意にインストールすると、侵入用のバックドアが設置され、攻撃者による不正アクセスや情報の盗み出しなどが行われる。

ボット型マルウェア

ボット (Bot)

 コンピュータに侵入し、外部からの遠隔操作による指示を実行するマルウェア。具体的なサービス名は出せないために仮にXとするが、そのXのサービス上で延々と短文を投稿し続けるという、マルウェアではないプログラムもボットとよばれる。

スпам (Spam)

 しつこく一方的に送られてくる広告メールやDM。SNSのアカウントはさておき、メールアドレスはどこから仕入れられたのかわからないので送られた方は気持ちが悪い。南国のおにぎりに入っている同じ名前の缶詰肉ではない、と言いたいところだが、その由来はその缶詰肉のCMがしつこかったからという何となくも哀愁な風評被害である。

ワーム型マルウェア

ワーム (Worm)

 システム設定の改竄を主目的としてコンピュータに侵入し、自身をコピーした後に他のコンピュータへの転移を行おうとするマルウェア。虫を意味する英単語の“worm”がもとになっており、感染先の内容を書き換えるウイルスに対し、単体で被害を及ぼすようにコンピュータ上でウヨウヨ蠢くことが特徴である。虫が苦手な読者さん、ごめんなさい。

ランサムウェア (Ransom Ware)

 コンピュータ内の機密データを暗号化して内容がわからないようにし、元に戻すためのお金を請求するプログラム。身代金を意味する英単語の“ransom”とソフトウェアの“ware”を組み合わせた新語であり、意外なことに日本国外ではランサムに応じる事案も少なくない。決して身代金要求に屈しないマインドの国、それが日本。



1-1 情報セキュリティ 確認問題

001

令和元年秋期間 63

チェーンメールの特徴として、適切なものだけを全て挙げたものはどれか。



- a グループ内の連絡や情報共有目的で利用される。
- b ネットワークやサーバに、無駄な負荷をかける。
- c 返信に対する返信を、お互いに何度も繰り返す。
- d 本文中に、多数への転送を煽る文言が記されている。

ア a、c イ a、d ウ b、c エ b、d

002

令和4年 問91

ソーシャルエンジニアリングに該当する行為の例はどれか。



- ア あらゆる文字の組合せを総当たりで機械的に入力することによって、パスワードを見つけ出す。
- イ 肩越しに盗み見して入手したパスワードを利用し、他人になりすましてシステムを不正利用する。
- ウ 標的のサーバに大量のリクエストを送りつけて過負荷状態にすることによって、サービスの提供を妨げる。
- エ プログラムで確保している記憶領域よりも長いデータを入力することによってバッファをあふれさせ、不正にプログラムを実行させる。

003

令和2年秋期 問58

受信した電子メールに添付されていた文書ファイルを開いたところ、PCの挙動がおかしくなった。疑われる攻撃として、適切なものはどれか。



- ア SQL インジェクション
- イ クロスサイトスクリプティング
- ウ ショルダーハッキング
- エ マクロウイルス

004

令和5年 問58

Web サイトなどに不正なソフトウェアを潜ませておき、PC やスマートフォンなどの Web ブラウザからこのサイトにアクセスしたとき、利用者が気付かないうちに Web ブラウザなどの脆弱性を突いてマルウェアを送り込む攻撃はどれか。



- ア DDoS 攻撃
- イ SQL インジェクション
- ウ ドライブバイダウンロード
- エ フィッシング攻撃

001

「10日以内に10人に回さないと不幸になる。いたずらだと思って止めた人が実際に失踪している」などと不安を煽り、不特定多数に同じ内容で転送することを求める迷惑メールをいう。当初の発信者が不明で、拡散されることを面白がる迷惑行為であるため、反応せず削除するようにしよう。なお、当初のメディアはメールのためチェーンメールという名称になっているが、現在ではダイレクト・メールで同様の迷惑行為が確認されている。

- a. 転送により内容を拡散させることがチェーンメールの目的なので、誤り。メールではメーリングリスト、SNSではグループ機能がこれにあたる。
- b. 5G通信が一般的になった現代ではメールのデータ量は比較的小さいと考えられるが、無駄であることに変わりはないため、正しい。
- c. 送信者に返信するわけではないため、誤り。不特定多数に同じ文面で繰り返し転送されるのがチェーンメールの特徴である。
- d. 恐怖を感じるような文章で転送を迫るのが特徴なので、正しい。

正解 **イ**

002

ア 考えられる全てのパスワードを試してユーザ認証を突破しようとするブルートフォース攻撃の説明なので、誤り。

イ ショルダーハッキングによってパスワードを手に入れているため、ソーシャルエンジニアリングに該当する。

ウ サーバが処理しきれないほどの大量のアクセスを短時間に行い、サーバが応答できないようにするDoS攻撃の説明なので、誤り。

エ 一時的にデータを記憶しておくバッファという装置に誤作動を起こさせるバッファオーバーフロー攻撃の説明なので、誤り。

正解 **イ**

003

ア データベースを操作するためのプログラムに攻撃用データを注入する攻撃なので、誤り。

イ リンクをクリックすると攻撃用プログラムを作動させる攻撃なので、誤り。

ウ 画面を盗み見てパスワードなどの重要な情報を取得するソーシャルエンジニアリングの一例なので、誤り。

エ マクロウイルスは仕込まれたファイルを開くことで感染が広がる。「文書ファイルを開いたところ、PCの挙動がおかしくなった」と問題文にあることから、文書ファイルに仕込まれているマクロウイルスが動き出したと推測できるため、正しい。

正解 **エ**

004

ア インターネット上の多数のコンピュータを乗っ取って操り、タイミングを合わせて処理しきれないほどの大量のパケットをサーバに同時に送り付けて利用できない状態にする攻撃なので、誤り。

イ データベースを操作する命令の中に不正なデータを与えて本来想定していない動作を起こし、データベースを破壊したり個人情報を盗み取ったりする攻撃なので、誤り。

ウ ウェブサイトにアクセスしただけでブラウザを通じてウイルスに感染させる攻撃なので、正しい。

エ 実在するウェブサイトとそっくりの偽サイトを通して利用者を騙し、入力データを盗み取る攻撃なので、誤り。

正解 **ウ**

1-1 情報セキュリティ 確認問題

005

令和4年問95

攻撃対象とは別のWebサイトから盗み出すなどによって、不正に取得した大量の認証情報を流用し、標的とするWebサイトに不正に侵入を試みるものはどれか。



- ア DoS 攻撃
- イ SQL インジェクション
- ウ パスワードリスト攻撃
- エ フィッシング

006

令和元年秋期問100

脆弱性のあるIoT機器が幾つかの企業に多数設置されていた。その機器の1台にマルウェアが感染し、他の多数のIoT機器にマルウェア感染が拡大した。ある日のある時刻に、マルウェアに感染した多数のIoT機器が特定のWebサイトへ一気に大量のアクセスを行い、Webサイトのサービスを停止に追い込んだ。このWebサイトが受けた攻撃はどれか。



- ア DDoS 攻撃
- イ クロスサイトスクリプティング
- ウ 辞書攻撃
- エ ソーシャルエンジニアリング

007

令和5年問73

攻撃者がコンピュータに不正侵入したとき、再侵入を容易にするためにプログラムや設定の変更を行うことがある。この手口を表す用語として、最も適切なものはどれか。



- ア 盗聴
- イ バックドア
- ウ フィッシング
- エ ポートスキャン

008

令和元年秋期問98

攻撃者が他人のPCにランサムウェアを感染させる狙いはどれか。



- ア PC内の個人情報をネットワーク経由で入手する。
- イ PC内のファイルを使用不能にし、解除と引換えに金銭を得る。
- ウ PCのキーボードで入力された文字列を、ネットワーク経由で入手する。
- エ PCへの動作指示をネットワーク経由で送り、PCを不正に操作する。

005

- ア 処理しきれないほどの大量の packets を攻撃するサーバに送り付けて利用できない状態にする攻撃なので、誤り。
- イ データベースを操作する命令の中に不正なデータを与えて本来想定していない動作を起こし、データベースを破壊したり個人情報を盗み取ったりする攻撃なので、誤り。
- ウ ウェブ上のサービスから盗み出したユーザ ID とパスワードの組み合わせを他のサービスでも試して不正アクセスを行う攻撃なので、正しい。
- エ 実在するウェブサイトとそっくりの偽サイトを通して利用者を騙し、入力データを盗み取る詐欺行為なので、誤り。

正解 ウ

006

- ア マルウェアで多数の IoT 機器を乗っ取って操り、タイミングを合わせて処理しきれないほどの大量の packets をサーバに同時に送り付けて利用できない状態にする攻撃なので、正しい。
- イ 攻撃用プログラムを仕込んだウェブサイトアクセスさせるために作成した別のウェブサイトのリンクをクリックさせ、攻撃用プログラムを実行させる攻撃なので、誤り。
- ウ パスワードに使われそうな安易な文字列が大量に登録されたデータを利用して、ユーザ認証を突破しようとする攻撃なので、誤り。
- エ 情報機器を悪用する方法ではなく、人の不注意につけてこで情報を取得する方法なので、誤り。

正解 ア

007

- ア 他人が通信しているデータを途中で盗み取ることなので、誤り。スニффィングともよばれる。
- イ 一度侵入に成功した OS の設定を書き換えて攻撃者が再侵入しやすくなるように仕掛けるプログラムのことなので、正しい。
- ウ 実在するウェブサイトとほぼ同じ見た目の偽サイトに誘導して会員 ID やパスワードなどを入力させた情報を盗み取ることなので、誤り。
- エ 通信ポートにメンテナンス目的で外部から調査を入れることなので、誤り。

正解 イ

008

暗号化したデータを人質とみなしてお金を要求することから、ランサムウェアは身代金要求型ウイルスともよばれる。

- ア 個人情報はフィッシングサイトやスパイウェアなどを介して盗まれることが多く、ランサムウェアの主目的ではないため、誤り。
- イ データを暗号化して内容がわからないようにし、お金を請求するランサムウェアの主目的のため、正しい。
- ウ キーボードで入力された文字列を記録するのはキーロガーの機能であるため、誤り。
- エ コンピュータを遠隔操作するためのウイルスの一種であるボットの主目的のため、誤り。

正解 イ

ISBN978-4-7898-5108-4

C3055 ¥1800E

CQ出版社

定価 1,980円(本体1,800円)⑩



9784789851084



1923055018006