問040009解説

◆解答

設問１　イ

設問２　エ

設問３　ウ

設問４　ａ　オ　　ｂ　イ　　ｃ　ア

◆解説

セキュリティに関する問題である。

ＳＱＬインジェクション攻撃について

ＳＱＬインジェクションは、アプリケーションのセキュリティ上の不備を意図的に利用し、アプリケーションが想定しないＳＱＬ文を実行させることにより、データベースシステムを不正に操作する攻撃方法のことである。

ユーザがフォームから送信した検索語などのパラメータを受け取り、これをＳＱＬ文に埋め込んでデータベースへの問い合わせや操作を行う。このとき、ＳＱＬ文の断片として解釈できる文字列をパラメータに含めることで、プログラムが想定していないＳＱＬ文を合成し、不正にデータベースの内容を削除したり、本来アクセスできない情報を表示させたりすることができてしまう場合がある。このような攻撃手法をＳＱＬインジェクションという。

設問１

アは、ＤＮＳサーバーの情報を改ざんして、不特定多数のインターネットユーザーを偽のＷｅｂサイトに誘導し、口座番号などの個人情報を盗み出すオンライン詐欺行為である。これを「ファーミング」という。「ファーミング」は「フィッシング」の一種で、フィッシングは、偽メールでユーザーを偽サイトへ誘導するが、偽メールの代わりに、「ＤＮＳサーバーの情報の改ざん」が使われる

イのＷｅｂサイトの入力項目に対し、命令文を送り込むことによって、データベースへの不正操作を行うのが、ＳＱＬインジェクション攻撃である。求める答えはイとなる。

ウは管理ツールの脆弱性を使用して不正アクセスする。

エはデータベース管理者のＩＤとパスワードを盗聴し、不正操作する。

設問２

会員への事故対応の依頼に関する問題である。

クレジットカード情報が漏洩している場合、不正使用を防止するために、登録されたクレジットカードの停止および番号変更の手続きを会員に依頼する。求める答えはエとなる。

アの内容は事故発生を防止するために事前から依頼しておく内容である。

イの会員情報をマガジン購読の場合、商品購読の場合に分けて、異なるレベルで管理する

ことは好ましいことではない。

ウのＤ社が事故発生時、事故対応のために個人情報を利用することは好ましくない。

設問３

ネットワーク回線を二重化して負荷上昇への対応を行っても、ＳＱＬインジェクション攻撃を防ぐ対策にはならない。求める答えはウとなる。

設問４

ａは、セキュリティ考慮した設計および実装を行うために、セキュアプログラミングのルールを作成することが重要である。求める答えはオとなる。

ｂは暗号化によって、万が一情報の漏洩が発生しても、直ちに被害が発生しないようする。求める答えはイとなる。

ｃは、事故が発生したときの原因の分析には、アクセスログやエラーログの保管が必要である。求める答えはアとなる。