H24. 秋. セキュリティ

問4　セキュリティ事故の対応（情報セキュリティ）　(H24秋-FE 午後問4)

【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】

SQLインジェクション攻撃に関する問題である。全体的に，SQLインジェクション攻撃に対する知識がなくても，問題文の中でSQLインジェクションの手法に関する説明がなされているため，情報セキュリティに関する基本的な知識をもって，説明文をきちんと読めば解答できる。設問4は，情報セキュリティ対策の概要を理解しているとイメージしやすいが，理解不十分でも，空欄の前後にある記述に注目すれば解答できる。午後問題では，正解を導き出す記述が埋め込まれていることが多いので，それを活用するノウハウを修得したい。

［設問1］

SQLインジェクション攻撃とは，Webサイトの入力項目に対し，不正なSQL文を送り込むことによって，不正に情報を入手する攻撃である。例えば，パスワードを入力するテキストボックスに，「`xyz' OR 'a' = 'a`」と入力したとする。この場合，SQLインジェクション攻撃への対策を施していないと，次のように，条件が常に真となるSQL文になってしまう。

```
SELECT * FROM 会員 WHERE パスワード = 'xyz' OR 'a' = 'a'
```

この結果，パスワードを知らなくてもログインできるようになる。したがって，(イ)が正解である。なお，SQLインジェクション攻撃への対策として，「'」のような特殊な文字を使えないようにするといった対策を行うことが一般的である。

SQLインジェクション攻撃に対する知識がなくても，〔セキュリティ事故の発生〕の「利用者IDとパスワードの入力を行うログインの処理に不備があり，外部からSQLインジェクション攻撃を受けていた」という記述から，正解を特定できる。

ア：DNSポイズニングを利用したフィッシング攻撃の説明である。

ウ，エ：データベースの管理ツールや管理者のID，パスワードについて記述されているが，問題文にデータベースの管理ツールに関する記述はない。このような選択肢は，通常，正解にならないので，正解を選択する際参考にするとよい。こうした攻撃手法はデータベースサーバに特化した攻撃ではなく，名称も特にない。

［設問2］

セキュリティ事故発生時における会員への対策と対応に関する設問である。〔セキュリティ事故の発生〕に「クレジットカード情報が漏えいしていることも考えられる」と記述されている。こうした状況では，自社のシステムを守ることも重要だが，それ以上に流出してしまった情報による2次被害を防ぐことが最も重要である。不正利用を防止するため，クレジットカードの停止及び番号変更の手続を，早急に実施する必要がある。したがって，(エ)が正解である。

ア：パスワードを設定する条件としては，正しい記述である。しかし，SQLインジェクション攻撃では，設定したパスワードそのものを不正に入手，あるいはパスワードのチェックをすり抜けてしまう可能性があるため，不適切である。

イ：パスワードの変更を依頼することは，SQLインジェクション攻撃によってカード情報ではなく，ログイン用のパスワードが漏えいしてしまった場合の対応としては正しいが，これは商品の購入を行う会員だけでなく，全員に依頼すべきである。また，データベースを分離しても，不正なSQL文でアクセスするSQLインジェクション攻撃に対して，効果は期待できない。また，パスワードはデータベースに平文(ひらぶん)で格納することは推奨できるものではなく，ハッシュ値として格納するなど暗号化して格納することが一般的である。

ウ：個人情報の事故対応に関する規定を設けて，会員に同意してもらっても，情報を不正取得した攻撃者の行動はなんら制約を受けない。攻撃者はあくまでも第三者であるため，技術的な対策を行う必要がある。

［設問3］

SQLインジェクション攻撃は，Webサイトの入力項目に対し，不正なSQL文を送り込むことによって，不正に情報を入手する攻撃であるである。そのため，ネットワーク回線を二重化しても，SQLインジェクション攻撃を防ぐ対策にならない。したがって，(ウ)が正解である。なお，ネットワーク回線の二重化は，一般的に，信頼性向上のための対策であり，セキュリティ事故への対策として行うものではない。

［設問4］

SQLインジェクション攻撃への追加対策と，その他のセキュリティ対策に関する設問である。

・空欄a：空欄aの前後にある「セキュリティを考慮した設計及び実装を行うことで回避できる」，「アプリケーション開発時に脆弱性が作り込まれる可能性を減らす」という二つの記述がヒントになる。

　実装とは，プログラミングのことである。この記述から，セキュリティを考慮したプログラムを作成するようにすればよいことが分かる。したがって(オ)が正解である。

　ア，イ，ウ：アプリケーション開発時ではなく運用時の対策である。

　エ：SQLインジェクション攻撃ではなく，内部犯行に起因する情報漏えいを防ぐための対策である。

　カ：負荷分散装置は性能向上や信頼性向上に役立つが，SQLインジェクション攻撃のようにセキュリティホールを突いた攻撃に対する効果はない。

・空欄b：空欄bの直前に記述されている「データベースサーバへの不正アクセス対策」がヒントになる。さらに，〔会員情報の登録〕の前に記述されている「データベースサーバのデータは平文で保存」が決め手になる。したがって，(イ)が正解である。会員情報が暗号化されていれば，SQLインジェクション攻撃を受けても，会員情報が漏えいするリスクは大きく減少する。

　ア：セキュリティ事故発生時，ログを正確に分析するため，Webサーバとデータベースサーバの時刻を同期させることは望ましい。しかし，ここで問われているのは再発防止策であるため，適切ではない。

　ウ：インターネットから社内に対するフィルタリングが対象であれば，不正アクセス対策として，効果が期待できる。しかし，社内からのインターネット利用時にフィルタリングを実施しても，効果は期待できない。

　エ：共有IDを利用すると，利用者の特定が困難となり，不適切である。

　オ：RAID構成にすると，信頼性や性能は向上するが，不正アクセス対策とは関係しない。

・空欄c：空欄cの直前の「情報漏えいが発生した場合の原因の分析や犯人の追跡を行うための証拠の確保」という記述から，正解を導き出すことができる。原因の分析や犯人の追跡を行うためには，どのサーバにいつどのようなアクセスがあったのか，又は，どのようなエラーが発生したかなどを保管したログが必要になる。したがって，(ア)が正解である。その他の選択肢は，再発防止に向けた対策であり，事後の原因分析や追跡を行うための証拠の確保とは関係しない。