問1　情報セキュリティ事故と対策（情報セキュリティ）　(H30秋-FE 午後問1)

【解答】

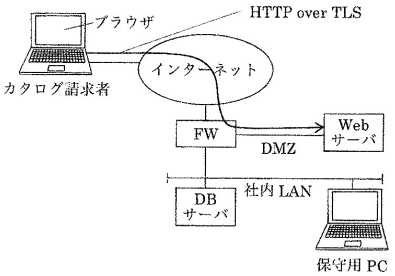
［設問1］　ウ
［設問2］　a－エ，b－ア，c－エ
［設問3］　イ

【解説】

公開サーバのWebアプリケーションソフト（本問ではWebアプリ）への攻撃，及びセキュリティ対策をテーマとした出題である。「SQLインジェクション」，「クロスサイトスクリプティング」，「WAF」などのセキュリティの専門的な言葉が数多く登場する。しかし，これらはいずれも基本情報技術者試験の出題範囲に含まれる用語である。なお，表1の「プレースホルダ」は，「?」などの特別な文字列を使ってSQL文を完成させるSQLインジェクション対策である。

この問題は，難易度は標準的と言えるが，たとえ難しい問題であっても，4択という利点を生かし，基礎知識を使って消去法で正解を導くテクニックも活用して，合格ラインを突破してほしい。

さて，設問の解説に入る前に，問題文から想定されるA社のシステム構成図を図Aに示す。構成図をイメージしながら設問を解くことは重要である。



図A　A社のシステム構成図

［設問1］

下線①は，「インターネット経由でSQLインジェクション攻撃を行い」とある。この攻撃の説明として適切な答えを，解答群の中から選ぶ。

SQLインジェクション攻撃では，攻撃者がWebアプリに対して，データベース操作の命令文（SQL文）を混入（インジェクト）したデータを入力することで，データベースを不正に操作する。したがって，（ウ）が適切である。

ア：攻撃者が，DNSに登録されているドメインの情報を改ざんして攻撃者のWebサイトに誘導する攻撃は，DNSキャッシュポイズニングである。

イ：「インターネット経由でDBサーバに不正ログインする」とあるが，A社のDBサーバは社内LANに接続されており，インターネットから直接アクセスできない。誤りである。

エ：「攻撃者が，インターネット経由で送信されている情報を盗聴する」とある。SQLインジェクション攻撃とは無関係である。盗聴をするには専用の盗聴ツールや暗号を解除する仕組みが必要である。

［設問2］

表1中の空欄に入れる対策を答える。

・空欄a：「SQLインジェクション攻撃からの防御」に関する対策を選ぶ。

SQLインジェクション攻撃は，データベース操作の命令文の組立てを，文字列連結を悪用して行われる。例えば，入力された「`' OR 1=1`」などの文字列をデータ操作の命令文の一部分にすることで，SQL文の`WHERE`句の結果を強制的に真にするといった手法である。そこで，文字列にエスケープ処理（文字列の変換）を施し，命令文ではなく単なる文字列にすることが有効な対策となる。したがって，（エ）が正解である。

ア：「Webサーバ内のファイル名を直接指定できないようにする」という対策は，ディレクトリトラバーサルへの対策である。

イ：SQLインジェクション攻撃は，Webサーバのメモリを直接操作されなくても発生し得る脅威である。一方で，Webサーバのメモリが直接操作されることによる攻撃としては，DoS攻撃や，root奪取が挙げられる。この対策はこうした攻撃に対して有効である。

ウ：SQLインジェクション攻撃は，Webページに不正な文字列を入力して攻撃が成立する。したがって，「Webページに出力する要素に対して，エスケープ処理を施す」ことは対策にならない。

・空欄b：「情報流出リスクの低減」に関する対策を選ぶ。

〔情報セキュリティ事故を踏まえたシステム面での対策〕で焦点になっているのは，カタログ請求者の情報流出であることを踏まえて考える必要がある。「カタログ請求者の情報の適切な保管期間を定め」，「保管期間を過ぎた時点でデータベースから消去」すれば，情報を保持する期間が短くなり情報流出のリスクが低減される。したがって，（ア）が適切である。

イ：「カタログ請求者の情報を，カタログ送付後に直ちに，データベースから消去」してしまうと，〔カタログ請求者の情報の登録〕の要件が満たされない。具体的には，カタログ請求者が別のカタログを請求したいときなどに，登録した電子メールアドレスとパスワードによるログインができない。

ウ：「電子メールにディジタル署名を付ける」ことは，データの改ざんの検知などには有効であるが，データを暗号化するものではないため，情報流出リスクの低減にはつながらない。

エ：「情報を定期的にバックアップする」ことは，データの破壊などによる対策にはなるが，情報流出リスクの低減にはつながらない。

・空欄c：「情報流出の原因と流出した情報の範囲の特定」に関する対策を選ぶ。

「データベースへのアクセスログを取得」すれば，どこからのアクセスなのか，いつ流出したか，どの範囲のデータにアクセスしたのかなどが分かる。その結果，情報流出の原因と流出した情報の範囲の特定につながる。したがって，（エ）が適切である。

ア：保守用PCを必要なときだけ起動しても，情報流出の原因特定などにはつながらない。

イ：インストールするミドルウェアを必要最低限にすれば，流出するリスクが低減するかもしれない。しかし，情報流出の原因特定などにはつながらない。

ウ：ハードディスクのデフラグメンテーションによって，処理のパフォーマンス向上は期待できる。しかし，情報流出の原因特定などにはつながらない。

［設問3］

クロスサイトスクリプティングなどの攻撃の対策として適切な答えを選ぶ。

Webアプリでは，その入力データに不正な通信が含まれる場合に，通信を遮断したり，出力内容をマスキングしたりすることで，情報流出を防ぐという対策が有効であるが，これを装置（あるいはソフトウェア）として行うのがWAF（Web Application Firewall）である。したがって，（イ）が適切である。

ア：「DBサーバを，Webサーバと同じく，DMZに設置する」と，攻撃者がDBサーバに直接アクセスできるようになる。その結果，攻撃されるリスクが増えてしまう。

ウ：「Webサーバを増設して冗長化」すれば，可用性の向上にはつながるが，情報流出を狙った攻撃の防御策にはならない。

エ：保守用PCのログインパスワードを推測が難しい複雑なものにすれば，保守用PCへの不正ログインへの有効な対策となり得る。しかし，Webサーバへ直接攻撃を仕掛けるクロスサイトスクリプティングの対策にはならない。