●平成27年度春期

午後問題 解答・解説

問1　インターネットを利用した受注管理システムのセキュリティ（情報セキュリティ）（H27春-FE 午後問1）

【解答】

［設問1］　イ
［設問2］　a－イ，b－ウ
［設問3］　ウ
［設問4］　イ

【解説】

インターネットに公開するサーバのセキュリティ対策に関する問題である。最近ではサイバー攻撃や標的型攻撃，ホームページ改ざんなどの事件が増えている。そのような事件で被害を受けると，問題文にあるように自社だけでなく取引先にも損害を与える可能性がある。この設問で問われている基本的なセキュリティ対策は，ITに携わる人であれば，誰もが知っておきたい内容であり，ぜひとも正解したい。

幅広い攻撃手法の特徴やその対策が問われており，難しかったと感じる人も多かったと思う。覚えるべきセキュリティの用語はたくさんある。無理やり覚えようとするよりも，日ごろの業務やニュースなどを見聞きした際に，情報収集する習慣を身に付けると，覚えやすくなるだろう。

［設問1］

取引先PCからWebサーバにアクセスするときに，HTTPS通信が行われる区間について問われている。Webサーバに関する知識がある人であれば，すぐに答えが分かったかもしれない。しかし，仮に知識ベースで答えが分かったとしても，問題文に制約がある可能性がある。問題文と照らし合わせて解答を導き出してほしい。

今回は，問題文の次の部分にWebサーバに関する知識が乏しい人にとってのヒント，逆に詳しい人にとっては制約事項が記載されている。「RPSには，ディジタル証明書を設定しておく。受注管理システムを利用する取引先の担当者は，取引先PCのブラウザからRPSを経由して受注管理アプリケーションにアクセスし，ログイン画面で利用者IDとパスワードを入力してログインする。その際，取引先PCのブラウザからの通信には，HTTP over SSL/TLS（以下，HTTPSという）を使用する。RPSではディジタル証明書を使って，HTTPSからHTTPにプロトコルを変換する」

まず，RPSについて補足する。RPSとは，「Webサーバを使ったシステムにおいて，インターネットから受け取ったリクエストをWebサーバに中継する仕組み（平成21年秋NW本試験午前II 問17より）」である。このとき，RPSでSSL通信を紐解く役割をもつことが多い。この知識をもった上で，前記の問題文を見る。取引先PCからRPS（リバースプロキシサーバ）にHTTPSで通信し，RPSでHTTPに変換されることが分かる。つまり，インターネット側からK社内のネットワーク内に設置されたWebサーバに向かう通信は，RPSを経由することになる。このとき，表2の経路番号1の「取引先PCとFW3との間」，2の「FW3とFW1との間」，3の「FW1とRPSとの間」までがHTTPSである。参考までに，4の「FW1とFW2との間」と5の「FW2とWebサーバとの間」はHTTPである。

したがって，経路番号1，2，3の（イ）が正解である。

［設問2］

Z社からの指摘事項にある空欄を埋める問題である。この内容は，各種攻撃手法の特徴や原因に関する知識を前提としており，これらを押さえていれば，答えられる内容になっている。

・空欄a：問題文には「受注管理アプリケーションには，想定していない操作をDBサーバに実行させて，DBに不正アクセスするような［　a　］」とある。ヒントは“DB”というキーワードである。解答群の中で，DB（データベース）に対する攻撃は選択肢（イ）の「SQLインジェクション」である。SQLインジェクションは，悪意ある入力データを送りこむことで，データベースのデータを改ざんしたり不正に情報取得したりする攻撃である。したがって，（イ）が正解である。

・空欄b：空欄bを含む文には「攻撃者によってWebページ内にスクリプトが埋め込まれてしまう［　b　］の脆弱性」とある。ヒントは“スクリプト”というキーワードである。Webページにスクリプトを埋め込む攻撃は「クロスサイトスクリプティング（XSS）」と呼ばれる。クロスサイトスクリプティングは，クロスサイトとあるように，一つのサイトではなく複数のサイトにまたがった攻撃である。この点が，この問題文にある，「取引先の担当者が他のWebサイトに誘導されて」という内容に合致する。したがって，（ウ）が正解である。

参考までにその他の選択肢を確認する。（ア）のDoS（Denial of Service）攻撃とは，その言葉が意味するとおり，「Service（サービス）のDenial（拒否）」をすることである。サーバのサービスが提供できないようにすることを目的とした攻撃である。そのためには対象サーバに異常な負荷をかけたり，ソフトウェアのバグを突いて，システムを異常停止させたりする。

（エ）の辞書攻撃と（キ）のブルートフォース攻撃は，不正ログインのためのパスワードクラックの方法である。ブルートフォース攻撃は，いわゆるログイン情報に対する総当たり攻撃である。一方の辞書攻撃は，辞書の言葉を組み合わせて効率的にパスワードを破ろうとする攻撃である。

（オ）のディレクトリトラバーサルは，管理者が意図していないパスを指定することで，本来は許されないファイルに不正にアクセスすることである。トラバーサル（traversal）とは「横断」という意味で，ディレクトリに関する不正な横断と考えればいいだろう。

（カ）のトラッシングとは，スキャベンジングと同じ意味で，ゴミ箱に捨てられた機密情報や個人情報を盗むソーシャルエンジニアリングの手法の一つである。

（ク）のポートスキャンとは，サーバなどで使用しているサービス（ポート番号）を全て探索することである。攻撃をしかける前段階の処理で，どんな攻撃ができるかを探すために行われる。

［設問3］

下線①は表1の指摘事項「取引先の担当者がWebサーバ上の任意のファイルをダウンロード可能である」に関する原因「受注管理アプリケーションでのファイルのダウンロード処理に問題がある」にかかっている。取引先の担当者は，任意のファイルをダウンロードできてはいけない。アクセス権が許可されたものに限定すべきであり，今のままではダウンロード処理に問題があると言わざるを得ない。

そこで，その対策を解答群から選ぶ。

一般的な対策には，「ダウンロード可能なファイルの種類を限定させる」，「ファイルのパーミッションを適切に設定する」，「取引先ごとにフォルダを分ける」などがある。解答群と比較すると，（ウ）が「取引先ごとにフォルダを分ける」に該当する。したがって，（ウ）が正解である。ポイントは，「取引先ごとに決められたフォルダ内」に限定してダウンロードの処理をさせていることである。

他の選択肢も見てみよう。（ア）と（イ）は，絶対パスと相対パスの違いはあるが，どちらの場合も「該当ファイルが存在」すればダウンロード処理ができてしまう。つまり，アクセス権がなかったとしても，ディレクトリトラバーサルの攻撃によって不正にダウンロードが可能である。よって不正解である。

（エ）も不適切である。まず，「Webサーバ上の全てのフォルダ構成及びファイルを表示」させてしまうと，他の取引先に向けたデータファイルのほか，サーバの設定ファイルなども見られてしまうため，セキュリティ上問題がある。

［設問4］

問題文の下線②には，「取引先の担当者がログイン時にパスワードを連続して間違えても利用者IDがロックされない」とある。この脆弱性から考えられるセキュリティ事故を解答群から選ぶ。

セキュリティ対策の観点から，パスワードを連続して間違えた場合，アカウントをロックするべきである。正規の利用者なら連続してパスワードを間違えることが少ない。しかし，悪意のある攻撃者であれば，パスワードを知らないことから，連続して間違えることがある。よって，攻撃者がパスワードの候補を次々と入力してログインしようとする攻撃には，アカウントロックが有効である。ちなみにこの攻撃が，設問2の選択肢にあるブルートフォース攻撃である。

この問題では，アカウントをロックしないことによるセキュリティ事故を答えるものである。したがって，（イ）の「パスワードの候補を自動で次々と入力するプログラムを利用することで，ログインできてしまう」が正解である。

なお，他の三つの選択肢は，いずれもパスワードを知っていることを前提とした攻撃内容である。パスワードを連続して間違えることもなく，利用者がロックされることもない。このため，アカウントロックはこれらの攻撃に対する対策にはならない。