平成１９年度　春期　テクニカルエンジニア（情報セキュリティ）　午後Ｉ　解答例

この解答例は、独立行政法人 情報処理推進機構　情報処理技術者試験センターが公表しているものです。著作権は、同センターにありますので、その点ご注意ください。

問１

出題趣旨：

情報システムの構成要素は多岐にわたるが，中でも顧客の要求に応じて開発されるアプリケーションプログラムのセキュリティ脆弱性を少なくすることは、ソフトウェアエンジニアリングとしても重要な課題である。

本問では，システム開発の過程で脆弱性低減のために実施すべき作業についての知識を確認した上で，脆弱性を発生させないための具体的なプログラミングにおける技術的対策に関する知識・能力を問う。

設問１

(1) a ― スタック　　b ― val2　　c ― val1
　　d ― 権限昇格　　e ― 関数呼出し　　f ― ヒープ

設問２

(1) ア ― 128

(2)・攻撃者に読取り権限のない任意のファイルの内容が表示されてしまう。
　　・プログラムが意図したファイル以外の任意のファイルの内容が表示されてしまう。

(3)・最初のコマンドライン引数が 128 バイト未満であるという条件を論理積として加える。
　　・`if (argc > 1 && strlen(argv[1] < 128 ) {`

設問３

・変数と戻りアドレス格納部分の間に特別な数値をあらかじめ埋め込んでおき，この数値がプログラム実行時に変更されていないことを確認する。
・変数と戻りアドレス格納部分の間に乱数値をあらかじめ埋め込んでおき，この乱数値がプログラム実行時に変更されていないことを確認する。

講評：

問 1 では，C++言語におけるセキュアプログラミングについて出題した。全体として，正答率は低かった。

設問 1 では，d の正答率が低かった。バッファオーバフローが起きると，権限昇格やシェルコードの実行などが起こり得ることを十分に認識してもらいたい。

設問 2 では，バッファオーバフローの発生の仕組みが理解できていないと思われる解答が散見された。特に (2) で，`afile` の内容の表示についてだけ記述した解答が多かった。コマンドライン引数を変更すれば，任意のファイルの内容を表示できることに気づいてほしかった。

設問 3 も正答率が低かった。セキュアプログラミングだけでなく，コンパイラや実行環境による検知と防止機能を併せて使用することによって，バッファオーバフローに対する多層防御が図れることを理解してほしい。

問２

出題趣旨：

ネットワーク再構築において，ネットワークセキュリティの確保は避けて通れない。ネットワークセキュリティには，ネットワーク境界を守るファイアウォール（FW），不正な通信を監視する IDS，監視に加えて遮断まで行う IPS などの対策がある。

本問では，FW のフィルタリングルールの設計，IDS や IPS に関する技術的な知識，導入検討における判断力などを問う。

設問１

（1）a － 任意　又は　社内 LAN　　b － 任意
（2）c － 拒否

設問２

（1）d － SSH
（2）パスワードが平文で送信されるから
（3）DMZ 上のサーバを踏み台にして，社内 LAN にアクセスする攻撃

設問３

（1）e － 統計
（2）下線⑤－正常なものまでも攻撃として検知してしまうエラー
　　下線⑥－検知すべき攻撃を検知できないエラー
（3）・パケットのヘッダ情報だけで攻撃か否かを判断しているから
　　・ペイロードの内容を見ていないから
（4）攻撃を発見してから防御手段が有効となるまでの間に通過したパケットによる攻撃が，成功する場合があるから

講評：

問 2 では，ネットワークのセキュリティについて出題した。全体として，正答率は高かった。

設問 2（3）は，正答率が低かった。“ウイルスによる攻撃”という解答があったが，本文中の下線②にある“インターネットからの不正なアクセス”とはいえない。DMZ 上のサーバは攻撃を受けやすく，管理者権限を奪われて社内 LAN が攻撃されるリスクがあることを認識してもらいたい。

設問 3（2）では，“フォールスポジティブ”と“フォールスネガティブ”を取り違えている解答が見られた。それぞれの特徴を把握して，正確に理解しておいてほしい。

設問 3（4）では，IDS が FW と連携する機能として，TCP のリセットパケットの送出や FW のフィルタリングルールの動的な追加などに気づいてほしかった。FW との連携における問題点ではなく，IDS や FW 単独の問題点を指摘した誤った解答も見受けられた。また，単に“タイムラグがある”というだけではなく，タイムラグがあることによってどのようなリスクが発生するのか，まで解答に含めてほしかった。

問３

出題趣旨：

近年，企業の社会的責任（CSR）がますます重要視されてきている。企業における多くの情報システムでセキュリティ上の機能として利用者の認証アクセス制御は行っているが，監査ログのセキュリティ対策は十分に行われていない。

本問では，監査ログの設計・開発を主題とし，監査ログの設計要件から監査ログメッセージの正当性を実現するために、ハッシュ関数，タイムスタンプ技術などの技術的対策を適切に実施する能力を問う。

設問１

（1）a ― 役割ベース　又は　ロールベース

（2）盗聴によるリプレイ攻撃を防ぐことができるから

設問２

（1）・利用者の認証やアクセス制御のすべての動作を記録し，その記録の有効性を確認できる。
・後日の監査において IT による統制が正しく遂行されたことを確認できる。

（2）b ― 役割　　c ― 権限　　※順不同

（3）監査ログデーター監査ログデータが改ざんされていないこと
複数の監査ログレコードー・監査ログレコード間の順序性
・監査ログレコードの抜けがないこと
・監査ログレコードが挿入，削除されていないこと

設問３

（1）d ― ハッシュ値
e ― タイムスタンプ局　又は　TSA　又は　タイムスタンプオーソリティ

（2）・監査ログバックアップファイルがタイムスタンプ発行時に存在していたこと
・監査ログファイルがタイムスタンプ発行時に存在していたこと

講評：

問 3 では,採取するログ情報の証拠能力に関わるセキュリティ技術について出題した。全体として，正答率は低かった。

設問 1 は，正答率が低かった。パスワード攻撃は現実にも多く発生しており，想定される脅威や，類推されにくいパスワードにするための手段に関する基礎知識をもってほしい。

設問 2（1）では，“イベントを記録する”のように監査ログの機能を記述した解答が多かった。“記録されたイベントによって発生した事実を確認できる”ことが監査ログの役割であり，目的である。技術を理解するだけでなく，対象業務システムにおいて，その技術が何のために必要であるか，どのような効果を業務システムにもたらすかを理解することが求められる。

設問 3 も，正答率が低かった。時刻の保証が，その時点での情報の存在証明になるという基本原理を理解しておいてほしい。

問４

出題趣旨：

セキュリティ機能を具備したシステムの設計においては，様々なアルゴリズムを適切に選択し，使用する必要がある。

本問では，社内アンケートシステムを題材に，公開鍵暗号に関する基礎知識，及びプライバシ保護を伴うセキュリティシステムの方式設計能力を問う。

設問１

（1）a ― 秘匿　又は　隠ぺい　又は　読めなく
b ― 8

（2）全通りの回答について提出ファイルを作成し，回答者のファイルと比較する。

設問２

(1) ①②
- 集計担当者以外はアンケートの回答を閲覧できないこと
- 従業員が匿名でアンケートに回答できること
- 部門の担当者が提出漏れをチェックできること
- アンケートの回答を１人１回答に制限できること

(2) シリアル番号とその署名は各回答者しか知り得ず，また，シリアル番号の偽造は困難であるから

設問３

(1) シリアル番号から回答者を特定できないようにする必要があるから

(2)
- 同じシリアル番号の回答がないかどうかをチェックする。
- 使用していないシリアル番号の回答がないかどうかをチェックする。

講評：

問 4 では，社内のアンケートシステムにおける暗号方式について出題した。全体として，正答率は低かった。

設問 1（2）では，“線形攻撃を行う”といった誤った解答が見られた。対象業務の特性を正しく把握した上で，暗号技術を適切に利用することを理解してほしい。

設問 2（2）は，“各回答者しか知り得ない”，“署名が偽造できない”のどちらか一方だけを記述している解答が多かった。また，“本人しかアンケートファイルを開けないので”という解答が多かったが，自分のアンケートファイルから得られる情報を基に，他人のアンケートファイルを偽造する攻撃を防止する必要性があることを理解してほしかった。

注：この解答例に関するメールでのご質問には、応じかねます。あしからずご了承ください。