平成２１年度春期　情報セキュリティスペシャリスト　午後Ⅰ試験　解答速報

（株）アイテック　情報技術教育研究グループ　2009,4,21

発表

問１　パケットログ解析

【解答例】

［設問１］

(1) a：(r)

(2) b：ウ　　c：詐称（または，偽装）

(3) d：イ

(4) e：(Ⅰ)　　f：(Ⅴ)

修正：再帰的な問合せは内部に限定し，外部からの問合せを受け付けないように設定する。

［設問２］

(1) 不審な通信挙動：DNS クエリのあて先が，インターネット側になっている。

g：エ

(2) ア，ウ

［設問３］

(1) DNS クエリなしにあて先 IP アドレスをインターネット側にしているもの

(2) ウイルス対策ソフトの配布サイトにアクセスするパケット

問２　ソフトウェアの脆弱性への対応

【解答例】

［設問１］

(1) 不正な OS コマンドが実行されることによって，システムの機能が全面的に停止する可能性があるから。

(2) X-Sender で任意の OS コマンドが実行される（または，Exploit コードが公開されている）。

［設問２］

(1) input

(2) 利用者が入力した情報が URL のクエリストリングとして，そのまま Web ブラウザのキャッシュや履歴に残ってしまうから。

(3) HTTP ヘッダに X-Sender という文字列が含まれているもの

(4) 記号：(f)

対策の内容：Web サーバプログラムを一般ユーザ権限で動作させる。

［設問３］

(1) b：負荷分散の対象から外す

(2) 修正プログラム適用後の Web サーバの動作を検証しておくこと

問３　アプリケーション開発時の脆弱性対策

【解答例】

［設問１］

(1) ログイン日と会員番号を適当に組み合わせてセッション識別子を生成して Web サーバにアクセスする。

(2) 行番号：24

修正方法：URL リンク中の絶対パスを相対パスに修正する（または，http という文字列を https に修正する）。

(3) ①　A タグの href 属性

②　IMG タグなどの src 属性

［設問２］

(1) エ

(2) パスワードにユーザごとに異なるランダムなソルト値を付加してハッシュ値を生成する。

問４　情報システムの特権管理

【解答例】

［設問１］

(1) イ

(2) a：特権 ID の共用

(3) b：特権 ID のログ監査

［設問２］

(1) ア

(2) c：syslog

(3) d：ほかのサーバ管理者がログインできないようにログサーバ専用の ID を設定

(4) 特権 ID によるログインが拒否されたとき

(5) 下線④：特権 ID の不正な使用を監視していることを周知するため。
下線⑤：特権 ID 使用時のアラート発生の意図的な回避を防止するため。

(6) 確認する内容：誰が，いつ，どのデータに対し，どのような操作を行ったかについての改ざんが行われていないこと
立証としようとしていること：財務内容に関する電子データとしての証拠性を保証すること