Copyrights by ITEC,inc. 2022

令和４年度秋期　情報処理安全確保支援士　午後Ⅰ試験　解答速報

（株）アイテック　IT 人材教育研究部　2022.10.12 発表

問１　IoT 製品の開発

【解答例】

［設問１］

(1) a：DNS キャッシュポイズニング

(2) b：エ

(3) 次のうち，1 点が指摘されていればよい。

・トランザクション ID が名前解決要求の ID と一致する。

・権威 DNS サーバの DNS 応答よりも早く到達する。

(4) W サーバのサーバ証明書を検証し，当該証明書を用いて W サーバを TLS 認証する。

(5) c：コードサイニング

［設問２］

d：パラメータ中の特定の文字列を OS コマンドとして実行して

［設問３］

(1) 攻撃リクエストを submit する HTML 中のスクリプトを利用者の Web ブラウザに実行させる。

(2) e：予測が困難である

［設問４］

脆弱性 A：ア

脆弱性 B：オ

Copyrights by ITEC,inc. 2022

問２　脆弱性に起因するセキュリティインシデントへの対応

【解答例】

［設問１］

a：a3.b3.c3.d3

［設問２］

(1) run プロセスの親プロセスが BSoftMain という T ソフトのプロセスだから。

(2) b：13:04:32　　c：13:05:50

d：a8.b8.c8.d8　　e：LDAP　　f：JExp

［設問３］

(1) 認証前のアクセスにもログ出力処理の対象となる文字列が含まれるから。

(2) 会員サーバから攻撃者が用意したサーバへの通信は FW によって拒否されるから。

［設問４］

g：予約サーバ

h：SNS 投稿用のサーバ

i：全て

問３　オンラインゲーム事業者でのセキュリティインシデント対応

【解答例】

［設問１］

(1) a：376

(2) prog プロセスの実行ファイルを取得して実行する。

(3) b：一時ディレクトリのログ

(4) ゼロデイ攻撃

［設問２］

(1) ステータスコード及びレスポンスヘッダの情報

(2) 上書きされた可能性のあるゲームイメージを削除する。

［設問３］

(1) c：a3.b3.c3.d3

(2) d：エ

(3) 攻撃者がサーバの IP アドレスを変更した場合

(4) e：オ

以上