

令和3年度春期 情報処理安全確保支援士 午後Ⅱ試験 解答速報

(株) アイテック IT人材教育研究部 2021.4.21 発表

問1 インシデント対応体制の整備

【解答例】

[設問1]

- (1) 実在する利用者IDとパスワードのリストを転用して、標的サイトにログイン試行する攻撃
- (2) 他のサービスで設定しているパスワードは通販サイトに設定しないこと
- (3) 接続元IPアドレスやUser-Agentヘッダの値を用いるリスクベース認証を実装する。
- (4) a : タイムゾーン
- (5) b : 9

[設問2]

データ受渡しに用いるUSBメモリに侵入し、さらに管理用PCを経由して店舗管理サーバへ侵入する。

[設問3]

- (1) c : オ
- (2) d : イ e : カ f : ウ

[設問4]

- (1) 5
- (2) 当該ファイルの性質として、参照には管理者権限が必要だが、脆弱性Mだけの悪用ではOSの一般利用者権限でコマンドが実行されるから。
- (3) R1サーバの/etc/hosts.allowファイルのSSH接続元の設定を全てに変更する。
- (4) 24
- (5) FW2において、開発用システムの各サーバへのSSH接続及びHTTP接続は、V社及びN社だけを接続元として許可するように設定変更する。

[設問5]

複数の脆弱性を組み合わせて悪用される可能性の観点

問2 クラウドセキュリティ

【解答例】

[設問1]

- (1) オ
- (2) 多くの個人所有機器を C 社内 LAN に接続させたことによって、DHCP サーバがリリース可能な IP アドレスが枯渇する問題
- (3) 稼働させたまま行う方法：調査用の PC から DHCPDISCOVER を送信し、UTM の DHCP サーバ以外からの応答の有無を確認する。
停止させて行う方法：調査用の PC から DHCPDISCOVER を送信し、応答の有無を確認する

[設問2]

サービス R にこれまで投稿したメッセージやアップロードしたファイルの内容

[設問3]

- (1) a : C-PC b : AP
- (2) c : エ

[設問4]

- (1) 顧客への提案や企画の立案時に情報を収集する業務
- (2) 2
- (3) 1
- (4) 記号：ウ
方法：デジタル証明書のクレデンシャルを検証する。

[設問5]

- (1) ISMS クラウドセキュリティ認証
- (2) d : 4

[設問6]

- (1) デジタル証明書と秘密鍵が抽出できないように設定する。
- (2) P ソフトを、一般利用者権限では無効化することができないように設定する。

以上