

テクニカルエンジニア(情報セキュリティ) 解答例

【午 後】

問 1 (配点 50 点)

設問 1 (12 点:2 点×6)

- a:スタック
- b:val2
- c:val1
- d:権限昇格
- e:関数呼出し または サブルーチン または 関数
- f:ヒープ

設問 2 (26 点:(1)6 点,(2)8 点,(3)12 点)

- (1) ア:128
- (2) 一般利用者の権限でシステム管理者所有のファイルを参照でき、機密性を維持できない
- (3) コマンドライン引数の任意の文字列が 128 バイト未満の場合に val2 へのコピーを許可する条件を加える
(プログラムコードで示す場合) `if(argc > 1 && strlen(argv[1]) < sizeof(val2)) {`

設問 3 (12 点)

変数領域と戻りアドレス領域の間にバッファオーバーフロー検知用の値を挿入し、呼び出した関数から戻る際にその値が変更されていないことを確認する

問 2 (配点 50 点)

設問 1 (6 点:(1)2 点×2,(2)2 点)

- (1) a:任意
b:任意
- (2) c:拒否

設問 2 (14 点:(1)2 点,(2)4 点,(3)8 点)

- (1) d:ssh
- (2) パスワードが平文のまま送信されるから
- (3) インターネットから DMZ 上のサーバを踏み台にして社内 LAN に侵入する攻撃

設問 3 (30 点:(1)2 点,(2)下線 5 点,下線 5 点,(3)6 点,(4)12 点)

- (1) e:統計
- (2) 下線 : 正当な通信パケットを攻撃パケットと判断してしまうエラー
下線 : 攻撃パケットを正当な通信パケットと判断してしまうエラー
- (3) http, https, telnet による攻撃が可能だから
- (4) IDS で攻撃を検知してから連携によって FW がその攻撃の防御を開始するまでの間に行われる最初の攻撃を防御できないから

問3 (配点 50 点)

設問1 (8 点:(1)2 点,(2)6 点)

- (1) a:ロールベース
- (2) パスワードのリプレイアタックを防止できるから

設問2 (30 点:(1)10 点,(2)2 点×2,(3)項目 C_i 8 点,項目 C_{i-1} を利用 8 点)

- (1) アクセス制御による安全性維持の運用状況を監査するために必要かつ十分な情報を保全し提供する
(別解) アクセス対象情報に誰がいつどのような権限でアクセスしたのかを追跡可能にする証跡を提供する

- (2) b:役割
c:権限

(b,C は順不同)

- (3) 項目 C_i :監査ログデータが改ざんされていないこと
項目 C_{i-1} を利用:監査ログレコードの挿入や消去が行われていないこと

設問3 (12 点:(1)2 点×2,(2)8 点)

- (1) d:ハッシュ値 または ダイジェスト
e:タイムスタンプオーソリティ または 時刻認証局 または タイムスタンプ局 または TSA
- (2) タイムスタンプ日時でのバックアップファイルの存在とその内容が完全であることの証明

問4 (配点 50 点)

設問1 (12 点:(1)2 点×2,(2)8 点)

- (1) a:秘匿
b:8
- (2) 攻撃者が入手した暗号化された回答内容と,すべての回答パターンの暗号文を照合する

設問2 (22 点:(1)6 点×2,(2)10 点)

- (1) ・1 人 1 回答というルールを守りつつ匿名でアンケートに回答できること
・限られた集計担当者以外の従業員に回答内容が漏れないようにすること
- (2) なりすましやすり替えにはシリアル番号とその署名が必要で,その復号は回答者の秘密鍵でしかできないから

設問3 (16 点:(1)8 点,(2)8 点)

- (1) 集計担当者がシリアル番号から回答者を特定することを困難にするから
- (2) 以前配布したシリアル番号と署名が再使用されていないかをチェックする

【午後】

問1 (配点 200 点)

設問1 (20 点:10 点×2)

- a:物理
- b:論理 または 技術

設問2 (50 点:(1)20 点,(2)30 点)

- (1) 機密情報や極秘情報は、必要最小限の運用管理者だけが入室可能なエリアに保管する
- (2) 業務アプリケーション管理者が DB サーバを直接操作できないようになり、機密情報や極秘情報の保護レベルが向上する

設問3 (50 点:(1)30 点,(2)20 点)

- (1) ログに記録された DB ユーザ ID は複数の利用者で共用されており、アクセス元の個人を特定できないから
- (2) Web サーバ A でログ取得を行い、業務ユーザ ID を記録する

設問4 (80 点:(1)20 点,(2)20 点,(3)10 点×4)

- (1) レコードを順次読み込み、変更前の鍵で復号し、変更後の鍵で暗号化し、順次書き込む
- (2) データ移行時間が計画停止時間は 2 時間以内という品質要件を満足していないから

(3)

テーブル名	キー項目	データ項目
変換 TBL	口座番号	内部 ID
検索 TBL_A	内部 ID	カナ姓
検索 TBL_B	内部 ID	カナ名
顧客 TBL	内部 ID	暗証番号,住所,電話番号,生年月日,勤務先

問2 (配点 200 点)

設問1 (20 点:(1)5 点×2,(2)10 点)

- (1) a:停止
b:アクセスログ または ログ または 通信ログ
- (2) 利用者 ID の確認だけでは本人確認として不十分であること

設問2 (65 点:(1)5 点×3,(2)10 点,(3)15 点,(4)モード 5 点,採用理由 20 点)

- (1) c:IKE
d:ESP
e:Diffie-Hellman
- (2) 事前共有鍵を設定した相手であることを認証すること
- (3) 鍵共有アルゴリズムの出力値を計算するために必要な一時鍵情報がないから
- (4) モード:アグレッシブモード
採用理由:動的 IP 割当てを利用する環境なので、端末の IP アドレスを ID に使用できないから

設問3 (25点:(1)5点×3,(2)10点)

(1) f:バイOMETリクス または 生体

g:本人

h:他人

(2) 紛失物と共有する事前共有鍵を無効にする

設問4 (35点:(1)15点,(2)20点)

(1) 本社にリモートアクセスできない環境ではデータを利用できなくなる

(2) 認証デバイスに格納された事前共有鍵を活用してハードディスク全体に対するデータ暗号化を行う

設問5 (55点:(1)15点,(2)原因15点,理由10点,(3)15点)

(1) メールを送信元IPアドレスがプロキシモードでFWに変更され,社外からのメールであることを認識できないから

(2) 原因:不正メールであることに気付かずに,指示に従ってソフトウェアをダウンロードし実行した後,PCを再起動したこと

理由:SMTP以外のプロトコルを用いた通信にFWのウイルスチェック機能が働かないから

(3) 社内ネットワークのパッチサーバ以外からセキュリティパッチをダウンロードして適用しないこと

以上