

## 令和 3 年度 春期 情報処理安全確保支援士

### ＜午後 I 解答・解説＞

#### ＜問1＞ 認証システムの開発

##### 【試験センターによる解答例】

- (1) 多要素認証の実装を S サービス側に用意しなくてよい。(25 字)
- (2) T サービスの障害時に S サービスを利用できない。(23 字)
- (3) a : ア  
b : イ  
c : ウ
- (4) α : (え)

#### ●設問 1

##### ＜解説＞

- (1) S サービスは、前回の脆弱性診断で指摘を受けた多要素認証への対応が課題となっていた。T サービスとの ID 連携を利用することにより、S サービス側で多要素認証の機能を実装せずとも、新規登録の S 会員に対しては多要素認証に対応したサービスを提供することが可能となる。
- (2) T サービスと ID 連携することにより、S サービス単体でのサービス提供ではなくなるため、可用性の面で、T サービスの障害時には S サービスを利用できないという欠点がある。
- (3) 図 2 のシーケンスにあるように、アクセスする側が S サービスであり、アクセス対象となるリソースを提供するのが T サービスである。図 3 に示す権限を S サービスに与えるのは利用者である。したがって、a にはアの“S サービス”、b にはイの“T サービス”、c にはウの“利用者”が入る。
- (4) 図 2 のシーケンスのあるように、利用者は S サービスに与える権限を (え) の通信の際に確認している。

●設問 2

【試験センターによる解答例】

- (1) d : ウ  
e : ア
- (2) ファイルのアップロード : 攻撃者  
ファイルのダウンロード : 攻撃者
- (3) β : (い)  
γ : (か)

<解説>

- (1) 図 2 のシーケンスと対比してみるとよい。□ d □ の直前に T サービスから認可コードが送られてきているので、攻撃者はそれを利用者に送ることで、図 2 の (お) と (か) のシーケンスを再現する。その後、図 2 の (き) と同様に S サービスから T サービスにアクセストークンの要求が行われる。したがって □ d □ にはウの“認可コード”、□ e □ にはアの“アクセストークンの要求”が入る。
- (2) 図 4 のシーケンス Xにあるように、T サービスとの間で認証・認可を行っているのは攻撃者であり、利用者ではない。したがって、S サービスへのファイルのアップロード、ダウンロードともに、T サービスの攻撃者のアカウントによって行われる。
- (3) state パラメタは、S サービスが利用者とのセッションの正当性を確認するために使用する。図 2 のシーケンスで S サービスが利用者に state パラメタを送信できるのは (い) であり、その後 S サービスが利用者から state パラメタを受信できるのは (か) である。

●設問 3

【試験センターによる解答例】

- (1) (エ)
- (2) S 認証モジュールに利用者 ID とパスワードを登録していない S 会員 (31 字)

<解説>

- (1) 図 2 の注記にあるように、S サービスは T サービスとの ID 連携によって、S 会員登録希望者による利用の初回に S 会員登録希望者がログイン中の T サービスから取得したアカウント名 (T-ID) を S サービス内に登録する。したがって、図 3 の中で必要最小限の権限に該当するのは (エ) の利用者のアカウント名、電子メールアドレスなど登録情報を取得する権限である。
- (2) T サービスに深刻な脆弱性が報告された場合には、T サービスとの ID 連携を一時的に停止し、S 認証モジュールだけで認証することになる。そうなった場合には、S 認証モジュールに利用者 ID とパスワードを登録していない S 会員 (T サービスのアカウントで S サービスを利用している S 会員) は S サービスを利用できなくなる。

●設問 4

【試験センターによる解答例】

T サービスで認証された S 会員の T-ID が、S サービス内に登録されていることを確認する。(43 字)

<解説>

S 認証モジュールを停止した後は、全ての S 会員が T サービスとの ID 連携によって認証を行う方式となる。前述の図 2 の注記にあるように、T サービスとの ID 連携においては、S 会員登録希望者がログイン中の T サービスから取得したアカウント名 (T-ID) を S サービス内に登録する。したがって、S サービスは、T サービスで認証された S 会員の T-ID が、S サービス内に登録されているのを確認することによって S 会員を認証する。