

平成 31 年度 春期 情報処理安全確保支援士試験 解答例

午後 I 試験

問 1

出題趣旨	
Web サービスには、Web ブラウザから利用するものだけでなく、サービスの機能の一部をプログラムから Web API として利用するものもある。ある Web サイトから読み込まれたスクリプトが異なるオリジンの Web API にアクセスする場合、Same-Origin ポリシによって制限される。CORS (Cross-Origin Resource Sharing) を利用すれば制限を回避することができるが、セキュリティを考慮して実装する必要がある。 本問では、小売業が運営している Web サイトでの情報連携を題材に、Web API を設計する能力を問う。	

設問	解答例・解答の要点		備考
設問 1	(1)	a Same-Origin	
	(2)	b イ	順不同
		c キ	
		d ク	
	(3)	Web サイト B へのログイン	
設問 2	e	(v)	
設問 3	(1)	f https://site-a.m-sha.co.jp	
	(2)	g 売れ筋商品情報配信の申込ページのオリジン	
	(3)	h Origin ヘッダフィールドの値	
		i 許可するオリジンのリスト	
		j 一致	

問 2

出題趣旨	
近年、クラウドサービスに対するパスワード認証が破られての不正アクセス事件が度々発生している。さらに、利用するサービスが増えると、サービス毎に別々のパスワードを人が記憶することも難しくなるので、クラウドサービス利用においては、認証連携及びより強力な認証方式が必要になってきている。そうした背景もあり、パスワードレス認証方式の標準化が進められている。 本問では、クラウドサービスの利用における認証方式の強化を題材に、認証方式の安全性を評価する能力を問う。	

設問	解答例・解答の要点		備考
設問 1	(1)	ホテル Wi-Fi と同じ SSID と事前共有鍵	
	(2)	a メールサービス P	
		b 攻撃者が用意した Web サーバ	
	(3)	HTTP で接続が開始されたから	
設問 2	(1)	OTP の入力进行要求し、OTP を認証サーバ X に中継する処理	
	(2)	c ウ	
		d ア	
		e エ	
		f イ	
	(3)	認証サーバ X でオリジン b とオリジン s の一致を確認しているから	

問 3

出題趣旨	
近年，IoT 機器が増加しており，そのセキュリティ対策も重要になってきている。IoT 機器はネットワーク経由だけでなく，物理的なアクセスも可能なので，それも考慮してセキュリティ設計を進める必要がある。また，IoT 機器が接続するサーバが複数あると，それらを連携して動作させるために，認証連携が必要になることも多い。 本問では，家庭用ゲーム機の開発を題材に，IoT 機器と複数のサーバ間での認証連携について設計する能力，及び IoT 機器のセキュリティ対策を検討する能力を問う。	

設問	解答例・解答の要点		備考
設問 1	エ		
設問 2	(1)	ゲームプログラム ID	
	(2)	ゲームサーバに認証サーバと同じ共通鍵を保存する。	
	(3)	仕様 MAC の生成に共通鍵を使用する。	
		範囲 自身が管理するゲームサーバ上で動作する全ゲームプログラム	
	(4)	a オ	
		b エ	
		c カ	
	(5)	SSD を取り出し，PC などにつなげる。	
	(6)	耐タンパ性	
設問 3	ハッシュ値リストを TPM に保存する。		