

令和4年度 秋期 情報処理安全確保支援士試験 解答例

午後Ⅱ試験

問1

出題趣旨	
サイバー攻撃が高度化する中、有効なセキュリティ対策を行う上で重要な要因の一つとして、攻撃者の行動、マルウェアの挙動を観測によって解析することが挙げられる。	
本問では、セキュリティ関連会社での脅威情報調査及びCTFを題材に、マルウェアの動的解析システムの安全な運用方法の設計能力、及び攻撃者の攻撃手法を想定した事前対策の立案能力を問う。	

設問	解答例・解答の要点		備考
設問1	(1)	エ	
	(2)	C&C サーバの IP アドレス	
	(3)	仮想マシンではない実機環境を使う。	
設問2	a	ア	
	b	ウ	
	c	エ	
	d	イ	
設問3	(1)	e 1	
	(2)	f ア	
		g イ	
		h ウ	
		i ウ	
	(3)	j ア	
		k ウ	
		l ウ	
		m イ	
		n ウ	
		o ア	
設問4	(1)	ハッシュ化を繰り返す処理	
	(2)	ログイン失敗が5回連続した場合に当該利用者IDをロックする機能	
	(3)	p エ	
	(4)	変数nの値を5桁の文字列に変換して“Admin”に結合した文字列	
設問5	(1)	同一のMACアドレスのエントリが複数存在する状態	
	(2)	q デバッグログに認証情報を出力しないこと	

問 2

出題趣旨		
未知のマルウェアに対応するため、EDR (Endpoint Detection and Response)の導入が進んでいるが、これを有効に活用するためには、インシデントレスポンス体制の整備が必要である。 本問では、未知のマルウェアへの対応に EDR を活用するための技術的な知識、及びインシデントレスポンス体制を整備する能力を問う。		

設問	解答例・解答の要点		備考
設問 1	下線①	メールフォルダ内のファイルが読み込まれた。	
	下線②	HTTP でファイルがアップロードされた。	
設問 2	(1)	a 15:03	
		b PC1	
		c file1.v	
		d file2.v	
		e PC2	
	(2)	ア, ウ, エ, オ, キ	
設問 3		V ソフトのデータファイルが読み込まれた後に、1 分以内に、パス名が同一のファイルが上書きされた。	
設問 4	(1)	f 添付ファイルの名称	順不同
		g 添付ファイルのサイズ	
	(2)	h サイズ	
	(3)	i アップロードされたファイルのサイズ	
		j アクセス先の URL	
	(4)	k ファイル圧縮	
		l ファイル名	順不同
		m ファイルサイズ	
設問 5		情報システム課が管理する USB-ID のいずれにも一致しない USB-ID の USB メモリが装着された。	
設問 6	n	社外向けの通報窓口を設置する。	
	o	最初の判定に加え、影響の大きさ又は影響の広がりについての事実が見つかるたびに、再判定を行う。	