

問番号			正解	備考
問 1	設問 1	a	エ	
		b	イ	
	設問 2	c	イ	
		d	エ	
	設問 3		エ	

## 問 1

問 1 では、Web サービスにおけるパスワードの保存を題材に、ハッシュ関数の特性や利用方式について出題した。

設問 1 では、a の正答率は低く、あまり理解されていなかった。ウと誤って解答した受験者が見受けられた。解答群に挙げたものは、いずれも基本的かつ重要なものなので、その意味を正しく理解しておいてほしい。b の正答率は高く、よく理解されていた。

設問 2 の正答率は平均的で、おおむね理解されていた。

設問 3 の正答率は平均的で、おおむね理解されていたが、ウと誤って解答した受験者が多く見受けられた。ストレッチング方式を用いる場合であっても、一つのパスワードの候補から求める、照合に用いるハッシュ値は一つであることと、その一つのハッシュ値を求めるためにハッシュ化の操作を繰り返すので、計算時間がより多く必要になることに気がつけば、正答できた。

ハッシュ関数は、様々なサービスや製品で、安全性を向上させるために使われている。ハッシュ関数の特性を正しく理解し、ハッシュ関数をどのように用いると、より安全に利用できるのかを把握できる能力を身につけておいてほしい。