問4

出題趣旨
インシデント対応については，様々なログからインシデント発生の検知と内容の把握をし，インシデントを封じ込めるための対策，根本原因の把握と解決，フィードバックからの運用強化が重要になる。本問では，その一連のプロセスを正確に理解し，事態に対処できる能力を問う。

設問		解答例・解答の要点		備考
設問1		CPU の使用率を確認することで，普段と異なる事象が発生している時間帯が見極めやすくなるから		
設問2	(1)	a	△△.123.123.123	
	(2)	表 5(3)，表 6(1)		
	(3)	該当通信は，Web サーバのステータスコードが 200 であるから		
設問3	(1)	b	送信元 IP アドレス	
		c	・https ・SSL	
		d	秘密鍵	
	(2)	Web サーバプログラムで制限している最大同時セッション数の不足		
	(3)	機器①	ウ	機器①，設定内容①と機器②，設定内容②は順不同
		設定内容①	X-Forwarded-For ヘッダフィールドの追加	
		機器②	オ	
		設定内容②	X-Forwarded-For ヘッダフィールドのアクセスログへの出力	