

【H19 春-SV 午後Ⅱ問 2 の解答例・解答の要点】

設問		解答例・解答の要点	
設問 1	(1)	a	停止
		b	アクセスログ
	(2)	適切な本人確認を行わずに新しいパスワードを伝えている。	
設問 2	(1)	c	IKE
		d	ESP
		e	DH 又は Diffie-Hellman
	(2)	<ul style="list-style-type: none"> ・相手を認証するため ・相手がもつ事前共有鍵の正当性を検証するため 	
	(3)	一時鍵情報 p や一時鍵情報 q を攻撃者が入手できないから	
	(4)	モード	アグレッシブモード
		理由	利用するインターネット接続環境では IP アドレスは固定ではないから
設問 3	(1)	f	生体 又は バイオメトリクス
		g	本人
		h	他人
	(2)	登録されている事前共有鍵の無効化	
設問 4	(1)	ネットワーク接続ができないところではデータを利用できない。	
	(2)	ノート PC のハードディスクを暗号化し、復号鍵を認証デバイスに保管する。	
設問 5	(1)	社外からのスパムメールを送信する SMTP の送信元アドレスが FW のアドレスに書き変わってしまったから	
	(2)	感染してしまった原因	図 5 は偽のアラートメールであり、ウイルス付きのソフトウェアをダウンロードして実行してしまったから
		検知できなかった理由	HTTP アクセスに関するウイルスチェックは行っていなかったから
	(3)	セキュリティパッチや修正プログラムは、パッチサーバ以外からダウンロードしない。	