問１

出題趣旨
近年，日本でも被害が報告されている標的型サイバー攻撃に対しては，従来のウイルスや愉快犯によるサイバー攻撃と比べて，攻撃者の攻撃手法やその目的が異なることを念頭において対策することが重要である。 本問では，具体的なマルウェア感染の事例をもとに，マルウェア解析の知識と，標的型サイバー攻撃を受けた際に適切に状況を把握する能力を問う。

設問		解答例・解答の要点		備考
設問１	(1)	ML2		
	(2)	**機器**	FW	
		ログ	PC から攻撃者のサーバへの HTTP 通信のログ	
設問２	(1)	a	USB メモリ	
	(2)	攻撃者のサーバの URL を，プロキシサーバのブラックリストに登録する。		
	(3)	PC の Z ブラウザのバージョンを全て 3 にする。		
設問３	(1)	① ②	・パック処理されていること ・タイムスタンプを変更していること	
	(2)	RD-LAN と他のネットワークとの物理的な隔離		
	(3)	b	新薬の研究報告書を窃取	