

### 附件3 事中應變階段查核清單

事中應變階段查核清單			
至證券期貨市場資通安全通報系統 <a href="https://sfevents.twse.com.tw">https://sfevents.twse.com.tw</a> 完成攻擊事件初步通報	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
攻擊事件分析			
確認遭攻擊原因：_____	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
備份重要業務資料	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
保留相關攻擊紀錄	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
分析攻擊手法與執行損害管制-頻寬消耗型攻擊			
路由器 啟用速率限制以及存取控制(ACL)機制，並針對封包之 來源 IP 位址進行檢測和過濾	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
DDoS 防禦系 統 暫時調整 DDoS 設備防護至高等級，阻擋可疑攻擊行 為	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
攔截異常封包內容，例如不完整、格式錯誤的標頭或不 完整封包等	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
針對特殊性質以及特定通訊協定方式之 DDoS 攻擊， 例如 ICMP Flood、UDP Flood 攻擊等進行防護	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
限制每秒單一來源 IP 連線數	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
利用查問驗證機制防禦機器人攻擊	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用

	IP 信譽偵測，阻擋已知惡意來源 IP	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	透過國別 IP 清單，阻擋來自特定國家的 IP	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
入侵防禦系統	針對已知漏洞或異常網路傳輸行為設定阻擋	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
交換器	啟用速率限制以及存取控制(ACL)機制，並針對封包之來源 IP 位址進行檢測和過濾	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	針對攻擊流量進行流量過濾	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
CDN	利用查問驗證機制防禦機器人攻擊	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	減少至原始主機的網路流量與降低主機資源消耗	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
流量清洗服務	針對攻擊流量進行清洗動作或轉導，阻擋境外或來自特定國家的 IP	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用

#### 分析攻擊手法與執行損害管制-資源消耗型攻擊

	暫時調整 DDoS 設備防護至高等級，阻擋可疑攻擊行為	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
DDoS 防禦系統	攔截異常封包內容，例如不完整、格式錯誤的標頭或不完整封包等	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	針對特殊性質以及特定通訊協定方式之 DDoS 攻擊，例如 SYN Flood、應用層 DDoS 攻擊等進行防護	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	調整 DNS 查詢失敗阻擋規則，例如每秒查詢失敗 X 次即進行阻擋	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用

	分析攻擊 payload，設定正規表示法(Regular expression)規則進行阻擋	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	限制每秒單一來源 IP 連線數	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	利用查問驗證機制防禦機器人攻擊	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	IP 信譽偵測，阻擋已知惡意來源 IP	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	透過國別 IP 清單，阻擋來自特定國家的 IP	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
入侵防禦系統	針對已知漏洞或異常網路傳輸行為設定阻擋	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
網站應用程式 防火牆	確認網站攻擊來源 IP 及 HTTP 欄位特徵	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	阻擋使用慢速請求佔用每筆連線之慢速攻擊	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	限制特定頁面存取頻率限制	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	分析攻擊封包內容，並視攻擊特徵客制化攔阻規則	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
CDN	針對攻擊流量進行流量過濾	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	利用查問驗證機制防禦機器人攻擊	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
	減少至原始主機的網路流量與降低主機資源消耗	<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
啟用雲端備援		<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
至證券期貨市場資通安全通報系統 <a href="https://sfevents.twse.com.tw">https://sfevents.twse.com.tw</a> 完成攻擊事件正式通報		<input type="checkbox"/> 是	<input type="checkbox"/> 否	<input type="checkbox"/> 不適用
填寫日期：_____年_____月_____日 撰寫人簽名：_____				

