中華民國證券投資信託暨顧問商業同業公會
分散式阻斷服務防禦與應變作業程序範本

第一條（規範目的）

為能有效強化投信投顧業者分散式阻斷服務（Distributed Denial-of-Service, 下稱DDoS）防護能量，以減緩DDoS攻擊影響，使資訊設備或服務能儘速恢復正常營運，特訂定本作業程序範本。

第二條（適用對象）

本作業程序範本適用於具網路電子交易服務之投信投顧業者。

第三條（因應DDoS之防護作為）

DDoS攻擊防禦與應變作業著重在事前準備作業，資訊單位應依內部網路架構與資源進行相關防護準備作業；攻擊事件發生時，透過事前準備的防護機制，採取應變措施以緩解攻擊事件造成的影響；攻擊事件結束，檢討各種軟硬體設備或資安防護設備不足之處，並提出建議改善方案，以提升整體資安防護能力。

第四條（事前準備）

資訊單位在事前應檢視內部資源情況，調校系統設定，預先申請相關防禦服務或其他官網防禦措施，以強化DDoS防禦能量。

一、維護系統及網管人員/廠商聯繫資訊：

除內部資訊人員聯繫資訊外，亦須維護相關系統及網管人員/廠商聯繫資訊，確保聯繫管道的暢通，當DDoS攻擊事件發生時，可快速依狀況聯絡所需之人員協助處理。

二、更新網際網路相關服務版本及關閉特定功能：

(一)、升級校時系統(NTP)版本至較安全版本，並關閉 Monlist 功能，避免校時系統被利用發動 DDoS 攻擊。

(二)、停用網域解析(DNS)服務的遞迴查詢功能，並設定限制網域服務回復速率(DNS RRL)，避免網域服務被利用發動 DDoS 放大攻擊。

(三)、上述設定可依 DDoS 攻擊狀況不同，而調整設置相關的防禦技術設定及安排。

三、申請相關防禦服務：

(一)、提供網路電子交易服務之投信投顧業者應導入流量清洗或流量分流服務。

(二)、可與前款服務業者事先協商，如發現網路頻寬異常狀況，須即時告知，並協助阻擋異常之網路連線，提升網路可用性。

第五條（事中應變）

當資訊單位自行監控發現，或經由提供防禦服務業者主動告知發現有 DDoS 攻擊流量時，採行以下措施進行通報及緩解 DDoS 攻擊：

一、事件通報：

(一)、對外通報

1、當知悉資安事件發生時，應依「證券期貨市場資通安全事件通報應變作業注意事項」至「證券期貨市場資通安全通報系統」(https://sfevents.twse.com.tw 以下同)辦理通報事宜。

2、得視情節向警政機關報案。

(二)、對內通報

為確保各項業務正常營運，投信投顧業者應訂定公司內部通報程序，並參考以下通報機制措施：

1、DDoS 攻擊通報原則及流程：

當知悉資安事件發生時，投信投顧業者應依內部通報程序進行通報作業。

2、建立 DDoS 緊急通報窗口通訊錄，並指定權責單位及專責人員

二、事件應變：

(一)、啟用流量清洗或流量分流等外部 DDoS 攻擊緩解服務。

(二)、請提供防禦服務業者阻擋異常之網路連線。

(三)、引導電子交易投資人採替代方式下單。

第六條（事後處理）

一、事件解除確認：

(一)、當確認 DDoS 攻擊已停止，評估恢復系統設定，以使業務正常運作。

(二)、持續監控網路流量或系統狀況。

二、事件解除通報：

依「證券期貨市場資通安全事件通報應變作業注意事項」至「證券期貨市場資通安全通報系統」辦理解除通報事宜。

三、事件紀錄及檢討：

記錄事件發生過程與處理程序，包含攻擊原因及手法等資訊，及因應該次 DDoS 攻擊採取的應變措施、解決方案與後續處理情形。

第七條（附則）

為因應DDoS攻擊，應適時審視相關防禦措施與應變作業程序內容，並進行修正與調整。

第八條（施行及修訂）

本作業程序經總經理核定後實施，修訂時亦同。