# 中華民國證券商業同業公會

**分散式阻斷服務防禦與應變作業程序（範本）**

中華民國證券商業同業公會106年3月31日中證商電字第1060001720號函公告

中華民國證券商業同業公會114年9月18日中證商電字第 號函公告

### 第一條（規範目的）

為能有效強化證券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下單服務或設有官方網站之證券業者。

### 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）

資訊單位利用現有設備與資源，於事前規劃多層次防護架構，完成系統/服務之設定與申請，作好DDoS防禦準備，「事前準備階段查核清單」詳附件1。

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應處。「系統及網管人員/廠商聯繫表」詳附件2。

二、調校系統/服務設定

服務主機應定期進行系統安全更新，避免遭駭客入侵利用外，同時可透過其他防護設備防止遭DDoS攻擊，針對其提供之服務進行安全防護設定，透過「連線數量」、「連線速率」、「通訊埠(Port)」及「主機防火牆」等限制/過濾流量方式，抵擋大量連線需求，以維持提供服務之主機的可用性，亦可避免遭利用造成主機本身成為或間接參與DDoS攻擊，而導致其網路頻寬耗損。

### 三、修改程式設定

透過適當的程式撰寫及設定，不僅能確保資料的安全，更能增進網站抵禦來自網路上的攻擊，任何資料輸入的地方都應嚴格審查及控管，網站維運時更應勤快更新補洞，針對程式的設定建議做法如下：

### (一)排除不合理的查詢條件，如長時間區間、輸出內容過大之搜尋結果進行查詢限制。

### (二)限制查詢格式，檢查輸入的格式是否含有非法字元。

### (三)限制API查詢方式，利用token或key進行查詢次數(頻率)限制。

### (四)限制自動化工具，搜尋結合動態驗證碼。

### 四、設置網路流量/系統資源監控機制

透過設置網路流量與系統資源監控流量監測等工具，即時監控網路及系統使用率外，亦可計算業者網路每日流量與使用量平均值，藉以定義網路流量與系統資源門檻值，確保業者能即時發現網路攻擊行為；另可定期檢視業者網路架構或狀態，並視情況進行調校，確實掌握業者網路流量與系統資源狀況。

### 五、啟用網路/防護設備DDoS防禦功能

一般的網路設備例如防火牆、交換器、路由器等，多有配置類似功能可協助防禦DDoS攻擊，針對應用層的攻擊則多需借助DDoS防禦系統、網站應用程式防火牆(Web Application Firewall，WAF)或內容傳遞網路(Content Delivery Network，CDN)服務，以達到多層防護的效果。若業者發現開啟相關功能後造成系統效率不彰或使用者體驗不佳，可評估將此步驟移至「第五條（事中應變）」執行。

### 六、申請/建置流量清洗服務

### 流量清洗(Cleaning Pipe)是一種由邊界閘道器協定(Border Gateway Protocol，BGP)對路由進行廣播，將原本的攻擊流量導向流量清洗中心(Scrubbing Center)，藉由資安廠商自有的封包深度分析、連線特徵等技術來檢查、分析、過濾惡意封包之服務。此時再把過濾後的流量導回原本對應的伺服器後，即便流量中仍有殘存的惡意攻擊封包，原本的防護設備應有足夠的能力來因應。

### 目前已有多家網際網路服務提供者(Internet Service Provider， ISP)與資安設備廠商提供流量清洗服務，業者可視網站流量需求採購所需服務項目，於事前提出申請，並支付月租費用，後續可視情況選購清洗流量。

### 七、申請CDN服務

### 業者可評估申請CDN服務，其目的是依照現有的網路架構，藉由內容分散式儲存、系統平衡負載、網路服務請求重導等功能，將網站的內容轉發至最接近用戶的網路節點，使用戶可就近取得服務的內容，解決單一服務主機因網路擁塞而造成服務效能不彰的狀況，進而在提高用戶訪問網站的回應速度、降低頻寬成本的同時，仍能維持服務品質。

### 當導入CDN服務的網頁伺服器主機遭受DDoS攻擊時，封包會導向最靠近攻擊者位址的服務主機，有助於稀釋攻擊封包流量。此外，透過CDN內部的DNS轉址與HTTP重導功能，可讓正常使用者轉接到負載較輕的其他服務主機，以維持網站服務的可用性。

### 八、建置/申請雲端備援

### 業者可評估透過雲端服務系統設置重要系統/服務之雲端備援機制，以確保攻擊事件發生時，重要系統/服務可持續對外提供服務。

### 惟採購雲端虛擬資源時，業者亦須規劃相關系統/服務資料庫同步方式，並確認雲端服務系統提供DDoS防禦機制。

### 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，應至「證券期貨市場資通安全通報系統」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，證券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，證券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、事件分析

### 為能有效防禦DDoS攻擊，資訊人員應於攻擊事件發生時，蒐集並分析相關紀錄，以判斷DDoS攻擊類型，並依攻擊類型採取對應之防禦措施，「事中應變階段查核清單」詳附件3。

### (一) 確認遭攻擊原因

### 攻擊者發動攻擊目的不同，其中涵蓋了政治立場、經濟利益或其他多樣化的意識形態，可透過網路平台相關管道，了解遭攻擊原因，勾勒攻擊事件全貌。

### (二)備份重要業務資料

### 由於在攻擊結束前，皆無法得知該次攻擊強度與攻擊持續時間，因此若遭受攻擊之設備存有重要業務資料時，建議即刻進行備份。

### (三)分析攻擊手法與執行損害管制

### 監控網路及資安設備現況，透過日誌保存機制蒐集相關攻擊紀錄，分析攻擊手法為頻寬消耗型攻擊或資源消耗型攻擊，並執行相對應的損害管制，有關「頻寬消耗型攻擊及資源消耗型攻擊建議做法」詳附件4。

### (四)保留相關攻擊紀錄

### 如相關日誌檔與側錄攻擊封包，可供日後資訊人員分析、判斷攻擊手法與特徵等，俾進一步提出相關防禦措施。

### 三、啟用雲端備援

### 如業者已申請雲端虛擬資源，可啟用備援設備，並利用雲端系統的DDoS防禦機制，緩解攻擊流量，以維持系統/服務正常運作。

### 第六條（事後處理）

### 事後處置階段大致可分為「復原作業」與「結案作業」等內容，當確認DDoS攻擊已停止，即可評估恢復系統設定，或停用備援機制，以恢復系統業務正常運作。此外，亦需記錄事件處理經過，檢討因DDoS攻擊事件所造成的影響進行評估，檢討網路安全措施或其他具體改善方案。「事後處置階段查核清單」詳附件5。

### 一、復原資訊設備運作

### 資訊設備若於受到DDoS攻擊後已進行關機，抑或停止/限制提供部分網路服務(如變更部分設定檔)時，經過妥善處理後，應恢復其正常運作，若有啟用備援機制，建議一併進行運作，並持續觀察網路流量，確認DDoS攻擊已停止後，再行評估是否需停用備援機制。

### 二、持續監控網路流量

### 資訊人員均完成各項復原作業後，應持續監控網路流量，並觀察資訊設備運作情況，密切注意DDoS攻擊是否再度發生。

### 三、記錄事件處理過程

### 資訊人員需記錄整個事件發生過程與處理程序，包含攻擊原因及手法等資訊，同時記錄因應該次DDoS攻擊所採取之應變措施或解決方案，以及後續處理情形與追蹤事項，可提供未來發生類此事件時參考，有助於加速降低受DDoS攻擊後所造成的損害。

### 四、攻擊事件結報

### 攻擊事件結束後，業者應至證券期貨市場資通安全通報系統(https://sfevents.twse.com.tw)進行結案作業，提供事件處理過程與解決方案，以完成資安事件通報作業。

### 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）

證券商「分散式阻斷服務防禦與應變作業程序」經總經理核定後實施，修訂時亦同。