DDoS 事件通報與應變作業程序

(一)連線單位準備措施

1. 網域名稱系統（Domain Name System, DNS）服務與管理集中化
   為避免 TANet 學術網路受 DDoS 攻擊而導致損害，各連線單位應將單位內的 DNS 服務向上集中管理，並將單位內的 DNS 服務指向 TANet DNS，以保障 TANet 使用者之權益。

2. 網路拓樸圖清查與更新
   為確保 DDoS 清洗服務達預期效果，各連線單位應事先清查單位內線路並更新單位內網路拓樸圖，以為 DDoS 清洗服務之策略研判依據。網路拓譜圖應包含以下資訊，並事先提供本部及 DDoS 清洗服務單位備查：
   (1)欲保護核心系統伺服器之 IP 位址；
   (2)核心系統伺服器所提供的網路服務類別（如 80/TCP、53/UDP 等）；
   (3)各單位對外所有線路，包含臺灣學術網路及商用網路服務供應商。

(二)分級措施

當連線單位遭受 DDoS 攻擊事件時，應依「教育機構 DDoS 攻擊通報應變流程」（如附錄）進行相關作業；以下說明不同單位的分級措施。

1. 連線單位
   (1)連線單位受到疑似 DDoS 攻擊時，應確認該攻擊事件是否影響單 位內重要設施之運作，並通報上級連線單位（區、縣(市)網路中心）評估是否有 DDoS 攻擊流量清洗服務之必要性；倘若評估結 果為必要，並由上級連線單位至「台灣學術網路危機處理中心（TACERT）」提出申請。
   (2)連線單位於 DDoS 清洗服務結束後，可參考《教育機構資安通報 應變手冊》以及《國家資通安全通報應變作業綱要》，判定 DDoS 攻擊事件之事件等級，並依據各資安事件等級之規定，於時限內 至 TACERT 的「教育機構資安通報平台」填寫《資安通報單》， 以完成通報應變作業。「教育機構資安通報平台」網址為：https://info.cert.tanet.edu.tw/。

2. 區、縣（市）網路中心
   (1)當區、縣(市)網路中心或轄下連線單位有必要申請 DDoS 清洗服務時，應由區、縣(市)網路中心至 TACERT 之「資安通報報表系 統」項下的「DDoS 通報」提出申請。「資安通報報表系統」網址為： https://portal.cert.tanet.edu.tw/index.html。
   (2)當區、縣（市）網路中心本身受攻擊而申請 DDoS 攻擊清洗服務結束後，亦應比照連線單位作為，判定 DDoS 攻擊事件之事件等 級，並依據各資安事件等級之規定，於時限內至教育機構資安通 報平台完成通報應變作業。
   (3)區、縣（市）網路中心協助連線單位申請 DDoS 攻擊流量清洗服 務應於服務結束後，由區、縣（市）網路人員登入 TACERT 之「教育機構資安通報平臺」就連線單位所填寫的《資安通報單》 內容進行審核，確認資安通報單內容的完整

性，以及事件等級判 斷的正確性。

(4)區、縣（市）網路中心的資安人員應掌握 DDoS 攻擊事件狀況，並提供必要之技術支援，協助連線單位進行事件之應變處理。

3. 學術資訊安全維運中心（Academic Security Operation Center, A-SOC）

(1)南區與北區的學術資訊安全維運中心（A-SOC）在偵測到大規模 DDoS 攻擊時，應分析 DDoS 攻擊流量以及攻擊手法，並發出資安警訊通知連線單位。

(2)南區與北區的 A-SOC 應依其服務範圍，於接獲 TACERT「DDoS 通報」申請或在教育部緊急通知時，提供 DDoS 攻擊流量清洗服務，並掌握重大 DDoS 攻擊事件細節，如攻擊事件之樣態、時間、來源與目標、攻擊軌跡以及緩解記錄等。必要時，A-SOC 可聯繫其他電信業者進行協同作業。