附件1 會員說明列表

N-ISAC 會員資格與責任說明如下：

表1　N-ISAC 會員說明列表

會員類型		會員資格	會員責任
一般會員	領域管理	▪ 管理國內特定範圍，掌管明確之網段與 IP 區間 ▪ 監控其管理範圍之網路流量與資安事件 ▪ 必要時能協調執行緊急應變處理措施	▪ 分享資安情資或資安事件訊息 ▪ 針對業務轄管範圍(或 CI 領域)，提出資安防護執行報告 ▪ 於 N-ISAC 會員會議中分享資安防護案例或專題報告 ▪ 應定期提供並更新所管理之 IP 位址範圍，以及資安事件統計資訊 ▪ 針對接收國家資通安全研究院提供之中繼站黑名單，每月應回饋其阻擋統計資訊
	應變聯防	▪ 協調處理國內特定範圍之資安事件 ▪ 協調執行緊急應變處理措施	▪ 分享資安情資或資安事件訊息 ▪ 於 N-ISAC 會員會議中分享資安防護案例或專題報告
	執法機關	▪ 偵蒐國內資安情資 ▪ 處理國內網路犯罪事件	▪ 分享資安情資或資安事件訊息 ▪ 於 N-ISAC 會員會議中分享資安防護案例或專題報告
技術會員	監控服務	▪ 具備資安事件監控與分析能量 ▪ 具備惡意行為研究與偵測能量 ▪ 定期產製資安情資並配合法規要求落實提供監控情資	▪ 分享資安情資或資安事件訊息 ▪ 協助會員分析資安事件或惡意程式 ▪ 於 N-ISAC 會議中分享資安威脅趨勢或資安防護技術等議題 ▪ 針對接收國家資通安全研究院提供之中繼站黑名單，每月應回饋其阻擋統計資訊 ▪ 定期分享資安威脅清單
	技術支援	▪ 對其服務或產品具備異常偵測與事件監控等防護能量 ▪ 對其服務缺失或產品漏洞具備及時處理與修補等防護能量 ▪ 能將漏洞資訊或惡意攻擊資訊轉化為資安情資並提供會員參考	▪ 分享資安情資與資安事件訊息 ▪ 協助會員分析資安事件或惡意程式 ▪ 於 N-ISAC 會議中分享資安威脅趨勢或資安防護技術議題 ▪ 針對接收國家資通安全研究院提供之中繼站黑名單，每月應回饋其阻擋統計資訊 ▪ 定期分享與自身服務或產品相關資安情資，供其他會員做為資安防護參考

資料來源：國家資通安全研究院整理

TLP:WHITE