◎資訊安全宣導

—5G 中的資安風險—

回顧我們的公開金鑰系統，「安全」有兩個目標，一者是「祕密性」、另一者是「真實性」。5G 裡所有的基礎來自前世代的通訊架構，是得以延伸而發展出來， 所有 G 世代的安全問題如出一轍，卻也隨著資訊生活的普及，使得資安生活的安全意識更顯得重要。近年來網路通訊技術 5G 的推動，科技大國美國早已有所警覺並「超前部署」。根據美國負責「安全」的國土 安全部與國家情報總監於 2019 年 5 月執行「保護資通技術及服務之供應鏈的行使命令」，藉此國土安全部緊接著發布「美國採用 5G 引發的風險概述」(Overview of Risks Introduced by 5G Adoption in the United States)，列舉 5G 網路風險的脆弱性包含：供應鏈公司製造 5G 組件未經妥當的認證、傳承先前世代所承受的「網路安全」風險、5G 未來普及化部署實施過程安全配置、市場競爭機制不恰當、5G 技術操作標準等因素將增加 5G 執行的風險。

藉此，其中的「網路安全」，延續世代交替的密碼基礎，即 5G 系統的訊息正確性傳遞，需為通訊雙方所認可。若以密碼機制的公開金鑰系統來看此部分，也就是傳送方的訊息經網路傳遞的資訊，得被接收方能正確的判斷訊息來源真實性。在公開金鑰系統的運作下，此一目標可以用傳送方的祕密 key 對訊息先做「驗證碼」的提供，而接收方將以傳送方的公開 key，對所接收的「驗證碼」進行檢驗，即可清楚判斷訊息來源真實性。

【文章擷取-清流雙月刊】

臺中榮民總醫院提醒你!也關心你!