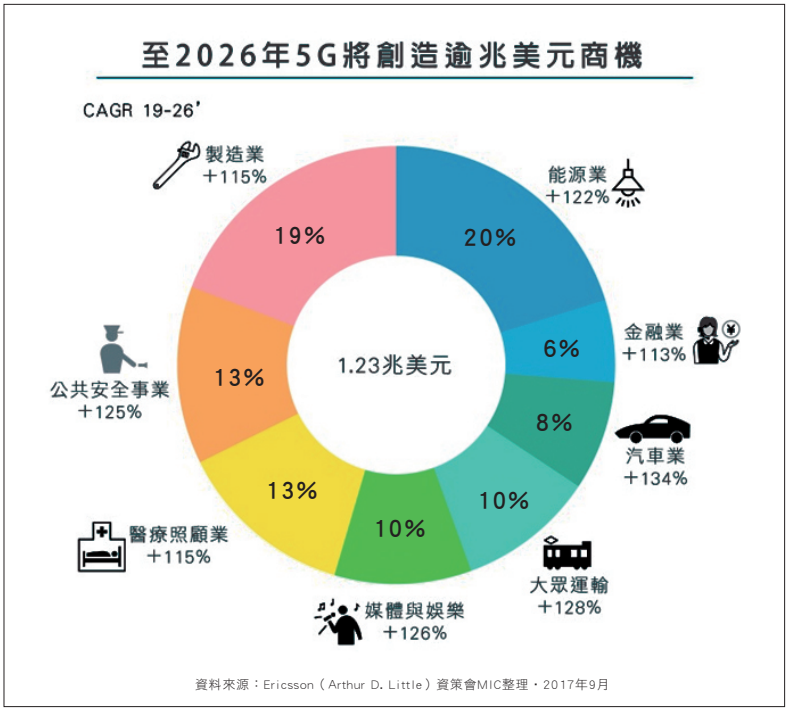
5G在產業的應用情境與資安因應

資策會資安處主任⊙施叔良

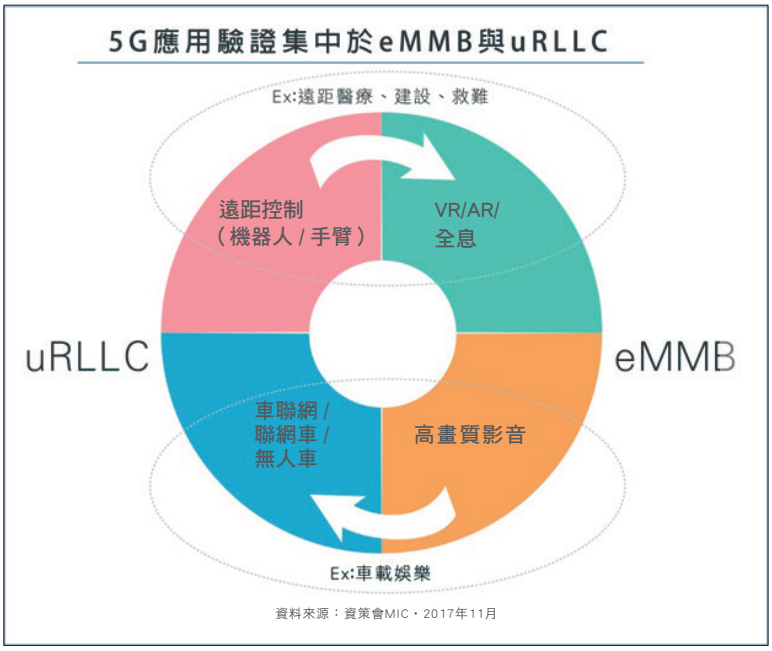
5G的應用

5G世代與4G的差異，在於4G LTE是高速行動寬頻世代，用戶擁有高速行動連網的享受體驗，5G的速度是4G的100倍，延遲的時間只有十分之一，而5G世代除提供比4G更高速、更大頻寬的行動連網體驗外，能支援的應用服務情境，也比4G更寬廣、更深入，5G提供低延遲、高品質、大規模的連網特性，更充份支援以往許多4G所無法達成的應用情境及服務，如更高畫質影音、擴增實境（AR）與虛擬實境（VR）的應用、個人AI應用、智慧家庭、智慧城市、遠距手術機器人、工業自動化、大規模物聯網、傳輸超高畫質影音串流（如4K以上影音傳輸）、自動駕駛車等應用服務，過去在4G 時代受限於速度及穩定度困擾的問題，都可以逐一獲得解決。原預估在2020年才能開始商轉的5G應用服務，資策會MIC預估，可望提早在2019年即進入商轉，至2026年，5G世代將會為垂直產業帶來1.23兆美元的數位化商機。



2015年國際電信聯盟（ITU）公布5G願景與藍圖規劃，聚焦5G使用情境區分為「增強型行動寬頻（eMMB）、超可靠且低延遲通訊（uRLLC）、大規模機器通訊（mMTC）」等三個應用範疇，而目前的技術應用測試，則是以同時結合eMMB與uRLLC為主流。2016年，標準組織第三代合作夥伴計畫（3GPP）提出最新版的「新服務與市場技術實現方法（SMARTER）」。

就「增強型行動寬頻（eMBB）」來說，是對應需要高傳輸速度、高容量的應用服務，而「超可靠且低延遲通訊（uRLLC）」是對應工業控制、雲端機器人、無人機等穩定度要求極高的通信應用，「大規模機器通訊（mMTC）」則對應智慧城市、智慧電表等需要有大量終端連結需求的應用，「網路運作（NEO）」則對應網路切片（Network Slicing）應用及需要更多網路彈性應用的工作，「增強型車聯網（eV2X）」則對應車對車通訊（V2V）、車對行人通訊（V2P）等車聯網應用。



2018年2月在南韓平昌舉辦的冬季奧運會，是5G進行大規模試驗的重要場域。韓國電信公司Korea Telecom（KT），從2016年就開始與國際合作夥伴投入測試發展五項5G的創新應用，包括提供收視者與參賽者同一視角的同步視角（Sync View）影像串流服務、360度VR多視角、全景即時現場影視串流、全息虛擬影像現場（Hologram Live）即時訪談直播、使用無人機穿梭會場攝影、經由AI進行智慧辨識提供全場保安服務、在會場安裝大量攝影機，從各個角度拍攝選手競賽過程，提供評審更詳實的判讀證據，減少誤判可能或釋疑，同時也可以提供觀眾從不同角度欣賞選手競技過程的每個細節。南

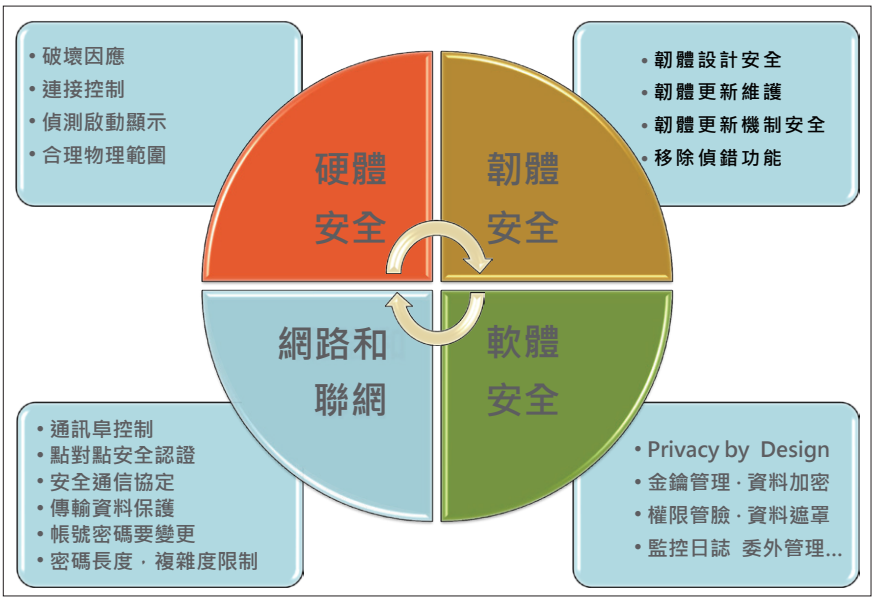
韓平昌冬季奧運會的5G通訊技術大型試驗結果，為全球帶來指標性的意義，且為全球觀眾帶來全新的觀賽體驗，同時正式邁入商業應用的5G服務，提供寶貴的標竿經驗。

當金融服務逐步朝向更無人化、行動化之際，充分運用物聯網的發展趨勢，將服務應用升級、支付方式更行動化以及防止詐欺的行為，是一個值得思考的議題。

5G資安

網際網路隨著5G的興起，網路活動愈來越被廣泛且大量應用之際，資安的問題也就順勢更快速發生新型態的資安問題，不論是因為企業內部管控不當或是外部駭客侵害行為所造成的資安問題，隨著科技技術的興起，影響層面也越來越深入且嚴重，事件的發生除了企業內部遭受損失以外，對一般無辜的民眾更是因為企業的資安事件造成個人隱私的傷害，因此各國相繼訂定隱私保護法規要求（例如我國資安法及個資法，日本，韓國個資法，歐盟GDPR，美國COPPA等等）來對當事人的隱私進行安全保護要求，以達到企業遵循法令行為規範及安全防護，尤其GDPR及COPPA除了與其他國家共通性的隱私保護要求外，進而於法律條文上明確增加對於未成年隱私的保護規範，禁止未經監護人同意而蒐集個資，各國政府對於隱私保護不當之企業，也都紛紛祭出高額的罰款，以達到企業對於法令要求的高度重視。

5G的興起讓各應用領域的發展更為活躍，企業必須改變過去僅以應用系統服務安全為主的思考模式，同時評估提供客戶服務的終端設備安全，通訊網路安全，伺服器安全及雲端安全等相關領域，各領域也同時必須涵蓋硬體，韌體，應用服務軟體等層面因素，各層面應考慮的因素如下圖說明。



資訊安全考慮因素圖

硬體安全面

企業除了提供應用軟體服務外，如果還有硬體相關設備的提供（ex：智慧投資語音設備），必須由硬體面考量以下四個因素：a.該設備是否有被破壞後，駭客藉由該設備進行網路入侵活動，系統又應該如何因應；b.產品對外連接介面是否為絕對必要，該介面的安全控制如何被控制使用目的也必須思考，以阻絕被透過介面入侵的風險；c.如果有應用到偵測互動的設備，就應該要注意到當事人是否有被告知並取得當事人或是監護人同意；d.設備物理控制（溫度，電壓…）是否被有效控制在適當的範圍內都是相當重要。

應用服務系統的軟體安全

我國資安法及歐盟的GDPR都在立法上已經明確要求企業針對所提供的服務，不再如過往採取被動式的資安防禦而已，在功能規劃設計之初始，就必須將資安議題納入整個發展生命週期中，執行必要的風險評估，再就不可被企業接受的風險訂定因應策略（Privacy by Design），並落實改善。

所謂Privacy by Design的規範要求，就是必須從軟體規劃、需求發展、系統設計、程式轉寫、系統測試、上線服務以及到服務下架的整個發展生命週期中，詳細評估可能涉及到的資安議題，進行風險評估活動後，再而執行必要的安全防護，除了Privacy by Design的資安要求外，還必須同時評估七個軟體開發應用環境的議題：a.使用金鑰作為身分驗證，該金鑰管理強度是否適當？b.保存資料的方式是否達到必要的安全防護水準？c.系統權限設定是否適當且必要授權等要求？d.如何防止合法使用者進行非授權的異動變更？e.針對使用者職權設定是否正確？f.資料顯示管控機制是否適當或是特定欄位的必要遮罩？g.所有重要的活動行為都應保留監控日誌，以做為異常監控或是問題追蹤的重要依據。

韌體安全面

韌體的設計亦必須參照Privacy by Design的要求，就四大因素進行資訊安全評估，a.在設計之初就將架構安全納入評估；b.對於韌體更需要因為時空環境，建立更新維護機制，以降低資安隨時可能產生的議題；c.更新機制的整個架構與協定是否安全足夠防護外部駭客入侵破壞；d.各企業的研發人員在研發的過程當中，常常因為業務分析的需要，須啟動偵錯功能，可是問題解決之後卻忽略予以移除，以致造成駭客入侵，資料外洩的嚴重問題。

網際網路傳輸面

透過網際網路進行資料傳輸，應就下列四大因素進行資訊安全評估：a.如何確認兩端的設備確實是已經經過企業授權同意使用的設備，因此安全認證方法就非常重要；b.傳輸的機制所使用的通信協定是否足夠安全；c.傳輸中的資料保護強度是否足夠；d.帳號及密碼安全管控以及密碼複雜度的要求，上述都是關係到網路通信安全的關鍵因素。

因產品或服務內容是企業主要獲利的來源，故資訊安全多著重在產品或服務本身，因此很容易忽略內部資訊安全管理的重要性，建立一套良善的資訊安全管理制度，讓員工對於各項資訊安全有所遵循依據，同時透過定期對同仁資安及個資教育訓練，更是讓員工瞭解內外環境的要求，亦是建構資訊安全非常重要的一環。

假如企業的部分服務項目或產品是委外開發設計或執行，委外管理對企業就是一個非常重要的議題，依照國內外的資訊安全標準，企業應該注重委外事前， 事中以及事後三大時期的資安管控，在委外之前企業應該對可能接受委託的單位進行必要的資訊安全評估，確保受委託的機構所開發的產品或是服務，未來足以符合企業的資訊安全需求，在執行的過程中，企業應該對委外單位進行監控，確保委託單位有依照企業要求的水準落實實施，當委託計畫結束後，更要確保受委託單位將所有處理的資訊進行繳還或是銷毀。

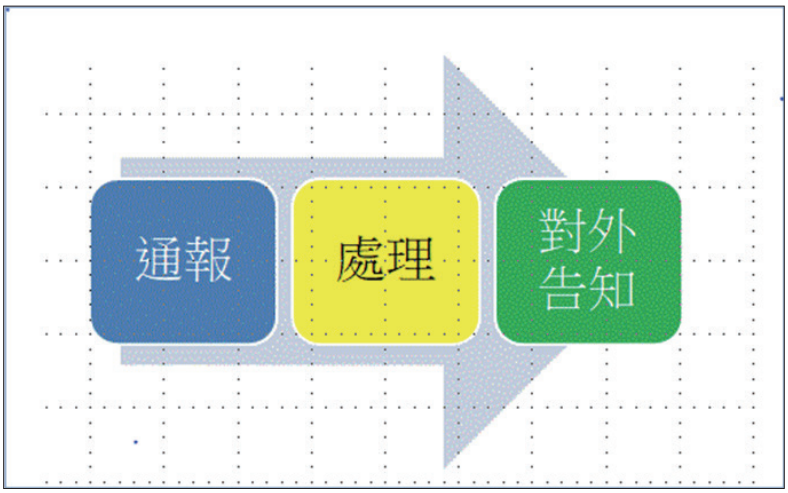
如何落實符合企業的服務要求並做好資訊安全防護要求，國際資訊安全標準ISO27001是國際上普遍認同可以參考的依據，國內外許多非營利機構也受政府委託，針對國內的環境設計各項資訊安全標準規範，例如電子商務資訊安全，智慧城鄉資訊安全規範，物聯網資訊安全規範等予以遵循，這也都是因應5G的發展，業者重要的參考依據。

資安聯防

除了企業本身因應5G應建構安全的服務及產品管理與訓練外，由於駭客的活動日新月異，各國政府紛紛建立起資安聯網通報平台，金管會也為我國金融體系打造了「金融資安資訊分享與分析中心（Financial Information Sharing and Analysis Center，F-ISAC），主要就是因應金融機構面對愈來愈多全球的資安攻擊，化被動為主動，全面分析預防系統性風險的發生，針對銀行、保險、證券期貨、投信投顧等各業別金融機構，提供通報、情資研判分析、資安資訊分享、協助資安諮詢與評估、研討會教育訓練及國際交流、協助資安事件應變處理、金融機構資安演練、協助資安規範評估與建議等9大服務功能，透過所有的企業組成一個“面”的聯防機制，可以協助整個企業更快速的因應可能發生的資安事件以及提昇應變能力。

資安事故因應

有了金管會所建立的F-ISAC平台，只是讓企業可以預防事故發生於未然，或是透過別人的經驗，得以快速解決相同事故處理的時間與能力，但事故萬一真正發生時，企業是否有能力就像社會上發生治安事件時，民眾如何知道該如何通報， 警務人員知道處理才不至於造成證據被破壞而無法追究原因，因此企業是否有一套標準程序讓企業同仁遵循就非常重要，事件發生時基本上分為下列三大階段。



資安事故通報流程圖

通報：當同仁知曉發生資安事件後，企業是否有一套標準的通報機制以記錄相關的必要資訊，並快速的將事故資訊傳遞與相關人員，組成應變處理小組，並確保事故確實可以追蹤管理是首要關鍵。

處理：包含了事故偵測、證據保存、分析研判、阻斷事故擴張、事故排除、業務活動復原及檢討等活動。

透過有效的處理步驟與方法，協助企業能在最短的時間內回復業務的正常運作、並確實找出事故發生的根因，徹底解決，避免再發生的機率。

對外告知：依據行政院資安通報、金管會及歐盟GDPR都有明確要求依據事故等級必須完成通報的時間要求，因此通報的程序不盡然是在處理之後才會啟動，但該資安事故如果涉及到民眾的權益，依照我國個資法要求，就必須儘速告知當事人，內容應包括個人資料被侵害之事實及已採取之因應措施，雖然沒有明確的要求告知期限，但仍然應該要在合理的範圍內施行之。

參考來源：資策會5G焦點報導