行政院及所屬各機關出國報告

（出國類別：會議）

拜會新加坡科技局並參加微軟公司資訊安全研討會報告

服務機關：國家發展委員會
姓名職稱：潘國才 處長
楊蘭堯 高級分析師
服務機關：行政院資通安全處
姓名職稱：施雅亭 分析師
派赴國家：新加坡
出國期間：106 年 3 月 14 日至 17 日
報告日期：106 年 5 月 10 日

行政院及所屬各機關出國報告提要

出國報告名稱：拜會新加坡科技局並參加微軟公司資訊安全研討會

頁數：23　含附件：是

出國計畫主辦機關/聯絡人：

國家發展委員會/楊蘭堯

出國人員姓名/服務機關/單位/職稱：

潘國才/國家發展委員會/處長

楊蘭堯/國家發展委員會/高級分析師

施雅亭/行政院資通安全處/分析師

出國類別：其他（出席會議）

出國期間：106 年 3 月 14 日至 17 日

出國地區：新加坡

報告日期：106 年 5 月 10 日

分類號/目：

關鍵詞：雲端服務、網路安全、資訊安全、資通訊技術、資料中心

內容摘要：

隨著網路技術與通訊科技不斷地推陳出新，無論是政府機關或民間企業，均面臨嚴峻的資訊安全威脅，觀察政府機關目前仍大多數使用微軟的產品，不論是伺服器端或是個人電腦的 Windows 作業系統、資料庫等，其產生的漏洞都常成為駭客利用攻擊的目標，因此微軟每年投資大量經費進行安全研發工作，也宣布多項防護計畫，包括成立全新的網路防禦營運中心(Cyber Defense Operations Center)提升對客戶資料的保護，另一方面微軟新一代的產品包括 Windows 10、Office 365、Microsoft Azure Stack 等也提供多項創新作法及新功能設計，避免用戶端遭到刻意的破壞或受駭時能立刻進行回應阻絕。

本次應中華民國資訊安全協會之邀，前往新加坡參訪微軟公司「技術透明中心(Transparency Center）」和「網路安全中心(Cyber security Center）」，此 2 中心是微軟首度結合擅長的兩個領域於同一處，專門為亞太地區提供全面性的資安解決方案。「微軟技術透明中心」提供政府機關可以檢視微軟產品的程式原始碼，獲取網路安全威脅和漏洞的相關資訊；「微軟網路安全中心」則是微軟蒐集全球微軟產品所產生的事件，透過資安平台進行巨量資料分析，為資安服務和雲端資安提供全面性的防護；另外也參訪微軟全球眾多資料中心中唯一位處熱帶地區(新加坡)的資料中心，瞭解其設計、維運及管理模式，作為我國後續推動機房整併，以部會為集中設置資料中心之參考；本次也藉此機會拜會新加坡科技局，針對電子化政府、智慧國家之發展經驗及資訊安全等議題進行意見交流，期能對我國政府推行相關政策或服務有所幫助。

目　錄

壹、目的

隨著網際網路的發達與電子化服務的發展，如何確保資訊安全更是企業或政府面臨的重要挑戰，近年來雲端服務、物聯網(IoT)、手持行動裝置上網、智慧城市應用等服務蓬勃發展，衍生出更多更複雜的安全議題，2013 年南韓多家銀行、保險公司、電視臺和電信網路業者遭受大規模駭客攻擊，讓將近 5 萬臺電腦、數千臺 ATM 提款機在同一時間停擺；2014 年發生 SONY 影業事件，大量的 SONY 公司內部資料被駭客公布在網路上，另一個則是開源軟體安全漏洞如 SSL Heartbleed 及 Shellshock 問題；2015 年 12 月烏克蘭電力網路受到駭客攻擊，導致大規模停電事件；2016 年台灣發生駭客入侵一銀 ATM 遭盜領 8,000 多萬元。從上述案例可以發現在高度資訊化的社會下，資訊安全除與個人的日常生活息息相關，也威脅國家關鍵基礎設施，駭客攻擊手法已越來越新穎，潛伏期也越來越長，除了企業加強資安防護外，各國政府也制定更嚴苛的標準或成立專責單位，以因應日益嚴重的資安環境；如美國政府在 2016 年 7 月公佈重大資安事件發生的準則，並指派聯邦調查局、國家網路調查聯合行動小組，作為重大資安事件的主要執法、調查單位，以便能有效對抗各種突如其來的資安威脅。新加坡於 2016 年 10 月成立科技局，掌管新加坡政府資訊通信科技系統、提供數位服務及推動各項 IT 政策及安全規範，以提高新加坡政府系統安全性，我國亦在 2016 年 8 月成立「行政院資通安全處」，直接將資安拉升至國安層級。另一方面我國刻正推動「第五階段電子化政府」，運用雲端與物聯網巨量資料特性，以資料導向之角度重新設計政府服務樣態，打造領先全球的數位政府，整合分散於各機關之個人資料及生活攸關公共服務資訊，以數位保險箱概念，提供便捷安心之個人化服務。在推動數位服務過程中，資訊安全更是不可或缺的重要基磐。

本次拜會新加坡科技局並參加微軟資訊安全研討會，除了瞭解新加坡在推動個人化服務的經驗外，也藉由交流分享新加坡在政府資

通安全的一些政策及推動作法；另外參加微軟資訊安全研討會，瞭解微軟在資料中心的設計理念及其產品在資訊安全上的努力，並實際參訪「技術透明中心(Transparency Center)」、「網路安全中心(Cybersecurity Center)」及「資料中心(Data Center)」，透過專家解說及交流討論機會，了解微軟因應雲端時代資訊安全發展趨勢及資料中心從規劃設計到實際運作、日常維運管理方式及面對客戶問題解決方式，作為我國推動數位政府服務、資料中心管理及資安防護之參考。

貳、過程

一、 3月14日下午：拜會新加坡科技局

新加坡科技局（Government Technology Agency, GovTech）係新加坡通訊及新聞部(Ministry of Communications and Information, MCI)下的法定機構，於2016年10月1日由原資訊通信發展管理局(Infocomm Development Authority,IDA)及媒體發展管理局(Media Development Authority,MDA)改組而成，掌管新加坡政府資訊通信科技系統、提供數位服務及推動各項IT政策及安全規範，以提高新加坡政府系統安全性。

本次拜會由新加坡科技局負責網路安全組組長CHAI接待，CHAI於簡報中提出目前新加坡推動之個人化服務，其中GovTech經由新加坡財政部結合金融管理局推出的MyInfo網站，讓民眾在網路上就可以申請信用卡或開設銀行戶頭，也讓銀行可以取得政府單位的用戶資料，省去重複填寫個人資料的不便，另民眾在新加坡註冊公司時，將會自動收到申請執照的資料，不用擔心遺漏必要的申請程序。這些服務和我國政府現在推動的第5階段電子化政府計畫中的數位服務個人化及一站式整合服務模式相同。

使用 MyInfo 必須取得民眾授權同意，任何個人資料傳輸之前，也須取得民眾同意，民眾亦可以選擇在電子服務使用其個人資料時收到訊息，選擇使用該平台的民眾只需要向政府提供一次個人資料，而不用每次電子交易時都要重複填寫，有助於節省民眾時間及避免錯誤，MyInfo 目標是不需要紙本證明文件作為完成交易的驗證，並作為貫徹 Whole-of-Government 理念的平臺。

此外新加坡政府極力推動 OneService@SG 服務，例如讓民眾可透過行動裝置立即反映市政問題，可以定位及上傳照片，此可視為反映市政問題的單一窗口；其優點是除了讓民眾立即回饋市政建議，並可促進跨機關的合作，而後端更有一套資料運算分析平臺，可發掘潛在問題，加速智慧國家(Smart Nation)的正向發展。舉例來說，新加坡運輸局及科技局共同開發名為 Beeline 的「個人化巴士服務」，它是一個實踐群眾外包(Crowd source)概念的行動 APP，市民可以透過 Beeline 建議他們心目中理想的點對點巴士服務路徑，補強公共交通運輸服務不足的地區，如經資料分析後認為該路線確實符合大眾需求且具經濟效益，則政府會開設此服務路線。

CHAI 表示新加坡政府自 2017 年 5 月起，將禁止所有政府機關公務人員公務用電腦連接網際網路，也禁止將公務電子郵件轉寄到私人信箱之政策交換意見，此項措施推動後預計將影響公部門約 10 萬臺電腦。公務員只能用個人平板、手機上網，這些設備並不需要登入政府資訊系統；如因工作需要使用網際網路者，則會配發專用的上網設備。新加坡政府為防範日新月異且複雜的網路攻擊，致力於創造公務同仁「更安全的工作環境」，至於在推動過程中是否遇到強大的阻力或反對聲浪？CHAI 表示在擬訂任何政策前，皆會進行嚴謹的意見蒐集與討論過程，並研擬相關配套方案，政策制定後則會編撰相關說明

或操作文件告知為何要採取這樣的管控措施，讓所有公務員有所依循，以有效降低阻力，促使政策順隧推動。

二、 Day2（3 月 15 日）：參訪微軟「網路安全中心(Cybersecurity Center)」、「技術透明中心(Transparency Center)」和「資料中心(Data Center)」

面對越趨複雜與多變的網路攻擊趨勢，網路安全已成為各國政府面臨的重要議題。在政府推動數位服務並追求靈活彈性的同時，如何建立並保有全方位和敏捷的資安平臺成為防護的重要關鍵。微軟於 2016 年在新加坡啟用首座結合「技術透明中心」和「網路安全中心」的安全聯合機構，透過智慧資安的防護(Protect)、偵測(Detect)及回應(Respond)等三大面向(圖 1)，建構安全可信賴的環境，專門協助亞太地區的政府與企業強化資安威脅的應變能力，並提供全方位資安解決方案。

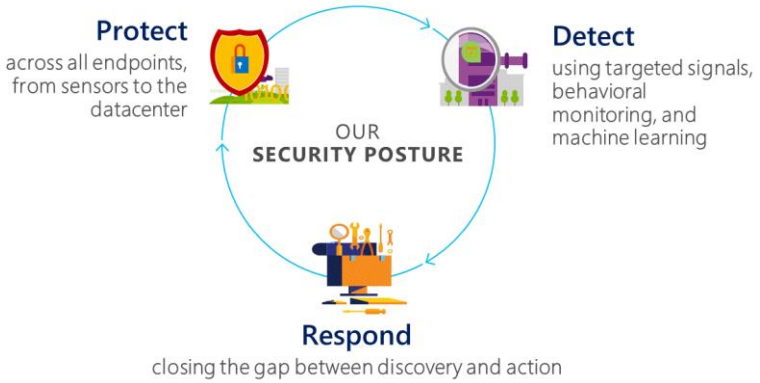


圖 1 微軟整體安全策略

(一)微軟網路安全中心

微軟「網路安全中心」是蒐集微軟來自全球各系列產品事件的回應、偵測器等組成一個巨大的資料庫，透過智慧型巨量資料分析平臺進行關連分析、進階威脅防護、機器學習能力等，提供即時性資料進行防護，為資安服務和雲端安全

帶來全面性的防護，以降低資安威脅，同時透過公私部門合作，幫助政府機關強化調查、攔截網路犯罪。

在全球網路犯罪模式逐漸朝向具針對性且複雜的方向發展之際，政府或組織面臨的問題是識別和回應資安漏洞與風險的時間較長。據調查顯示，亞太地區的組織平均高達520天才會發現遭受攻擊，比起全球平均值146天足足高出3倍有餘。為了因應此趨勢，微軟開始加強作業系統及應用服務的安全，提出包括進階威脅分析(Advanced Threat Analytics, ATA)及進階威脅防護(Windows Defender Advanced Threat Protection, WDATP)等解決方案。在個人電腦作業系統安全上，微軟提出新一代作業系統Windows 10充分利用最先進的硬體技術以協助保護使用者身分識別、資訊和裝置不受到駭客和惡意程式的威脅，其新增加功能簡要說明如下：

1. Windows Hello和Windows Passport 功能：在任何資安環境下，密碼都是最大的弱點，透過 Windows 10的 Windows Hello和Windows Passport 功能，能整合多因素認證並使用生物辨識功能，例如臉部辨識、指紋辨識等，以識別使用者並且嚴格控管存取權，確保密碼不會被駭取。
2. 強化對抗威脅與裝置安全性：利用信賴平台模組(Trusted Platform Module, TPM)防止內嵌於硬體本身的惡意程式執行或在系統載入前執行；信任式開機（Trusted Boot）功能則協助維護作業系統的完整性；裝置防護(Device Guard)下確保只有被允許的程式碼才能在裝置上運行；機密防護(Credential Guard)功能則利用硬體建構的虛擬化環境來保護密碼。
3. Windows Defender：提供惡意軟體防護，目前每天將近有30億個Windows裝置受到保護。

在進階防護部分，WDATP彙整各端點和可疑事件的關連，

協助管理者檢視端點電腦發生事件的狀態，結合了全球超過10億台Windows裝置、250萬兆網路索引地址及無數的可疑檔案及行為(如圖2)，用以偵測類似的匿名行徑、病毒及攻擊。這項服務安裝於微軟的巨量資料分析平台並追查行為記錄，再整合到作業系統內建的Windows Defender特徵碼中，由防毒軟體執行自動阻擋機制。

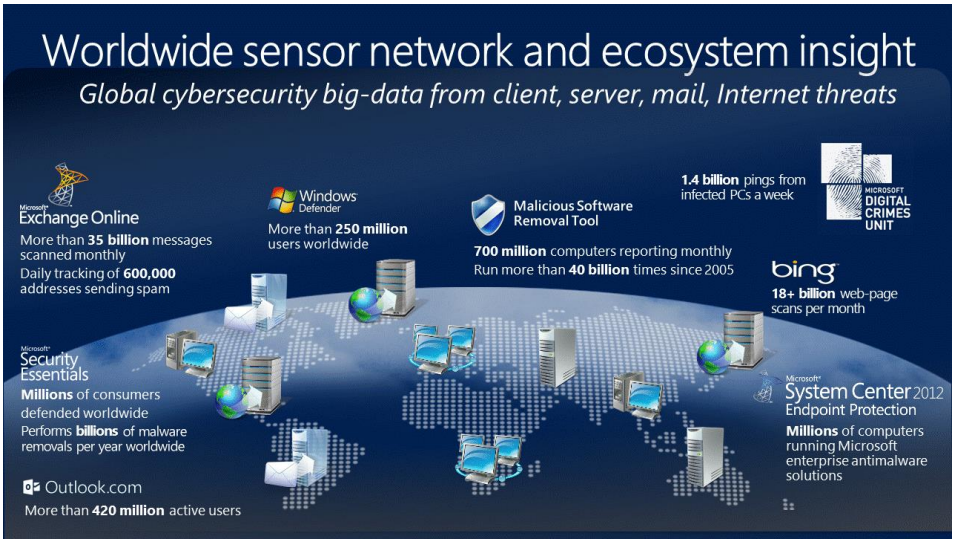


圖 2 微軟全球感測生態系統

此外，微軟設置資訊安全意外處理小組(Incident Response Team, IRT)協助客戶解決安全問題，如客戶懷疑遭受駭客入侵時，由微軟IRT積極協助找出駭客的入侵軌跡，及判斷哪些資料被非法竊取。至於現在盛行以Open source快速開發應用服務或軟體，與會的代表也討論是否其安全性較低，有些人則對相關支援的可用性與品質提出質疑，微軟安全專家則認為重點是引用Open source時要多方考量安全的問題，而不該刻意避免使用Open source，且open source軟體的開放性，其安全性或功能性的缺點與漏洞皆能透過程式設計者社群的共同開發，快速的被修正與改善，因此在資安或品質上也具有一定的保障，但由於微軟有整個專業團隊進行研究開發，因此相較Open source產品而言，微軟還是

對自家產品深具信心。

(二)微軟技術透明中心

對政府機關而言，除了重視來自網路上的各種安全威脅外，對於使用的產品或服務也需確保沒有漏洞，以往對於微軟產品較為封閉性，設計人員不知道其原始碼是否存在資安漏洞，「技術透明中心」是微軟長期投注於政府安全計畫(Government Security Program, GSP)的重要基礎，加入GSP的會員可以在該中心內運用測評工具，檢視和剖析微軟產品的原始碼，以便政府能更及時、充分地瞭解微軟產品的安全性，加強微軟安全專家和政府機關的交流與合作，提供政府機關更多網路安全威脅和漏洞的相關資訊。目前已有近 40 個國家和國際組織參與微軟的政府安全計畫，其中有 10 位參與者是來自亞洲，行政院國家資通安全會報技術服務中心也是會員之一，加入GSP會員有3個好處說明如下：

1. 幫助政府機關評估微軟產品的可靠性，檢視其是否有後門程式或資安漏洞。微軟也提供GSP成員提供各種漏洞及網路威脅報告，遇到資安問題時可依據微軟提供的報告更快速有效地進行處置。
2. 政府機關可以透過微軟技術透明中心中的軟硬體設備，對微軟提供的服務和部署的產品在安全性上更加全面的了解，同時可以分析產品的效能，作為決策的依據。
3. 微軟也會為GSP成員提供服務開發、設計和部署，利用微軟產品與服務設計更加完善的IT系統。

此外，在會議中亦提到面對APT網路攻擊及行動化趨勢，如何強化作業系統的安全性，尤其是在個人電腦的防護上更是重要，因此微軟推出的Windows 10作業系統也提供更多安全性的概念，例如Windows 10會使用受信任的平台模組(TPM)來驗證裝置完整性和整合可延伸韌體介面(UEFI)的功能、信

任式開機功能檢查開機資訊未遭到竄改，採用生物識別技術代替使用者需輸入密碼的方式，另外為了有效阻擋使用者密碼遭受未經授權的認證竊取攻擊， Windows 10 也導入新的安全性機制稱之為機密防護(Credential Guard)，它使用虛擬化安全性的方式來隔離使用者帳號的密碼，因此只有具備特殊權限的系統軟體才能夠存取它們，一旦遭到入侵，ATA 可偵測異常的模式並提供變更設定建議，協助保護使用者的環境，有效提升使用者端電腦的安全防護。

(三)微軟資料中心(Data Center)

微軟在全球共有 38 個資料中心，新加坡是微軟資料中心設置地點唯一在熱帶國家的資料中心，本次參訪係由微軟負責維運資料中心的 Frank Yang 介紹，由於新加坡面積小、電力無法自足且氣候炎熱，而資料中心是非常耗能的產業，因此與會者很好奇微軟為什麼選擇新加坡設置資料中心？

Frank 表示微軟在評估資料中心的設置地點時，會考慮許多因素，包括：網路環境、法規開放程度、稅率、政治與經濟環境等。選擇新加坡設置資料中心的原因除了新加坡為亞太地區重要經濟樞紐外，政治情勢相對穩定、電力傳輸網路的成熟度跟穩定性，及法律規範上也較開放，這些因素吸引微軟於地狹人稠、土地取得成本相對高昂的新加坡設置資料中心。

Frank 表示，考量建築物載重及風險，資料中心建置多數採低樓層、大坪數之設計，微軟新加坡資料中心是少數採高樓層(9 層)設計之資料中心，這主要也是因應新加坡地狹人稠而設計，微軟資料中心透過虛擬化軟體定義方式，將全球客戶之重要資料以雲端分散儲存於全球各地的資料中心，以降低資料遺失之風險。因此單一資料中心遭受攻擊對客戶之影響非常小，為了確保資料中心的安全性，微軟訂定嚴格之措

施，例如：受邀參觀之訪客僅可由微軟安排之接駁車接送往返資料中心，亦不對外公布資料中心地址(雖然大家都知道地點，但法規要求而不在文件或網站上公開地址)；採取嚴格之門禁系統設計，內部員工可透過識別證與指紋辨識通過獲得授權的路徑，且進出每道門的時間皆受嚴格之限制，如需連續穿越兩道門，則需先關閉第一道門後始可獲得第二道門之穿越許可。

本次參訪資料中心行程，所有參訪同仁之個人物品皆須留置於會議室內，不可攜帶進入資料中心內部(包括手機、皮帶、金屬物等)，參訪者須配戴識別證始可進入管制區，且訪客識別證被設定效期，一旦效期已過識別證即呈現粉紅色，警衛可從監視器上清楚判別人員是否獲准進入管制區，並做適當的處置。進入資料中心核心區後要通過類似安檢門之檢查，如 X 光機發出異常警告則由警衛再一次檢查是否攜帶違禁品，資料中心除採取嚴格的安全要求外，在實體設計或安全管控措施還包括：

1. 在土地稀少且昂貴的新加坡，微軟除花費大量成本建置資料中心，資料中心旁亦留有空地為未來擴建預作準備，此外在大門至資料中心入口間設置大型停車場作為安全緩衝空間，且車道採彎道式設計，以降低攻擊行為所產生之風險。
2. 資料中心整體空間經過巧妙設計，所有須與外界聯繫之作業空間均由一大型走廊作為緩衝區，以與內部作業區隔離。資料中心因硬體設備需求量龐大，大量採購之硬體備品僅可由廠商運送至資料中心之緩衝區，再由微軟工作人員接手將備品搬運至內部儲藏區。資料中心具高度安全要求之空間，會以高強度的頂天立地防護網作區隔，避免有心人士攀爬進入竊取或破壞；資料中心之建築結構、空間、空調電力、電信線路、電話線路等亦於設計之初即妥善規劃在不同區域，

各廠商維修時不會互相干擾,以避免有心人士假冒維修人員進入破壞,在資料中心生命週期間(約 10-15 年)不再變動,因此亟須仰賴 DC 相關專業從業人員的建置與維運經驗,方可建置出一個完善的資料中心。

3. 微軟資料中心對客戶之資料有保密之義務,因此全球各資料中心間以自有的光纖網路連結,非透過網際網路交換資料;另一旦硬碟故障或毀損後遭置換下來,則一律置放在專用回收桶中並予以上鎖,待累積至一定數量再統一進行實體銷毀作業,以確保客戶資料不會外洩。

4. 客戶主機機架必須上鎖,並符合各國法規需求,因此每年都會進行合規性審核。微軟在進行設計時會參考主要國家、主要行業及主要標準進行設計與驗證,以符合大部分國家之要求。

5. 以雲端服務的特性設計,一旦某設備元件毀損並不會造成伺服器無法提供服務,因此若硬碟故障或毀損並不需要馬上更換,大量降低人力的需求。

6. 管理人員和系統人員權責分開,管理人員不知道機器上運營那些服務,他只負責機器設備是否正常使用;而各服務擁有者不知道其服務是放在那台機器設備中,這樣可降低人員須實體接觸機器造成之風險。

7. 運用新興節能技術優化資料中心能源效率,包括冷熱通道設計、機櫃隔板、使用高密度氣密機櫃等,從 2005 年以前能源使用效率(PUE)值在 2.0 以上,至 2015 年時已大幅降低至 1.07 ~ 1.19 之間。

此外 Frank 也提到微軟正在實驗海底資料中心的計畫,把資料中心放入海底的好處是可快速部署,滿足有時效性的需求,像是自然災害救援或世界盃這種全球活動;第 2 個好

處是低延遲性，將資料中心建於近海可大幅縮短資料傳輸的延遲性，最後則可運用海底低溫防止伺服器因溫度太高而當機，並減少冷卻電力，也可減少發電機、電腦與維修人員的數量。

三、 Day3(3月16日):介紹微軟新一代雲端運算平台Azure stack及其安全性

面對雲端服務的發展趨勢，不管是政府或企業亦逐漸往「雲端服務」移動，雲端運算的特性是建立在虛擬化(Virtualization)、易擴充(Scalability)、用多少付多少(Pay-As-You-Go)的概念。藉由虛擬化的技術，不需要很多的主機堆放在機架上，而是以某種形式存在於一個廣大的資源池(Resource Pool)中，而易擴充特性則是在特定尖峰時間可以很快擴充所需的運算資源，這樣便可以大幅降低主機閒置時間的運算成本；微軟也因應這些需要推出雲端運算平台Microsoft Azure，Azure是公有雲服務平台架構，一開始與其競爭對手Amazon Web Services (AWS)一樣是以IaaS作為切入點提供基礎運算服務，然而企業或組織將內部的機敏資料存放至公有雲環境仍有疑慮，覺得機敏資料放在內部資料中心來得安心，MAS（Microsoft Azure Stack）則是微軟專為新世代混合雲運作架構而設計的平臺，企業或組織可以透過MAS自行打造出如同Microsoft Azure公有雲的靈活性和運作規模，此平臺可以完全由企業或組織所掌握，並且在需要時能夠輕鬆地與公有雲介接達成混合雲的運作架構,如圖3所示。

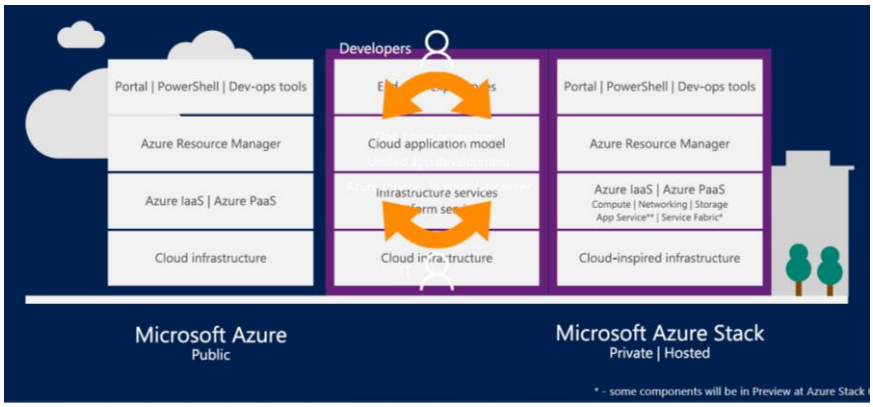


圖 3 Microsoft 混合雲平臺

Azure Stack 提供下列三種方式以確保用戶安全

(一)建立安全策略

Azure stack 平臺的安全策略為 Protect、Isolate、Detect 及 Respond，如圖 4，分述如下：

1. 保護(Protect)：透過找出設計漏洞、認證、完整性及稽核等方式避免駭客找到平臺弱點，並潛入竊取資料。
2. 隔離(Isolate)：透過加密、DoS 防禦、授權等方式達到隔離平臺的效果，限制駭客的行動。
3. 偵測(Detect)：提供入侵和偵測的日誌檔進行大數據分析、採用阻斷服務攻擊的預防措施及定期進行滲透測試等方式，以監控、偵測並預測可疑的活動，預測可能的安全威脅。
4. 回應(Respond)：持續從各種攻擊手法及經驗學習，並且修補安全漏洞。

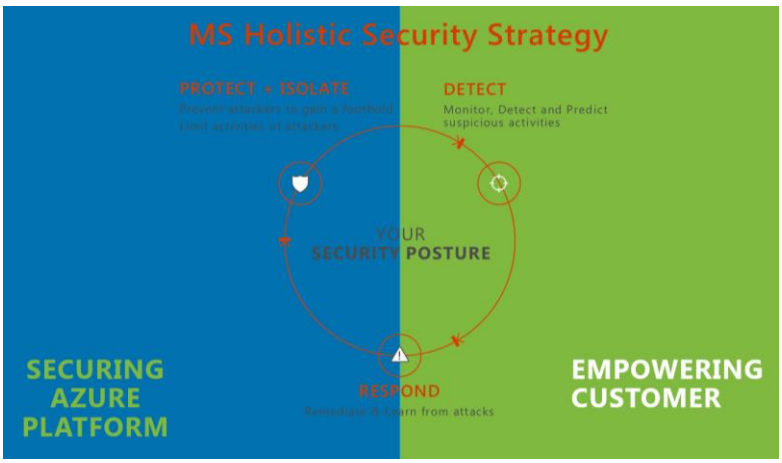


圖 4 Microsoft Azure Stack 安全策略

(二)通過第三方認證

MAS 提供集中的安全中心,讓用戶可以確認微軟如何履行其對安全性的責任。同時微軟亦透過各種第三方認證(包括 CJIS、FRAMP、FERPA、ISO27001、ISO27018、PCI DSS Level 1、SOC 1 Type 2 和 SOC 2 Type 2 等)如圖 5 所示，細節請參考網站 https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings，以確保整體資訊安全，讓客戶安心且無縫接軌至雲端。

圖 5 Microsoft 通過之第三方認證

(三)完善資料保護方式

在雲端服務上，微軟採取下列方式確保客戶存放之資料安全

1. 實體隔離

將每個客戶的資料進行實體隔離，避免單一客戶資料遭受入侵或竊取時影響其他客戶。

2. 資料加密及跨境資料保護

在儲存或傳輸中的資料進行加密，且可由客戶自行部署選擇加密方式，以符合確保資料的機密性和完整性。

3. 資料複製

提供客戶多種資料複製選項，包括複製數量和複製於哪個資料中心。

4. 資料銷毀

當客戶刪除資料或離開 Azure 時，微軟將遵循合約要求進

行刪除，並確保客戶存儲的資料不可被存取。

參、心得及建議

在數位時代，各國政府為了使公眾服務更有效率，除了思考如何讓民眾透過一站式服務即可串接各項服務，亦逐漸將服務雲端化，以因應民眾各項服務需求，然因資訊科技的快速演進、駭客攻擊手法日趨新穎多變，為了確保政府服務安全，網路安全亦已成為不容忽略的關鍵課題。本次參加微軟公司資訊安全研討會，除藉機拜會新加坡科技局瞭解新加坡在推動個人化服務的想法及未來規劃，亦彼此交換在政府資訊安全的做法，惟因適逢該局正在預算審議期間，會議時間僅有 1.5 小時，致無法有更深入之探討；另外在微軟資安研討會過程中，瞭解微軟公司在網路安全及新一代產品所做的資安努力外，對於其資料中心的管理及維運更留下深刻之印象，綜整本次會議有以下幾點心得及建議：

一、新加坡政府在管理與技術能力上展現優越的主導力，尤其組織調整設置新加坡科技局作為統籌國家整體的網路安全政策方針和因應措施，並主導所有公務機關公務系統與電子郵件實體隔離的任務。我國在 105 年 8 月 1 日也成立專門負責國家資通安全政策的行政院資通安全處，將資安提高到國安層級，全力保護我國的數位國土安全，這點和新加坡政府及國際趨勢不謀而合，後續可加強與新加坡政府合作交流，參採其經驗，提升政府機關資訊安全能量。

二、對政府或企業來說，以往多將資料存放在傳統的資料中心或是自建的資料中心，隨著雲端運算技術趨於成熟，傳統的資料中心也逐漸轉型為雲端資料中心，微軟透過軟體控制方式將客戶資料存放在全球不同的雲端資料中心，除了讓駭客難以得知感興趣的資料究竟存放在何處，也達到異地備援及備份的目的，即使單座雲端資料中心遭受攻擊，對客戶也無太大影響，將客戶之風險降至

最低，後續推動政府機房整併，資料中心建置可參考其模式逐步規劃建置。

三、為確保各機關提供為民服務資訊系統安全，以往都會要求上線前進行原始碼檢測，上線後也會進行弱點掃描、滲透測試等作業，技服中心也定期進行攻防演練作業，針對一些重要系統如戶政、報稅、公路監理等，後續亦可參考微軟GSP計畫，與資安廠商簽訂保密協定下開放原始碼讓資安公司進行檢視，以確保系統安全。

四、資料中心建置、管理及維運須具備專業的技能，同時須要長期經驗累積，維運過程中也會面臨很多意想不到的事，因此政府機關除使用專業的資料中心外，如果機關係自行建置維運資料中心，應加強機房專業人才的培養及機房管理能力之訓練。

五、我國政府機關許多租用GSN IDC機房，惟在門禁管理、機房安全等均有很大改善空間，後續可逐步要求承商參考微軟資料中心機房管理方式逐步進行改善。

肆、附錄

附錄一、會議議程

	時間	議程/行程
Day 1 – 03/14	09:55 - 14:30	搭乘長榮航空前往新坡樟宜機場
	14:30 - 15:30	通關手續
	16:30 – 18:00	拜會新加坡科技局(GovTech)

	時間	議程/行程
Day 2 – 03/15	08:30 - 09:00	前往新坡微軟技術透明中心
	09:00 - 09:30	開場歡迎致詞
	09:30 - 11:00	參訪微軟「技術透明中心」和「網路安全中心」
	11:00 - 12:00	參訪微軟技術中心(MTC)
	12:00 - 13:00	午餐
	13:00 - 18:00	參訪微軟資料中心(DC)

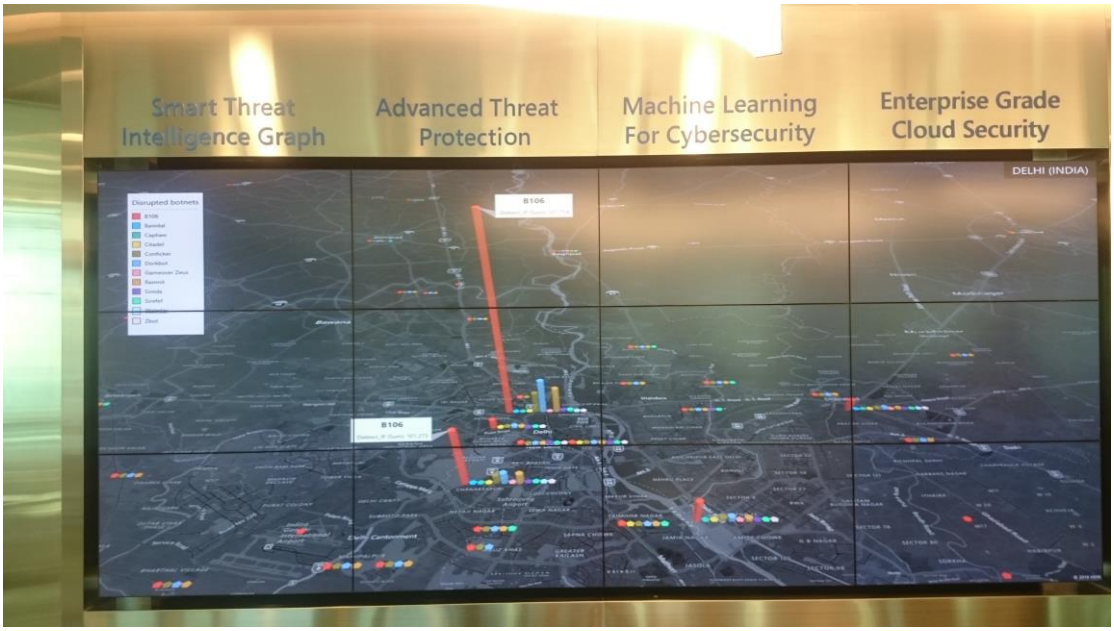
	時間	議程/行程
Day 3 – 03/16	09:00 - 09:30	前往新坡微軟技術透明中心
	09:30 - 11:00	Next Generation DC Platform : Azure Stack Briefing
	11:00 - 12:00	國家資訊安全政策研討
	12:00 - 13:00	午餐
	13:00 - 18:00	Government Showcase and Partner Solution

	時間	議程/行程
Day 4 – 03/17	10:00 - 11:00	前往新坡樟宜機場/集合辦理登機
	13:10 - 17:40	賦歸

附錄二、照片剪輯

拜會新加坡科技局後合影

微軟位於新加坡總部



微軟網路安全儀表版

微軟位於新加坡之「技術透明中心」和「網路安全中心」

資安研討會