**熱點聚焦**

# 零信任網路下的資訊安全防禦

## Cyber Security Defense under the Zero-Trust Network

蔡一郎

財團法人國家實驗研究院國家高速網路與計算中心

網際網路發展至今，目前已進入零信任網路（Zero Trust Network）的時代，新興資訊科技打破典型資安防禦架構，行動化與數位化的時代讓資安防禦更加困難，由台灣學研網路部署的誘捕網路，到近年來政府積極建立的情資分享與分析架構（Information Sharing and Analysis Center），期待從資通訊技術（Information Communication Technology, ICT）走向維運技術（Operation Technology, OT）時，都能夠掌握資安威脅，而網路上隨著不同應用類型資料與資訊交換，雲端服務平台的發展，目前已進入萬物聯網的時代，除了典型的資安架構，因應資訊科技的發展，又增加許多型態服務，加上與行動裝置整合，讓資訊安全的防禦機制，更難有一套通則，反而面對不同的企業或是服務平台，都必須採用服務導向的方式，進行資安風險的評估，以確定所建立的數位邊界，能夠有效的掌握進出這個數位邊界的通訊行程以及交換的資料。

目前已進入一個由軟體定義安全邊界（Software Define Perimeter, SDP）的時代，不論雲端服務、物聯網應用到 AI 應用，都需要考量到資安議題對於應用科技所帶來的影響，而其中最重要的都是應用

軟體的開發安全，多數的程式開發人員在撰寫程式時，早期主要注重在程式功能面或是使用者界面的開發，在資訊安全的考量上較少，造成了應用程式在運作時一些資安的問題，OWASP（The Open Web Application Security Project）發佈的 The Ten Most Critical Web Application Security Risks，就不難看出許多網站應用程式所存在的重大風險，其中許多的風險，都能夠透過程式設計的改善，就能夠避免該風險的發生。

如何掌握網路上的異常通訊，或是發掘異常通訊行為，然後加以阻止或減緩所造成的影響，以符合資訊安全防護期待，這是一個值得思考的問題，典型作法是透過網路封包的截取，然後進行網路通訊解析，以掌握網路通訊行為，不過當加密的流量成為常態，原本網頁服務在 2018 年已有超過 30%採用加密通訊協定，如果以雲端服務而言，更高達 70%網路流量採用加密通訊協定，依照此趨勢繼續發展，在 2019 年雲端服務採用加密通訊的比例，有機會一舉超過 80%的門檻，這麼高比例的加密流量，除了原本確定應用程式的使用者可以擁有安全的通訊之外，另一隱憂是同樣也有越來越多的惡意程式，採用加密通訊流量進行資料傳輸，以往可用於網路上進行特徵比對或是過濾通訊內容的防護機制，當它面對這些被加密的通訊時，已無法發揮預期功能，甚至無法對於這些隱藏在其中的惡意行為進行任何的阻絕，這將會企業營運上的隱憂；另一個需要正視的問題是雲端服務大量出現，除了便利性，也帶來新的資安風險，以大多數人經常使用的雲端儲存服務而言，企業對於營業秘密的保護尤其重視，這些都是攸關企業競爭力的重要因素。

進入 AI 時代，多樣化的創新應用不斷的出現，當然在資訊安全的領域，也有人不禁會問，當人工智慧發揮到極致，人類是否將無

法掌控這個世界，出現類似電影情節中來自未來的魔鬼終結者，唯一目標就是執行天網（Skynet）賦予的任務，殺掉未來世界中挺生而出對抗天網的反抗軍，試圖改變歷史，這些情境從現在來看仍有些困難點，但我們不禁也擔心在資安防禦的領域，導入人工智慧是否能夠真正防禦外來攻擊，或是將人類視為最大的敵人呢？2019 年初 Yelp 的神經網路除錯程式，將程式開發人員所安的程式全刪了，也刪除了資料庫中的資料，造成網站營運中斷；AI 運算時代讓以往許多耗費時日才能夠解決的題目，因為資訊科技的發展，縮短了原本需要花費的時間，改善了原本分析的結果，加上數據分析的加值應用，也讓許多的領域在新興的議題上，能夠更往前邁進，這些都是需要整體環境的成熟，目前國網中心的「台灣杉 II」更扮演著國內 AI 運算平台的重要角色，提供學研與產業界可以取得 GPU 運算以及 AI 研發所需要的環境。

物聯網路成為下一個世代的主角，目前已有越來越多裝置透過網路的接取，成為網路世界中的一員，配合這些裝置上所開發的應用程式，建構起資料交換的機制，透過網路的連結，進行裝置與遠端（雲端）的資料交換管道，也衍生了許多的資安議題，包括了裝置本身的安全設計是否到位？應用程式的開發是否妥善的保護了使用者的機敏資訊，或是通訊的方式是否已經考慮了資料傳輸時的安全？遠端使用者的身份認證方式也挑戰進入系統時的第一道門檻是否強固？這些不同的議題再配合著各種不同型態的雲端服務，讓整個資安防禦的邊界更難以定義。

參考由雲端安全聯盟（Cloud Security Alliance, CSA）發佈的 SDP 安全框架，目標以避免來自網路的攻擊行為，包括分散式阻斷服務攻擊（Distribution Deny of Services）、中間人攻擊（Man-in-the-Middle）

以及參考 OWASP 所發佈針對 伺服器服務查詢（Server Query）等相關的攻擊行為，安全架構涵蓋了 3 個主要的角色，分別為用戶端 SDP Client、控制端 SDP Controller 以及閘道端 SDP Gateway，其中將身份識別（Identity）以及公開金鑰基礎建設架構（Public Key Infrastructure, PKI）納入安全框架構，這些都是目前雲端平台在提供網路應用服務時可以參考的架構，不過面對目前複雜的服務架構而言，如何建構安全的服務機制仍會是一大挑戰，加上近幾年行動化與數位化的普及，智慧型行動裝置的普及，延伸了企業的服務終端，不再局限特定的場合或是平台才能夠使用資訊平台所提供服務，反而因為網際網路的連結以及頻寬不斷的提昇，讓原本許多需要網路頻寬支持的應用服務，得以在目前的行動通訊世代中實現，對於原本的服務平台而言，更是不得不重視的使用者行為與使用型態的上的轉變，所帶來的影響與衝擊，不得不讓我們必須重新審視現有的資通訊架構，除了效能上的問題之外，在資安的議題上該如何看待。

企業對於營運而言，其重視程度往往大於對於資安議題的重視程度，從過往層出不窮的資安事件就不難得知，從「服務營運」的角度看待「事件應變」，從典型企業的思維，當發生資安事件時，大家多數認識這些「資訊部門」的事，或是買套防毒軟體或是買台防火牆就可以搞定，其實以目前資安事件的種類而言，並不是如此的單純，在目前的時代中，「沒有人是局外人」正印證了企業面對資安事件發生時，應變的範圍多數與整個企業有關，每個員工都必須擔負著資安防護的責任，也必須有相關的認知，從資訊科技以及通訊科技，到產業獨有的維運科技，其中以維運科技的角度來看，經常被認定與企業的資通訊並不相關，不過在工業 4.0 以及智慧製造潮流之後，典型產業面臨的轉型壓力，也需要利用大數據分析，或是人

工智彗的運算，找到最佳化的解決方案或是生產製造的參數，這些都必須仰賴前端的感知網路對於數據資料的收集，越完整，越真實的資料，將會更有機會在更短的時間內，找到預期的目標。

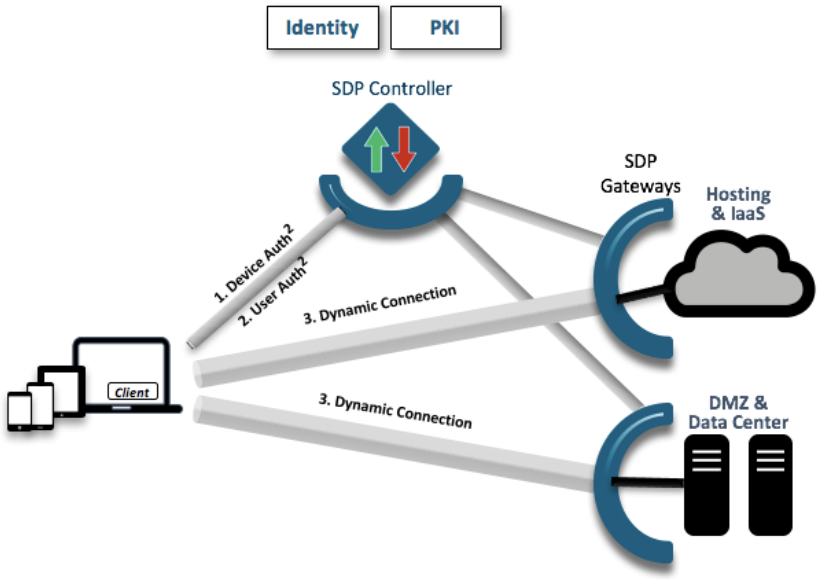


圖 1：CSA 的 SDP 第一版的安全框架

在「網路攻擊」與「企業防禦」兩個面向，後者的複雜程度遠高於前者，因為網路攻擊手法變化快速，而且透過網路的連結，就算遠在地球的另一端，只要攻擊者連上網際網路，就能夠輕易的對企業發動攻擊，對於攻擊目標進行資料的竊取或是阻擋服務，都讓企業在目前的時代中更難加以防範，尤其對於分散式的阻斷服務攻擊而言，更是攻擊來得快，去得也快，在遭受攻擊期間，這些對於服務的網路服務，輕易影響其營運的效能，重則可能直接遭到阻斷服務，而對於攻擊來源的追蹤更是不易，因此資安技術已不再局限於傳統的資安領域，駭客的攻擊手法更是如此，經常每半年或是更

短的時間，都有新型的網路攻擊手法出現，對於負責企業資安防禦的人員而言，就必須能夠發覺阻絕或是偵測的方式，才能夠阻擋這些以前未發生過的攻擊手法，同時必須確保營運的範圍內不會因為受到網路攻擊，而影響到對於資料的保護或是服務平台本身的營運，這些目標對於企業而言多數是處於弱勢，採取初動的角色進行資安的防禦工作。

一個「零信任」網路的來臨，對於來自於遠端使用者，不論是雲端平台或是終端的使用者，融合了行動化、數位化以及虛擬化的世代，在目前的環境中更需要考慮各種不同的層次的資安問題，對於防禦而言更需要設計出多層次的資安防禦機制，保護企業重要的數位資產，同時也需要考量這些數位資產的生命週期，確保所投入的資源能夠最精準的應用在需要重點保護的標的物上，目前駭客有興趣的目標已經涵蓋許多以往資安防禦所忽略的，隨著新興資安科技的應用，除了帶來便利之餘，也將帶來新的資安問題，而目前許多的使用者對於資安的意識已大幅提升，在使用便利的行動通訊之餘，也需要留意可能對於使用者本身造成的資安風險。