淺談零信任架構

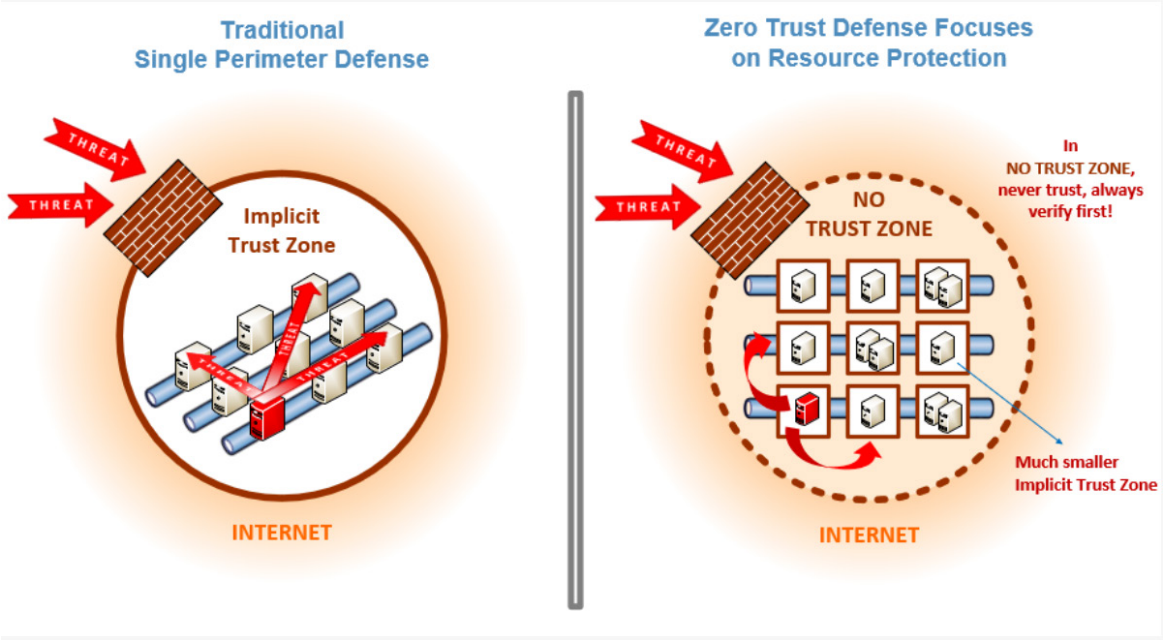
蘇柏鳴 / 金融聯合徵信中心 資安部

一、何謂零信任 (Zero Trust)

關於零信任概念的發展，追溯最早的起源，為2003年Jericho論壇上[1]討論的主軸，是關注於網路資源在不同企業的共享與利用，可以去除企業之間的邊界，因此主要是聚焦無邊界趨勢下的網路安全解決方案。不過，當時論壇延伸出的技術探討，也成為了零信任後續發展的基礎。

較為具體的零信任概念，是在2010年由John Kindervag提出。John Kindervag認為裝置不再有信賴與不信賴的邊界，以及不再有信賴與不信賴的網路與使用者，像是不因內網或外網而有信任或不信任的情況，也會不會有絕對信任的使用者，而是判斷用戶確切行為與使用情境，再去決定相關權限，簡單來說就是基於「永不信任、持續驗證」原則。

圖一、Zero Trust 與傳統防禦比較[2]



1 查士朝，https://s.itho.me/ccms_slides/2021/5/13/1fbdd0b1-493b-4943-aa73-fdaf070b596b.pdf

2 【臺灣資安大會直擊】看懂零信任架構，先釐清對於ZTA常見的3大迷思，https://www.ithome.com.tw/news/144551

二、NIST SP 800-207零信賴架構的教條 (Tenets of Zero Trust)

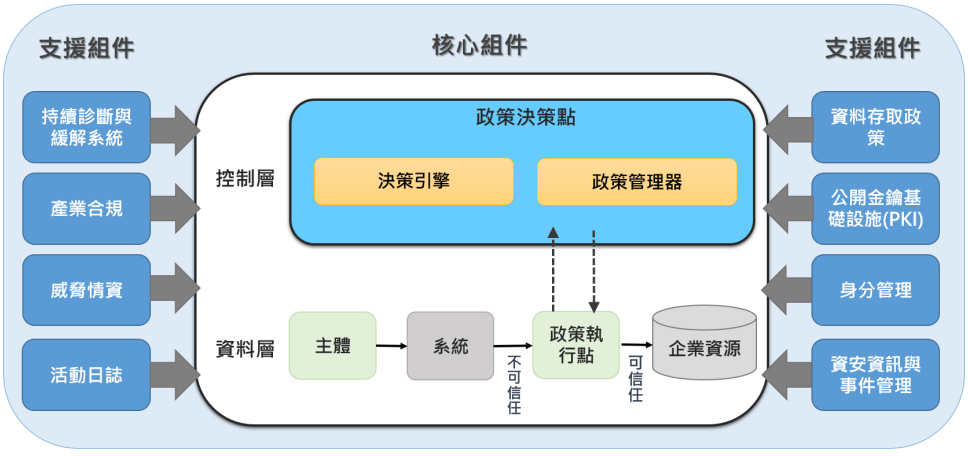
2020年國家標準暨技術研究院（National Institute of Standards and Technology，簡寫為NIST）公布了關於零信任架構（Zero Trust Architecture，ZTA）的SP 800-207，這是一個美國政府採用ZTA的重要參考標準文件，提供架構面的建議與實作概念，以下為SP 800-207對於Zero Trust的七個教條：

1. 所有的資料來源與運算服務都要被當作是資源
2. 不管是和哪個網路位置的裝置通訊，都需要確保安全：
   不要依照網路位置來決定是否信賴。要先評估要求者的可性度，存取而是以該次連線為基礎。之後才可讓他存取。
3. 對於個別企業資源的存取要求，應該要以每次連線為基礎去進行許可。
4. 資源的存取應該要基於客戶端識別（client identity）、應用服務（application/service），以及要求存取資產可觀察到的狀態，以及可能包括的行為或環境屬性去動態決定。
5. 企業監控與衡量所有擁有與相關資訊資產的正確性與安全狀態：沒有資訊資產本身是可以信賴。
6. 在允許存取之前，所有的資源的身分鑑別與授權機制，都要是依監控結果動態決定，並且嚴格落實監控裝置與資源風險。
7. 企業應該要儘可能收集有關資訊資產、網路架構、骨幹，與通訊的現況並用這些資訊來增進安全狀況。

三、NIST SP 800-207之零信任架構

1. 核心組件：執行鑑別、決定授權及管理連線。
2. 支援組件：支援存取決策的資訊與系統。
   (1) 決策引擎（Policy Engine，PE）：作為給予取存權限語法的過濾點
   (2) 政策管理器（Policy Administrator，PA）：建立取存管道的閘門
   (3) 政策決策點（Policy Enforcement Point，PEP）：啟動, 監督或中斷取存的檢查點

圖二、NIST SP 800-207之零信任架構



3 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf，p.6

四、目前推行進度

目前世界主要國家陸續推出與零信任相關之規範，相關規範如下:

1. 新加坡：2021年10月發布《2021年新加坡網路安全戰略》，積極推動網路安全思維與防護模式創新，要求相關機構實現安全防護思維的轉變，實現從邊界防護向零信任安全模式轉變，成為亞洲首個在全國範圍推行零信任的國家。
2. 美國：2021年5月美國總統拜登行政命令（EO 14028）發布，顯現零信任已經成為美國政府看重的網路安全策略，2021年9月美國行政管理和預算局（office of Management and Budget，OMB）[4]提出「聯邦零信任戰略」草案[5]，此策略在2022年1月26日正式發布（圖三），該備忘錄要求各機構於2024 年前實現特定的零信任安全目標，備忘錄中規定的戰略目標與CISA的五個支柱[6]一致:
   (1) 識別（Identity）：機構工作人員工作中，使用企業級的識別來存取使用的應用程序，並使用防網路釣魚的多因子認證(MFA) ，來保護這些人員免受到複雜的網路攻擊。
   (2) 裝置（Device）：機構需要擁有其運行的每台設備的完整清單，包含所有授權於政府使用，這些設備要可以預防、偵測和回應事件。
   (3) 網路（Network）：機構對於環境中所有DNS請求和HTTP流量加密，並制定網路分隔計畫。
   (4) 應用程式（Application）：機構將所有應用程式視為已連接網路，並定期對應用程式進行嚴格的實證測試，並樂於接受外部漏洞報告。
   (5) 資料（Data）：機構需有清晰的資料共享的路徑，以部署利用徹底的數據分類。要利用雲端服務與工具的優勢來監控對其敏感數據的訪問，並實施了企業範圍的日誌記錄和信息共享。

圖三、M-22-09備忘錄

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

4 https://www.whitehouse.gov/omb/

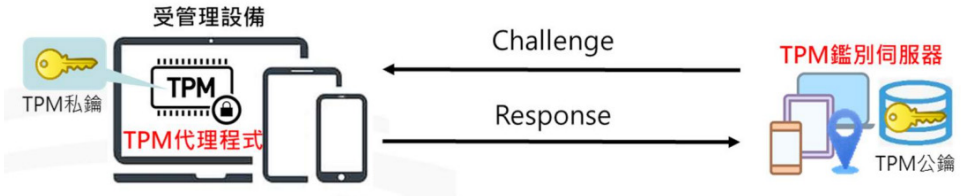
5 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf，M-22-09 Federal Zero Trust Strategy

6 CISA，Zero Trust Maturity Model https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf，p.7

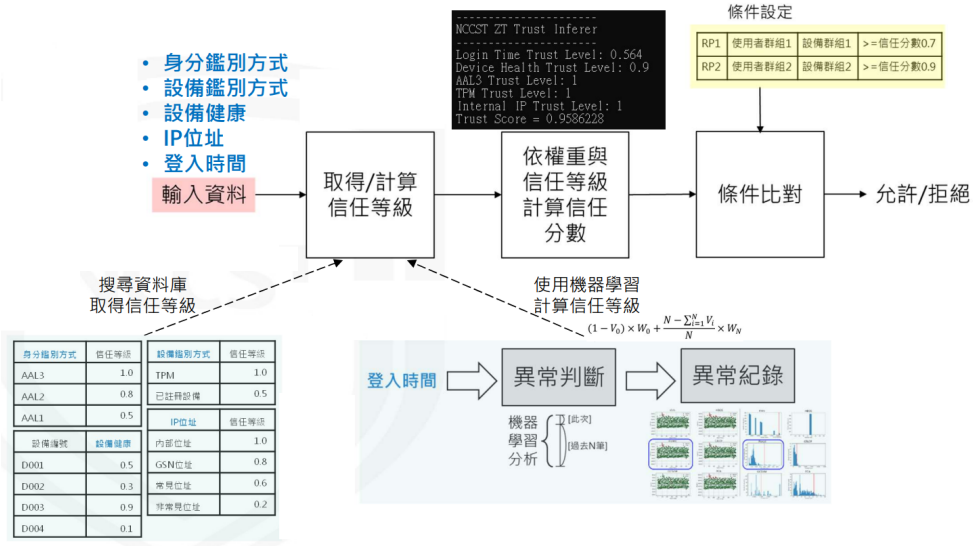
台灣依據第六期「國家資通安全發展方案（110年至113年）」[7]之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，將發展零信任網路資安防護環境，推動政府機關導入零信任網路，完善政府網際服務網防禦深廣度，主要參考美國NIST零信任架構，目前優先推動A級公務機關導入，政府零信任網路採存取門戶部署方式，具備身分鑑別、設備鑑別及信任推斷3大核心機制：

1. 身分鑑別：FIDO2身分鑑別與鑑別聲明。
   (1) FIDO2無密碼雙因子身分鑑別：通過FIDO聯盟驗證之FIDO2伺服器與生物識別鑑別器。
   (2) 簽章與加密之身分鑑別聲明：提供JWT與SAML 2種標準格式之函式庫，以供機關資通系統（RP）介接時取得與驗證鑑別聲明。
2. 設備鑑別：TPM（Trusted Platform Module）設備鑑別與設備健康管理。
   (1) 基於信任平台模組（TPM）之設備鑑別方法：執行基於TPM內私鑰之公開金鑰密碼系統鑑別協議。（圖4）
   (2) 設備健康管理：持續更新設備健康狀態，依設備健康狀態隨時換算設備健康信任等級。
3. 信任推斷：持續更新設備健康狀態，依設備健康狀態隨時換算設備健康信任等級 (圖5)。

圖四、基於信任平台模組 (TPM) 之設備鑑別方法[8]



圖五、基於分數與情境之信任推斷機制[8]



7 國家資通安全發展方案(110年至113年)，https://cloudschool.chc.edu.tw/open-message/074738/get-file/6041e464285d5d58af198572.pdf

8 政府零信任網路說明，https://download.nics.nat.gov.tw/UploadFile/zerotrustnetworks/%e6%94%bf%e5%ba%9c%e9%9b%b6%e4%bf%a1%e4%bb%bb%e7%b6%b2%e8%b7%af%e8%aa%aa%e6%98%8e_V1.9_1110712.pdf

五、結論

由上所述目前零信任導入已經為主要新進國家重視之項目，除了行政院推動資通安全責任等級A級公務機關推動導入外（圖六），金管會也於2022年12月27日發布「金融資安行動方案」2.0[9]，在方案中的精進重點提到「鼓勵零信任網路部署，強化連線驗證與授權管控」，「零信任是資安的策略或原則，並非產品」，所以沒有任何一個獨立產品能符合零信任架構需求，目前提的框架也需要視各機構目前的狀況作調整，所以檢視目前架構盤點及資訊資產，為評估後續的第一步，再來評估目前架構需要做多大的變動，畢竟任何資安架構都需要在系統穩定前題下推動。

圖六、A級公務機關之導入時程

9 「金融資安行動方案」2.0，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=202212270001&dtable=News