數位轉型的挑戰 - 資安零信任

中國文化大學財務金融學系 助理教授⊙陳 曦

先從一則膾炙人口的故事說起，關於世界歷史上最知名的通關密碼（或者說是通關密語），在「阿里巴巴與四十大盜」的故事裡，在森林中砍柴的阿里巴巴無意間聽到強盜首領對著山壁大喊神奇的「芝麻開門」，山洞外的大石塊便打開了。阿里巴巴趁著強盜離開以後如法泡製，進到山洞裏面發現了強盜存放的滿滿金銀財寶。但看來阿里巴巴並不貪心，或說考慮到搬運問題，只取了一袋金幣離開，顯然，阿里巴巴是還有趁強盜還沒發現可以再回來把金銀財寶一點一點弄回家的打算。接下來故事情節雖然曲折，但強盜發現的並不算晚，而最終結局還是善良的主角獲勝。這故事要告訴小朋友的應該是善良的品格很重要，而現代人應該理解的是：密碼要是沒有保管好，金山銀山甚至性命也可能不保。

維護資產安全並不是新的概念，只是以往人們相信山洞門口的石塊、家的圍牆和一句密語就足以防護的概念，可能從數百年前就已經被視為不可靠，寓言故事中事實上隱喻了零信任的概念在其中，即強盜相信隱密的山洞、巨石和通關密碼足以保護資產，結果破口仍然在無意間，甚至還是被首領所洩露。

今天，相信有軟體防火牆就可以把敵人成功擋在護城河外、使用者必須靠著帳號密碼登入就可以讓系統運作高枕無憂的時代已經一去不復返。企業、基礎設施、政府與非政府機構遭到攻擊、入侵、勒索和個資外洩的新聞屢見不鮮，即便在城牆內也潛藏著威脅。此外，現在還有太多企業和組織的資源位在圍牆外面，包括系統、應用服務、用戶、數據資料等等。而員工使用自己的裝置在外和公司的系統連結以便工作、不同行業的合作夥伴或客戶運用系統連結到企業的系統存取資料等等新型態業務情形更把問題進一步複雜化，已經很難區分威脅來自於圍牆內或外，因此，推動一個更有效的防護方法和機制顯得格外重要，本文介紹「「零信任」基本概念、實施與挑戰提供讀者參考。

概念與原則

近期的零信任（Zero Trust）具體概念是2010年由Forrester Research前副總裁John Kindervag所提出，其後被各界逐步確認的基本前提假設是1. 所有內外部的使用者、裝置和指令都是不可信任的。2. 邊界與系統存在漏洞，就算在已防護的信任邊界範圍內，也不是都確保一定安全。3. 系統與網路外圍邊

界已經或將會遭到侵犯。基於「永不信任，始終驗證（“never trust, always verify”）」這樣的設定，2020年美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）在特別出版物 SP 800-207 中提供了比較完整的「零信任」和「零信任架構（Zero Trust Architecture, ZTA）」定義，簡要來說，即零信任提供了一系列概念和想法，目的在最大程度地降低網路存取時的不確定性，目標是「防止對數據和服務未經授權的存取，同時使存取管控執行盡可能細化」；而「零信任架構（ZTA）」則是組織的網路安全計畫，使用零信任概念，包括元件關係、工作流程規劃和存取策略。

此後包括美國國家安全電信諮詢委員會（NSTAC）、美國網路安全暨基礎安全局（CISA）、白宮行政管理和預算局（OMB）、美國國防部（DoD）等單位均提出了相關政府機構的作業規範準則。綜整其中包括三項重要原則：

1. 明確驗證（Verify explicitly）：需要驗證的包括使用者身份、位置、裝置、網路、設備（包括健康狀態）、應用程式和交易等等。驗證方式也要採取多重驗證、持續驗證、多階段驗證等等方式，像是帳號密碼之外，再加入指紋等生物特徵的辨識。
2. 最小權限原則（Principle of least privilege）：只允許或授予通過驗證的裝置及使用者執行在特定時間內可完成工作的最低限度（Just-In-Time and Just-Enough-Access, JIT/JEA）存取。對於資源的存取基於動態授權，包括客戶端身份識別、聯網裝置、應用程式/服務以及要求存取資產的可觀察狀態，或其他行為和環境屬性等等；並可以透過資料保護限制存取，比如區分唯讀、寫入或執行的不同權限。
3. 假設違規（Assume breach）：在系統與網路外圍邊界已經或將會遭到侵犯的前提下，是一種壞人已經存在內部的概念。系統對任何存取要求預設拒絕並監控檢查所有內外部使用者、設備、配置、網路流量和存取是否存在可疑活動；將資產資料網路分段區隔以將損失降到最低，並強化動態檢測分析與防禦能力提升可視性來對抗滲透和攻擊。

特性與風險防範

簡單的說，零信任重視數據、資產、服務、工作流程、網路帳戶等實質資源的防護，而不是只以網路和系統外圍防護為主。比起防火牆區分系統內部、外部的常見做法，或是端點偵測防護、數據封包分析等等資安措施，零信任架構可以提供更全面且有效的防護。從企業服務的角度來看，零信任採取動態且實時的管控，可以根據使用者不斷變化的狀況即時更新存取權限，對內部資源的防護更加有保障。至於經常發生的如使用者因為木馬等惡意軟體、釣魚郵件導致帳號密碼被盜用等狀況，尤其是在企業外部或遠端的設備，零信任架構也可以透過實時監控、異常偵測、行為分析或信任推斷來辨識

侵入網路的惡意並啟動防護。而最小權限存取管理和網路微分段的做法，讓惡意侵入者即便在獲取權限突破邊界後，也不易取得或操控大部分的資源，即便小規模受到侵害，大部分的資源仍可被有效防護，將損害降到最低。

因此，零信任可以有效對應常見的風險像是資訊系統內的數據資料如個資被竊取、數據資料被竄改、進階持續性滲透攻擊（Advanced Persistent Threat, APT）如潛伏在企業內部持續蒐集與竊取資料的木馬程式、以資料加密與竊取要脅公布機敏資料迫使企業支付贖金的勒索攻擊（Ransomware）、聯網設備裝置或網路控制權被奪取、被當作攻擊跳板或是系統癱瘓等等。

實施重點

2023年4月美國網路安全暨基礎安全局（CISA）發表零信任成熟度2.0的文件，確認包括身分（Identity）、設備（Devices）、網路（Networks）、應用程式與工作負載（Applications and Workloads）、數據（Data）五大零信任架構要素（pillar），並分別針對此五大要素提出階段性（傳統/初始/進階/最佳）執行綱要做法及成熟度評估（如圖1）。此外，CISA也提出了三項跨要素能力，即可視性與分析（Visibility and Analytics）、自動化與編排（Automation and Orchestration）及治理（Governance），提供整合五大要素持續進步的機會。

可視性和分析支援資訊全面的透通可見，為政策決策提供資訊並促進對應行動；自動化和編排功能利用分析見解來支援強大且簡化的操作，以處理安全事件並在事件發生時做出回應；治理使機構能夠管理和監控其監管、法律、環境、運營等要求，以支持基於風險的決策。治理能力還可以確保支援任務、風險和合規目標的合適人員、流程和技術到位。整體而言，零信任架構的規劃與做法可說已相當明確。

在國內，基於「資安即國安」的重大國策，零信任概念與架構也已經積極在政府、重要產業與民間企業布局。行政院國家資通安全研究院在112年發表「政府零信任架構說明」及「政府零信任網路身分鑑別機制導入建議v1.1」，內容除表明與美國國家標準與技術研究院NIST SP 800-207採取相似一致的架構措施之外，還強調零信任網路將在政

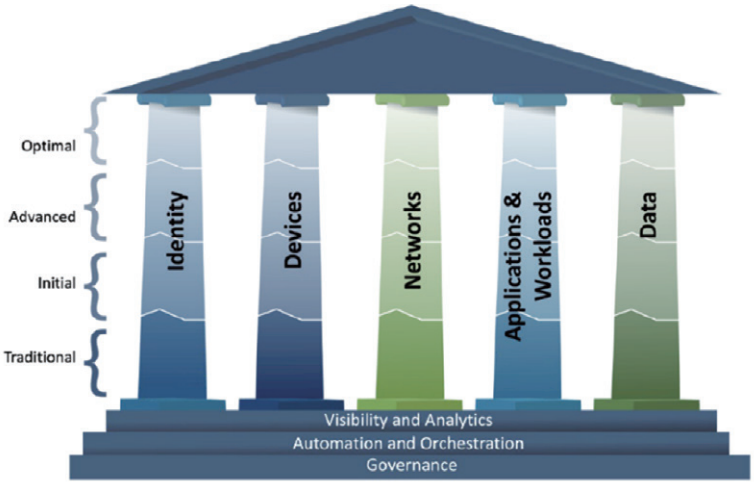

圖 1、零信任五大要素與成熟度階段
資料來源：Zero Trust Maturity Model. V.2.0., CISA 2023, Department of Homeland Security. P.9

府機構逐步導入決策引擎之身分鑑別、設備鑑別及信任推斷三大核心機制，其中身分鑑別包括多因子身分鑑別與身分鑑別聲明兩類做法；設備鑑別包括設備鑑別與設備健康管理等工作；信任推斷則是採用使用者情境信任推斷機制，包括身分鑑別、設備鑑別、使用者情境等結果的綜合評估與計算。完整的政府零信任登入流程如圖2所示。

目前優先導入的是零信任網路身分鑑別，分為規劃階段、建置階段與驗證階段，相關流程如圖3所示。

另外，以金融相關產業來說，重大法規除了個人資料保護法、資通安全管理法及資通安全責任等級分級辦法之外，在金融控股公司及銀行業內部控制及稽核制度實施辦法第38-1 條、證券暨期貨市場各服務事業建立內部控制制度處理準則第36-2 條、保險業內部控制及稽核制度實施辦法第6-1 條、公開發行公司建立內部控制制度處理準則第9-1條等都規範了資安專責主管、組織、業務與人員的配置；而金融資安行動方案2.0當中也明確加入零信任架構並鼓勵企業機構實施前瞻部署。

問題與挑戰

零信任是一種觀念、原則和策略，零信任架構則牽涉了包括硬體、軟體的技術和部署，重點是也規範了工作流程和相關機制。不論美國或國內各相關機構機關，都強調導入零信任架構是一段逐步成熟之過程，不是一次大規模替換基礎架構與存取流程。此外，實施內容不只是牽涉到資訊或資安部

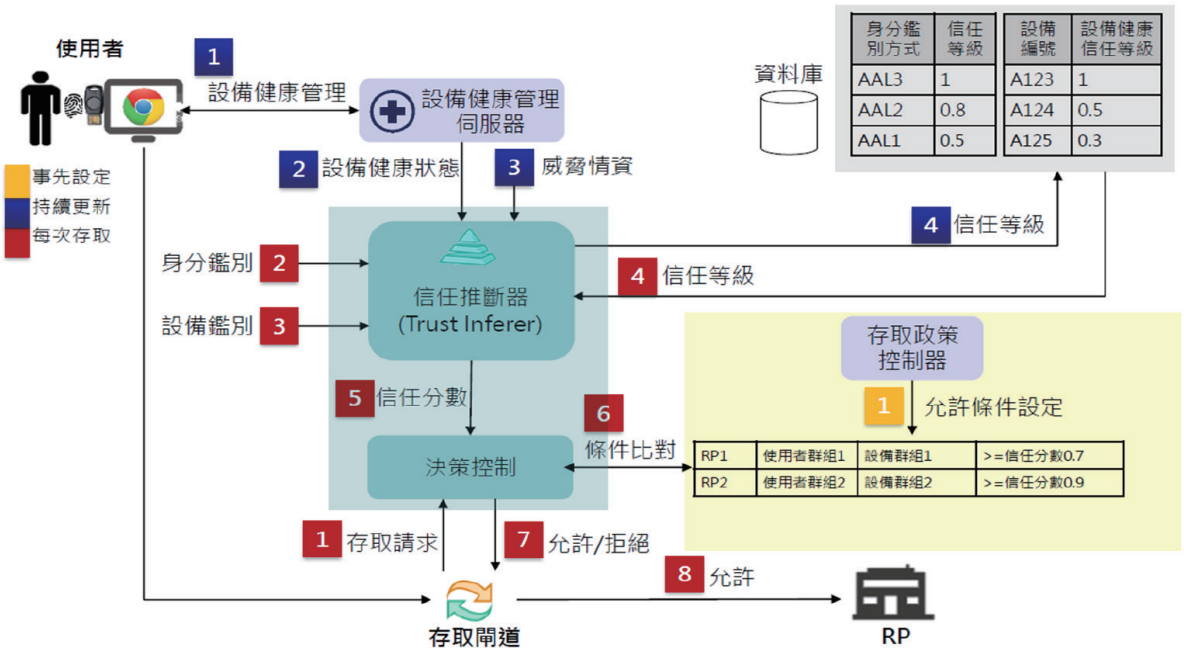

圖 2、政府完整零信任登入流程
資料來源：政府零信任架構說明，2023，國家資通安全研究院。P.15

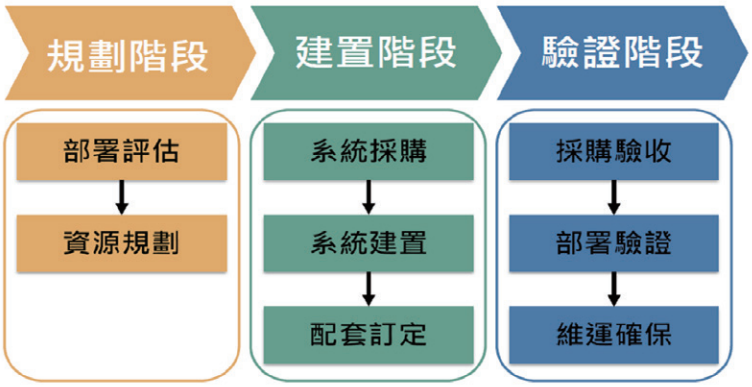

圖 3、政府零信任架構身分鑑別機制導入流程
資料來源：政府零信任網路身分鑑別機制導入建議 v1.1，2023，國家資通安全研究院。P.17

門，而是擴及包括各部門、夥伴和顧客，因此，其間與企業自身業務操作實務結合的實施過程格外值得重視。談太多的軟硬體技術可能讓有意理解支持的非資訊專業使用者難以消化和退縮，本文最後不擬著重軟硬體技術布局細節的探討，而主要從組織和使用者角度出發，提出若干筆者觀察到常見的問題與挑戰分享。

從組織角度來看，零信任架構必須投入相當人力與金錢成本，也增加營運的經常性支出，成果效益卻不易顯現，畢竟零信任不是購買甚麼軟體、硬體安裝後就可以宣告完成的事，使得這類投資花費通常不受管理階層青睞。而組織內部原系統的開發與使用往往歷史久遠，自行開發系統軟體程式散亂，很多來源與功能不明，人員退離頻繁，或位於不同地點部門管理，有如多年前Y2K問題評估曠日廢時，盤點不易。至於小型企業，可能大多認為尚無此需求，等到逐漸長大才發現導入實施更加困難麻煩。另外，管控制度、權限的設定與管理增加資料資源存取的困難與困擾，可能造成內外部使用者為存取資源讓工作流程更加繁冗的狀況，進而影響業務的執行效率；愈趨複雜的驗證手續、流程及軟硬體設置可能讓外部使用者或企業明顯感受不便，增加改變習慣的困擾，甚至不堪負荷。

再者，市場上基於零信任概念與架構，多有民間從事資訊軟硬體、系統導入和資安等各類業務的公司，基於自身的產品銷售而提出各式各樣的闡釋，並宣稱自家產品或方案才是企業最佳或最終的解決之道。這樣的做法導致企業或組織更容易感到困惑，以為零信任就是購買特定硬體軟體，或是改變帳號密碼，甚至不知道從何做起。

最後是人的問題，「疑人不用，用人不疑」是一般組織基於傳統智慧所形成的用人原則，要在組織與員工、員工與員工甚至部門與部門、組織對組織間建立穩固的信賴關係殊屬不易，組織和個人都投入大量的心血小心呵護維繫；推行零信任意味著在某種程度下雙方或多方的信賴關係有隔閡，不太符合傳統企業內外文化的交往習慣，要求長期且嚴格遵循較繁冗死板的規範制度並不容

易。其次，組織內部資訊與資安部門人員權責區分不易，新成立的資安部門內人員倘多係內部資訊人員調任，與資訊部門人員多有原主管、部屬、同事的關係，很可能有利益衝突的疑慮，而企業內部高層人員的存取權限更加難以管理；又倘若是新聘任外來的資安部門主管與人員，雖有一定權責，在組織和諧的考量下，亦不易指揮調動或調整其他各部門行之有年的組織架構與工作流程，並確保合規行為在各個部門都被貫徹。

無論如何，全面推動零信任架構還只是處於開始階段，還有很長一段路要走，在過程中相關內容做法也會不斷的滾動調整和細化。但可以確認的是零信任不會單單是資訊、資安部門的技術工作，而是考驗組織和企業對資安整體的危機意識、認知、堅定的意志及貫徹理念，進而帶動組織文化的轉變，因此，組織內外所有的利害關係人都有責任與義務理解和遵循，趁此時機認真檢視企業自身的五大要素，並盡最大可能調整配合以提升資訊安全防護。

參考資料

- Rose, S., Borchert, O., Mitchell, S., & Connelly S.（2020）. Zero trust architecture. National Institute of Standards and Technology, special publication, 800-207. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf?TB_iframe=true&width=370.8&height=658.8
- Cybersecurity and Infrastructure Division （2023）. Zero Trust Maturity Model. V.2.0. Cybersecurity and Infrastructure Security Agency, Department of Homeland Security. https://www.cisa.gov/sites/default/files/202304/zero_trust_maturity_model_v2_508.pdf
- DoD （2022）. DoD Zero Trust Strategy. Department of Defense. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
- Office of Management and Budget （2021）. Moving the U.S. Government Towards Zero Trust Cybersecurity Principles. Office of Management and Budget, The White House. https://zerotrust.cyber.gov/downloads/Office%20of%20Management%20and%20Budget%20-%20Federal%20Zero%20Trust%20Strategy%20-%20DRAFT%20For%20Public%20Comment%20-%202021-09-07.pdf
- 金融監督管理委員會（2022）「金融資安行動方案2.0」，行政院金融監督管理委員會。
- 國家資通安全研究院（2023）。「政府零信任架構說明」，國家資通安全研究院。
- 國家資通安全研究院（2023）。「政府零信任網路身分鑑別機制導入建議 v1.1」，國家資通安全研究院。

陳曦

現任文化大學財金系助理教授、臺灣數位科技與政策協進會理事。

曾任財團法人資訊工業策進會執行長特別助理、台北市電腦公會前瞻商務推動中心總監。