論述 》管理 · 資訊

不再爲密碼焦慮！讓便捷與資安同行

密碼所帶來的困擾，相信是許多人日常生活中的共同經驗，傳統密碼機制不僅考驗個人記憶力，更已成為潛在的資安弱點。近年來，隨著科技持續進步，數位服務的登入方式正逐步從傳統密碼轉向更高層次的驗證機制。本文將探討傳統密碼所面臨的挑戰，以及無密碼登入技術所帶來的便捷效益與安全升級。

賴柏宇（行政院主計總處主計資訊處科長）

壹、前言

一、全球網路威脅加劇，身分竊取風險升高

根據世界經濟論壇「Global Cybersecurity Outlook 2025」報告，高達 72％的受訪組織認爲網路風險持續升高，網路犯罪日益頻繁且手法也愈加精密，例如勒索軟體攻擊、人工智慧（AI）強化的網路釣魚、語音詐騙（Vishing）、深僞技術（Deepfake）及供應鏈攻擊等。更令人憂心的是，身分竊取（Identity theft）已躍升爲個人層面最主要的網路風險，並成爲企業資訊安全長（CISO）與執行長（CEO）高度關注的議題。

與此同時，生成式 AI（GenAI）雖然帶來諸多便利，卻也成爲網路犯罪的雙面刃。AI 技術不僅降低了網路犯罪的成本與技術門檻，更加速「網路犯罪即服務」（Cybercrime-as-a-Service, CaaS）商業模式的擴張。就像訂閱影音服務一樣，犯罪份子毋須具備高深技術，便能輕易「訂購」各類攻擊工具，並透過 AI 技術使攻擊手法更加精準自動，釣魚郵件也更具欺騙性。

二、警鐘長鳴的日常威脅

微軟最新發表的「Microsoft Digital Defense Report 2024」亦指出，全球網路安全正承受前所未有的攻擊壓力。報告顯示，僅微軟用戶每天便遭遇超過 6 億次網路攻擊。如此驚人的數字凸顯自動化攻擊工具的

普及、雲端服務與遠距工作模式所帶來的資訊安全挑戰，以及國家級駭客組織將網路行動納入地緣政治目標的常態化趨勢。

儘管科技日新月異，密碼攻擊依然是當前最普遍且成功率最高的入侵手法。報告顯示，每日 6 億次攻擊事件中，超過 99％為密碼攻擊。這項數據充分反映駭客對人性弱點的精準掌握與操作。雖然資訊安全技術持續進步，但弱密碼、密碼重複使用，以及缺乏多因素驗證等問題，仍使密碼攻擊成功率居高不下，成為駭客突破防線的主要途徑。

貳、傳統密碼所面臨之挑戰

在資訊安全領域，密碼的設計與管理是一個重要議題，它同時涉及了嚴謹的「數學題」與複雜的「記憶題」。駭客透過暴力破解（Brute-Force Attack）手法，嘗試窮舉所有可能的密碼組合以入侵帳號，因此密碼的強度高度依賴其長度與組成的多樣性。

例如，一個僅由四位數字組成的密碼，其組合數為一萬種；然而，若是一個包含大小寫字母、數字及常用符號，長度為十二位數之密碼，其組合數將暴增至約 2.7 垓（2.7×10^{20}），從數學層面來看，這幾乎是難以被暴力破解的天文數字。

然而，這道「數學題」卻成了我們日常生活中的「記憶題」，密碼複雜度提升反而造成「密碼疲勞」（Password Fatigue）現象。當面對定期更換密碼的要求，多數人為減低記憶負擔，常採取下列高風險捷徑，帶來重大資安隱憂：

一、多帳號共用單一或變形密碼

這是最常見的高風險行為。為求便利，許多人會將同一組密碼或其簡單變形用於多個網路服務。一旦其中任何一個網站資料庫遭駭，所有關聯帳號將同時面臨入侵風險。

二、採用易於記憶的個人資訊作為密碼

將生日、電話號碼、身分證字號等個人化資訊設定為密碼，駭客可透過社交工程輕易獲取這些公開或半公開資訊，進而大幅提高猜測破解的成功率。

三、使用看似複雜卻實為常見的組合

例如鍵盤上的特定順序（如 qwerty123）、或基於在地化輸入習慣形成的特殊詞組（如利用注音輸入組合）。這些密碼雖對個人而言或許獨特，但在駭客的常用密碼字典庫中早已榜上有名。

四、發明自認安全的「密碼公式」

例如在固定組合後加入網站名稱（如 MySecret@A_web、MySecret@B_web），若其中一組外洩，駭客便能推演其他密碼，輕易大舉入侵。

五、將密碼直接寫在觸手可及處

將密碼記在螢幕旁的便利貼、辦公桌抽屜裡的筆記本，甚至儲存在電腦桌面名為「密碼」的檔案中，無異於將保險箱鑰匙直接掛在門上。這不僅方便自己，也為周遭有心人士

或惡意軟體大開方便之門，使得所有數位防護形同虛設。

這種「密碼疲勞」現象使得我們的數位防線充滿了可被預測的漏洞。「ji32k7au4a83[1]」即是一個經典案例，表面看似隨機，實則因注音輸入法在臺灣廣泛使用，早已被收錄在駭客攻擊字典中，常被利用於「撞庫攻擊[2]」與「密碼噴灑[3]」等手法，構成身分竊取的重大風險。

參、告別密碼，擁抱 FIDO 的便捷與安全

面對日益嚴峻的網路安全挑戰與密碼機制的先天弱點，我們需要的不是更複雜的密碼，而是一場根本性的數位身分驗證革命－無密碼登入。

FIDO 聯盟（Fast Identity Online Alliance）是一個由全球主要科技公司、金融機構及政府組織共同組成的國際性非營利組織，致力於降低對傳統密碼的依賴，推動更安全、便利的數位身分驗證方式。FIDO 聯盟所制定的開放式國際標準，專門針對長期困擾使用者的密碼問題提出創新解決方案，加速無密碼身分驗證技術的普及與應用。

一、FIDO 標準的核心技術優勢

（一）強化安全性

運用先進的公私鑰加密技術，其安全強度遠超越傳統密碼。

（二）杜絕釣魚攻擊

驗證過程綁定特定服務，避免認證資訊被釣魚網站冒用。

（三）完善隱私保護

生物特徵資料（如指紋、臉部辨識數據）僅儲存於使用者裝置中不會外流，有效保護個人隱私。

（四）跨平臺相容

支援多種作業系統與主流瀏覽器，方便廣泛部署與應用。

二、全國主計網 eBAS 導入符合 FIDO 標準之「行動自然人憑證」登入機制

為順應國際趨勢，全國主計網 eBAS 作為整合多項重要主計資訊系統的單一登入（SSO）平臺，已於 114 年 6 月正式導入「行動自然人憑證」作為無密碼登入解決方案，使用者只須透過智慧型手機的指紋或臉部辨識功能，即可迅速完成身分驗證（下頁附表、附圖）。此流程不僅符合 FIDO 標準，更帶來直觀、流暢的使用體驗。這項變革對使用者而言，最直接的效益如下：

（一）徹底告別密碼困擾

從此毋須再記憶、定期更換或擔心忘記密碼，大幅減輕心理負擔。

（二）便捷高效的登入體驗

登入僅須透過手機的指紋或臉部辨識，動動手指即可輕鬆搞定，快速又不費力。

肆、結語

在網路威脅日益嚴峻的今日，傳統帳號密碼不僅不再是可靠的防護機制，反而成為資訊安全中最脆弱的一環。眞正有效的資安防護，應當能無縫融入使用者的日常操作。全國主計網 eBAS 導入行動自然人憑證登入機制，為同仁打造一個既順暢又安全的數位辦公環境。誠摯邀請您立即體驗全國

主計網 eBAS 的行動自然人憑證登入功能，親身感受「動動手指即可登入」的便捷與安心，一同邁向更高效、更安全的數位公務新時代。

註釋

1. ji32k7au4a83：是用電腦鍵盤的注音輸入法，依照中文「我的密碼」的發音對應英文鍵盤的按鍵順序，未經選字直接輸入，最終形成特殊的英數組合。
2. 撞庫攻擊（Credential Stuffing）：駭客會利用資料外洩事件中取得的大量帳號密碼組合，透過自動化工具嘗試登入其他網站或服務。由於許多人習慣在不同平臺使用相同密碼，致使這種攻擊的成功率相當高。
3. 密碼噴灑（Password Spraying）：駭客會使用一組或幾組常見的弱密碼（如 !QAZ2wsx、P@ssw0r 或本文中提及的 ji32k7au4a83 等），去嘗試登入大量不同的使用者帳號。這種方式可以有效繞過單一帳號嘗試次數過多被鎖定的機制。

附表　登入方式比較表

登入方式	便利性	安全性	使用體驗
傳統帳號密碼	低	低	須設計多組密碼、容易忘記、不小心就被鎖帳號
自然人憑證實體卡	中	高	必須隨身攜帶卡片，使用時較不方便
行動自然人憑證	極高	極高	一指登入，生物辨識驗證，走到哪都能安全使用

資料來源：作者自行整理。

附圖　全國主計網 eBAS 已導入「行動自然人憑證」登入方式

資料來源：行政院主計總處全國主計網 eBAS。

參考文獻

1. 臺灣網路認證股份有限公司 TWCA，FIDO ID 行動金鑰，網址：https://www.twca.com.tw/product/c0281542-f034-4ba9-8164-c517ebc5e0c0
2. 許家銘（2024），DQ 地球圖輯隊經授權轉載，「1234 那不叫密碼啦！」2024 全球最爛密碼稱霸六年　專家：只能靠無密碼技術了，網址：https://dq.yam.com/post/16316
3. 內政部（2022），免插卡！內政部推手機即是自然人憑證，網址：https://www.moi.gov.tw/News_Content.aspx?n=4&s=258671
4. 華視新聞（2019），「ji32k7au4a83」是什麼意思？只有台灣人能解答，網址：https://news.cts.com.tw/cts/life/201903/201903061953891.html
5. FIDO Alliance.https://fidoalliance.org
6. WEF Global Cybersecurity Outlook 2025.https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
7. Microsoft Digital Defense Report 2024.https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024❖