數位安全守門人：構建圖資專業人員的資安基礎知識與實踐策略

胡馨元

國家資通安全研究院 人才培力中心 研究推廣組經理

鄭瑋

數位發展部資通安全署副署長、
國立臺灣大學圖書資訊學系副教授

緒論：圖資專業新挑戰與資安意識重要性

圖書館長久以來被視為知識流通與公共信任的場所。然而，當圖書館角色不斷擴展，數位化與人工智慧服務的導入日益多元，圖書館為了提供更精準且貼近需求的讀者服務，引進愈多新型應用與資料整合機制。這樣的轉變雖然提升了服務效能與使用體驗，卻同時讓資訊安全成為圖資專業者無法迴避的新課題，意即如何在同時保障資訊自由流通下，維護資安與讀者隱私。

資訊安全（cybersecurity）過去多被認為是資訊工程等偏重技術的領域，但如今它更是一種攸關公共治理的議題。開放存取與資料共享是圖書館核心價值，但也正因開放，使圖書館暴露於外界與更高的數位風險中。近年多起國際事件即顯示，圖書館早已成為駭客攻擊的新目標。

2024 年 10 月，加拿大卡加利（Calgary）公共圖書館因遭受網路攻擊而被迫關閉 22 間分館，系統停擺使所有借還書作業回到「紙本時代」改以人工進行，雖在數日後逐步恢復營運，但部分功能仍受限，影響到整體服務品質[1]。同年，另一間美國西雅圖公共圖書館遭勒索軟體攻擊，雖未支付贖金，但館方不得不投入龐大資金聘請資安顧問與法律團隊，修復期間所有電子系統停用。2025 年初，美國休士頓地方圖書館傳出網路攻擊事件，事發一個月後，讀者仍無法登入個人帳號或使用網站的檢索功能。

這些國際事件顯示圖書館已成為外部攻擊者鎖定的目標。然而，資安風險不僅來自外部。國內圖書館曾有約僱人員不慎遺留存有讀者個資的隨身碟，暴露了內部流程控制的薄弱環節[2]。即便是人為疏忽，亦足以引發個資外洩與法律風險。這些案例都顯示圖書館面臨的威脅是多源且複雜的。系統停擺是短暫的影響，但是資安事件的影響往往更為長期，更包括龐大的修復成本、複雜的資料恢復過程，以及長期公眾信任的重建。

圖書館所掌握的資料雖不如金融機構或醫療院所極度敏感，但是讀者個資、借閱紀錄、活動報名資料、甚至採購與研究合作文件，對威脅行為人（不論內外）而言都仍有價值，資安事件的後果不僅止於服務停擺或金錢損失，圖書館的社會地位建立在「可靠」與「安

[1]Calgary Public Library Implements Pathway to Recovery Following Cybersecurity Breach.
https://www.calgarylibrary.ca/library-news/calgary-public-library-implements-pathway-to-recovery-following-cybersecurity-breach

[2] 圖書館員遺留隨身碟 驚見 2000 多筆讀者個資。
https://news.ltn.com.tw/news/society/breakingnews/3406281

全」之上，一旦讀者懷疑其個資被外洩或系統頻繁中斷，公共信任便會動搖。

因此，圖資專業者的角色早已超越傳統的知識整理者或傳遞者，更是數位知識安全的核心掌控者：館員熟悉資料流向、理解使用者行為、並掌握系統操作權限，其位置正好位於資料使用與傳遞的節點，若能具備足夠的資安判斷力與風險意識，便能在威脅尚未擴大前，阻斷攻擊鏈的第一環，防止漏洞擴大。

本文將從圖書館實務出發，帶領讀者認識「CIA 三大安全原則」，探討資訊安全在圖資領域的內涵與應用，思考圖資專業者如何在不斷變動的環境中，成為「數位安全守門人」。

一、不成為「無意間的駭客」

資安的本質是探討三個基本的問題，我們要保護哪些資產？能夠達成哪些安全需求？又該防範誰的攻擊？

1. 保護「資產」

資安管理的第一步，是要盤點需要被保護的資產，確認保護的範圍。對圖書館而言，傳統上需要保護的資產是珍貴的手稿、特藏與實體館藏，但在數位世界中，資產的樣態更多樣，需要被保護的已延伸至數位資訊層面。其中最核心的資產，是館內系統的存取權限與身份憑證。一旦這些身份憑證被奪取，攻擊者便能更容易地存取後續所有資產 (資料庫的存取權限、電子郵件帳號密碼、讀者個人資料等)。其他具價值的內容，如未公開的原始碼、尚未出版的稿件、工作會議紀錄等，皆是要避免遭到濫用或盜取。

2. 達到「安全要求」

資安防護的目的，不僅是避免被攻擊，更在於保護資安的作為是否有達成預期的安全目的和目標。就如同圖書館必須確保特藏不損壞、不被盜竊一樣等注重於實體安全，資安代表的是虛擬的安全，需確保讀者個資或機密會議資料不外洩、維持會議記錄不被竄改、保證系統服務不中斷等，其核心目的正是保護資訊的 CIA 三大原則：

- 機密性：如確保讀者個資、機密會議資料等不外洩；
- 完整性：確保系統設定、會議記錄等不被未經授權地竄改；
- 可得性：保證館藏系統、電子資源服務不中斷

這三個原則將在下一章節深入探討。

3. 防範「攻擊者」

在傳統印象中，資安威脅主要來自於外部的惡意攻擊者：不論是企圖竊取個資的駭客、勒索金錢的網路犯罪組織，或是以破壞服務來展示技術能力的團體。這些攻擊者的目的多樣，可能是為了竊取個資以進行詐騙，勒索系統以獲取金錢利益，或破壞公共機構的服務以展示技術能力。這些行為雖帶有惡意，但更可怕的是，在現實中，許多資安事件的發生原因卻源自於內部人員無心的疏忽。這些使用者往往在毫無察覺的情況下，成為了外部攻擊的「幫助者」或「破口」。

舉例而言，在日常工作或生活習慣，在咖啡廳連上公共 Wi-Fi 處理公務，所有資料傳輸都可能被監聽，包含帳號密碼、公司機密文件都會被攔截；每個系統都用相同密碼，一旦駭客取得任何一組密碼，就能登入人員的所有帳號，造成連環資安事故；使用 CC 寄送群組信件，所有收件者的 email 都會外洩，可能被用來進行垃圾郵件攻擊或社交工程。

若以圖書館情境為例，館員為方便同事查閱資料，私下分享自己的系統帳號密碼，不只違反使用規範，還可能需要為他人的不當使用負責，甚至面臨法律問題；未經授權把內部文件帶回家，使用未加密的個人電腦處理重要文件，資料則可能在傳輸過程中外洩，或是家中電腦中毒導致機密外流，都是讓惡意攻擊者藉此滲透的機會。這些行為未必出自惡意，也並非無知，而是往往源於善意與便利的考量，希望協助同事、節省時間、或順利完成工作，但結果仍可能造成重大損害，讓資安防護成為破口。

二、以CIA三大原則建構圖書館資安思維

要避免成為「無意間的駭客」或是資安破口，除了建立嚴謹的安全意識與良好的工作習慣外，還必須掌握系統性的思考方法來應對資安問題。當館員初次面對資安問題，常會感到難以判斷該從何著手、哪些風險應先處理，何者又影響最大？

此時，可以運用資安領域中最基礎且最具指導性的「CIA 三大原則」—機密性（Confidentiality）、完整性（Integrity）、可得性（Availability）核心概念來協助判斷。

了解 CIA 資安原則，能幫助館員更容易分析威脅來源的動機、評估風險的嚴重程度、決定合適的防護措施，以及決定應變的優先順序。這三項原則亦可以對應到圖書館日常運作中的每個環節。

1. 機密性：保護資訊免於未經授權的揭露

機密性所指的就是確保資訊只能被授權的對象存取和使用，任何可能導致資訊外流、將資訊洩露給非相關人員或公開給大眾的行為，都屬於對機密性的違背。

在圖書館情境中的敏感資訊可能包含讀者的個人資料、借閱紀錄、講座活動報名資料、資料庫採購合約金額等。而當這些資料未經授權的揭露，即代表違反「機密性」。舉例而言，若承辦人員在寄送活動通知給多位互不相識的參與者時，錯誤地使用「收件人（To）」或「副本（CC）」欄位，而未正確使用「密件副本（BCC）」，導致所有收件者彼此的電子郵件地址被公開，就是一種明確的機密性破壞。

為了保護機密性，可以有各種不同做法，例如：權限分級管理、加密傳輸、強密碼設定、使用更長且複雜的密碼、以及環境防護（如螢幕防窺片、會議室資訊保密等）。這些措施都是能防止資訊外洩的第一道防線。

值得一提的是，「密碼管理」根據美國國家標準技術研究所最新的指南，鼓勵創造更長、複雜的密碼組合，而非鼓勵定期換密碼。定期更換密碼，反而會因為使用者行為造成反效果，實際上會產生幾個問題：使用者為了方便記憶，往往會選擇過於簡單的密碼，甚至越改越簡單。或者，使用者會循環使用規律字串與可預測的方式修改密碼，例如：password1 改成 password2，再下一次，就換成 password3。這樣的改法對於機密性的保護，其實效果很差，容易被破解與預測。

同時，頻繁換密碼會讓人更容易忘記，導致的結果是使用者會把密碼寫在便利貼上，或存在手機裡，反而造成資安風險。對單位來說，定期更換密碼的機制會增加技術支援成本，有些員工甚至會因為懶得輸入新密碼，造成使用者懶於登入系統減少使用電腦的次數，間接影響工作效率。因此，建立強密碼並妥善管理，比頻繁更換密碼更安全且實際。

2. 完整性：確保資料的正確性與真實性

完整性是確保資料在儲存、傳輸與使用過程中保持正確、真實，且未被未經授權地變更，讓資料能「正確如實」地呈現其狀態。

以圖書館情境而言，資料完整性亦關乎組織的信譽與專業。若讀者的借閱紀錄被竄改做不正確的對應、滯納金被誤刪、或統計資料遭竄改，不僅可能導致管理決策錯誤，也會使服務現場陷入混亂，甚至動搖民眾對圖書館管理能力的信任。

維護完整性的方法包括建立異動紀錄追蹤機制、版本控管制度、以及建立資料備份與還原制度。常見的「3-2-1 備份法則」即是重要資料備份三份、分別儲存於兩種不同載體、其中一份異地保存，就是一種實用的做法。若圖書館能在備份策略中同時考慮實體與雲端方案，便能兼顧效率與安全。

資料完整性同時也與透明度息息相關。當資料來源、修改歷程與權限分工皆能被清楚記錄與查核，便能有效預防惡意竄改與誤用。這種「可追溯性」（traceability）正是現代圖書館治理中不可或缺的元素。

3. 可得性：確保資訊與服務能持續被使用

對讀者而言，「系統無法使用」、「圖書館網站無法瀏覽」往往是最直觀的資安事件。可得性強調的是資訊與服務在需要時能被持續使用，確保運作不中斷。

如果圖書館的 OPAC 停擺，讀者無法查詢、借閱或預約館藏，這就是「可得性」受到影響。例如，這可能包含惡意的分散式阻斷服務攻擊（DDoS），企圖藉由流量突增癱瘓伺服器，也可能是系統維護程序失誤導致的服務停擺。此外，即便無惡意，例如瞬時湧入的大

量使用者同時登入，導致系統資源耗盡而發生當機或反應遲緩，同樣屬於「可得性」的範疇。

確保可得性需從多層面著手，包括定期維護硬體設備、更新軟體系統、建立備援機制，以及制定緊急應變與復原計畫。在組織管理層面，也應預先設定臨時替代方案，例如，若主伺服器故障時，是否能啟用備援線上介面或提供人工查詢服務。這些預備措施皆是圖書館確保服務不中斷、維持公共信任的關鍵，也是圖書館資安治理重要的一環。

CIA 三原則之間往往需取捨。過度強調機密性可能降低可得性，而放寬存取權限則可能削弱完整性。真正的挑戰在於平衡三者，使安全與服務並行不悖。

三、資安防護的現實與取捨

在資安領域，「完美防禦」是不可能的任務。理論上，最安全的系統是完全與外界隔離的系統；但在實務上，任何封閉環境都無法支撐現代圖書館的運作與服務需求。如何在「安全」與提供使用者「便利」之取得平衡，一直是資安與資訊治理的課題。

為什麼資安防禦不可能做到天衣無縫呢？這背後涉及幾個關鍵因素。

首先是預算限制，資安設備如同其他科技產品與解決方案，都需要投入成本，不論是防火牆、端點防護系統、事件監控系統等資安設備、聘請專業的資安人才，都需要長期且持續的經費支持。

安全措施與使用便利性之間，往往存在著互相牽制的關係。當安全防線加強時，必然會影響到操作的便捷性。例如，傳統的多重要

素驗證（MFA），若設定為每次登入都必須進行多重步驟驗證，雖然能大幅提升安全性，但也無可避免地會降低使用體驗，導致使用者抱怨系統過於繁瑣。然而，現今的資安思維已經進展到可以智慧地平衡兩者。如零信任（Zero Trust）架構，能動態調整驗證強度：當使用者在可信任的環境（如固定 IP、常用設備）存取時，可能只需相對單純的 pin 碼驗證；而當從陌生地點或設備存取敏感資料時，才要求更強的雙重因子驗證，更不可信任的環境時，甚至進行三重認證。這種動態調整機制，能夠在不犧牲安全性的前提下兼顧便利性。

第三，每個系統都可能存在尚未被發現的漏洞，也就是所謂的零時差攻擊。這些漏洞就像是隱藏的地雷，直到被攻擊時才浮現。最後，人為因素仍是最大的變數。即使有最嚴密的技術措施，若使用者操作不當或疏於警覺，防線仍會被輕易突破。因此，資訊安全防護的核心不在於「完全消除風險」，而是將風險降到可接受範圍，才是務實的做法。換言之，資安本質上是一種風險管理行為，而非追求「零風險」的理想狀態。

1. 認識假設條件與防禦邊界

若有單位宣稱其系統「百分之百安全」，這往往是對安全邏輯的誤解，因為實際上資安是一種權衡 (Trade-off)。任何防禦機制都建立在一組「假設條件」上，也就是在特定前提下，做了什麼「措施」，能夠防禦「特定威脅模型」。一旦這些前提被破壞，防禦就不再有效。舉例來說，圖書館的入口若是有門禁系統，設有護欄，防禦假設是「所有人都會刷卡進出」，且「每次刷卡只允許一人通過」。威脅模型是「未持有卡片的嘗試進入」。但若使用者跳躍過護欄或尾隨其他讀者進入館舍，原有的防護假設即被推翻，機制也隨之失效。

再以資訊系統後台為例：在「管理者遵守密碼安全準則且開發人員定期更新修補程式」的前提下，透過多重身分驗證與輸入錯誤鎖卡機制，能防止密碼盜用或非授權的惡意登入。但這樣的設計仍有侷限，若有人撿到門禁卡並反覆嘗試導致帳號被鎖，雖未造成資料外洩，卻影響系統的可得性。這些例子都一再說明：真正成熟的安全觀念在於，清楚知道自己系統「能防什麼」與「不能防什麼」，並意識到哪些部分是無法控制的外部變數，而不是全然相信產品是 100% 安全，或追求不切實際的 100% 安全。

2. 建立威脅模型與風險優先順序

面對有限的資源與不斷演變的威脅，圖書館可以利用威脅模型（Threat Model）來釐清風險類型與程度，再依據影響與發生機率進行排序。威脅模型強調以理性方式評估事件的「影響程度」與「發生機率」，從而計算風險值（Risk = Impact × Likelihood）。

例如：

- 高風險事件：讀者個資外洩（嚴重影響×中度常見機率）
- 中風險事件：電子資源遭盜用（中度影響×偶發機率）
- 低風險事件：臨時網頁錯誤（輕微影響×常見機率）

這樣的排序有助於單位在資源有限的情況下，優先處理已知的一般性漏洞，先確保所有系統都更新到最新版本，再考慮進階的防護措施，避免防護措施流於形式。防護的目標不在於「防住所有風險」，而是提高攻擊者成功的成本、延長其入侵時間、並爭取修復與應變的機會。

四、新興科技下的守門人養成作為

人工智慧、雲端運算與自動化工具正持續改變圖書館的運作方式。AI 系統能自動生成摘要、協助編目與推薦閱讀，甚至進行資料分析與使用者行為預測。當系統日益智慧化，館員的角色也逐漸從「資訊提供者」轉為「判斷者」與「守門人」。

近年來，政府在推動資安意識上非常積極，從制定資安法規、舉辦教育訓練、發布資安警訊等等，都展現政策端的努力。然而，科技發展的速度總是快於法規的建立，每項新興科技都伴隨新的資安挑戰。圖書館作為公共知識體系的重要節點，從現有架構中發揮，可以從教育與文化層面深化民眾資安素養。

1. 跨域合作與知識共享

數位發展部的資通安全署（資安署）與國家資通安全研究院（資安院）重視全民資安意識推廣，將資安意識推廣策略分為不同的推廣手法、目標族群與對應行動，以達成「全民資安長期紮根」的目標。這樣的推動並非單一機構能獨力完成，而需公私部門資源的持續互通與協作。

其中一項具代表性的實踐是資安院引進美國網路安全診所聯盟「Cybersecurity Clinic」模式。學生除修習資安課程外，也實地前往中小型企業或非營利組織進行資安輔導，形成「學習—實作—社會參與」的模式，此模式值得圖資界借鏡。圖書館可成為地方數位學習與資安推廣的中介站，運用館內資源舉辦教育訓練與社區活動，協助民眾提升資安素養與防護意識。這不僅延伸了圖書館的教育功能，也使圖書館在公民社會中扮演推動「數位公民意識」的重要角色。

具體而言，圖書館可參考資安院的框架以「知識型、形象化、遊戲化」的多元推廣手法，依不同族群設計對應方案：

- 對學生與教育機構，結合學校課程推動家庭與個人防護教育
- 對成年社會大眾，透過展覽與故事化設計強化資訊風險意識
- 對民間企業及從業人員，舉辦社會教育講座與資安實務演練
- 對公務員與政府單位，推動組織資安韌性與應變措施
- 對樂齡族與銀髮族，設計易懂且互動的數位防詐宣導內容

這樣跨域合作的推動思維，能有效擴大公共參與的層面。圖書館能夠扮演知識與社群的橋樑，將有機會連結公私部門資源，成為推動數位公民意識與資安素養普及的關鍵節點。

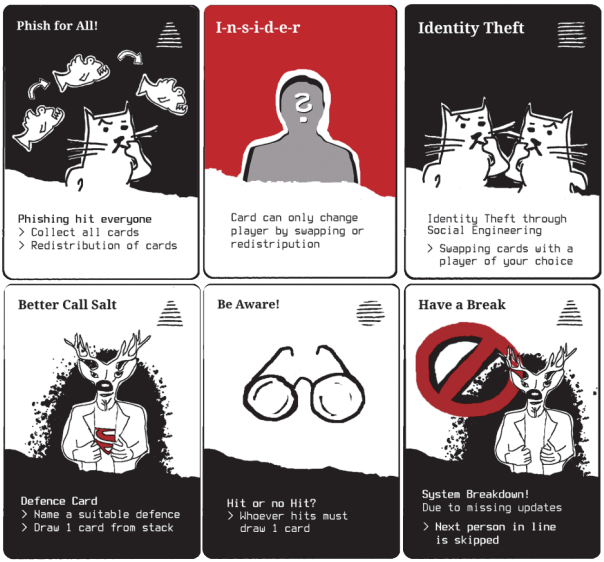
2. 遊戲化與形象化的教育設計

資安推廣，不應僅止於技術訓練或法規宣導，而應以更貼近生活、易於理解的方式融入公眾教育。對多數民眾而言，抽象的安全機制與風險警語往往難以轉化為具體行動，因此，如何將「資安」變得易懂易學，成為公共教育的新課題。在這樣的背景下，遊戲化（gamification）與形象化（visualization）設計成為極具潛力的教育策略。透過卡牌遊戲、故事敘事與角色扮演的方式，民眾能在模擬情境中自然學習應對風險，理解資安事件的成因與後果。例如，藉由模擬電子郵件詐騙、個資外洩或弱密碼設定等場景，使學習者在互動中內化防護原則。國際上已有多項案例可以參考：

- 德國奧格斯堡應用科技大學（Augsburg Technical University of Applied Sciences）Dominik Merli 教授團隊設計的Salt & Pepper Security Behavior Card Game，以類似UNO的玩法，將真實資安事件轉化為解謎卡牌[3]

[3]Salt & Pepper. https://github.com/thainnos/Salt-and-Pepper

- 愛沙尼亞塔林科技大學（Tallinn University of Technology）Birgy Lorenz 教授的 CyberSec juhtumid，以「海龜湯」式問答與推理，讓學習者了解真實攻擊案例[4]
- 印度的Powerplay則以隱私保護為主題，透過角色互動強化玩家的隱私風險意識[5]



圖一　德國學者團隊製作Salt & Pepper Security Behavior Card Game

[4]CyberSec Stories. https://sites.google.com/view/tty-csgame/avaleht

[5]Powerplay. https://ishitabegani.com/ui-ux/powerplay

圖二　愛沙尼亞學者團隊製作CyberSec juhtumid

圖三　印度團隊製作Powerplay

這些遊戲化教材展現了資安教育的另一種不必以說教或警告等方式，而能結合故事敘事、角色扮演與圖像思考，讓學習變得有趣。對圖書館而言，這種方法尤其適合，透過策展、闖關活動或主題講座，將資安知識融入讀者體驗，不僅提升民眾參與度，也強化館員的教學與倡議能力。

結語：重置自己、不斷懷疑、持續學習

在資安領域的實務場域中，沒有永遠穩固的防線。今日安全的系統，明日可能成為漏洞；原本可靠的作法，隨著技術演進與行為改變而失效。這種持續變化的情形，正是資安工作的本質。

對圖資專業者而言，這也意味著要持續的自我更新。安全不僅是技術能力，更是一種認知習慣：懂得懷疑、願意學習、並勇於調整。當館員能在每一次上傳文件、寄出郵件、或安裝應用程式前，停下來問自己一句：「這樣做安全嗎？」那便是良好的資安意識真正內化的時刻。

圖書館從來不只是知識的儲藏室，而是公共理性與社會信任的象徵。在數位時代的浪潮中，若能以資訊安全為基礎，持續守護資訊的可得性、完整性與可信度，那麼，圖書館將不僅是知識的守門人，更是數位時代信任的守門人。

隨時提醒自己，當初的經驗與習慣，隨時可能被新興科技顛覆。唯有不斷檢視與重估自己對風險的判斷標準，才能在瞬息萬變的環境中維持警覺。辨識資安威脅與資訊真偽是一場耐力賽，身為「守門人」它考驗的是持續觀察與反思的能力、吸收新知。不去死記硬背特定的辨識技巧或記住所有攻防手法，而是理解背後的原理，培養對

新興科技的基本認知，並持續補足知識差距。資安概念養成與資訊素養相似，與其說是「學會防禦」，不如說是「維持學習的開放性」，不只是提升自身的「免疫力」，也要幫助他人共同更新觀念。

註：本文作者皆為國立臺灣大學圖書資訊學系校友，近年投身資安領域，致力以社會科學的觀點，關注資安人才培育與資安意識推廣等相關議題。