博物館資安管理與防護——國立臺灣博物館資安推動與實施經驗分享

Implementation Experience of National Taiwan Museum in Information Security Management

林芙美｜國立臺灣博物館典藏管理組
Lin, Fu-Mei ｜ Collection Management Department, National Taiwan Museum

前言

數位時代，博物館內部管理、展館營運或是民眾教育活動，皆離不開資訊科技與網路的應用。由有線、無線與行動網路串聯而成的數位世界，穿越時空，縮短國與國、人與人之間的距離，卻存在大大小小的資訊安全（或簡稱為資安）漏洞，成為全球駭客利用的管道。駭客的威脅無所不在，不限定任何產業，即便是博物館等非營利機構或組織，都有可能遭受攻擊。2017 年於全球各地爆發的勒索病毒，在短時間內癱瘓大量電腦與系統，造成許多單位及個人數位資產及財物損失，資訊安全開始成為大眾關注的焦點。至今，駭客依然猖獗，甚至擴大威脅力道。當人們不理解駭客入侵管道，輕忽日常安全防範，長期下來便容易產生弱點與破口。

2019 年「資通安全管理法」（以下簡稱資安法）開始實施，凸顯當今資安管理的重要性。從駭客的觀點，博物館系統長期累積的民眾個資，是駭客最有利可圖的資料；從博物館營運觀點，重要系統服務中斷，將影響業務的執行，造成許多民眾的不便。資安管理屬於風險管理的一環，為降低潛在風險實施層層防護措施，透過管理制度確保措施的有效性，資安管理需要建立組織合縱連橫的防護網，將安全概念內化於電腦使用或操作中。

大多數博物館無專責資訊單位，資安管理與政策推動不易，加上經費與人力的不足，需要尋求符合效益的解決方案。本文期使讀者從近年來的博物館資安事件中，加深資安防範意識，引領讀者了解資安管理目標以及執行策略。藉由分享臺灣博物館（以下簡稱臺博館）資安推動與實施經驗，與博物館同業交流，期有助於運用有限資源打造資安防護網，維護資訊之可用性、完整性與機密性。

駭客也會攻擊博物館？

依據行政院國家資通安全會報發布之統計資料（2021），公務機關於 2020 年每個月遭受的資安威脅皆高於 2019 年，最高逼近 10 萬件。或許有人會認為，博物館屬於非營利單位，亦非屬民生關鍵產業，應該不是駭客眼中的「菜」。但，事實真的是如此嗎？

案例一

駭客入侵新北市坪林茶業博物館粉絲團

2020 年 7 月，新北市坪林茶業博物館發生粉絲團帳號被駭客竊取事件，一夕之間數千則貼文被刪除，原本擁有的 1.7 萬粉絲數也只剩下一半。據報導，該事件發生過程為管理員登入粉絲團時，突然跳出一則臉書系統通知，要求使用者覆核帳號密碼、確認身分，否則帳號就會在 24 小時內停權。管理員立刻依照指示操作，因而導致管理者帳密遭駭客盜用，並登入後臺大肆破壞。經警方調查，攻擊者的 IP 來自東南亞地區，不只鎖定坪林茶業博物館粉絲團，許多粉絲專頁都遭受攻擊。此事件雖然無關金錢損失，但博物館多年累積的服務內容已無法追回。

案例二

臺灣博物館接獲恐嚇勒索郵件

臺灣博物館為民服務信箱於 2020 年 10 月接獲來自駭客的恐嚇勒索信件（如圖 1），通知館方已遭駭客入侵，所有系統、郵件、社交平臺的帳號密碼皆被竊取，所有郵件訊息與電腦檔案亦同，即使更改帳號密碼亦無法阻止駭客的作為。駭客威脅臺博館於隔日傍晚前支付比特幣，否則所有資料將被公開，落入更多駭客手中。由於臺博館帳號、郵件伺服器與出口流量皆由文化部（上級機關）管理與監控，經緊急聯繫文化部，調查數個月內之帳號登入紀錄、系統紀錄與連線紀錄等等，皆未發現可疑事證及下載行為，加上不只一個單位接獲此類誇大之信件，因此研判為詐騙郵件暫時不予理會，事後亦未接獲駭客再次的通知與威脅。

Your Opinion

Hello! You've been hacked! Now we have all the information about you and your accounts: + all your logins and passwords from all accounts in payment systems, social networks, e-mail, messengers and other services (cookies from all your browsers, i.e. access without a login and password to any of your accounts) + history of all your correspondence by e-mail, messengers and social networks + all files from your PC (text, photo, video and audio files). Changing your username and password will not help, we will hack you again. Pay a ransom of $ 250 and you can sleep peacefully without worrying that all information about you and all your accounts, files and personal correspondence will not become public and will not fall into the hands of intruders. Bitcoin wallet to which you want to transfer $ 250 1MaRdde6X7SGuoCdFNL2fm gpLomdx7peGC. If you do not pay until tomorrow evening, then we will sell all this information on the dark net, there is a huge demand for such information Pay $ 250 and sleep well!

圖 1　來自臺博館為民服務信箱的恐嚇勒索信件

案例三

駭客竊取英美眾多博物館、大學及非營利組織機敏資料

2020 年英國與美國眾多博物館、大學與非營利組織陸續證實發生資料外洩事件，這些單位皆使用同一廠商（Blackbaud）提供之雲端服務系統。駭客於 2020 年 5 月時入侵雲端系統，竊取大量個資與機敏資料，然後以公開資料作為威脅，要求廠商支付贖金。Blackbaud 確認資料確實被駭客竊取後，在駭客不散布且刪除所有資料的承諾下支付比特幣贖金，同時委託資安專家至駭客活動的暗網中，確認資料並未遭外洩，期化解客戶的疑慮，但部分客戶仍因此終止與廠商的合作關係。

案例四

駭客竊奪荷蘭博物館與經銷商畫作買賣交易之價金

2020 年驚傳荷蘭特威特國家博物館（Rijksmuseum Twenthe）為購買一幅珍貴的 John Constable 畫作，與一家倫敦藝術品經銷商狄金森（Simon C. Dickinson）興訟。原因為該博物館與經銷商的通聯郵件遭網路駭客滲透，駭客偽裝成狄金森，將真實的付款細節置換成香港一個詐欺性銀行帳戶，博物館館員遭受誘騙，並將大額支付款項匯入駭客提供之帳戶，事後發現時已無法追回。此案件買賣雙方皆為受害者，並互相指控對方疏忽之處；法官初步駁回了博物館控告狄金森的疏失，因為博物館同樣負有維護電子郵件安全之責。雖然該畫作已交至博物館手中，但最終仍有待法官判決該畫作之歸屬。

從以上國內外案例顯示，博物館與非營利組織皆有可能遭受駭客攻擊，輕則影響單位營運，重則造成名譽與金錢損失。當博物館從業人員對於駭客入侵手法認知不足時，一不小心就會掉入陷阱。一旦駭客取得帳號密碼，且進一步發現有機可趁時，就會伺機而動。近年來駭客藉著間接入侵服務廠商電腦或系統竊取客戶資料，或設法侵入電子郵件系統、偽裝詐騙的手法，已經造成許多單位受害；駭客以亂槍打鳥、大量散布威脅恐嚇郵件詐騙，更容易造成單位與使用者的不安。當博物館疏於資安防範，缺乏駭客入侵軌跡調查能力時，就容易陷入恐慌，甚至受騙上當。

資安管理目標與執行策略

資安管理三大目標：（一）確保系統或資料的可用性，隨時可供使用者使用；（二）確保系統程式與資料檔案的完整性，未經他人竄改或刪除；（三）保護系統或資料的私密性，只有合法授權的使用者才可以存取，不被其他人竊取或揭露。由於駭客新的攻擊型態無法預測，已知電腦病毒變種快速難以阻隔，加上使用者行為百密總有一疏，即使於單位內部署先進的資安防護設施，也無法百分之百避免資安事件的發生。因此資安管理與防護採用風險管理概念及程序，從管理面與技術面建立事前防範、事中應變以及事後復原改善計畫，以達成降低風險、控制損害的目標。

資安防護涉及層面廣泛，包含個人電腦、網路通訊、機房設施、系統程式、存取授權與內外部人員等資訊資產的安全管理，需要評估各類資產潛在風險，打造相互鏈結的防護網絡，才能降低資安事件發生機率。萬一發生資安事件，也不容易造成嚴重損害。資安防護除了從技術面設定安全組態強化體質、建置資安產品阻擋大部分攻擊之外，從管理面訂定資安維護計畫，據以施行資安管理作業；制定資安管理作業規範，作為資訊資源利用準則；制定系統委外作業規範，強化系統與資料安全維護；制定資安通報與緊急應變程序，因應資安事件的發生等等，皆為當今資安管理不可或缺的一環。

資安管理措施必須隨時因應內外在威脅的變化彈性調整，維持措施之有效性。近年，來自大陸之資通訊威脅不斷升高，為遏止公務環境遭受滲透，政府自 2020 年起禁止公務機關使用大陸廠牌之資通訊產品，臺博館亦同步盤點資通訊設備、汰換具有疑慮的產品。又如使用者或管理者帳號與密碼，是駭客控制電腦或系統最想要竊取的資料。由於電腦運算速度越來越快，駭客破解密碼的能力也越來越強，為增加密碼破解的難度以及縮短密碼被破解後的有效可利用期間，加長使用者密碼、增加密碼複雜度（納入英文大小寫及符號）、縮短密碼有效期間等作為，是因應現況的有效措施，卻是相當惱人的規定，相信你我都很有感。

臺博館隸屬於文化部，為資安法適用單位，資安管理須遵循法令與文化部資安政策，並接受文化部的資安稽核。臺博館管理策略由文化部主政，與各附屬機關共同訂定「文化部及所屬機關資通安全維護計畫」。為落實政策，臺博館另針對實務需要自訂管理規範，譬如臺博館近年來非編制內人力成長迅速，為加強人員管理，臺博館非正式人員帳號須由管理人（正式人員）代為申請並負起督導責任；新進人員取得帳號前，必須詳閱最新資安管理規範並簽署共同維護資訊安全同意書，加強新人資訊安全認知。又，臺博館資訊維護工作，由委外廠商派駐工程師提供服務。為確保工程師依規定執行各項任務，建立維護作業表單及程序，留存相關紀錄，有助於管理與稽核。透過制度的建立，一面賦予資訊人員維護整體環境安全之任務，一面可以降低資訊資源不當的取用：當電腦或網路出現異常行為時，資訊人員得以立即處理與管控；當同仁有違反規定之要求時，資訊人員得據以勸導並拒絕提供服務。以下分享臺博館近年來資安管理重要措施與推動經驗。

臺灣博物館資安推動與管理

一、成立跨部門資安推動小組：資安政策推動關鍵

資訊安全政策，涉及各單位及所有使用者資訊資源的取用與管理，各項政策的推動與實施，需要所有單位配合，無法單靠資訊單位一肩挑起重任。由於大多數主管及使用者對於駭客入侵手法理解有限，而安全措施的實施可能降低作業效率或是改變使用者操作習慣造成不便，因此容易遭遇阻礙。例如臺博館於 2017 年勒索病毒開始流竄爆發之時，為了加緊保護儲存於網路硬碟的重要檔案，不得不停用微軟系統檔案共享服務。由於短期替代方案比不上微軟檔案分享機制，加上同仁不願意改變長期以來的習慣，因而引起少數資深同仁的反彈。最後經過一段時間的溝通以及在上級政令的要求下，才得以克服，但是防護措施落實的時間越晚，等於提供駭客更多入侵機會，對於臺博館越為不利。

臺博館無資訊單位編制，資訊業務指派典藏管理組兼辦，然而就資安涉及層面與可能引發的威脅，位階明顯不足。2019 年資安法施行後，臺博館設置資安長，由副首長擔任，並於 2020 年通過「資安推動小組設置辦法」，成立跨部門資安推動小組：由資安長擔任召集人，各部門主管為小組成員，資訊人員擔任技術幕僚，負責資安各項工作的規劃與執行。資安推動小組每年至少召開會議 1 次，藉由會議的宣導及討論，順利達成以下目標：

1. 由技術幕僚說明資安法規重點內容，使各部門主管了解依法需執行事項。
2. 依組織任務重新評定核心業務、核心系統標的及其可容忍中斷時間，作為施行資安防護策略之依據。
3. 由資訊人員協助業務單位重新評定自行委外開發系統之防護等級及應具備之防護措施，針對措施不足之處列入年度改善目標。
4. 將上級機關資安稽核結果以及改善情形提報會議審查，確保達成改善目標，同時使各部門了解應持續配合事項，維持措施之有效性。
5. 由技術幕僚就現況須優先加強方向提出改善建議，經會議認可後，交由相關單位執行。

從臺博館實施經驗得知，成立跨部門資安推動小組，負起推動資安政策之任務，為快速凝聚組織共識、提升資安行動力的關鍵。在資安長的帶領下，技術幕僚得以運用規劃（Plan）、執行（Do）、稽核（Check）、改善（Audit）之循環管理步驟，爭取經費逐步加強資安防護能力。當有新的資安威脅發生時，透過資安推動小組的運作，將更容易協調各部門採取短期因應措施，確立長期改善作為。

二、防範勒索病毒的危害：建構多層次防禦系統

2017 年曾在全球各地爆發的想哭病毒（WannaCry），具有網路散播能力，能在短時間內感染大量電腦、挾持電腦將檔案加密。檔案被加密後難以破解，受害者欲取得解密程式救回檔案，必須付出比特幣贖金，因而造成企業與個人極大的損失。時至今日，駭客加強勒索力道，謀取更大利益，以公開機敏檔案、損害機構信譽作為威脅，當受害者遲疑支付贖金的時間越久，需要付出的代價越高。更有甚者，有不法集團專門招募會員，提供會員勒索病毒進行攻擊，企圖與會員一起分贓贖金

擴大牟利。從趨勢公司年度病毒觀測報告顯示，2020 年新出現的勒索病毒家族比 2019 年增長 34%，想哭病毒發生率位居所有惡意病毒之首位，顯示勒索病毒的威脅不減反增，仍然為當今防駭的焦點。

勒索病毒透過系統漏洞或合法管道入侵，常見的入侵途徑為：（一）透過作業系統漏洞入侵，如 2017 年想哭病毒，就是利用微軟作業系統發布的漏洞，攻擊尚未更新系統的電腦。一旦入侵，會透過網路尋找下一個可以入侵的標的，持續向外擴散。（二）透過應用程式漏洞入侵，如曾廣為運用的 Flash Player 程式，因存在許多漏洞容易被駭客所利用，Adobe 公司宣布自 2021 年 1 月 12 日起停止更新，各大瀏覽器也不再支援瀏覽以 Flash Player 製作的網頁。（三）透過惡意網站或廣告入侵，當使用者點選廣告連結或下載影片、遊戲或軟體時，就可能遭受病毒感染。（四）利用社交工程手法，如透過電子郵件、社交通訊軟體等方式，散布惡意連結或夾帶病毒之圖片或附檔，當使用者不小心打開郵件、點選內容，病毒就趁機潛入。2020 年 COVID-19 疫情爆發，成為舉世關注的焦點，從趨勢公司觀測報告顯示，駭客利用 COVID-19 主題的攻擊行動，90% 來自惡意郵件，此與電子郵件攻擊技術門檻最低、容易利用當下流行話題與人們好奇心達成誘騙目的有關。

為了防範勒索病毒的入侵，臺博館一面加強內部資訊維護與人員管理、運用自動化管理機制加強管控；一面藉由文化部於共構機房設置中控安全閘道，並由委外廠商提供監控服務，建構層層鏈結的防禦措施，使病毒的危害降至最低。具體作法說明如下：

電腦管理與機敏資料處理

1. 電腦（含筆電）設備配發前，需依電腦安裝作業單確認作業環境符合安全規定；由 DHCP 伺服器依電腦 MAC 位址配發固定 IP，僅允許註冊之公務設備取得 IP、使用網路，防止未註冊或外來之電腦取用網路而帶進病毒。
2. 啟用防毒軟體即時掃描防護功能，定時自動掃描硬碟 1 次，清除潛在病毒。病毒碼及版本透過網域伺服器（以下簡稱 AD）自動派送更新，保持最佳防護力。
3. 電腦安裝軟體須取得合法授權，申請通過確認來源無虞後，由工程師到場安裝。
4. 建置掃毒工作站，提供館員存取外來硬碟檔案前，先行掃毒並刪除所有可疑檔案後再行利用。
5. 設置實體隔離（不連網）電腦工作站，作為機敏資料編輯、加密儲存以及浮水印列印服務，降低駭客竊奪機會。

帳密與權限管理

1. 定期盤點系統特權帳號存在必要性，限制使用人數，以免遭駭客竊奪。
2. 降低一般使用者電腦操作權限，以免任意下載安裝含惡意病毒軟體。
3. 所有系統及使用者帳號啟用強密碼設定，每 2 個月更新 1 次；以單一簽入機制（簡稱 SSO）整合各系統帳號管理，自動停用或刪除久未登入帳號。

區網分隔管理

為限縮勒索病毒的流竄範圍，將伺服主機與一般電腦網路分隔。一般電腦網路又依空間用途將會議室、展間與辦公室網路分隔開來。當某一網段遭受駭客入侵時，無法輕易跨越網段擴大攻擊。

系統安全管理

1. 建置 WSUS 服務，自動派送微軟安全性更新程式，及時修補漏洞；非微軟相關軟體、無法自動更新者，由工程師手動更新或以 AD 派送更新。
2. 建置應用系統防火牆，防止駭客透過已知網頁程式漏洞進行攻擊，並檢查正常網頁連線（https/http）是否存在異常存取行為並加以阻擋，避免機敏資料外洩。
3. 每半年進行系統安全性檢測 1 次，發現漏洞限期改善。

電子郵件使用管理

1. 透過垃圾郵件過濾器，隔離廣告及可疑郵件。
2. 依 Outlook 郵件安全設定規則，關閉預設郵件預覽及圖片下載功能、以純文字模式開啟郵件，避免不慎開啟郵件遭病毒入侵。資訊人員於平時維護及保養電腦時，加強檢核。

使用者教育訓練與演練

1. 每年提供線上資安課程，加強員工自我管理，參訓時數列入平時績效考核。
2. 每年透過文化部辦理郵件警覺性測試（社交工程演練）2 次，以不同主題類型的郵件進行誘騙。從近三年演練結果顯示，主旨與公務相關之詐騙郵件，開啟信件比例明顯增高，足見同仁容易因執行業務失去警覺心。舉凡未通過演練以及新進之同仁，皆須參加資安講習，加強資安認知。

資安監控

1. **導入端點防護系統（Forescout）**

   僅允許加入網域與套用安全組態設定之電腦連接區網使用，例外需求須經核准。當系統察覺電腦作業環境不符合安全要求時，如未更新軟體版本、私接手機上網等事態，皆禁止連網使用。

2. **SOC 委外監控**

   委託資安廠商監測及通報疑似遭病毒入侵的電腦，交由臺博館工程師檢視及清毒。提供系統安全性檢測及滲透測試、程式與網頁安全性診斷、病毒分析與清毒諮詢等專業服務。

3. **資安健檢**

   導入 Xensor 系統，偵測網路、個人電腦及伺服器是否存在惡意活動，及早揪出潛入病毒。

三、建立系統安全防護措施：從系統風險評估做起

資訊系統或網站因應業務需要而生。以往臺博館系統開發由業務單位委外建置，以業務需求為導向，專注於使用者功能分析規劃，忽略系統安全需求；因此，早期開發之系統或網站，若發現程式漏洞且已無維護廠商可協助時，就會面臨關站下架的命運。系統安全需求與其所面臨的風險密切相關，必須經過風險評鑑過程，識別風險、分析風險，並依系統的重要性、所處理資料之機敏性以及對組織信譽的影響，評估可能帶來的衝擊，據以規劃合宜的防護措施。依據資訊安全風險管理（CNS/ISO 27005）作業，系統風險評鑑可採取高階風險評鑑以及詳細風險評鑑 2 種做法，或是互相搭配使用。高階風險評鑑係透過事先建立之系統共同性威脅及衝擊，作為系統風險分級之基礎，並藉由訂定各級別應具備之控制措施作為共通性防護基準。詳細風險評鑑作法較為深入，針對每一系統潛在風險，綜合資產價值、威脅、脆弱性、發生機率評估其風險值，對於無法接受之風險，建立適當的防護措施，因此需要具備相當之專業知識及較長的時間成本。

臺博館業務屬性相對單純，無高敏感性系統。為協助業務單位參與評定，主要採用高階風險評鑑方法，以「資通安全責任等級分級辦法」（以下簡稱分級辦法） 附表九所訂之系統防護需求分級原則，將系統防護需求分成普、中、高三級，以機密性、完整性、可用性及法律遵循性分別評估遭受衝擊的影響程度，並以最高影響等級作為系統防護需求等級。當系統完成等級評估之後，採用該法附表十各級別共通性防護措施，作為系統應具備之防護基準。

系統安全防護措施涉及層面廣泛，包含帳號與身分驗證管理、權限管理、遠端維護管理、系統稽核紀錄管理、資料傳輸與儲存管理、系統漏洞修補與監控、系統備份（備援）與異常通報等，部分防護措施須納入系統開發階段實作，部分措施需透過作業管理落實。為確保系統上線時即達成應有的安全水準，減輕後續維運成本，臺博館自 2020 年起，新系統建置皆須由業務單位依分級辦法評定系統防護等級，將相應的安全防護措施納入開發需求規格中。針對業務重要系統，則另依其特殊需求建立防護措施，或參考行政院資通安全處訂定之「資通系統風險評鑑參考指引」進行深度評估，避免忽略重要弱點。

四、強化系統委外安全管理：以票務服務系統為例

系統委外建置歷經需求規劃、廠商遴選、程式開發、上線驗收與保固維護 5 個階段，每個階段皆涉及資訊安全議題。現今駭客透過入侵承包廠商電腦，間接入侵系統之資安事件時有所聞，系統開發除了須檢測系統安全無虞之外，委外作業加入資安思維，將有助於遴選兼具系統開發與資安管理能力的廠商，保障博物館權益。

由於資安議題具高度專業，非業務單位得以完全掌握，自 2019 年起，臺博館系統開發專案從規劃初期，即採取專業分工模式，由業務單位負責專案管理與業務功能規劃，資訊人員負責資安管理與功能規劃，期使系統於開發完成上線時，即達成應有的安全水準。以下以 2019 年委外建置之票務服務系統，說明建置過程資安規劃與管理重點：

系統建置地點（機房）選定

票務服務系統為臺博館因應 2020 年新加入營運之鐵道部園區，重新打造的資訊系統，目的為支援各展館售票、驗票、帳務管理與會員製卡，同時提供民眾電子支付與行動支付服務。為達成上述目的，系統須要介接：（一）文化部會員系統，提供會員卡申辦及製卡服務，方便會員現場領取；（二）信用卡代收銀行與悠遊卡公司系統，完成臨櫃刷卡交易；（三）文化部單一登入系統（SSO），整合使用者帳號及管理。

臺博館依據文化部資訊向上集中政策，新系統以建置於文化部共構機房為優先選擇，由文化部負責機房虛擬主機與資料庫的安全管理。票務服務系統為內部使用之系統，系統運作涉及 4 個展館的對外營運，每日售票服務量大，系統運作涉及之硬體設備眾多，包含位於服務臺之售票與印票設備、會員卡製卡機、信用卡與悠遊卡機，以及位於展場入

口之自動與手持驗票機，對於系統主機與資料庫回應速度以及網路穩定度的要求高。儘管文化部共構機房擁有優於臺博館機房的安全管理措施，規劃初期業務單位仍擔心系統建置於文化部，效能可能不如預期，影響民眾購票與驗票入場的順暢度。

票務服務系統為文化部轄下機關自建的第一個結合金流的資訊系統，為確保系統穩定性，經與文化部資訊處召開會議，確認系統建置於共構機房整體架構之可行性，以及系統所需資源可獲得資訊處大力支援下，選定建置於文化部機房，同時為降低網路不穩定或中斷的衝擊，規劃離線作業，強化應變能力。

系統安全開發規劃

1. 系統基礎安全需求

由業務單位依分級辦法進行系統防護等級評估，依評估結果採用同法相應之控制措施，作為系統安全防護基準。

2. 系統進階安全需求

票務系統資料流，從各展館行經臺博館 VPN 線路傳輸至行政大樓資訊主機房，再從主機房行經文化部 VPN 線路傳送至共構機房，網路架構複雜（詳如圖 2）。為降低網路服務中斷之衝擊，導致單一展館或所有展館無法使用系統，系統功能須提供離線售票、驗票與結帳作業，使重要作業得以正常進行。另為降低硬體故障風險，各展館售票電腦、票券列印機、自動或手持驗票設備，至少建置 2 套，互為備援。

3. 資料處理安全措施

系統以儲存最少量個資資料為原則設計，除了應具備的安全規範，會員卡製卡時自會員系統下載取得之個資，於製卡完成後定期自售票電腦硬碟刪除，降低個資外洩的風險。

4. 系統作業環境

採用微軟作業系統與資料庫，安裝當下新近且穩定的系統版本，取得原廠較長之系統安全維護期限。

5. 系統資料備份

由文化部機房每日進行系統與資料備份，包含磁帶備份；系統上線後，定期將資料備份至外接式硬碟，異地備存於臺博館。

系統部署安全管理

1. 系統安裝前，廠商需提交安全性檢測報告，排除已知之中、高風險漏洞，再由臺博館申請安裝於文化部機房。

2. 系統安裝依文化部網站（系統）作業申請程序，申請虛擬主機、資料庫所需資源，開通遠端維護連線，所有使用者帳號，一律使用強密碼設定，每 2 個月變更密碼 1 次。廠商提供建置於展館之設備，同樣須遵循安全規範，停用系統預設帳號，啟用強密碼設定，每 2 個月更新密碼 1 次。

3. 系統驗收前，須通過文化部安全性檢測，完成漏洞修補。驗收時，由資訊人員偕同業務單位檢

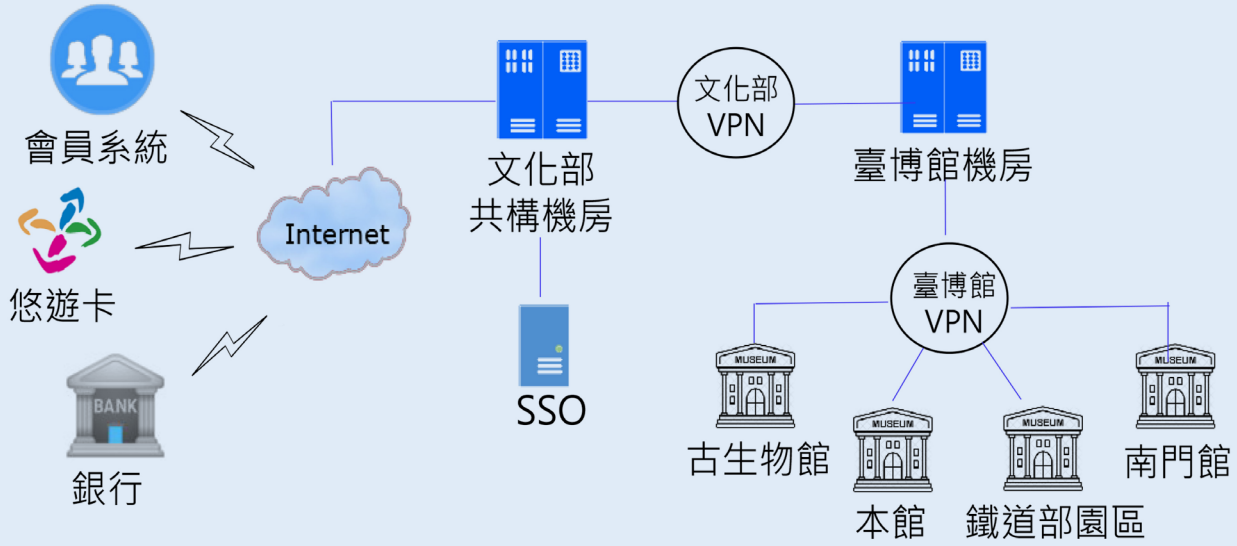

圖 2　臺博館票務服務系統架構

核系統功能與設定，是否依安全要求完成各項防護措施。

保固維護安全管理

票務系統於保固維護期間，廠商須維持系統正常運作，提供系統與程式安全維護，重點維護事項為：

1. 維護期間發現作業系統或程式漏洞，廠商應無條件於期限內完成漏洞修補，並於每季進行系統保養，確保系統與程式安全性版本更新至最新。

2. 系統程式應支援 Chrome、 IE 等主流瀏覽器最新安全性版本，維持系統可用性。

3. 廠商遠端維護連線需求，每 2 個月向文化部申請 1 次，每次皆須更改密碼，避免遭駭客竊取利用。

每年於憑證到期前 1 個月，匯出合於規定之憑證請求檔予臺博館重新申請憑證，維持 https 連線有效性。

需求規格書與契約書製作

系統需求規格書與契約書為廠商履約依據，需求規格書需要將上述安全規範事項納入，契約書條款則須依據資安法令最新規範，將資安相關履約事項納入。

系統委外契約書既往皆採用行政院公共工程委員會發布之最新資訊契約範本，經查該範本已將資安法令安全要求納入契約條款中，包含廠商應盡之資訊安全責任、機關稽核委外廠商資安辦理情形、廠商違反資安法令或知悉資安事件時之通報、補救等事項，因此票務系統委外契約直接採用該契約範本製作，不自行擬定減輕作業負擔。

有關履約管理，經評估票務服務系統功能並無特殊技術需求，可以由臺灣單一廠商提供服務，故契約不允許分包及轉包，降低委外作業複雜度；同時排除大陸廠商或人士參與專案以符合政令規定。為加強廠商人員管理，廠商參與專案之人員，須於專案啟動時提交保密同意書，維護資料之機密性。如有違反，機關得追究簽署人及其任職廠商之刑責，並賠償機關遭受的損害。

廠商遴選措施

系統安全性與廠商資安需求的了解程度、程式安全開發內控能力以及專案人員的資安素質密切關聯。為了解廠商資安專業與管理能力，將安全管理與資料保密規劃納入服務建議書章節，並將投標廠商資安管理與維護計畫納入評分項目中，由評選工作小組提供初審意見，有助於審查委員評選兼具資安管理能力的廠商。

臺博館票務系統在業務單位、資訊人員與承包廠商協力下，順利通過資安各項查驗，並於 2020 年 7 月正式上線。上線後出現驗票閘道機與伺服主機連線不穩定、信用卡交易不穩定事件，影響現場服務。經檢測與網路不穩定較有關。藉由設定臺博館與文化部之間各段 VPN 線路之保證頻寬後，問題迎刃而解，使得本建置案順利達成系統可用性要求。又，保固維護階段，透過每季維護作業以及半年 1 次的安全性檢測等作為，得以持續達成安全維運水準。

五、維持系統可用性：預防重於治療

博物館日常業務運作，皆離不開電腦、系統與網路，當系統效能緩慢、網路壅塞不順，可能導致業務執行效能降低；機房或網路設備故障，則可能發生系統中斷的資安事件。如何維持系統可用性，在可容許時間內完成修復，甚至面臨重大災難時，仍具有重建系統與回復資料的能力，為資安管理重點目標。預防重於治療，以下從跨館設備自動監控、例行性維護作業與資料備份管理三方面，說明臺博館具體措施。

跨館設備自動監控

臺博館館舍分散 6 處，主機房位於行政大樓，展館及庫房分別設置小型機房，主要提供網路服務，資訊人力集中於行政大樓上班。為了掌握各處機房狀況，建置中控之環控告警系統，偵測機房電力、空調、消防、漏水與門禁狀況。當發生異常時，資訊人員得以於第一時間收到系統通知、及早因應。同時為掌握配置於各館樓層網路設備運作狀況，設置中控之網路設備監控系統，回報設備運作狀態。當資訊人員收到設備離線通知時，可以立即處理，加速修復。

例行性維護作業

例行性安全維護目的，為及早發現危及系統服務的潛在因子，進行預防性改善措施。臺博館曾於 2019 年因政府網際服務網（簡稱 GSN）VPN 機房網路設定問題，導致單一系統長期不穩定，歷經數月才得以釐清問題所在，因此強化例行性安全維護作

業有其必要性。表 1 為臺博館例行性維護事項——每日可用性檢查作業，有助於掌握重要系統與網路效能，及早發現異常原因，改善作業模式或調整頻寬管理策略；機房系統每月保養作業，有助於掌握主機資源利用情形，必要時調整系統資源配置，並作為設備擴充與汰舊規劃之參考；每年檢視防火牆開放政策，將不必要的連線刪除，避免遭駭客利用。防火牆連線紀錄至少保留 6 個月，以利資安事件調查分析；定期檢視機房基礎維運設施並更新耗材，得以降低機房維運中斷的風險。因著例行性安全維護的落實，2020 年間工程師主動發現、進行障礙排除案件至少有 7 件，降低資安事件的發生，帶來明顯的效益。

每日 可用性檢查	1. 每日檢查官網及主題網站等重要對外服務網站效能
	2. 每日檢查員工入口網、公文、電子郵件等重要行政系統效能
	3. 每日檢查各館線路與連接文化部線路使用流量
機房 系統維護	1. 每月執行主機系統保養 1 次
	2. 每年進行系統安全檢測 2 次以及重要系統滲透測試 1 次
	3. 每年盤點防火牆連線政策 1 次，保留連線紀錄至少半年
機房 設備維護	1. 每日檢查機房設備是否出現異常警示
	2. 每季進行空調保養 1 次
	3. 每半年進行 UPS 保養及消防設施查檢 1 次

表 1　臺博館例行性維護事項

資料備份管理

資料備份為資安防護的最後一道防線，當檔案遺失或損毀時，將備份資料還原，可以回復系統或檔案可用性。臺博館資料備份標的，包含機房系統維運資料以及館員執行業務產出之重要檔案。

1. 機房系統資料備份

臺博館機房存放之資料，主要來自虛擬平台系統（VM）、大容量儲存系統（Storage）與網路磁碟（NAS）的系統、檔案與資料庫，其中以藏品管理系統數位圖檔增長量最為迅速。截至 2017 年初，機房儲存之資料量已達 63TB。傳統備份系統 D2T 架構，資料直接自系統讀取寫入磁帶，必須利用系統離峰時間（下班時段）執行，每日備份量有限。隨著資料量的增長，容易發生備份排程相互排擠現象。為提升備份整體效能，2018 年重新規劃備份架構、強化備份系統功能——以 D2T2T 架構，將資料自系統讀取備份至硬碟，再從硬碟備份至磁帶。利用資料去重（Data Deduplication）以及合成備份（Synthetic Backup）技術，大幅降低備份至硬碟所需空間及時間；整合虛擬平臺底層備份機制，將虛擬系統視為檔案進行備份與還原，得以有效縮短系統重建時間。從備份硬碟將資料寫入磁帶作業，因不影響線上系統的運作，可以 24 小時不間斷進行，大幅增加備份效能。備份系統自建置至今（2021 年中），依然可以順利達成系統每日異動備份、每週合成全備份、每 2 週完成所有資料備份至磁帶的目標，解決既往作業瓶頸。

2. 館員重要業務檔案保存

館員平時執行業務產出之檔案，除了上傳至系統儲存，仍有一大部分存放於個人管理之硬碟中。個人硬碟故障率相對較高，每年皆有硬碟損害的情事發生。為保存館員重要業務檔案降低遺失風險，臺博館於 2021 年初訂立「數位檔案保存作業要點」，定期將館員所擁有之重要檔案蒐集、上傳至機房儲存系統，並建立易於查詢之目錄架構，供各單位查詢利用。上傳的檔案皆經過整理、除去暫存版本，避免占據硬體資源，檔案維護權限僅授權資訊人員操作，可以防止館員誤刪檔案與病毒入侵機率，達成重要歷史檔案保存的目的。

3. 備份復原演練

臺博館每年辦理備份復原演練 1 次，使工程師熟練復原作業程序，至少包含：(1) 自硬碟及磁帶還原指定之系統與資料，並驗證備份資料的完整度；(2) 進行重建備份系統作業程序，確保重大災難發生系統損毀時，仍然可以重新打造備份系統將資料還原。

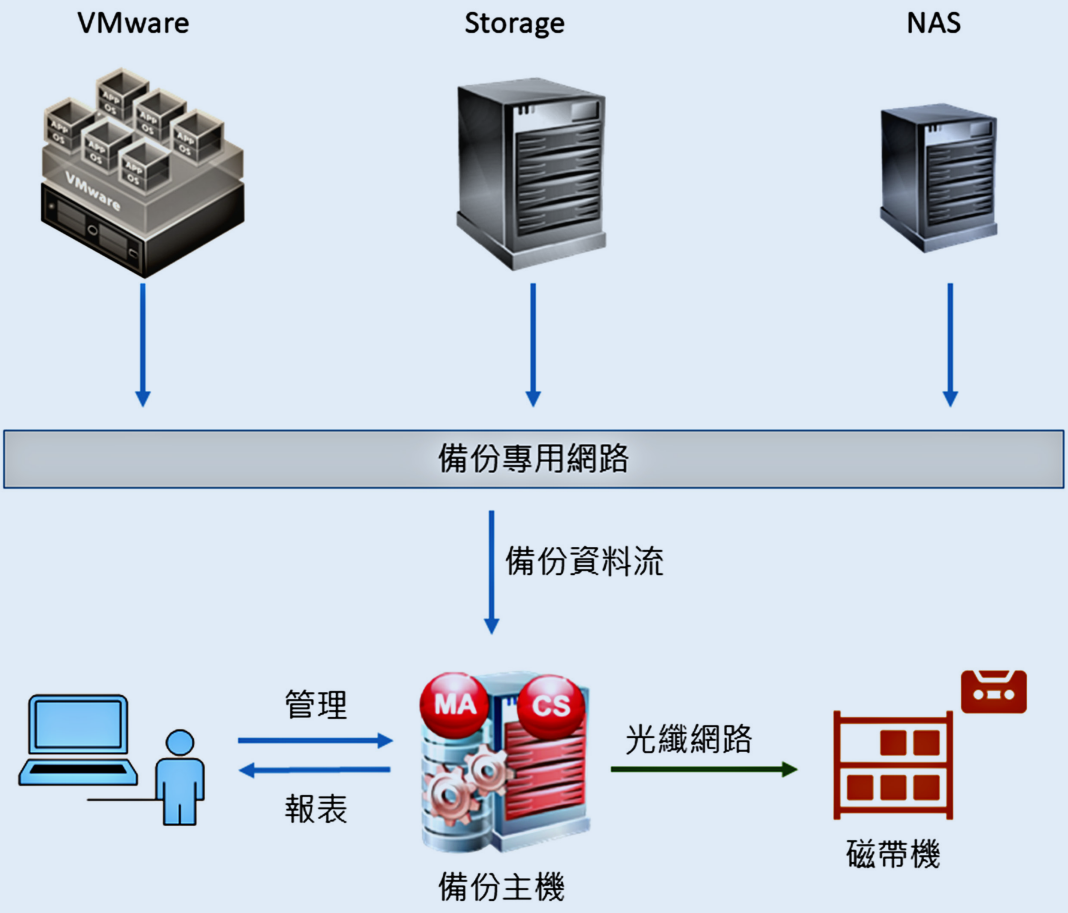

圖 3　臺博館資料備份架構

六、資安稽核與持續改善

資安稽核為資安管理滾動式改善的必要措施。臺博館資安稽核主要依據文化部及所屬機關資通安全稽核計畫，每二至三年至少接受文化部實地稽核 1 次，由文化部政風處、資訊處或外聘委員組成稽核小組。資安法實施後，臺博館於 2020 年計接受文化部內部及外部實地稽核各 1 次，稽核方式除了事先依稽核表進行自主檢核之外，稽核當日由稽核小組進行資訊機房、系統以及個人端設備實地查核。從實地稽核過程發現，從稽核前請各單位進行自主檢查，稽核時委員與館員面對面查核，以及稽核後就發現之缺失，訂定限期改善措施，對於提升館員資安認知及配合度有相當大的助益。每年，文化部實地稽核完成之後，皆以公函發布共同性缺失事項。臺博館即使未列入當年實地查核單位，仍然依共同性缺失進行自主檢視及改善，並透過資安推動小組追蹤管考，逐步落實資安政策。

結語

數位科技的應用帶來便捷的生活與服務，然而科技背後潛在的安全問題，不容忽略或心存僥倖。當安全與便利出現衝突時，必須有所取捨。資安管理涉及管理作為與資訊技術的應用，二者缺一不可。從臺博館資安管理實施經驗顯示，管理階層對於資安的支持與重視，可以加速帶動組織的資安意識，對於資安政策的推行具有事半功倍的效果；善用外部或上級單位資源，強化防駭、防毒管控機制，可以彌補專業能力與經費的不足；強化系統委外建置管理，並依系統風險等級建構相應的防護措施，才能有效提升系統安全性；落實資料備份管理，才能防範資安風險造成的損害。

資安維護人人有責，勒索病毒的入侵手法，可以經由使用者的不慎直搗內部網絡。由使用者良好的操作習慣所建構之「人因防火牆」，為阻擋病毒入侵的重要防線。因應後疫情時代大為興起的遠距上班需求，給予駭客更大的想像空間，員工自有設備很有可能成為駭客入侵跳板。他山之石可以攻錯，從行政院資通安全處每月發布之資安月報，可以獲知最新資安新聞與威脅；從國內外機關發生之資安事件案例，有助於博物館提高警覺，檢視防護措施的完備性，因應新局勢的發展。

延伸閱讀

- 公共工程委員會（2021）。資訊服務採購契約範本。公共工程委員會全球資訊網。https://www.pcc.gov.tw/cp.aspx?n=99E24DAAC84279E4
- 行政院國家資通安全會報（2021）。資安月報。行政院國家資通安全會報官網。https://nicst.ey.gov.tw/page/B55E97A3EFB37209%20%E8%A1%8C%E6%94%BF%E9%99%A2%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E6%9C%83%E5%A0%B1
- 行政院國家資通安全會報（2021）。資安管理法。行政院國家資通安全會報官網。https://nicst.ey.gov.tw/Page/EB237763A1535D65
- 吳亮賢（2020）。坪林茶博館粉專遭駭—數千貼文全刪光、粉絲數腰斬。聯合新聞網。https://udn.com/news/story/7320/4741908
- 趨勢科技（2021）。A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report（中文版）。趨勢科技官網。https://www.trendmicro.com/zh_tw/security-intelligence/threat-report.html
- T. Maxwell and T. Bell. (2020). It's high time art businesses beefed up their cybersecurity. Apollo Magazine. https://www.apollo-magazine.com/cybersecurity-art-businesses-constable-dickinson-rijksmuseum-twenthe/.
- P. Clolery. (2020). Breaking: Blackbaud Hacked, Ransom Paid. The Nonprofit Times. https://www.thenonprofittimes.com/npt_articles/breaking-blackbaud-hacked-ransom-paid/