國家圖書館

推動資訊安全及向上集中系統升級計畫

(111 年)

成 果 報 告

執行單位：國家圖書館

112 年 6 月 15 日

壹、計畫目標

一、計畫背景

鑑於網路技術與通訊科技不斷的推陳出新，資訊安全持續受到高度重視，唯有建構安全的資通訊環境與完整的資料安全防護，才能提供讀者便利安全的資訊服務，也才能面對未來資安議題的各種挑戰與衝擊。本館為重要的關鍵基礎設施，存有多個全國唯一且重要的資料及系統，常為測試攻擊目標，為提高防禦能力，期藉由計畫的推動來強化本館骨幹網路及端點設備的安全防護力。

本館對外提供且持續維運的資訊系統與服務平臺逾 60 個，本館已盤點、評估各資訊系統的資安風險，並持續地就具有資安問題的系統與設備進行安全漏洞的修補、作業系統及資料庫版本的升級等作業。110 年在補助經費的支持下完成「全國新書資訊網」、「國際標準錄音錄影資料碼系統」、「電子書刊送存閱覽服務系統」及「臺灣書目整合查詢系統」升級工作；111 年持續推動資安升級工作，在有限的經費額度下，依系統使用率、重要性及資安風險評鑑結果，擇選二個系統進行系統汰換升級並完成向上集中。

二、計畫目標

本案計畫目標有二：

(一)網路管理自動化、端點資安防護再升級

主要辦理汰換老舊網路設備並增購網路管理軟體、資訊資產管理軟體、資通訊系統日誌收集分析軟體，以及端點管理系統升級等。

(二)資訊系統汰換升級，提升系統安全並完成向上集中

主要辦理數位影音系統汰換改版與移轉、臺灣華文電子書庫升級與移轉、電子書刊送存系統會員認證機制優化等。

三、內容要項

(一)網路管理自動化系統建置及資通訊系統日誌收集分析軟體

1.因應本館網路應用及相關設備不斷增加，單以人工方式管理已無法負荷網路資安事件頻傳的現實環境，亟需汰換相關設備並建置日常網路管理維運與監控及預警之自動化系統。網路管理自動化系統之建置，將包含網路設備監控系統，針對重要設備進行實時監控與管理，並針對各網路狀態產製對應之電子文件。

2.因應 110 年 8 月 23 日公布實施之「資通安全責任等級分級辦法」規定，對於資通系統存取控制應訂定日誌之記錄時間週期及留存政策，並保留日誌至少 6 個月。鑑於本館資訊系統數量眾多，將採購資通系統日誌收集分析所需之軟硬體並進行系統設定，統一收集並管理重要資通系統之日誌，包括網路設備、各作業系統、重要應用系統、服務、資料庫等日誌以符合法規要求。

(二)端點資安防護升級

1.因應 110 年 8 月 23 日公布實施之「資通安全責任等級分級辦法」規定，擬於本館既有之資訊資產管理系統，增購 CPE 模組以簡化軟體資產盤點作業，並以指定 CPE 格式上傳行政院國家資通安全會報技術服務中心，並依後續比對結果進行修補，以降低各端點軟體資安風險。

2.為有效管理 IP 資源並進行資安管控，擬進行本館既有 IT 資源管理與網路安全防護系統升級，提供 IPv4、IPv6 偵測、封鎖等管理，並擴大管理範圍(約 1,300 個 IP)。

(三)資訊系統汰換升級、系統功能優化

1.數位影音服務應用程式改版與向上集中

此服務系統提供桌機版及行動版 2 種瀏覽介面，係整合微軟 IIS 6.0 Media Server 搭配運作；因微軟已終止 Windows 平臺的 IE 11 支援，且有微軟開發的串流多媒體格式(asf、wmv)檔案無法使用，影響影音服務的提供，亟需進行應用程式及檔案格式轉換。本案計畫辦理工作如下：

(1)相關 ASF 影音資料轉換為 HTML5 支援格式(MP4)

(2)前後台系統分離及改寫

(3)資料庫及相關影音檔案移轉

(4)完成 HTTPS 憑證申請

(5)完成系統向上集中

2.臺灣華文電子書庫作業系統、資料庫升級與向上集中

臺灣華文電子書庫因資訊安全考量及向上集中所需，需完成作業系統、資料庫升級等工作。本案計畫辦理工作如下：

(1)作業系統移轉至 Ubuntu Server，相關資料庫及 PHP 版本一併跟隨升級

(2)搜尋引擎(Solr)升級

(3)資料庫及相關書庫影像檔案移轉

(4)完成系統向上集中

3.電子書刊送存系統會員認證機制優化

電子書刊送存系統會員申請及認證機制，原結合本館單一登入系統，因單一登入系統老舊、部分功能已無法修復，亟需使系統的會員申請及申認自單一登入系統中分離，改以與圖書館自動化系統整合，提供讀者以閱覽證認證。本案計畫辦理工作如下：

⑴介接圖書館自動化系統讀者 API

⑵修正電子書刊送存系統登入介面、認證流程及相關說明

⑶修正原有 NCL Reader 讀者之認證

貳、計畫成果

一、網路管理自動化系統建置及資通訊系統日誌收集分析軟體

本項完成套裝系統軟體採購、系統導入、規則建立及施行

(一)設備監控管理系統建置，係為符應每二年一次資通安全健診所需「網路架構檢視」所需之管理系統，完成骨幹網路管理、網路設定及相關文件產出等工作。

(二)「資通系統日誌管理分析系統」建置，係為「資通安全威脅偵測管理機制」、資通系統防護基準「事件日誌與可歸責性」必要之控制措施，完成 LOG 管理系統及伺服器所需軟硬體建置等工作。

二、端點資安防護升級

本項為「資通安全弱點通報機制」所需辦理「端點資安防護軟體升級」案，完成套裝系統軟體採購、系統導入、規則建立及施行等工作。

三、資訊系統汰換升級、系統功能優化

(一)完成「數位影音系統」應用程式改版與向上集中

本項主要辦理作業系統、資料庫及相關軟體套件版本升級為最新版、前後臺改寫程式及影音檔案轉檔及重整，確保軟體系統版本符合當前最新的作業環境。

1.完成數位影音系統系統架構優化暨資安問題改善，包含主機環境之微軟作業系統 Windows 2022 Server 及資料庫 Microsoft SQL Server 2019 軟體升級等工作。

2.完成前後臺程式改寫，重新調整系統架構；關閉非必要的服務埠，導入政府組態基準作業；不存在中、高風險等級之弱點，符合資安

政策。

3.提供網站能跨平臺使用，前臺不限瀏覽器提供播放影音功能，網頁採用響應式網頁設計,不同載具的使用者皆能獲得最佳之瀏覽體驗。

4.完成不符現行播放格式之影音檔案轉檔與重整。

(二)臺灣華文電子書庫作業系統、資料庫升級與向上集中

本次升級案主要為核心系統的建構，由原本的 LAMP 架構(Linux CentOS、Apache、MySQL 及 PHP)，改採 Ubuntu、Nginx、MariaDB、PHP 作為為主網站開發與執行架構。此次轉換主要係評估各開源專案之穩定度與授權政策，力求最大程度的提高本系統在最低授權成本下能夠有最大使用年限。

1.檢索應用採用 Apache Solr 全文檢索伺服器功能模組，Solr 提供優異的全文檢索服務設計，能做快速的巨量資料檢索回應，Solr 目前亦為目前全球最多採用之自建搜尋引擎解決方案。

2.前端頁面則以 HTML5 為網頁語言，並透過 JavaScript 及 JQuery 等做使用者互動介面控制，以得到最佳的網頁瀏覽器呈現支援。

3.資料面以網頁瀏覽器能呈現的 JPEG 圖檔為主，並搭配圖書整本閱讀之需求提供 PDF 檔案格式做為數位閱讀版本之呈現標的。

4.調整各項系統功能，以符合資通系統防護基準普級之各項要求。系統經 ZAP 軟體執行 OWASP TOP10 弱點檢測，系統報告無中、高風險等級弱點。

(三)電子書刊送存系統會員認證機制優化

本案主要為「電子書刊送存系統」優化會員認證機制，由原已不符資安要求的單一登入系統，改以讀者閱覽證認證，完成圖書館自動化系統讀者 API 介接、修正電子書刊送存系統登入介面、認證流程及相關說明；並修正原有 NCL Reader 讀者之認證方式。

參、成效檢討

一、網路管理自動化,有效提供網路設備實時監控、加速網路問題的判斷、降低設備失效時之反應時間。

二、端點資安防護再升級,得以提供資訊資產管理系統各端點軟體版本之集中管理與派送，並得與行政院國家資通安全會報技術服務中心之資通安全弱點通報系統進行 API 介接，自動上傳館內各端點弱點及修補狀況。

三、IT 資源管理與網路安全防護系統升級，提供 IP 管理由觀察、監視到管控，逐步改善 IP 使用情形並管理館外 MAC，以避免未知設備任意使用館內網路資源，進而造成資安風險。

四、日誌統一收集留存及分析，可作為資安事件事後追查或防堵漏洞的依據，並符合法規要求。

五、重要的讀者服務系統，完成系統升級並向上集中。