教育部112年度補助國立圖書館發展館藏特色及強化營運服務計畫

強化系統資訊安全及資源向上集中計畫

執行成果報告

執行單位：國家圖書館

113年2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。111 年在補助經費的支持下完成官網主機架構調整、伺服主機及存儲設備升級；完成端點資安防護、網路管理及資訊系統日誌管理所需軟體購置；完成「數位影音服務系統」、「臺灣華文電子書庫」系統架構調整及資安問題處理；完成「電子書刊送存閱覽服務系統」會員認證機制改善資安防護控制措施……等工作；112 年為配合資訊資源向上集中政策，除以本館有限的經費投入系統及資安問題改善外，仍有諸多系統亟需爭取補助經費，推動主機弱掃及弱點修補、功能維護及優化、系統框架調整及移機等工作，俾能完成於政策指定期限前完成系統汰換升級並向上集中。

二、預期目標

本案計畫目標有二：

(一)向上集中之資訊系統，完成主機弱點評估

主要利用本館已購置之專業版資訊安全管理與弱點評估軟體(授權)，針對本館資訊系統主機全面進行弱點評估、產出報告，以作為系統弱點修補、強化資安防護力之依據。

(二)強化系統資安防護力，完成系統向上集中

主要辦理系統作業及安全維運所需之作業系統及資料庫版本升級、功能維護及優化、資安弱點修補、系統防護基準控制措施改善等，完成系統移置教育部雲平臺等前置作業。

三、內容要項

(一)向上集中之資訊系統，完成主機弱點評估

1. 利用本館已購置之專業版資訊安全管理與弱點評估軟體，將本館仍須持續維運的系統為標的，全面進行系統主機掃描。
2. 預計完成逾 100 臺主機掃描，並產出評估報告。

(二)強化系統資安防護力，完成系統向上集中

資訊系統向上集中的基本要件為—主機虛擬化、系統無中高資安風險問題，本館許多因服務需要仍持續維運之系統，多數建置年代久遠，存在有資安風險或資安防護措施不符問題；又因應系統向上集中，具多主機且架構複雜之系統須調整系統程式架構、網路環境調整或參數設定等。期透過此計畫，按各系統現況問題，辦理作業系統及資料庫升級、功能維護及優化、資安弱點修補、系統防護基準控制措施改善等適當處置工作，以使系統能順利移置教育部雲平臺。

1. 臺灣博碩士論文知識加值系統

此系統為本館核心系統之一，另包含博碩士電子論文獨立調閱系統及博碩士電子論文數位影音串流系統。此系統具前臺查詢檢索功能與研究生建檔功能，以及後臺國圖與學校管理功能，主機數計有 25 臺，本計畫預計改善以下問題：

(1)因應資安防護基準要求，改善後臺管理端身份驗證管理，包括系統須要求密碼複雜度與密碼歷程等項目；改善管理端事件日誌紀錄內容，增加特定事件之日誌稽核與輸出格式的一致性；調整優化資料庫表格，取代早期開發不符合現今資安規範的欄位；

(2)因應向上集中環境有無法識別本館內網 IP 之議題，以及大量系統早期開發進行之網路客製化設定與介接，須調整相對應綁定部分內網 IP 功能之機制與網路環境重新部署、系統程式架構調整及參數重新設定等；

(3)為向上集中需要，辦理功能維護及優化、資安弱點修補、負載平衡器(實體機)移置教育部雲平臺問題之改善措施規劃。

2.圖書館自動化管理系統及全國新書資訊網

圖書館自動化管理系統為本館核心資通系統，存有讀者個資及國家文獻書目資料，亦為本館各項服務會員認證之來源系統，主機數計有 5 臺；全國新書資訊網提供出版社申請 ISBN 服務，並提供新書資訊服務，主機數計有 3 臺。本計畫預計改善以下問題：

(1)因應系統安全防護基準要求，改善館藏查詢系統線上調閱有關帳號管理、密碼複雜度控管、身分驗證管理、漏洞修復等防護措施問題；

(2)館藏查詢系統資安防護升級，抵禦自動化程式或機器人等惡意程式侵入嘗試，以電子信箱驗證功能確認讀者身分；

(3)為向上集中需要，辦理功能維護及優化、資安弱點修補、各功能同步向上移轉所需架構調整及參數設定等。

3.電子書刊送存閱覽服務系統

本系統為出版社申請電子書 ISBN、出版社送存電子書、讀者閱覽送存電子書、館員資訊組織及電子書內容管理之服務平臺。系統開發迄今已逾 10 年，本計畫預計改善以下問題：

(1)因應系統安全防護基準要求，改善帳號管理、事件日誌紀錄內容、身分驗證管理、漏洞修復等防護措施問題；

(2)為向上集中需要，辦理功能維護及優化、各項客製化功能同步向上移轉所需架構調整及參數設定等。

4.座位預約系統、政府公報資訊網及政府統計資訊網

座位預約系統包含本館自修室、團體討論室之座位管理功能，並介接讀者認證來源系統供預約及門禁系統驗證，主機數計有 2 臺；政府公報資訊網及政府統計資訊網，提供讀者查詢中央與地方公報內容，以及官方各類重要統計、專論及調查報告，主機數計有 2 臺，本計畫預計改善以下問題：

(1)自修室、團體討論室預約座位系統環境重新建置並區隔、重建 2 臺座位預約主機；

(2)為系統向上集中需要，預計依系統個別需求辦理功能維護及優化、資安弱點修補、各功能同步向上移轉所需架構調整及參數設定等。

5.臺灣書目整合查詢系統

本系統為整合本館之全國圖書書目聯合目錄、博碩士論文、期刊文獻等50餘種圖書館資源，提供讀者單一查詢的入口網。系統建置已逾10年，主機數計有7臺，本計畫預計改善以下問題：

(1)因應系統安全防護基準要求，改善帳號管理、事件日誌紀錄內容、身分驗證管理、漏洞修復等作業；

(2)為向上集中需要，辦理功能維護及優化、各項客製化功能同步向上移轉所需架構調整及參數設定等。

貳、成果內容

一、執行方式

(一)辦理購買弱點掃描軟體Nessus 1年授權，針對目標系統的伺服器主機進行系統漏洞和弱點檢查和評估。有助於發現可能被攻擊者利用的安全漏洞，增強整體的資訊安全性。針對本館下列4個網段之伺服器主機執行弱點掃描並產出弱點掃描報告，依據該報告進行弱點修復。部分弱點修復完成之系統主機將安排向上集中作業。

網段	伺服器主機數量
192.83.186.0/24	131
192.168.7.0/24	180
192.168.8.0/24	77
192.168.101.0/24	33

(二)辦理「112年臺灣博碩士論文知識加值系統資安改善暨系統維護案」，依照系統防護基準控制措施之要求，針對博碩士系統內，閒置帳號與身分驗證管理進行功能新增與強化，依弱點掃描報告修補中高風險等弱點，並依現階段評估整體系統向上集中的可行性與評估對應的資安風險。承商完成履約後進行驗收與付款作業。

(三)辦理「圖書館自動化管理系統及全國新書資訊網資安防護升級、功能維護與優化」，建立新虛擬主機提供讀者帳密管控、及系統提醒機制。精

進讀者登入流程，以 RWD 方式設計新版登入畫面。新增 CAPTCHA 驗證碼欄位，登入時除帳密外，尚須輸入正確的驗證碼。新增密碼複雜度、90 天內須修改密碼、及密碼不得與前 3 次相同之檢核機制。提供「忘記密碼」功能，供讀者自行取回帳號所有權。承商完成履約後進行驗收與付款作業。

(四)辦理「112 年電子書刊送存閱覽服務系統資安問題改善暨年度維護案」，針對系統帳號與身分登入驗證機制進行改善，新增重要系統日誌事件，並設定上傳檔案格式之限制。由廠商於測試機進行資安問題改善及測試，廠商於測試機完成弱點檢測並改善完成後，再於功能上線至正式機後進行黑箱弱點檢測。承商完成履約後進行驗收與付款作業。

(五)辦理「112 年自修室預約選位及門禁管理系統資安問題改善暨年度維護案」與「112 年政府公報暨統計資訊網資安問題改善暨年度維護案」，召開專案啟動會議，商討調整系統架構與向上集中事宜，確認系統架構優化相關軟硬體資源配置。於新主機環境通過本館主機弱掃與教育部網站弱掃報告無中高風險問題後，進行系統向上集中作業。承商完成履約後進行驗收與付款作業。

(六)辦理「臺灣書目整合查詢系統資安防護升級暨功能維護及優化」，進行系統程式架構及參數設定調整，移至集中雲平臺後配合進行系統測試，如因系統發生執行或相容性之問題，應查明原因並調整系統程式架構、參數或更新相關軟體套件使系統能正常運行。依資通系統防護基準各項控制措施，改善帳號管理、事件日誌紀錄內容及身分驗證管理。並與業務單位評估過後，優化前臺登入機制，將統計圖表修改為免登入即可查看，便利讀者取得書目統計資料。承商完成履約後進行驗收與付款作業。

二、績效成果

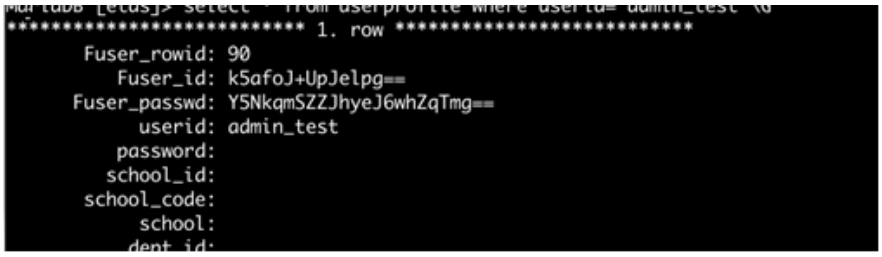
(一)向上集中之資訊系統，完成主機弱點評估

完成本館 4 個伺服器網段主機弱掃，共計 421 臺主機弱點掃描並產出報告，各系統承辦人依據產出報告修補主機弱點，以符合教育部資源向上集中政策要求。

(二)強化系統資安防護力，完成系統向上集中

1. 臺灣博碩士論文知識加值系統

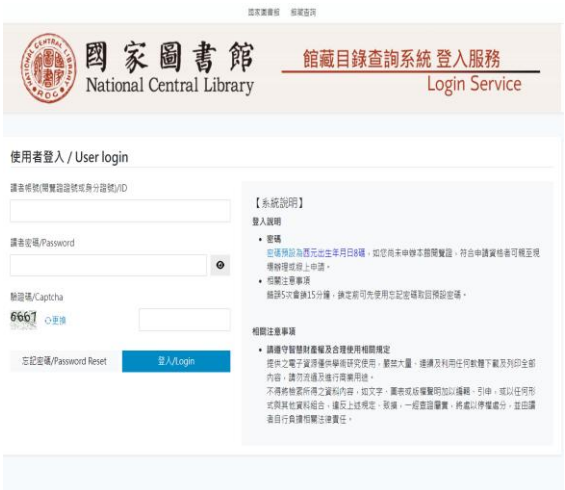
新增讀者帳號閒置帳號之功能，有效管理大量久未使用之讀者帳號，減少系統受攻擊的可能性。改善後臺管理端帳號身分驗證機制，強化學校、研究生等使用博碩士系統時帳號密碼登入機制。調整資料庫機敏資料儲



存格式，並改用雜湊值保護資料，減少資料庫被攻擊的風險。調整 FTP 上傳機制，改用更具安全性的 FTPS 作為學校送存論文的方式。向上集中的評估如附件。

2. 圖書館自動化管理系統及全國新書資訊網

有關圖書館自動化管理系統改善項目，升級讀者帳號管理機制並執行密



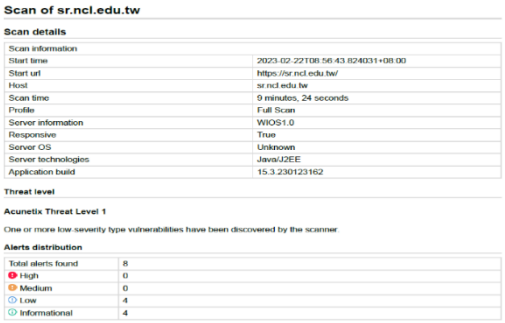
碼複雜度等多項檢核，提升系統安全性，降低被駭風險。新增 CAPTCHA 驗證碼欄位，有效降低自動化程式或機器人侵入風險。建立帳戶鎖定機制，密碼輸入錯誤 5 次將自動鎖定，讓有心人士無法持續嘗試密碼。提供"忘記密碼"功能，方便讀者自行取回帳號控制權，亦有效減輕館員人力負擔。

3. 電子書刊送存閱覽服務系統

調整前後臺使用 HTTPS 連線傳輸，身分認證相關機制不以明文傳輸。前台驗證碼更換 Google 驗證碼提高安全性。系統日誌週期保留 6 個月，內容包含登入、登出、驗證失敗、審核。系統上傳檔案格式限制，以白名單方式開放上傳檔案格式。完成資安風險改善及資訊系統資安防護基準自我檢核。

4. 自修室、團體討論室預約系統、政府公報資訊網及政府統計資訊網

(1)自修室、團體討論室預約系統、政府公報資訊網及政府統計資訊網網站弱掃報告無中高風險(使用教育部 Acunetix 弱掃軟體)



Scan of sr.ncl.edu.tw

Scan details

Scan information	
Start time	2023-02-22T08:56:43.824031+08:00
Start url	https://sr.ncl.edu.tw/
Host	sr.ncl.edu.tw
Scan time	9 minutes, 24 seconds
Profile	Full Scan
Server information	WIOS1.0
Responsive	True
Server OS	Unknown
Server technologies	Java/J2EE
Application build	15.3.230123162

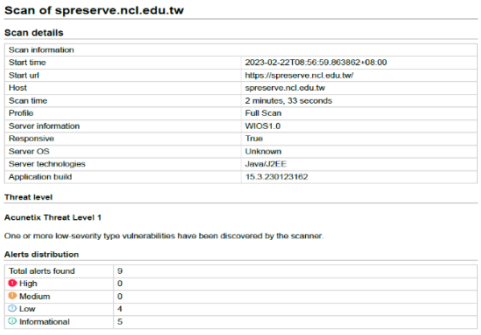
Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	8
High	0
Medium	0
Low	4
Informational	4



Scan of spreserve.ncl.edu.tw

Scan details

Scan information	
Start time	2023-02-22T08:56:59.863862+08:00
Start url	https://spreserve.ncl.edu.tw/
Host	spreserve.ncl.edu.tw
Scan time	2 minutes, 33 seconds
Profile	Full Scan
Server information	WIOS1.0
Responsive	True
Server OS	Unknown
Server technologies	Java/J2EE
Application build	15.3.230123162

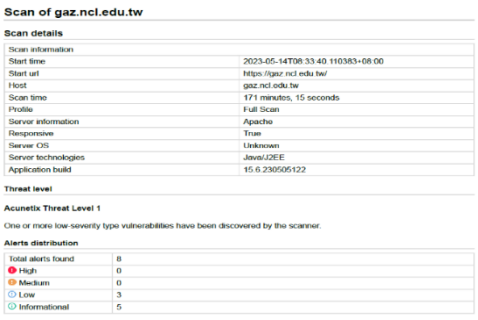
Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	9
High	0
Medium	0
Low	4
Informational	5



Scan of gaz.ncl.edu.tw

Scan details

Scan information	
Start time	2023-05-14T08:33:40.110383+08:00
Start url	https://gaz.ncl.edu.tw/
Host	gaz.ncl.edu.tw
Scan time	171 minutes, 15 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
Server technologies	Java/J2EE
Application build	15.6.230505122

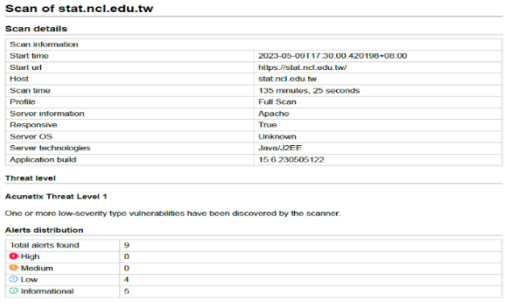
Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	8
High	0
Medium	0
Low	3
Informational	5



Scan of stat.ncl.edu.tw

Scan details

Scan information	
Start time	2023-05-09T17:30:00.420198+08:00
Start url	https://stat.ncl.edu.tw/
Host	stat.ncl.edu.tw
Scan time	135 minutes, 25 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
Server technologies	Java/J2EE
Application build	15.6.230505122

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	9
High	0
Medium	0
Low	4
Informational	5

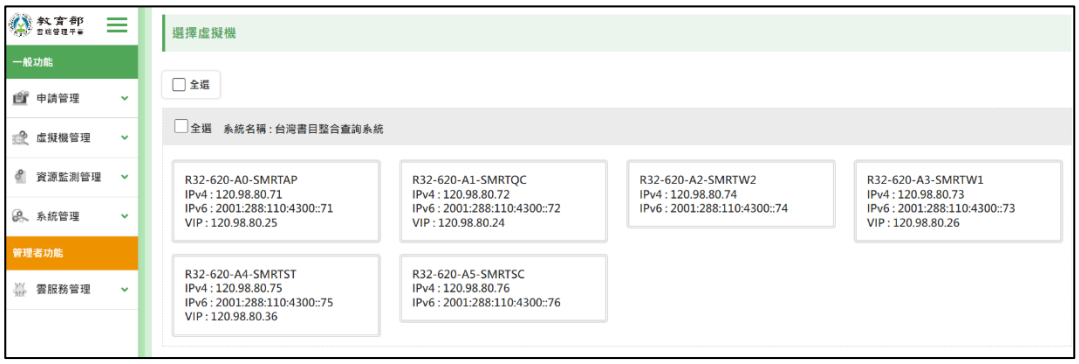
(2)自修室讀者預約座位-館內選位與教育部雲平臺主機同步測試

(3)向上集中後政府公報資訊網可正常連線及檢視全文電子檔

5.臺灣書目整合查詢系統

(1)系統向上集中強化資安防護及服務穩定度

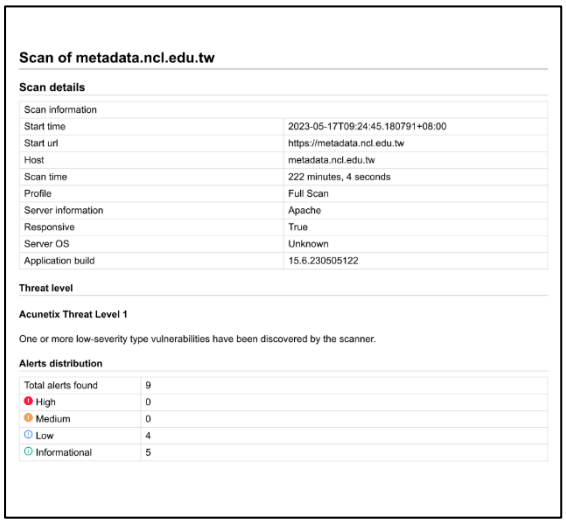
雲平臺提供更完善的資安防護措施及設備，強化資訊安全。另雲平臺提供更大的網路頻寬(提升 10 倍頻寬)，讓網站服務更流暢、穩定。



臺灣書目整合查詢系統主機已向上集中至雲平臺

(2)修補系統主機及網站中高風險，提升系統強韌度

歷經多次弱點掃描已修正主機(6 臺)及網站(1 前臺、2 後臺)，已修補 32 高風險及 3 中風險，系統主機及網站目前已無中高風險，提升系統強韌度。



Scan of metadata.ncl.edu.tw

Scan details

Scan information	
Start time	2023-05-17T09:24:45.180791+08:00
Start url	https://metadata.ncl.edu.tw
Host	metadata.ncl.edu.tw
Scan time	222 minutes, 4 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
Application build	15.6.230505122

Threat level

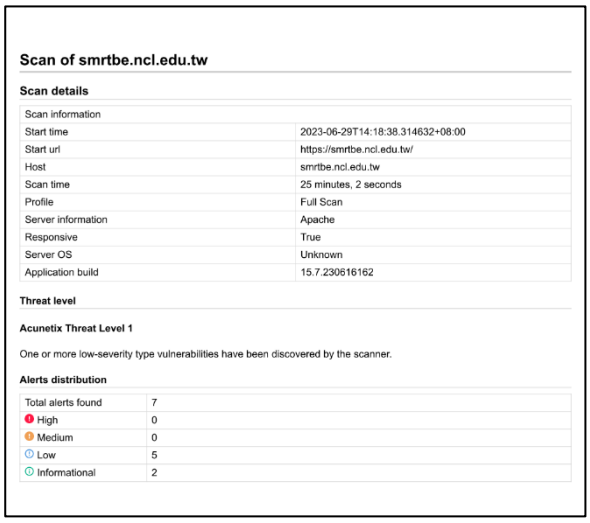
Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	9
High	0
Medium	0
Low	4
Informational	5

臺灣書目整合查詢系統網站
(前臺)弱掃報告



Scan of smrtbe.ncl.edu.tw

Scan details

Scan information	
Start time	2023-06-29T14:18:38.314632+08:00
Start url	https://smrtbe.ncl.edu.tw/
Host	smrtbe.ncl.edu.tw
Scan time	25 minutes, 2 seconds
Profile	Full Scan
Server information	Apache
Responsive	True
Server OS	Unknown
Application build	15.7.230616162

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	7
High	0
Medium	0
Low	5
Informational	2

臺灣書目整合查詢系統網站
(後臺)弱掃報告

參、成效檢討

一、向上集中之資訊系統，完成主機弱點評估

(一)補足教育部主機弱掃進度時程，能縮短本館系統向上集中作業進程。

(二)可完成本館逾100臺主機掃描或複掃，並產出評估報告。

二、強化系統資安防護力，完成系統向上集中

(一)臺灣博碩士論文知識加值系統完成後臺管理端身分驗證管理、事件日誌紀錄內容、優化資料庫表格等資安控制措施改善以符合資安防護基準要求;功能維護及優化、系統弱點修補、網路環境重新部署及參數調整等，完成向上集中所需作業之準備。

(二)圖書館自動化管理系統、全國新書資訊網及相關客製化功能維護及優化、系統弱點修補、系統架構調整等，並完成資安控制措施改善以符合資安防護基準要求及向上集中作業之準備；館藏查詢系統資安防護升級，提高讀者個資及帳戶安全。

(三)完成電子書刊送存閱覽服務系統之功能維護及優化、系統弱點修補、系統架構調整等，並完成資安控制措施改善以符合資安防護基準要求及向上集中作業之準備。

(四)完成座位預約系統、政府公報資訊網及政府統計資訊網之功能維護及優化、系統弱點修補、系統架構調整等，完成資安控制措施改善以符合資安防護基準要求，並完成向上集中作業。

(五)完成臺灣書目整合查詢系統及相關客製化功能之功能維護及優化、系統弱點修補、系統架構調整等，完成資安控制措施改善以符合資安防護基準要求，並完成向上集中作業。

肆、附件

臺灣博碩士論文知識加值系統向上集中評估報告

現況分析：

臺灣博碩士論文知識加值系統為現今第三代博碩士系統，分為 4 年（98~101 年）建置完成，並於 102 年至 111 年間陸續辦理功能擴充，改版建置與擴充經費累積大約 1,500 萬元。系統自 99 年 6 月上線以來，目前每月檢索人次約為 4,500 萬人次，尖峰時段同時上線人數突破 2 萬人，每天提供檢索人次亦超過 100 萬次，書目資料總筆數約有 133 萬筆，全文電子檔筆數約有 87 萬筆，已成為國內最重要的學術支援網站之一。

博碩士系統為了乘載大量使用連線，導入負載平衡機制，前臺查詢目前共有 5 臺，研究生建檔有 2 臺。也因負載平衡相關技術，系統需有額外特別的設定處理 SNAT 與 SESSION 綁定的問題。因此系統會與負載平衡的設定參數交互作用，才能正確執行功能。

過往博碩士系統歷經 1 次實體機移轉、1 次作業系統移轉、1 次虛擬機移轉，每次移轉均有花費 2 個月以上的錯誤排除作業，影響多數學校作業流程。廠商表示現有博碩士系統架構難以再承受任何的轉移作業，尤其教育雲的網路環境無法相容於現有的系統，若強制向上集中將可預期會損失大部分的功能性，並預計耗費半年以上的修復時間，造成各學校的作業困難。

博碩士系統經常受到外部惡意連線使用，通常是屬於在正常功能範圍下之惡意使用功能，例如：大量註冊帳號下載公開之論文電子全文、連續爬網檢索造成系統無法負荷不穩定等。類似情況往往基於網路架構中的防火牆進行阻擋，但向上集中後，國圖將沒有權限設定教育部的防火牆，可預見博碩士系統會承受更多的連線使用，以現有的系統舊技術將不足以乘載服務量能。

另外系統目前使用之作業系統（CentOS 7）將於 113 年 6 月底終止安全更新服務，因應現今資安要求，系統有採用新版作業系統之急迫性。然而變動作業系統勢必是一次系統的移轉，因此廠商建議直接在教育雲上以新的技術套件重新製作博碩士系統，再進行資料轉換作業，是綜合上述各項風險與經費評估後之最佳方案。

博碩士電子論文獨立調閱系統是於109年開發之系統，依法令規定，圖書館需提供博碩士電子論文現場調閱機制，為特殊開發之論文閱覽系統。其功能與網路架構緊密結合，經由閱覽區座位管理系統與限制電腦來源IP多重機制判斷才可進行使用。其資料來源由博碩士系統提供，其中包含未公開論文之敏感資料。若博碩士系統與獨立調閱系統向上集中後，將會因教育雲較嚴謹的資安環境，需要經費支援修改座管系統與獨立調閱系統之間的連線，而且論文全文資料會需要透過外網傳輸，增加網路流量的成本。

主要功能說明：

1. 提供全球讀者查詢博碩士論文書目資料網頁，特定條件下瀏覽論文全文功能，與個人研究室之加值服務。
2. 提供每篇論文獨立永久網址，與全球博碩士搜尋網站相互串聯檢索。
3. 提供全臺灣合作學校使用博碩士系統雲端服務、各校專屬論文查詢網頁，協助畢業研究生建檔與學校系所圖書館審核流程。
4. 提供全臺灣各學校電子論文送存之機制，以及依法令規定限制館內調閱電子論文功能。

系統架構說明：

目前博碩士系統共計有1臺實體機(負載平衡設備)與20臺虛擬機(VMware)，資源總使用需求約為CPU 350 Core、RAM 1.2T、硬碟空間50T。

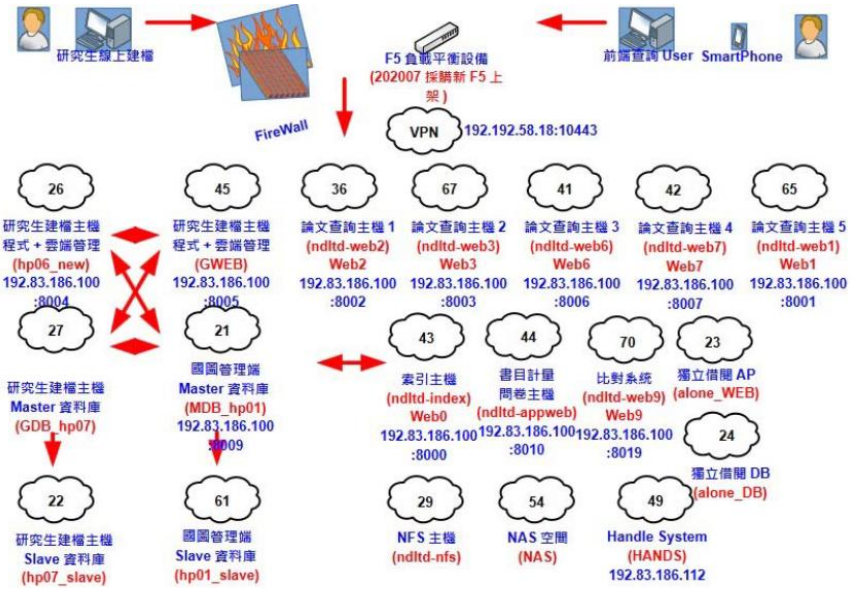
系統架構可大致分為4個部分：前端檢索查詢、學校雲端服務、國圖書目全文管理與獨立調閱服務，但 4 個部分並非獨立切開的子系統，彼此間依然有功能資料互相串連。詳細說明如下表：

部分	項目	名稱	VM主機規格	用途	網路IP
	1	負載平衡器 (F5)	N/A（實體機）	對外入口進入點，分流導向。	192.83.186.100 192.83.186.64 192.83.186.112 192.168.8.137

前端檢索查詢	2	查詢主機 （共5臺）	CPU: 24 Core RAM: 96G DISK: 450G CentOS 7	全球讀者查詢，依來源 IP 限制開放閱讀全文影像，並可配合館內單機軟體閱讀。	192.168.101.36 192.168.101.41 192.168.101.42 192.168.101.65 192.168.101.67
	3	問卷調查與書目計量主機	CPU: 16 Core RAM: 64G DISK: 450G CentOS 7	提供問卷調查、統計相關功能。	192.168.101.44
	4	停機公告主機	CPU: 2 Core RAM: 2G DISK: 16G Rocky Linux 9.2	臨時停機維修，切換網頁使用。	192.168.101.20
	5	索引主機	CPU: 24 Core RAM: 64G DISK: 1500G CentOS 7	提供查詢主機搜尋服務。	192.168.101.43
	6	Handle 主機	CPU: 8 Core RAM: 16G DISK: 500G CentOS 8	提供每篇論文永久網址服務。	192.168.101.49
學校雲端服務	7	建檔主機 （共2臺）	CPU: 24 Core RAM: 96G DISK: 750G CentOS 8	研究生畢業論文建檔，學校審核與管理論文。支援各校帳號驗證機制。	192.168.101.26 192.168.101.45
	8	建檔資料庫 （共2臺）	CPU: 16 Core RAM: 64G DISK: 500G CentOS 7	學校雲端網頁使用之資料庫。	192.168.101.22 192.168.101.27
國圖書目全文管理	9	管理主機與資料庫 （共2臺）	CPU: 24 Core RAM: 96G DISK: 750G CentOS 8	國圖管理後台，資料庫互為備援。	192.168.101.21 192.168.101.61
	10	介接主機	CPU: 4 Core RAM: 16G DISK: 450G CentOS 7	與論文比對系統資料介接用。	192.168.101.70
	11	NFS 主機	CPU: 16 Core RAM: 16G DISK: 2848G CentOS 7	前臺帳號資料儲存空間，各項功能資料空間。	192.168.101.29

	12	NAS 主機	CPU: 4 Core RAM: 16G DISK: 25180G CentOS 8	論文全文與備份空間。	192.168.101.54
獨立調閱服務	13	獨立調閱前臺主機	CPU: 16 Core RAM: 64G DISK: 850G CentOS 8	提供館內特定電腦調閱所有館藏之電子論文。	192.168.101.23
	14	獨立調閱後臺主機	CPU: 32 Core RAM: 64G DISK: 600G CentOS 8	管理獨立調閱系統後臺。	192.168.101.24

系統架構圖：



系統維運狀況與向上集中困難說明：

1. 多數功能不符合教育雲的資安規範，例如：學校使用 FTP 上傳大量全文電子檔案送存至系統、建檔主機與管理主機資料串連並有提供網頁服務、依國圖館內來源 IP 限制論文全文的存取權、可設定私有 IP 控管後臺登入權限等。廠商建議若要調整該些功能以符合教育雲環境，不如重新實作並更換使用套件較為經濟可行。
2. 博碩士的問題處理大部分有即時性，例如系統功能當機致使學校與研究生無法處理畢業流程事宜、論文下架但是仍然被前臺搜尋到、前臺查詢緩慢需立

即檢修、遭受大量爬網攻擊需要人工識別處理等。若依照教育雲遠端連線審核流程進行，廠商無法多人同時立即進行問題檢視與排除，嚴重時恐有法律議題產生。

3. 建檔主機會串連各學校的帳號做單一認證(SSO)，不同學校使用不同的方式做帳號驗證，其驗證機制多達 5 種以上。每一種驗證皆有不同的 IP 設定或與學校介接驗證主機等，因多年來推動的狀況，有多數學校漸漸加入國圖系統，因此每年皆會在後臺異動相關設定，難以盤查各項系統設定。但向上集中後該些功能將失效，系統功能無法與教育雲防火牆自動介接，人工設定將會有疏漏，影響學校作業。
4. 博碩士系統每年弱點掃描或滲透測試皆已修補完成，就系統所提供的功能應無額外的資安疑慮。就國圖現有的網路設備，大多已達使用年限，並已接近產品終止服務的時限，對於防禦網路設備的資安攻擊略顯不足，需要經費支援汰舊換新。
5. 系統距開發建置時間已餘 10 年以上，當年實作技術已老舊，廠商內部開發人員多已離職換人。國圖每年需投入約 110 萬元之經費進行系統維運，但對於系統錯誤修正成效不彰。廠商表示系統程式架構老舊、更改不易，任何的架構變更都可能產生某些功能失靈或是資料錯亂。

風險評估：

將資安威脅來源分為 4 類：天然災害、無意圖性的、機關內部有意圖性的與機關外部有意圖性的。並依國圖網路環境與教育雲環境作為比較各項可能的資安風險利弊，呈現如下表：

資安威脅來源			國圖網路環境	教育雲環境
天然災害		地震、斷電、戰爭等情形。	目前並無異地機房，無法防禦機房全滅之風險。	有異地備援機制，應可防禦單一機房全滅之風險。
無意圖性的		承辦人或廠商系統操作失誤、疏忽	遠端連線政策可開通 3 個月，廠商修復問題較彈性，但也產生更多的機會致使此風險。	遠端連線政策僅開通 8 小時，廠商無法即時修復錯誤，但系統越少的操作此風險也越小。
有意圖性的	機關內部	離職員工報復、內部有心人士攻擊。	系統除了有帳號密碼機制，另有綁 IP、電腦權限限制使用，該風險較低。系統會記錄各項操作日誌，可透過 IP 等紀錄追查犯人。	國圖與教育雲需作更多的設定才能更新綁定 IP，增加作業複雜度，作業期間難以防止此類攻擊。
	機關外部	DoS、DDoS 攻擊	系統有機制偵測來源 IP 連線數目，並進行自動阻擋。但若館內防火牆設備等不堪流量負荷仍是無解。	具有流量清洗機制。
		系統弱點攻擊	每年皆有作弱點掃瞄或滲透測試並修補各項中、高等級風險。連線封包也有經過 WAF 作一般性的攻擊阻擋。	WAF 政策較為嚴格，應能阻絕更多弱點攻擊。並有 VIP 機制，連線無法直接抵達主機。
		橫向擴散	系統建置在獨立的網路空間，並與其他 DMZ 上系統互相隔離。若它系統遭受攻擊，應無法橫向擴散至博碩士系統。	各臺主機原則上僅開放最小權限之防火牆，安全機制較嚴格。
		APT	系統主機目前並未封鎖對外網路的存取，若受到組織性攻擊將無法即時針對主機封鎖可疑封包。	各臺主機原則上不開放防火牆流出規則，若主機上已被入侵部屬相關病毒，可有效阻斷與駭客主機之間連線，不會立即產生風險。

各項方案規劃時程評估：

將以博碩士系統向上集中與否，與系統本身是否進行架構調整或優化作評估分析，根據廠商評估各項作業與時程規劃，如下表列：

	不向上集中 （網路設備需汰換）	向上集中 （多數功能調整測試）
維持系統原本功能,僅作資安修補加強	防火牆設備汰舊換新經費約450萬元。額外的資安防護機制（更換FTP上傳機制、各主機連線防火牆盤點與設定、設定更嚴格之WAF政策等）經費約300萬元。 總計需要經費750萬元，並花費半年時間設置調整。	廠商報價約400萬元,但廠商不建議只做這個項目，因為系統架構老舊，集中上去有高機率性損壞多數功能。須花費1年的工作時間調整測試。
上述+作業系統移機升級	作業系統升級廠商報價 500萬元，並需要3個月的工作時間。 合併上述網路設備項目，總計需要經費1,250萬元，並花費8個月的時間調整。	向上集中與作業系統升級廠商報價約600萬元,並需要1年工作時間調整測試。
上述+架構優化調整 （系統重新改寫）	廠商以建置總費用的2/3來作計算，需要經費1,000萬元,並須要一年的開發時間。 合併上述網路設備項目，總計需要經費1,750萬元，並花費1年的時間調整。	廠商須因應教育雲環境重新設計合適架構，其功接近餘重新建置，故報價1,600萬元，分三年期程，前兩年進行開發與舊資料轉換,後一年進行各學校介接測試與上線。廠商推薦以此做為首選方案，兼顧向上集中政策與系統更新優化。

結論：

綜合上述評估，目前博碩士系統面臨有三項非做不可的工作（向上集中、作業系統升級、系統架構老舊需進行優化調整),為了提供更優質博碩士系統服務，以及達成向上集中的目標，建議應請廠商直接在教育雲環境重新實做博碩士系統。於此能將業務與資安風險降到最小，待開發完成後，與各學校進行新的系統教育訓練即可正式改版切換。此方案所需經費約 1,600 萬元，約三年的建置與轉換。