

清華大學計算機中心 資通系統防護基準實務

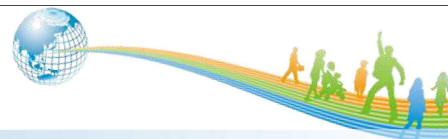


2024/04/19

中華電信

沈雅婷

報告人沈雅婷



■ 現任 資訊安全管理制度輔導顧問

■ 資歷

- 中華電信資訊技術分公司, 資安管理制度輔導顧問
- 中華電信數據通信分公司, 滲透測試資深工程師

■ 專長

- 企業資訊安全風險管理
- 企業營運持續管理
- 滲透測試安全評估

■ 證照

- ISO/IEC 27001、ISO/IEC 27701 主導稽核員、ISO 27017 & 27018、ISO 22301 主導稽核員
- BS 10012、PCI-DSS、NIST CSF 主導稽核員
- EC-Council ECSA 資安分析專家、CEH 道德駭客
- EC-Council CHFI 資安鑑識調查專家
- CCNA / CCNA Security 思科認證網路安全專家
- CompTIA, TCSE 趨勢防毒, SCTS 賽門鐵克 安全專家

報告人沈雅婷



❖ 公務機關及學校



勞動部勞工保險局
Bureau of Labor Insurance, Ministry of Labor



行政院衛生署
Department of Health, Executive Yuan, R.O.C.



❖ 其他機構



新光銀行



BANK OF KAOHSIUNG



新光人壽
Shin Kong Life

CHIMEI
a step up



新光產物保險
SHINKONG INSURANCE



新安東京海上產物保險股份有限公司
TOKIO MARINE NEWA INSURANCE CO., LTD.



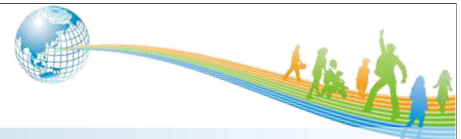
中華郵政全球資訊網
Chunghwa Post Co., Ltd.



中華電信
Chunghwa Telecom

3

簡報大綱



❖ 源起

❖ 資通系統防護需求等級分級暨防護基準說明

■ 資通系統防護需求分級原則

■ 資通系統防護基準說明暨實作案例(含驗證實務)

■ 資通系統防護基準自評檢查

❖ 問題與討論

❖ 附錄

4



中華電信
Chunghwa Telecom

源起



資通安全責任等級分級辦法(第11條第2項)

- ❖ 各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；(後略)。

資通系統防護需求等級分級

(資通系統防護需求分級原則)



資通系統防護需求分級原則(1/9)



❖ 附表九、資通系統防護需求分級原則

- 以「**四構面**」評定資通系統之防護需求
 - 機密性
 - 完整性
 - 可用性
 - 法律遵循性
- 資通系統防護需求分級為「**三等級**」
 - 普
 - 中
 - 高

防護需求等級
= MAX (機密性, 完整性, 可用性, 法律遵循性)
- 備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性、法律遵循性構面中，任一構面之防護需求等級之最高者定之。

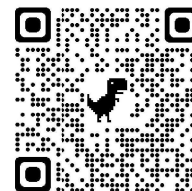
防護需求等級 構面	高	中	普
	發生資通安全事件致資通系統受影響時， 可能造成未經授權之資訊揭露 ，對機關之營運、資產或信譽等方面將產生 非常嚴重或災難性 之影響。	發生資通安全事件致資通系統受影響時， 可能造成未經授權之資訊揭露 ，對機關之營運、資產或信譽等方面將產生 嚴重 之影響。	發生資通安全事件致資通系統受影響時， 可能造成未經授權之資訊揭露 ，對機關之營運、資產或信譽等方面將產生 有限 之影響。

SRE The Reliability Engineering **CONFERENCE 2023**

展望 2023 趨勢
踏出 **實踐 SRE** 的第一步
4 月 21 日 | 富邦國際會議中心

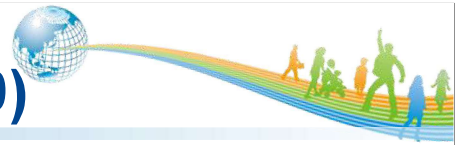
盲鳥優惠 **\$990** 搶先賣！
限時只到 3 月 2 日

立即購票



中華電信
Chunghwa Telecom

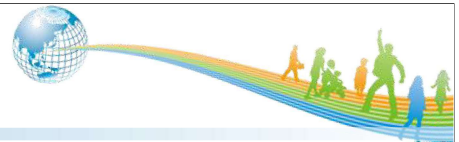
資通系統防護需求分級原則(4/9)



❖ 完整性 (Integrity, !)

防護需求 等級	高	中	普
構面			
完整性	發生資通安全事件致資通系統受影響時， 可能造成資訊錯誤或遭竄改等情事 ，對機關之營運資產或信譽等方面將產生 非常嚴重或災難性 之影響。	發生資通安全事件致資通系統受影響時， 可能造成資訊錯誤或遭竄改等情事 ，對機關之營運資產或信譽等方面將產生 嚴重 之影響	發生資通安全事件致資通系統受影響時， 可能造成資訊錯誤或遭竄改等情事 ，對機關之營運資產或信譽等方面將產生 有限 之影響

資通系統防護需求分級原則(5/9)- 案例(完整性)



iThome 新聞 產品&技術 專題 AI Cloud 醫療IT 資安 研討會 社群 IT EXPLAINED 搜尋

企業加速 綠色轉型 2023 iThome臺灣雲端大會 徵稿起跑！ 搶先報名2023最大規模資安會展

【手冊驗證不足、缺乏全局判斷、無必斷備案的三大教訓】日本KDDI七二大斷訊教訓的3堂課

過去KDDI也曾發生過嚴重通訊故障事故，但跟這次當機事故相比，3天服務中斷，影響數千萬用戶，讓他們徹底體會到，需要重建應變策略來因應這種超大規模又長期的災情

文/ 余至浩 | 2022-09-26 發表 讚 173 分享

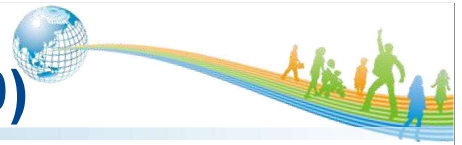


在7月29日事故說明會上，KDDI社長高橋誠偕同技術管理總部本部長吉村和幸，對服務中斷造成的不便公開道歉。(圖片來源 / KDDI)



資料來源：iThome (<https://www.ithome.com.tw/news/153208>)

資通系統防護需求分級原則(6/9)

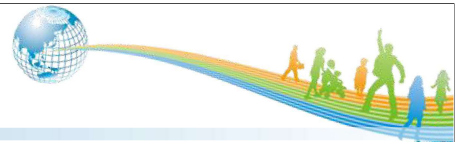


❖ 可用性 (Availability, A)

防護需求 等級	高	中	普
構面	發生資通安全事件致資通系統受影響時， 可能造成對資訊、資通系統之存取或使用之中斷 ，對機關之營運、資產或信譽等方面將產生 非常嚴重或災難性 之影響。	發生資通安全事件致資通系統受影響時， 可能造成對資訊、資通系統之存取或使用之中斷 ，對機關之營運、資產或信譽等方面將產生 嚴重 之影響。	發生資通安全事件致資通系統受影響時， 可能造成對資訊、資通系統之存取或使用之中斷 ，對機關之營運、資產或信譽等方面將產生 有限 之影響。
可用性			

13

資通系統防護需求分級原則(7/9)- 案例(可用性)



【獨家】【公視片庫全刪風暴1】公視片庫遭刪
「7大罪曝光」 高層嫌異地備份太貴釀大禍

文 | 顏凡裴 攝影 | 翁書坤



針對公視新聞「片庫」遭維護廠商刪除的重大缺失，文化部的調查報告，直指公視犯了7大罪，欠缺資安警覺。圖為公視大樓。

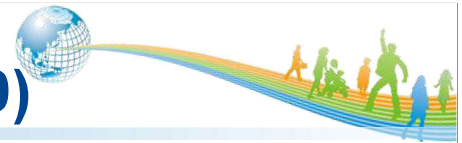
財團法人公共電視新聞「片庫」遭維護廠商刪除，共有約8萬餘筆資料遺失，文化部查出公視共有7大罪，例如經營管理團隊早知片庫未落實執行異地備份，卻因建置費用龐大而未指示立即改善，欠缺資安警覺，內部人員還放任廠商私自安裝遠端工具，廠商甚至未經同意就執行關鍵刪檔指令，因此釀成大禍。



資料來源：鏡週刊
(<https://www.mirrormedia.mg/story/20220424inv001/>)

14

資通系統防護需求分級原則(8/9)

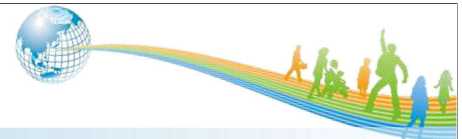


❖ 法律遵循性 (Legality, L)

防護需求 等級	高	中	普
構面			
法律 遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令， 可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令， 可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

15

資通系統防護需求分級原則(9/9)- 案例(法律遵循性)



自由時報
Liberty Times Net

即時 熱門 政治 社會 生活 健康 國際 地方 蒐奇 影音 財經 娛樂 藝文
汽車 時尚 體育 3C 評論 玩咖 食譜 地產 專區 TAIPEI TIMES 求職

懷疑藕斷絲連 移民官濫用職權偷查空姐女友前愛人個資



懲戒法院判李貞降一級改敘。(記者吳政峰攝)

2021/02/12 10:13

【記者吳政峰／台北報導】移民署國境事務大隊桃園機場李姓科員，懷疑空姐女友跟郭姓前男友還有聯絡，竟然用「內政部入出國查驗系統」偷查郭男個資，還傳給女同事看，女同事看完照片，正義感油然而生，通知郭男此事，李員因而被法辦。高等法院日前依洩密罪判李6月刑，懲戒法院再判他降一級改敘。



資料來源：自由時報
(<https://news.ltn.com.tw/news/society/breakingnews/3438718>)

16

資通系統防護基準說明暨 實作案例(含驗證實務)



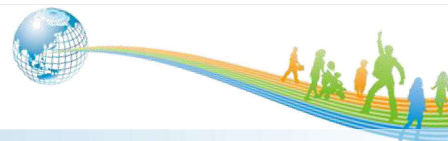
資通系統防護基準(1/42)－

附表十、資通系統防護基準 (110/08/23 修訂重點)



■ 機關應定義各系統之間置時間或可使用期限與資通系統之使用情況及條件。	■ 「稽核」屬名詞者修正為「日誌」。 ■ 「稽核」屬動詞者修正為「記錄」。	■ 於系統發展生命週期之維運階段，應執行版本控制與變更管理。 (須注意 -> 應執行)
■ 應監控遠端存取機關內部網段或資通系統後臺之連線。	■ 訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	■ 加密金鑰或憑證應定期更換。
■ 應採用加密機制。 (普、中、高皆適用)	■ 資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	■ 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 (三次 -> 五次，放寬)
■ 考量備援作法具多元性，爰增訂「其他方式」之規定，以利執行彈性。	■ 系統內部時鐘應定期與基準時間源進行同步。	■ 資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。

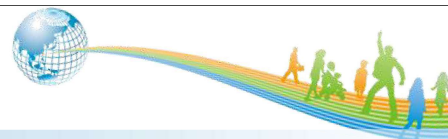
資通系統防護基準(2/42)



❖ 控制措施以「**七構面**」進行資通系統防護考量，共 29 項 控制措施類別

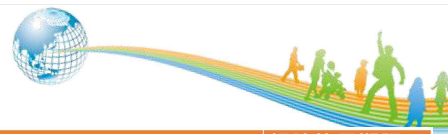
- 存取控制 (3)
- 事件日誌與可歸責性 (6)
- 營運持續計畫 (2)
- 識別與鑑別 (5)
- 系統與服務獲得 (8)
- 系統與通訊保護 (2)
- 系統與資訊完整性 (3)

資通系統防護基準(3/42)



項次	構面	控制措施
1	存取控制	▪ 帳號管理、▪ 最小權限、▪ 遠端存取
2	事件日誌與可歸責性	▪ 記錄事件、▪ 日誌紀錄內容、▪ 日誌儲存容量、 ▪ 日誌處理失效之回應、▪ 時戳及校時、 ▪ 日誌資訊之保護
3	營運持續計畫	▪ 系統備份、▪ 系統備援
4	識別與鑑別	▪ 內部使用者之識別與鑑別、▪ 身分驗證管理、 ▪ 鑑別資訊回饋、▪ 加密模組鑑別、 ▪ 非內部使用者之識別與鑑別
5	系統與服務獲得	▪ 系統發展生命週期 需求 階段、 ▪ 系統發展生命週期 設計 階段、 ▪ 系統發展生命週期 開發 階段、 ▪ 系統發展生命週期 測試 階段、 ▪ 系統發展生命週期 部署與維運 階段、 ▪ 系統發展生命週期 委外 階段、 ▪ 獲得程序、▪ 系統文件
6	系統與通訊保護	▪ 傳輸之機密性與完整性、▪ 資料儲存之安全
7	系統與資訊完整性	▪ 漏洞修復、▪ 資通系統監控、▪ 軟體及資訊完整性

資通系統防護基準(4/42)



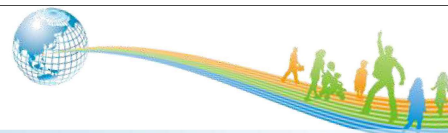
❖ 存取控制 (3)

類別	範例	帳號使用期限
臨時	開發人員帳號、測試人員帳號	30天
緊急	備援、移機用途帳號	1天
閒置	超過一定期間未有登入紀錄之帳號	90天 (Default)

系統防護需求 分級		高	中	普
控制措施 構面	措施內容			
存取控制	帳號管理	一 <u>機關應定義各系統之間置時間或可使用期限與資通系統之使用情況及條件。</u> 二 逾越機關所<u>許可</u>之間置時間或可使用期限時，系統應自動將使用者登出。 三 應依機關規定之情況及條件，使用資通系統。 四 監控資通系統帳號，如發現帳號<u>違常</u>使用時回報管理者。 五 等級「中」之所有控制措施。	一 <u>已逾期之臨時或緊急帳號</u>應刪除或禁用。 二 資通系統<u>閒置帳號</u>應禁用。 三 <u>定期審核</u>資通系統帳號之申請、建立、修改、啟用、停用及刪除。 四 等級「普」之所有控制措施。	建立帳號管理機制，包含<u>帳號之申請、建立、修改、啟用、停用及刪除</u>之程序。

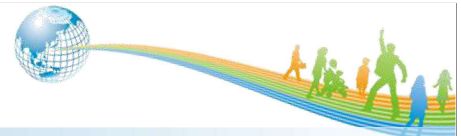
21

資通系統防護基準(5/42)－ 驗證實務



控制措施	建立帳號管理機制，包含帳號之 <u>申請、建立、修改、啟用、停用及刪除</u> 之程序
適用等級	普、中、高
內容說明	- 須建立資通系統帳號管理機制，以適切管理資通系統使用者帳號、後臺主機作業系統帳號及資料庫管理者帳號等。 - 內部使用者使用資通系統應符合機關訂定之帳號管理程序，包含帳號之申請、建立、修改、啟用、停用及刪除等作業規範並落實執行。除因緊急需求外，<u>原則上所有帳號異動不可由系統管理者任意調整異動</u>，宜由相關權責人員提出異動申請，並通過審核程序後始可進行異動作業。而帳號異動流程，一般可透過紙本或電子化系統完成，填寫相關表單(如：系統帳號/權限異動申請單等)。
系統人員	
驗證實務	- 如未建立帳號管理機制，或是雖訂定帳號管理規範卻未落實執行，則未符合此項控制措施。 - 驗證人員宜檢視機關實作之帳號管理機制，如使用電子化或紙本流程，並可檢閱機關訂定之帳號管理文件化規範，檢查是否在現有帳號管理機制中，已包含帳號申請、建立、修改、啟用、停用及刪除等各種帳號異動程序相關要求，以提供系統管理者與一般使用者進行帳號申請及異動之作業依據。 - 驗證人員宜檢視機關帳號管理規範之落實情形，此時可<u>抽查既有帳號之申請、建立、修改、啟用、停用及刪除等帳號異動相關紀錄</u>(可能透過電子化系統或是紙本表單等形式)，從中查找帳號違規使用情形。 - 驗證情境如驗證人員抽查資通系統中近期新建之內部使用者帳號(如系統管理者等)，檢閱其申請與審核相關紀錄，以確認是否為<u>未經核可卻私自建立或啟用之帳號</u>。同時，驗證人員亦可抽查系統是否仍留存應依程序完成停用或刪除作業卻仍繼續使用之帳號，<u>如已逾期之臨時帳號、緊急帳號及閒置帳號等</u>。
稽核人員	
佐證資料	- 機關訂定之資通系統帳號管理規範 - 資通系統帳號申請異動單(如<u>帳號權限申請表</u>、<u>使用者帳號異動申請單</u>等) - 系統線上帳號權限申請或異動紀錄

資通系統防護基準(6/42)－ 驗證實務



控制措施 定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除

適用等級 中、高

內容說明

- 應定期(如每季等)透過系統帳號清查活動，以審核帳號之申請、建立、修改、啟用、停用及刪除等相關紀錄，以發現未經授權之帳號變更行為。
- 帳號審核範圍，宜包含系統管理者帳號、後臺主機作業系統帳號及資料庫管理者帳號等，亦可評估實際執行需求，納入機關內部及外部一般使用者帳號，並應依機關規定清查應禁用或刪除之帳號，如臨時帳號、緊急帳號及閒置帳號等。系統帳號清查紀錄範例：

	A	B	C	D	E	F	G
1	範例系統-AP帳號權限審查紀錄						
2	系統名稱：範例系統						
3	OS管理員：王小明						
審查日期：000年00月00日 資通系統名稱：00000系統							
帳號	角色/權限	狀態(未啟用/使用中/停用)	最後一次登入系統時間	單位	姓名	帳號擁有者簽認	
審核人員及主管簽核：							

驗證實務 (略)

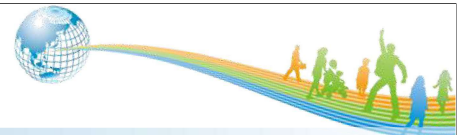
佐證資料

- 機關訂定之資通系統帳號管理程序
- 資通系統帳號申請異動單
- 資通系統帳號清查紀錄

資料來源：資通系統防護基準驗證實務(V1.1)

23

資通系統防護基準(7/42)－ 驗證實務



控制措施

- 一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。
- 三、應依機關規定之情況及條件，使用資通系統。
- 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。

適用等級 高

內容說明

- 資通系統之使用情況及條件，常見設計方向如下：
 - 時間(不允許非上班時間)
 - IP位址(限制白名單 IP / Intranet / VPN)
 - 裝置(裝置 MAC Address / 限制特定的作業系統 / 瀏覽器)
- 「違常使用」常見範例：
 - 時間、位址、裝置、行為(無效、大量上傳下載、觸發特定的 Http Status Code)
- 「回報管理者」常見方法：
 - 電子郵件、SMS、社群訊息

驗證實務

- (前略)
- 驗證人員可評估發展測試案例，以驗證這些條件限制是否確實有效。例如，若資通系統僅允許機關內部網路進行存取，驗證人員可測試使用外部網路能否連線登入系統。或可從系統日誌中檢視使用行為紀錄，查找違規使用行為，包含登入未經申請核可之帳號、從非許可網路來源或時段登入，以及違規之遠端存取行為等

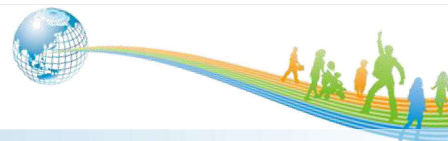
佐證資料

- 機關訂定之資通系統發展維護辦法
- 資通系統帳號清查紀錄
- 監控防護相關紀錄，如SOC維運紀錄、WAF日誌等
- 資通系統日誌

資料來源：資通系統防護基準驗證實務(V1.1)

24

資通系統防護基準(8/42)

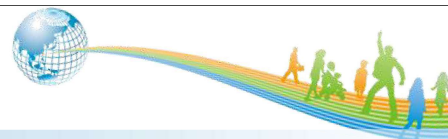


❖ 存取控制 (3)

系統防護需求 分級		高	中	普
控制措施	構面	措施內容		
存取控制	最小權限	採 最小權限原則 ，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		
	遠端存取	一 遠端存取之來源應為機關 已預先定義及管理之存取控制點 。 二 等級「普」之所有控制措施。 一 對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及 文件化 。 二 使用者之權限檢查作業應於 伺服器端 完成。 三 <u>應監控遠端存取機關內部網段或資通系統後臺之連線。</u> 四 <u>應採用加密機制。</u>		

25

資通系統防護基準(9/42)－ 驗證實務



控制措施	採 最小權限原則 ，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取		
適用等級	中、高		
內容說明	(前略) - 資通系統應具備存取控制安全機制，採用最小權限之設計原則，機關可以考慮增設程序、使用者角色及系統帳號，並透過服務組態參數與存取控制列表等方式設定授權存取以實現最小權限。最小權限原則設計示意圖如下：		
驗證實務	(前略) - 資通系統原則上應區分一般業務使用之權限與系統管理維護之權限，僅允許特權帳號存取系統管理維護相關功能頁面。驗證人員可評估發展測試案例，如利用一般業務使用之測試帳號，試圖存取系統管理維護網址及功能，系統應禁止存取該功能頁面。		
佐證資料	- 機關訂定之資通系統發展維護辦法 - 資通系統存取控制功能之測試紀錄		

資通系統防護基準(10/42)－ 驗證實務

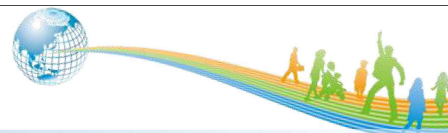


控制措施	使用者之權限檢查作業應於 伺服器端 完成
適用等級	普、中、高
內容說明	資通系統應檢查使用者存取權限，禁止未經系統授權存取行為；惟若系統將權限檢查作業實作於使用者端(如JavaScript、Mobile App等)則可視為無效，因其可能被惡意使用者利用竄改網站Cookies內容或網路封包內容等手法繞過檢查機制，故資通系統應於伺服器端實作授權檢查。
驗證實務	(前略) - 欲驗證授權檢查之實作方式，驗證人員亦可評估發展測試案例，建置OWASP Zed Attack Proxy (ZAP)或Burp Suite等代理伺服器(Proxy)，模擬惡意攻擊者攻擊手法以繞過客戶端之授權檢查。測試情境示意圖：  - 原理： - 利用一般業務使用之測試帳號，試圖存取系統管理功能頁面。 - 透過Proxy竄改網路封包內所攔截之授權資訊，對伺服器進行提權攻擊。常用手法如檢視是否存在「role」、「user」及「admin」等常用來記錄使用者身分之參數，例如將「role=user」竄改為「role=admin」，以將一般使用者權限提升至系統管理者權限。

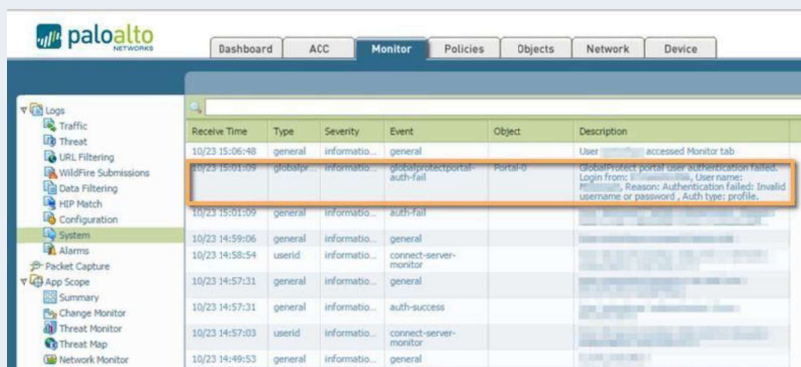
資料來源：資通系統防護基準驗證實務(V1.1)

27

資通系統防護基準(11/42)－ 驗證實務



控制措施	應 監控遠端 存取 機關內部網段或資通系統後臺 之連線
適用等級	普、中、高
內容說明	機關可能因使用需求，而允許機關內部使用者(如外點單位、居家辦公等)或廠商自遠端來源存取機關內部網段或資通系統後臺，以進行系統管理維護作業。實務上常透過VPN建立安全通道，以保護連線過程之機密性與完整性，惟此種遠端連線行為因具備高度資安風險，很可能被惡意攻擊者利用作為系統入侵管道，故機關宜使用網路安全監控設備(如Firewall、WAF及IPS/IDS等)或服務(如SOC監控等)，監控遠端存取機關內部網段或資通系統後臺之連線，以及時發現異常連線或惡意攻擊行為。監控資通系統後臺範例，詳見下圖：
驗證實務	(略)
佐證資料	- 機關訂定之系統監控程序 系統監控紀錄



Receive Time	Type	Severity	Event	Object	Description
10/23 15:06:48	general	informational	general		User [redacted] accessed Monitor tab
10/23 15:01:09	globallog	informational	globalprotectportal-auth-fail	Portal-0	GlobalProtect portal user authentication failed. Login from: [redacted], User name: [redacted], Reason: Authentication failed: Invalid username or password, Auth type: profile
10/23 15:01:09	general	informational	auth-fail		
10/23 14:59:06	general	informational	general		
10/23 14:58:54	userid	informational	connect-server-monitor		
10/23 14:57:31	general	informational	general		
10/23 14:57:31	general	informational	auth-success		
10/23 14:57:03	userid	informational	connect-server-monitor		
10/23 14:49:53	general	informational	general		

資料來源：資通系統防護基準驗證實務(V1.1)

28

資通系統防護基準(12/42)－ 驗證實務



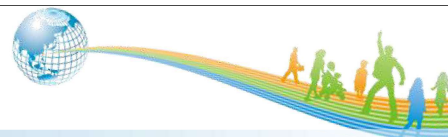
控制措施	應採用 <u>加密機制</u>
適用等級	普、中、高
內容說明	- 為保護遠端存取連線之機密性與完整性，應採用如啟用HTTPS TLS 1.2加密傳輸或系統維護人員遠端存取內部系統時，可限制遠端來源以降低存取風險。 - 如資通系統允許管理人員透過遠端桌面服務入侵之機率，亦應強化為：「電腦設定\系統管理範本\需要安全的RPC通訊」。



資料來源：資通系統防護基準驗證實務(V1.1)

29

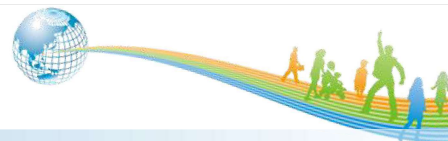
資通系統防護基準(13/42)



❖ 事件日誌與可歸責性 (6)

系統防護需求 分級		高	中	普
控制措施	措施內容			
事件日誌與可歸責性	記錄事件	一 應 定期審查 機關所保留資通系統產生之日誌。 二 等級「普」之所有控制措施。		一 訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二 確保資通系統有記錄特定事件之功能，並 決定應記錄之特定資通系統事件 。 三 應記錄資通系統 管理者帳號 所執行之 各項功能 。
	日誌紀錄內容	資通系統產生之日誌應包含 事件類型 、 發生時間 、 發生位置 及 任何與事件相關之使用者身分識別 等資訊，並採用單一日誌機制，確保輸出格式的一致性，並應依資通安全政策及法規要求納入其他相關資訊。		

資通系統防護基準(14/42)

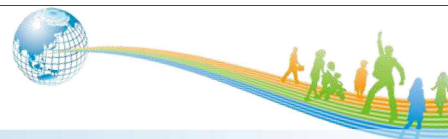


❖ 事件日誌與可歸責性(6)

系統防護需求 分級		高	中	普
控制措施	構面	措施內容		
事件日誌與可歸責性	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。 (Tips：可利用 <u>單週</u> 或 <u>單月</u> 日誌量進行推估，保留6個月的日誌容量。)		
	日誌處理失效之回應	一 機關規定需要即時通報之 <u>日誌處理失效事件發生</u> 時，資通系統應於機關規定之 <u>時效內</u> ，對 <u>特定人員</u> 提出警告。 二 等級「中」及「普」之所有控制措施。	資通系統於日誌處理失效時，應採取適當之行動。	

31

資通系統防護基準(15/42)



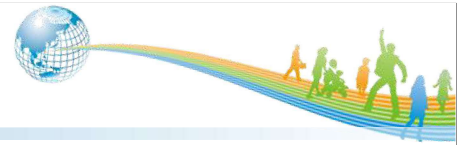
❖ 事件日誌與可歸責性(6)

系統防護需求 分級		高	中	普
控制措施	構面	措施內容		
事件日誌與可歸責性	時戳及校時	一 系統內部時鐘應 <u>定期</u> 與 <u>基準時間源</u> 進行同步。 二 等級「普」之所有控制措施。		資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
	日誌資訊 →保護	一 <u>定期備份</u> 日誌至 <u>原系統外之其他實體系統</u> 。	一 應運用 <u>雜湊</u> 或 <u>其他適當</u> 方式之完整性確保機制。	對 <u>日誌之存取管理</u> ，僅限於有權限之使用

提醒：含有機敏性資料之日誌應以「加密」進行日誌備份檔案之儲存及傳輸。

32

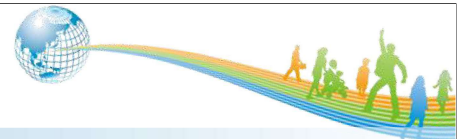
資通系統防護基準(16/42) - 日誌留存面向-1



❖ **資通系統(含資料庫)** (依「資通安全責任等級分級辦法」之「附表九、資通系統防護需求分級原則」識別重要性)

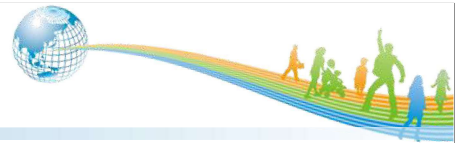
- 何謂「重要」？
 - 優先順序：高 > 中 > 普
- 留哪些？(人、事、時、地、物)
 - **OS層**：登入出帳號、時間及操作行為，及SA各項操作
 - **AP層**：Application Server 及 應用程式本身
 - 前端：使用者登入出帳號、時間及操作行為
 - 管理後端：後端管理介面之登入出帳號、時間及操作行為(如：帳號異動)，且管理者帳號之各項操作皆應留存日誌
 - **DB層**：DB 特殊權限(DCL/DDI等)、DBA 各項操作等
- 留多久？(至少六個月)

資通系統防護基準(17/42) - 日誌留存面向-2



控制措施	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		
適用等級	普、中、高		
內容說明	• 應訂定相關管理辦法以妥善留存資通系統日誌，如作業系統日誌(OS event log)、網站日誌(Web log)、應用程式日誌(AP log)及登入日誌(logon log)等，以符合程式除錯、行為歸責、稽核取證及法律規範等用途。資通系統日誌留存期限應至少保留6個月。 • 依據「各機關資通安全事件通報及應變處理作業程序」之規定，各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌，並定期備份於外部設備，其保存範圍及項目詳見下表。		
	資通安全 責任等級	保存範圍	保存項目
	A	機關應保存 全部 資通系統與 各項 資通及防護設備最近六個月之日誌紀錄。	1. 作業系統日誌 (OS event log) 2. 網站日誌 (web log)
	B	機關應保存 全部 核心資通系統與 相連之 資通及防護設備最近六個月之日誌紀錄。	3. 應用程式日誌 (AP log)
	C	機關應保存 全部 核心資通系統最近六個月之日誌紀錄。	4. 登入日誌 (logon log)
驗證實務	• (略)		
佐證資料	• 機關訂定之日誌相關管理辦法 • 資通系統日誌		

資通系統防護基準(18/42) - 日誌記錄特定資通系統事件範例



- ❖ 實務上建議可包含(但不限於)以下系統事件：
 - 管理者行為(如調整系統組態、異動系統帳號等)
 - 身分驗證失敗(如帳號登入失敗、觸發帳戶鎖定等)
 - 存取資源失敗(如頁面失效、資料庫連線失敗等)
 - 功能錯誤(如系統功能無法使用、帳戶無法登入等)
 - 重要資料異動(如存取個人資料或機敏資訊等)
 - 重要操作行為(如變更個人密碼、金融轉帳交易等)

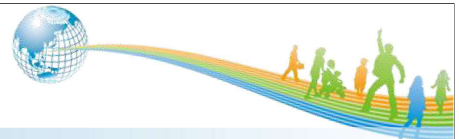
- ❖ 管理者帳號功能執行紀錄，建議至少可抽查以下項目：
 - 管理者帳號登入與登出
 - 管理者帳號密碼變更
 - 異動使用者帳號密碼、鎖定狀態及存取權限等
 - 異動系統重要功能組態
 - 存取機敏資訊，如使用者個人資料、帳戶資訊等

資料來源：資通系統防護基準驗證實務(V1.1)

35



資通系統防護基準(19/42) - 日誌紀錄的Sample Code範例



- ❖ <Web應用程式安全參考指引>建議如何使用 NLog 進行日誌紀錄的 Sample Code：

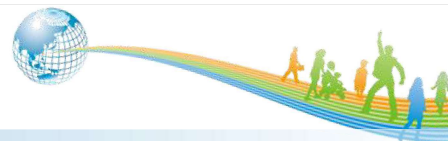
```
NLog.Logger logger = NLog.LogManager.GetCurrentClassLogger();
if (UserLogin(this.TextBoxAccount.Text, this.TextBoxPassword.Text)){
    logger.Info(TextBoxAccount.Text + "登入成功!!");
}
else{
    logger.Warn(TextBoxAccount.Text + "登入失敗!!");
}
```

資料來源：Web應用程式安全參考指引(修訂)v2.1

36



資通系統防護基準(20/42)

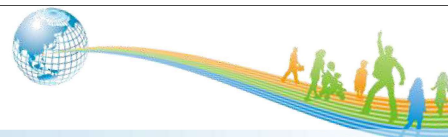


❖ 營運持續計畫 (2)

系統防護需求 分級		高	中	普
控制措施	構面	措施內容		
營運 持續 計畫	系統備份	一 應將備份還原，作為營運持續計畫測試之一部分。 二 應在與運作系統 不同地點之獨立設施 或 防火櫃 中，儲存重要資通系統軟體與其他安全相關資訊之備份 三 等級「中」之所有控制措施。	一 應 定期測試備份資訊 ，以驗證備份媒體之可靠性及資訊之完整性。 二 等級「普」之所有控制措施。	一 訂定系統 可容忍資料損失之時間(RPO) 要求。 二 執行 系統源碼與資料備份 。
	系統備援	一 訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二 原服務中斷時，於可容忍時間內，由備援設備 或其他方式 取代並提供服務。		無要求。

37

資通系統防護基準(21/42) - 驗證實務



控制措施	執行系統源碼與資料備份																																				
適用等級	普、中、高																																				
內容說明	- 資通系統應依機關資安政策及規範進行系統源碼(含原始程式碼、目的程式(Object Code)等)或資料(如系統業務資料等)備份作業。套裝軟體、租賃系統，或因合約特別規定允許委外廠商可不提供系統源碼者，不在此限。可建立集中式存放空間，以方便管理保存，備份實作範例如下。 本機 > [redacted] > 遠端管理 > 範例系統 > <table><thead><tr><th>名稱</th><th>修改日期</th><th>類型</th><th>大小</th></tr></thead><tbody><tr><td>系統文件</td><td>2021/6/30 下午 0...</td><td>檔案資料夾</td><td></td></tr><tr><td>原始碼</td><td>2013/6/8 下午 07...</td><td>檔案資料夾</td><td></td></tr><tr><td>管理紀錄</td><td>2013/6/8 下午 07...</td><td>檔案資料夾</td><td></td></tr><tr><td>營運通式單</td><td>2013/11/16 下午 ...</td><td>檔案資料夾</td><td></td></tr><tr><td>Windows Server 2019安裝-2019-12-25...</td><td>2019/12/25 上午 ...</td><td>Microsoft Word ...</td><td>1,285 KB</td></tr><tr><td>系統開發SOP_範例系統</td><td>2019/1/16 下午 0...</td><td>Microsoft Excel ...</td><td>23 KB</td></tr><tr><td>系統資訊_範例系統-2018-12-18</td><td>2019/12/18 下午 ...</td><td>Microsoft Excel ...</td><td>20 KB</td></tr><tr><td>系統資訊_範例系統-2019-12-26</td><td>2019/12/26 上午 ...</td><td>Microsoft Excel ...</td><td>28 KB</td></tr></tbody></table> (略) 系統源碼之版本控制與變更管理，以機關自行維護為原則，不宜全委由廠商負責變更管理作業。機關至少應留存系統源碼備份，避免委外廠商因故倒閉或更換後，無法再行還原系統源碼情形。	名稱	修改日期	類型	大小	系統文件	2021/6/30 下午 0...	檔案資料夾		原始碼	2013/6/8 下午 07...	檔案資料夾		管理紀錄	2013/6/8 下午 07...	檔案資料夾		營運通式單	2013/11/16 下午 ...	檔案資料夾		Windows Server 2019安裝-2019-12-25...	2019/12/25 上午 ...	Microsoft Word ...	1,285 KB	系統開發SOP_範例系統	2019/1/16 下午 0...	Microsoft Excel ...	23 KB	系統資訊_範例系統-2018-12-18	2019/12/18 下午 ...	Microsoft Excel ...	20 KB	系統資訊_範例系統-2019-12-26	2019/12/26 上午 ...	Microsoft Excel ...	28 KB
名稱	修改日期	類型	大小																																		
系統文件	2021/6/30 下午 0...	檔案資料夾																																			
原始碼	2013/6/8 下午 07...	檔案資料夾																																			
管理紀錄	2013/6/8 下午 07...	檔案資料夾																																			
營運通式單	2013/11/16 下午 ...	檔案資料夾																																			
Windows Server 2019安裝-2019-12-25...	2019/12/25 上午 ...	Microsoft Word ...	1,285 KB																																		
系統開發SOP_範例系統	2019/1/16 下午 0...	Microsoft Excel ...	23 KB																																		
系統資訊_範例系統-2018-12-18	2019/12/18 下午 ...	Microsoft Excel ...	20 KB																																		
系統資訊_範例系統-2019-12-26	2019/12/26 上午 ...	Microsoft Excel ...	28 KB																																		
驗證實務	(略) - 驗證人員宜檢視資通系統源碼備份結果，機關至少應留存1份最新之系統源碼備份，不可全數交由廠商管理保存。 - 驗證人員宜檢視資通系統資料備份結果，如依機關訂定之復原點目標(RPO)要求定期執行備份作業。																																				

資通系統防護基準(22/42) - 營運持續計畫-1

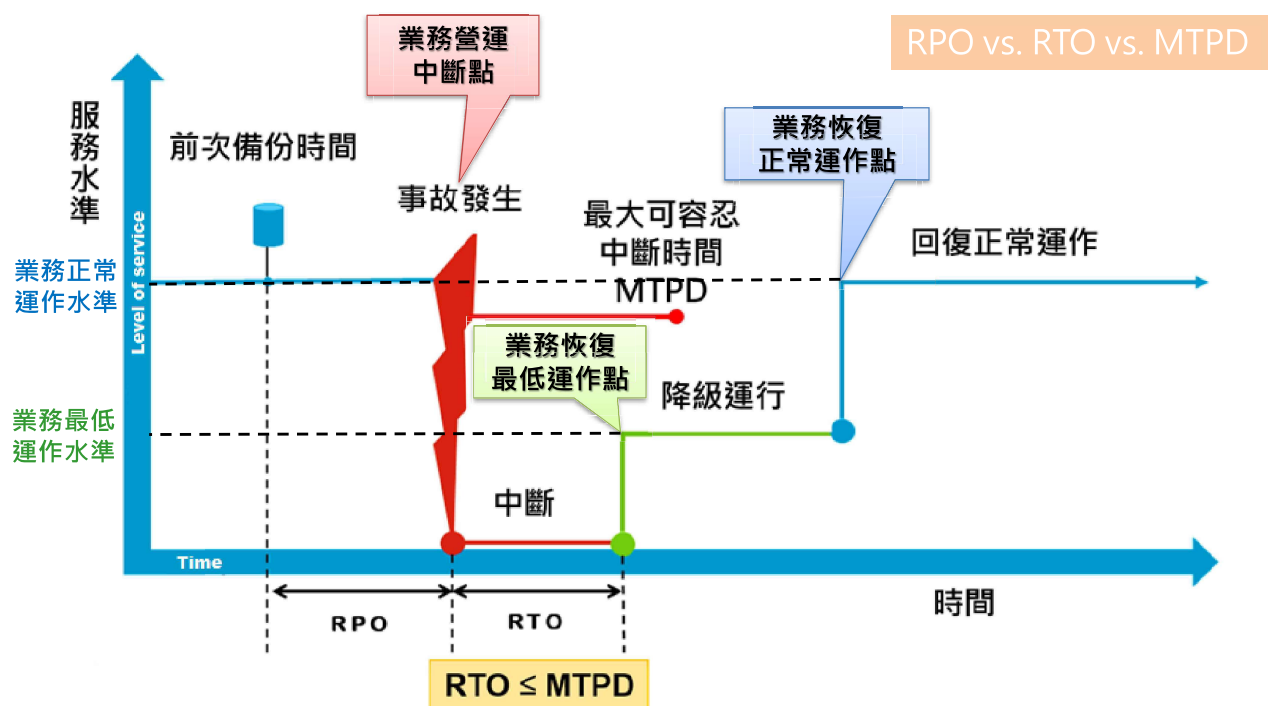
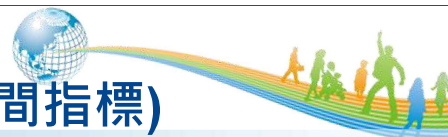


❖ 營運持續管理(BCM)概論

- 系統從中斷後至重新恢復服務之可容忍時間 → 最大可容忍中斷時間 (Maximum Tolerable Period of Disruption, MTPD)
- 服務中斷時，於可容忍時間內，由備援設備取代提供服務之時間 → 復原時間目標 (Recovery Time Objective, RTO)
- 系統可容忍資料損失之時間 → 資料復原點 (Recovery Point Objective, RPO)

39

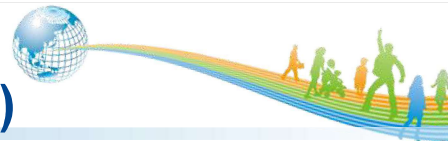
資通系統防護基準(23/42) - 營運持續計畫-2 (BCM的3個重要時間指標)



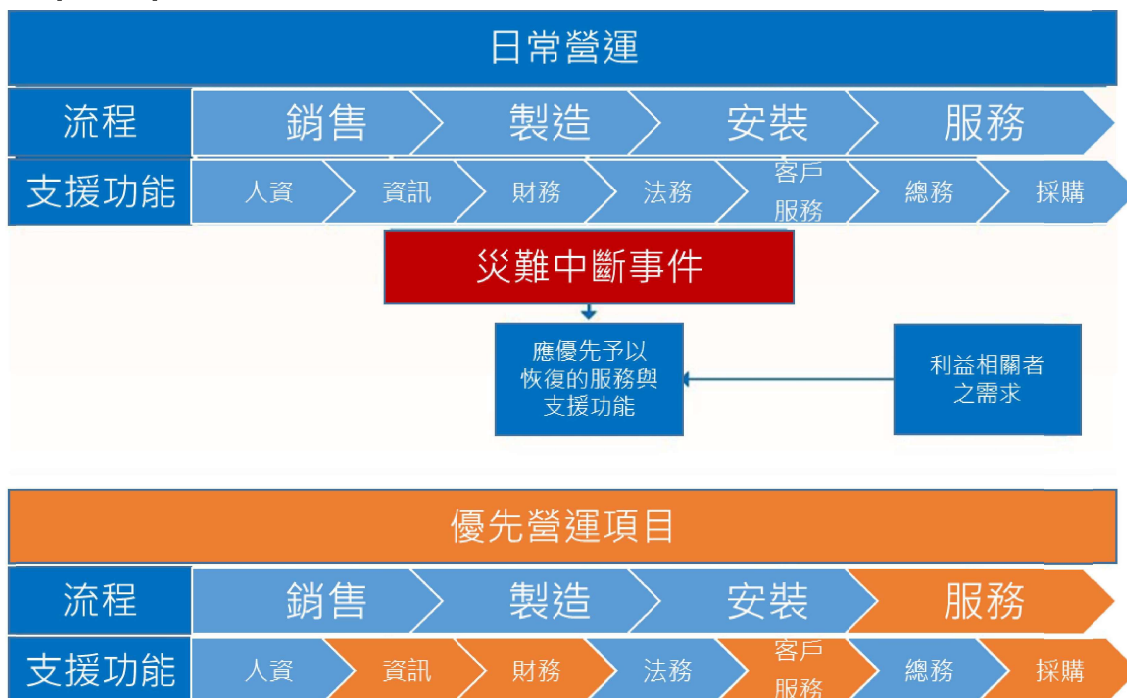
思考營運持續管理措施要從 "worst case" 出發，
如此才會充分考量到中斷事故所帶來之最大損害。

40

資通系統防護基準(24/42) - 營運持續計畫-3 (業務最低運作水準)

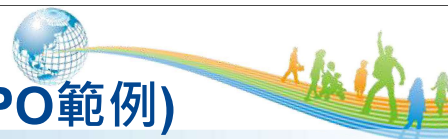


❖ (範例)



41

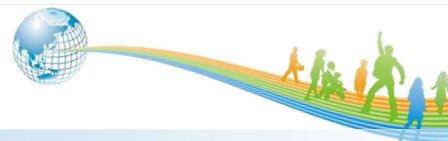
資通系統防護基準(25/42) - 營運持續計畫-4 (MTPD、RTO及RPO範例)



關鍵次序	業務服務	復原時間目標 RTO (hrs)	最大可容忍中斷時間 MTPD (hrs)	復原時點目標 RPO (hrs)
1.	電力、空調、消防設施	0.5	0.5	NA
2.	重要網路、資安服務	6	8	24
	資料庫、AD	6	8	24
3.	SSO (single sign on)	6	8	24
	高級 資通系統	6	8	24
4.	報表產製列印服務	7	8	24
5.	中級 資通系統	12	16	24
6.	普級 資通系統	20	24	24

42

資通系統防護基準(26/42)

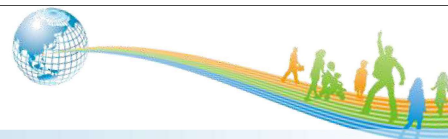


❖ 識別與鑑別 (5)

系統防護需求 分級		高	中	普
控制措施				
構面	措施內容			
識別與鑑別	內部使用者之識別與鑑別	一 對資通系統之存取採取 <u>多重認證技術</u> 。 二 等級「中」及「普」之所有控制措施。		

資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。

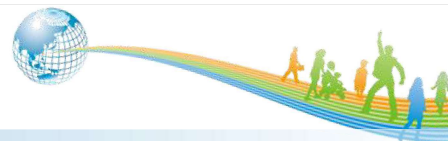
資通系統防護基準(27/42)



❖ 識別與鑑別 (5)

系統防護需求 分級		高	中	普
控制措施				
構面	措施內容			
識別與鑑別	身分驗證管理	一 身分驗證機制應防範 <u>自動化程式之登入或密碼更換嘗試</u> 。 二 密碼重設機制對使用者重新身分確認後，發送 <u>一次性及具有時效性</u> 符記。 三 等級「普」之所有控制措施。		

資通系統防護基準(28/42)

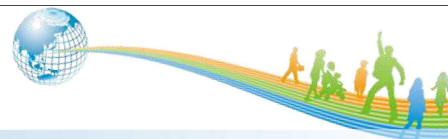


❖ 識別與鑑別 (5)

系統防護需求 分級		高	中	普
控制措施 構面	措施內容			
識別 與鑑別	鑑別資訊 回饋	資通系統應遮蔽鑑別過程中之資訊。		
	加密模組 鑑別	資通系統如以密碼進行鑑別時，該密碼應 加密或經雜湊處理後儲存 。		無要求。
	非內部使 用者之識 別與鑑別	資通系統應識別及鑑別 非機關使用者 (或代表機關使用者行為之程序)。		

45

資通系統防護基準(29/42) - 驗證實務-內部使用者之識別與鑑別



控制措施	資通系統應具備唯一識別及鑑別使用者(或代表使用者行為之程序)之功能， 禁止使用共用帳號
適用等級	普、中、高
內容說明	- 資通系統應具有身分驗證機制，內部使用者如系統管理人者與其他雇員，亦包含臨時人員、駐點廠商及工讀人員等所有可能之資通系統使用者。除允許匿名存取之功能頁面外，資通系統應利用身分驗證(如帳號密碼或自然人憑證等)機制識別內部使用者(或代表使用者行為之程序)。 - 共用帳號行為可能出現在系統特權帳號或業務使用帳號，為提高可歸責性，應避免使用共用帳號。資通系統帳號僅提供已取得授權人員使用，並以開立個人帳號為原則，除非有特殊使用需求另行規定外，不應製發匿名或多人共用帳號。
驗證實務	(略) - 驗證人員宜檢視資通系統日誌，查找是否存在共用帳號之行為。例如，若日誌顯示某使用者帳號登入來源包含3個網路位址，而這3個位址卻分別屬於3位不同業務使用者所擁有，故可能存在共用帳號行為，惟驗證人員仍須進一步透過訪談等方式進行確認。
佐證資料	- 機關訂定之系統發展維護辦法 - 資通系統功能規格書 - 資通系統身分驗證功能測試紀錄 資通系統日誌

實務分享：

Q1. 老舊設備或軟硬體，只能有一組「管理帳號」？

Q2. 以「**帳號數目**」計價的軟體？

資通系統防護基準(30/42) - 驗證實務-多重認證技術

控制措施	對資通系統之存取採取多重認證技術
適用等級	高
內容說明	- 內部使用者存取高等級資通系統應用服務時應採取多重認證技術，使用情境如系統管理者登入系統後臺管理功能頁面進行系統維護。 - 多重認證技術係指採用<u>兩種(含)以上</u>不同身分驗證因子(MFA, Multi-Factor Authentication)。 - Something you know (所知之事)：密碼、PIN Code - Something you have (所持之物)：憑證、晶片卡、SMS簡訊驗證碼及一次性密碼(OTP) - Something you are (所具之形)：臉部、指紋、聲紋、虹膜
驗證實務 (常見缺失)	(前略)惟若同時多次使用<u>同一種類型</u>之身分驗證因子，如同時使用密碼與安全問答作為驗證關卡，並<u>不符合</u>多重認證技術之精神。 - Captcha 圖形驗證碼 作用僅為辨別人為或自動化程式之操作行為，<u>不可</u>視為身分驗證因子之一。 - 驗證人員宜檢視資通系統多重認證技術是否為全面性適用，包含所有內部使用者或登入方式。例如，若資通系統允許使用者利用自然人憑證或是帳號密碼擇一方式進行登入，雖自然人憑證符合多重認證技術，惟若允許使用者僅以帳號密碼即完成登入，則仍<u>未完全符合</u>此項控制措施要求。 - 資通系統如將網路位址(如IP或MAC等)作為身分驗證因子之一，則應可識別其為特定使用者之專屬設備，始符合「所有之物」之定義，惟建議仍需仔細評估偽冒網路位址之風險。
佐證資料	- 機關訂定之系統發展維護辦法 - 資通系統功能規格書 - 資通系統身分驗證功能測試紀錄

身分驗證

驗證方式：自然人憑證

讀卡機狀態

身分證統一編號

PIN碼

讀卡成功!

身分證統一編號

如何取得自然人憑證?

忘記 PIN 碼怎麼辦?

重新檢測

執行身分驗證

資料來源：資通系統防護基準驗證實務(V1.1)

47

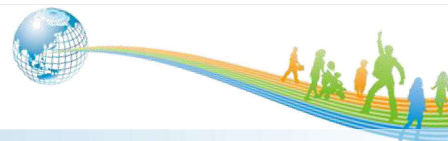
資通系統防護基準(31/42)

❖ 系統與服務獲得 (8)

系統防護需求分級		高	中	普
控制措施	措施內容			
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求 (含機密性、可用性、完整性) 進行確認。		
	系統發展生命週期設計階段	一 根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二 將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		無要求。

48

資通系統防護基準(32/42)



❖ 系統與服務獲得 (8)

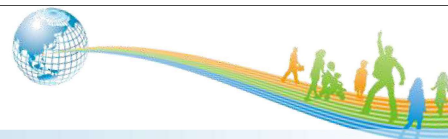
系統防護需求 分級		高	中	普
控制措施	措施內容			
系統 與服 務	系統發展 生命週期 開發階段	一 執行「 源碼掃描 」安全檢測。 二 系統應具備發生嚴重錯誤時之 通知機制 。 三 等級「中」及「普」	一 應針對安全需求實作必要控制措施。 二 應注意避免軟體常見漏洞及實作必要控制措施 。 三 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細	

實作分享：(「**上傳檔案**」之檢查管控建議)

1. 限制上傳檔案格式及大小。
2. 檢查上傳檔案格式及內容。(於 Client 端及 Server 端都要檢查)
3. 檔案上傳前於 Server 端進行病毒掃描，如發現異常，直接拒絕上傳檔案。(留存**掃毒異常之紀錄**，包含時間、檔名及其掃描結果等。)
4. 上傳目的資料夾，**停用「執行程式」之權限**。
5. 定期掃描上傳目的資料夾內的檔案。(或搭配**檔案清洗機制**)

49

資通系統防護基準(33/42)



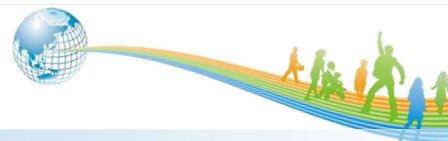
❖ 系統與服務獲得 (8)

系統防護需求 分級		高	中	普
控制措施	措施內容			
系統 與服 務獲 得	系統發展 生命週期 部署與維 運階段	一 於系統發展生命週期之維運階段， 應執行 版本控制與變更管理。 二 等級「普」之所有控制措施。		一 於部署環境中應針對相關資通安全威脅，進行更新與修補，並 關閉不必要服務及埠口 。 二 資通系統 不使用 預設密碼。
	系統發展			

實作分享：委外辦理資通系統之建置、維運或資通服務提供時，應依專案性質遵循「**資通系統籌獲各階段資安強化措施**」需求、**建置及維運各階段要求**。

50

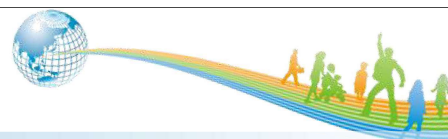
資通系統防護基準(34/42)



❖ 系統與服務獲得 (8)

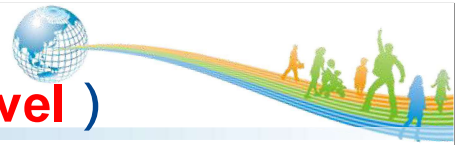
系統防護需求 分級		高	中	普
控制措施 構面	措施內容			
系統 與服 務獲 得	獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
	系統文件	應儲存與管理系統發展生命週期之相關文件。		

資通系統防護基準(35/42) - (OWASP Top 10 2017 vs. 2021)



排名	風險(中文名稱)	風險(英文名稱)
A1	權限控制失效	Broken Access Control
A2	加密機制失效	Cryptographic Failures
A3	注入式攻擊	Injection
A4	不安全設計 (NEW)	Insecure Design
A5	安全設定缺陷	Security Misconfiguration
A6	危險或過舊的元件	Vulnerable and Outdated Components
A7	認證與驗證機制失效	Identification and Authentication Failures
A8	軟體與資料完整性失效 (NEW)	Software and Data Integrity Failures
A9	資安記錄及監控失效	Security Logging and Monitoring Failures
A10	伺服器端請求偽造 (NEW)	Server-Side Request Forgery

資通系統防護基準(36/42) - (OWASP Top 10 2021 Threat Level)



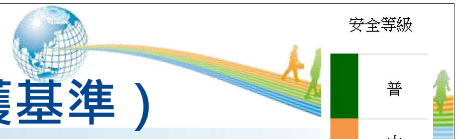
排名	風險名稱	可對照CWEs數量	最大發生率	平均發生率	最大覆蓋範圍	平均覆蓋範圍	平均加權漏洞	平均加權影響	出現次數	所有相關CVEs數量
A1	Broken Access Control (權限控制失效)	34	55.97%	3.81%	94.55%	47.72%	6.92	5.93	318,487	19,013
A2	Cryptographic Failures (加密機制失效)	29	46.44%	4.49%	79.33%	34.85%	7.29	6.81	233,788	3,075
A3	Injection (注入式攻擊)	33	19.09%	3.37%	94.04%	47.90%	7.25	7.15	274,228	32,078
A4	Insecure Design (不安全設計)	40	24.19%	3.00%	77.25%	42.51%	6.46	6.78	262,407	2,691
A5	Security Misconfiguration (安全設定缺陷)	20	19.84%	4.51%	89.58%	44.84%	8.12	6.56	208,387	789
A6	Vulnerable and Outdated Components (危險或過舊的元件)	3	27.96%	8.77%	51.78%	22.47%	5.00	5.00	30,457	0
A7	Identification and Authentication Failures (認證與驗證機制失效)	22	14.84%	2.55%	79.51%	45.72%	7.40	6.50	132,195	3,897
A8	Software and Data Integrity Failures (軟體與資料完整性失效)	10	16.67%	2.05%	75.04%	45.35%	6.94	7.94	47,972	1,152
A9	Security Logging and Monitoring Failures (資安記錄及監控失效)	4	19.23%	6.51%	53.67%	39.97%	6.87	4.99	53,615	242
A10	Server-Side Request Forgery (伺服器請求偽造)	1	2.72%	2.72%	67.72%	67.72%	8.28	6.72	9,503	385

- CWE-540 Inclusion of Sensitive Information in Source Code
- CWE-601 URL Redirection to Untrusted Site ('Open Redirect')
- CWE-651 Exposure of WSDL File Containing Sensitive Information

53



資通系統防護基準(37/42) - (OWASP Top 10 vs 資通系統防護基準)



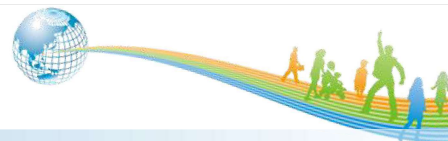
安全等級



❖ 善用及實作「防護基準」以預防 OWASP Top 10 風險

OWASP Top 10 2021 (防禦項目)	資通系統防護基準 (構面)	資通系統防護基準 (措施內容)	需求說明	行政院資通安全處需求範例
A3. Injection 注入攻擊	系統與服務獲得 (System and Services Acquisition)	系統發展生命週期開發階段 (System Development Life Cycle-Develop)	應注意避免軟體常見漏洞 (如OWASP TOP 10) 及實作必要控制措施	以「源碼檢測」確認排除常見漏洞
			應針對資訊系統之錯誤與例外進行適當處理	設置「客製化」錯誤頁面
	系統與資訊完整性 (System and Information Integrity)	軟體及資訊完整性 (Software, Firmware, and Information Integrity)	使用者輸入資料合法性檢查應置於應用系統 伺服器	以「正規表示式」規範使用者輸入欄位，並實 作於伺服器端
A7. Identification and Authentication Failures 身份識別與驗證機制失效	存取控制(Access Control)	帳號管理(Account Management)	資訊系統具備帳號管理機制，包含帳號之申 請、開通、停用及刪除之程序	帳號申請、審核、停用、刪除功能
			資訊系統具備刪除或禁用已逾期之臨時或緊急 帳號之功能	臨時帳號機制，逾期需有自動停用功能
			資訊系統具備禁用閒置帳號之功能	帳號未登入達半年以上，系統自動停用
			當超過機關所規定之預期閒置時間或可使用期 限時，資訊系統應自動將使用者登出	逾時自動登出、手動登出確實失效
	識別與鑑別 (Identification and Authentication)	內部使用者之識別 與鑑別(Identification and Authentication for Organizational Users)	資訊系統應識別及 鑑別非機關使用者(或代表機關使用者行為的程 序)	系統使用者具有唯一帳號，且須通過身分驗證 機制
		身分驗證管理(Authenticator Management)	使用預設密碼登入系統時，應於登入後要求立 即變更	系統若有預設密碼，登入後要求立即變更
			基於密碼之鑑別資訊，系統應強制最低密碼複 雜度；強制密碼最短及最長之效期限制	設定/修改使用者密碼功能，限制使用者密碼 強度(密碼長度12個字元以上，包含英文大小 寫、數字)
			使用者更換密碼時，至少不可以與前3次使用過 之密碼相同	登入時檢查密碼效期，必須定期90天更換密碼 ，且至少不可以與前3次使用過之密碼相同
			具備帳戶鎖定機制，帳號登入進行身分驗證失 敗達5次後，至少15分鐘內不允許該帳號繼續 嘗試登入或使用機關自建之失敗驗證機制	帳戶鎖定機制，帳號登入進行身分驗證失敗達 5次後，至少15分鐘內不允許該帳號繼續嘗試 登入
	識別與鑑別 (Identification and Authentication)	身分驗證管理(Authenticator Management)	身分驗證機制應防範自動化程式之登入或密碼 更換嘗試	採用圖形驗證碼(CAPTCHA)機制
			密碼重設機制對使用者重新身分確認後，發送 一次性及具有時效性符記	密碼重設機制：發送一次性及具有時效性符記 (Token)，如：簡訊驗證碼、EMAIL 驗證連結 ，檢查傳回符記之有效性後，才允許使用者進 行重設密碼動作
			對帳號之網路或本機存取 採取多重認證技術	多重因素認證(MFA)技術 (憑證、IP、OTP等)

資通系統防護基準(38/42)



❖ 系統與通訊保護 (2)

系統防護需求 分級		高	中	普
控制措施 構面	措施內容	資通系統應採用加密機制，以防止未授權	無要求	無要求

實作分享：

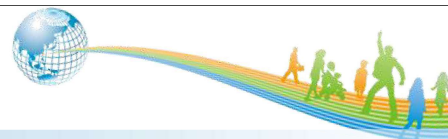
1. 加密類型：Web App (HTTPS)、Database (Encryption Connections)、FTP (SFTP)、Remote Maintenance (SSH、Secure RDP)。
2. 已遭破解或有資安疑慮的傳輸協定或加密/雜湊演算法：
 - ① 停用 SSL 3.0、TLS 1.0、TLS 1.1 等不安全的傳輸協定。
 - ② 停用 RC2、RC4、DES、3DES、SHA、MD5 等不安全的演算法。
3. 自行檢測方式：

```
nmap --script ssl-enum-ciphers -p 443 192.168.1.1
```

資料來源：資通系統防護基準驗證實務(V1.1)

55

資通系統防護基準(39/42) - 驗證實務



❖ 已遭破解或有資安疑慮的傳輸協定或加密/雜湊演算法應停用或移除！

啟用HTTPS

PORT STATE SERVICE REASON
443/tcp open https syn-ack

ssl-enum-ciphers:

TLsv1.1:

ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (secp256r1) - A
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (secp256r1) - A
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (secp256r1) - C
- TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1) - C
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C

compressors:
NULL

cipher preference: server

warnings:
64-bit block cipher 3DES vulnerable to SWEET32 attack
Broken cipher RC4 is deprecated by RFC 7465
Ciphersuite uses MD5 for message integrity
Weak certificate signature: SHA1

站台仍支援TLsv1.1，應移除

使用了3DES、RC4及MD5等演算法，應移除

TLsv1.2:

ciphers:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (secp256r1) - A
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (secp256r1) - A
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA384 (secp256r1) - A
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
- TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
- TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (secp256r1) - C
- TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1) - C
- TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
- TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C

compressors:
NULL

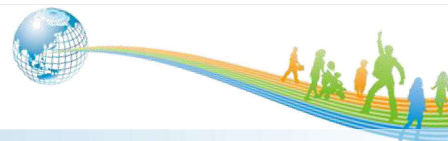
cipher preference: server

warnings:
64-bit block cipher 3DES vulnerable to SWEET32 attack
Broken cipher RC4 is deprecated by RFC 7465
Ciphersuite uses MD5 for message integrity
least strength: C

資料來源：資通系統防護基準驗證實務(V1.1)

56

資通系統防護基準(40/42)

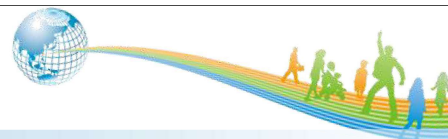


❖ 系統與資訊完整性 (3)

系統防護需求 分級		高	中	普
控制措施 構面	措施內容			
系統 與資訊 完整性	漏洞修復	一 定期確認 資通系統相關漏洞修復之狀態。 二 等級「普」之所有控制措施。		系統之漏洞修復 應測試 有效性及潛在影響，並定期更新。
	資通系統 監控	一 資通系統應採用 自動化工具 監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二 等級「中」之所有控制措施。	一 監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二 等級「普」之所有控制措施。	發現資通系統有被入侵跡象時， 應通報機關特定人員 。

57

資通系統防護基準(41/42)

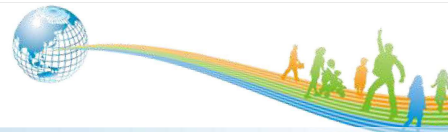


❖ 系統與資訊完整性 (3)

系統防護需求 分級		高	中	普
控制措施 構面	措施內容			
系統 與資訊 完整性	軟體及資 訊完整性	一 應定期執行軟體與資訊完整性檢查 。 二 等級「中」之所有控制措施。	一 使用 完整性驗證工具 ，以偵測未授權變更特定軟體及資訊。 二 使用者 輸入資料合法性檢查 應置放於應用系統 伺服器端 。 三 發現 違反完整性 時，資通系統應實施機關指定之安全保護措施。	無要求。

58

資通系統防護基準(42/42) - 驗證實務-多重認證技術

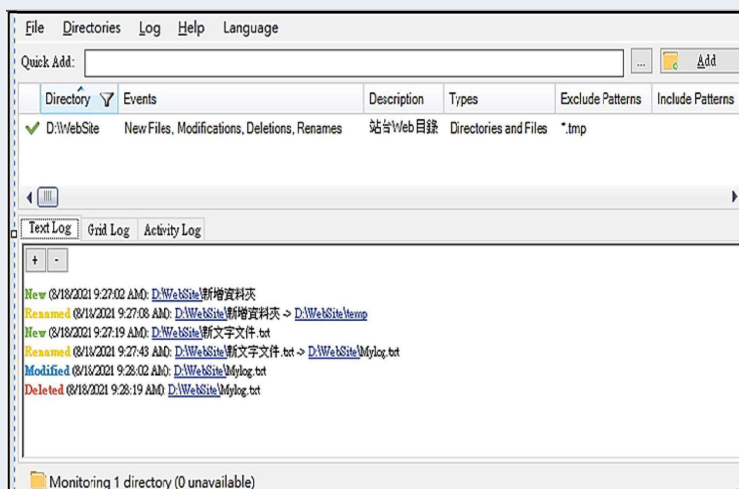


控制措施 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊

適用等級 中、高

內容說明

- 資通系統軟體及資訊，包含應用程式、網站重要目錄與組態設定檔等，皆是惡意攻擊者最喜愛目標，如植入惡意檔案或竄改網頁內容等手法，破壞資通系統完整性。應使用適當技術與工具，檢查重要軟體及資訊內容是否被惡意竄改。
- 完整性檢查技術如使用密碼雜湊函數、同位元檢查及循環冗餘檢查等。亦可評估採用目錄檔案監控工具，可自動偵測應用程式與網站目錄或檔案之異動事件，當發現檔案異動時會留下相關日誌紀錄並提出示警。目錄檔案監控工具操作畫面範例詳下圖。



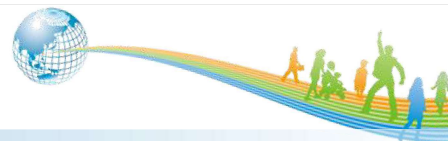
資料來源：資通系統防護基準驗證實務(V1.1)

59

資通系統防護基準檢核表 (資通系統防護基準自評檢查)



善用防護基準檢核表自評



❖ 依現況判斷系統符合程度，如：符合、部分符合、不符合或不適用。

❖ 數位發展部資通安全署「資通系統防護基準檢核表」範例！

構面	類別	項次編號 (原由)	最低系統 等級要求	安全控制措施	是否符合	構面	類別	項次編號 (原由)	最低系統 等級要求	安全控制措施	是否符合	現況說明	依據	矯正作為	目標日期	備註說明
事件日誌與可 歸責性	記錄事件	15	普	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	符合	系統與 服務獲 得	鑑別資訊 存取	41	普	密碼變更時，至少不可以與前3次使用過之密碼相同。 (對非內部使用者，可依機關自行規範辦理)	符合	含12個字元，並包含英數字及特殊符號。	密碼變更頁面提示畫面截圖			
		16	普	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	符合			42	普	上述兩點所定措施，對非內部使用者，可依機關自行規範辦理。	符合	本系統前臺無設計帳號登入機制，後臺登入管理後台密碼登入頁面截圖				
		17	普	應記錄資通系統管理帳號所執行之各項功能。	符合			43	普	資通系統應鑑別與過程中之資訊。	符合	本系統前臺無設計帳號登入機制，後臺登入管理後台密碼登入頁面截圖				
		18	中	應定期審視機關所保留資通系統產生之日誌。	符合			47	普	資通系統應鑑別及鑑別與使用者之資訊(或代表機關使用者行為之程序)。	不符合	本系統為公開站點，前臺無設計帳號登入機制。	系統功能規格書			
日誌紀錄內 容		19	普	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一記錄機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	符合		系統發展生命週期需求階段	48	普	針對系統安全需求(含機密性、可用性、完整性)，進行確認。	符合	本系統RFP已具體描述系統安全需求，並確認符合資通系統防護基準之規範。	系統RFP			
		20	普	依據日誌儲存需求，配置所需之儲存容量。	符合			51	普	應針對安全需求實作必要控制措施。	符合	本系統RFP已具體描述系統安全需求，並要求開發人員確實實作相關功能。	1.系統RFP 2.系統功能規格書			
日誌儲存容 量		20	普	依據日誌儲存需求，配置所需之儲存容量。	符合	系統發展生命週期開發階段		52	普	應注意避免軟體常見漏洞及實作必要控制措施。	符合	已要求開發人員注意安全程式撰寫原則，避免OWASP Top 10等常見網站弱點，並配合弱點掃描活動，檢測是否存在安全漏洞。	1.系統RFP 2.系統功能規格書 3.弱點掃描報告			
日誌處理失 效之回應		21	普	資通系統於日誌處理失效時，應採取適當之行動。	符合			53	普	發生錯誤時，使用者應獲顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。	不符合	使用伺服器預設錯誤頁面，發生錯誤時可能直接顯示詳細錯誤資訊，如程式碼位置。	系統錯誤頁面	設定客製化錯誤頁面	110年10月1日	
時數及校時		23	普	資通系統應使用系統內部時鐘產生日誌所需時數，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	符合	系統發展生命週期測試階段		56	普	執行「弱點掃描」安全檢測。	符合	已於系統上線前完成弱點掃描，並納入中心每季維護系統範圍，並保存弱點掃描及修復紀錄。	1.弱點掃描報告 2.弱點掃描修復紀錄			
								58	普	於部署環境中應針對相關資通安全威脅，進行更新與修	符合	1.進行作業系統之安全性更新，定期於每月底評估、紀錄	1.每季系統元件更新紀錄			

問題與討論 (Q & A)

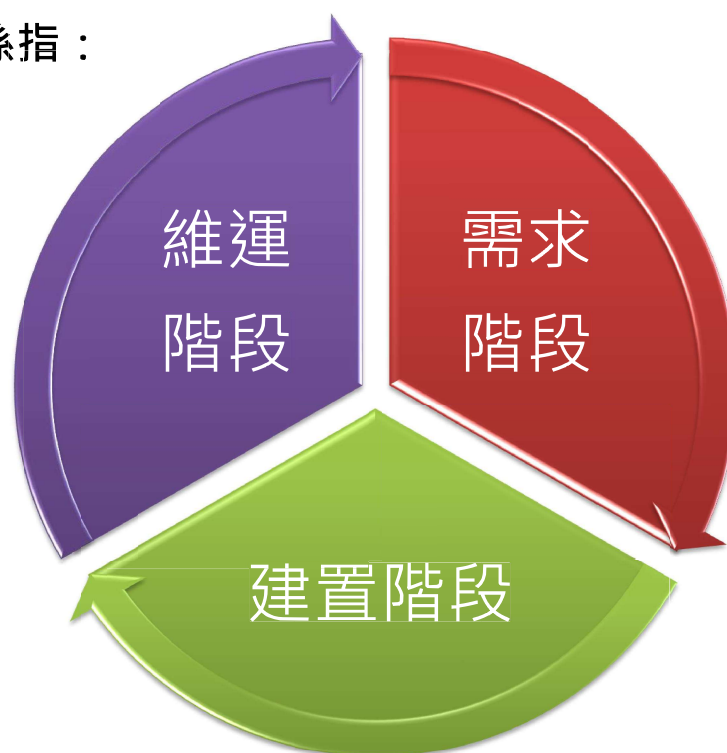


附錄

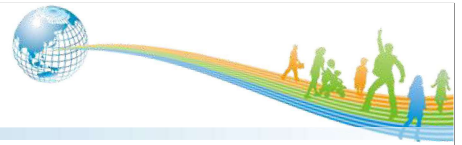


資通系統籌獲各階段資安強化措施

❖ 各階段係指：



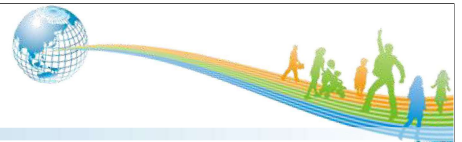
需求階段(1/2)



1. 涉資通系統籌獲，於徵求時應由委託機關依資通安全責任等級分級辦法、附表九所定資通系統防護需求分級原則，評估及標示資通系統之防護需求等級供受託者知悉。
2. 前述「防護需求等級評估結果」應經「資安長」確認。
3. 應估算資安資源需求：
 - 1) 委託機關應評估訂定受託者應配置之資通安全專業人員人數及所需能力等相關需求。
 - 2) 應至少以資通系統籌獲案資訊經費百分之五估算資安經費；如因實務作業無法達成上開要求，應敘明原因及採行之資安作為簽陳資安長核准。
 - 前述資安經費之成本分析，建議依該措施之附件、廠商估價單格式辦理並納入招標文件中。

65

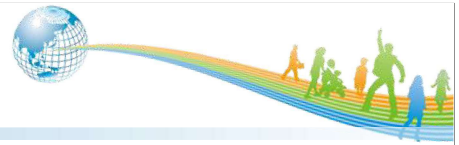
需求階段(2/2)



3. 應估算資安資源需求：
 - 3) 採購評選時，應將投標廠商之資安作為納入評選項目，並依下列規定辦理：
 - 應將委託案之相關資安作為納入評選項目，且配分至少占總分之百分之十。
 - 應要求投標廠商說明履約之資安作為，並填列該措施之附件、相關資安管理作業自我評估表。
 - 參考「資通系統防護基準驗證實務」指引，依資通系統之防護需求等級，於規劃(招標)階段，訂定對應之廠商專業能力需求資格，俾選任合適受託者。
 - 4) 資通系統籌獲涉及委託機關之核心資通系統且採用評選方式選任受託者時，評選委員應包含至少一位資安專業人員，其資格詳參該措施(P.3)。

66

建置階段



❖ 資通系統籌獲專案資安作業分工：

	管理及需求單位	資通安全專責人員
遵循安全軟體開發生命週期(SSDLC)	監督、確認	(第二線) 勾稽確認
履約(執行)及專案里程碑資安管理	訂定、監督、確認	(第二線) 勾稽確認

註1.SSDLC：應至少包含資通安全責任等級分級辦法附表十、資通系統防護基準之「系統與服務獲得」構面對應防護需求等級之各項控制措施。

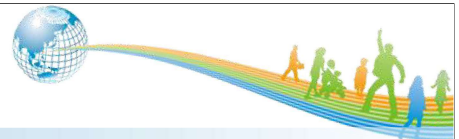
註2. 資通安全專責人員建議參考該措施之 [附件、資通系統籌獲各階段資安強化措施執行檢核表](#) 進行勾稽、確認。

❖ 委託機關之**核心資通系統**籌獲案，**應聘請外部資安專家**為顧問或委員，協助機關於專案重點里程碑中，檢視履約(執行)程序與成果之相關資安管理作為。

❖ 為確保核心資通系統品質，針對受託業務包括委託機關之**核心資通系統**且委託金額達新臺幣一千萬元以上者，委託機關應評估導入獨立驗證與認證機制(IV&V)，評估結果應經資通安全長確認。

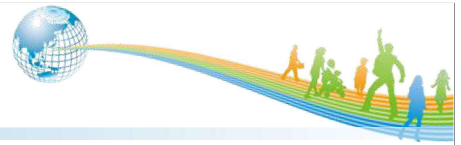
67

維運階段



- ❖ **落實資安管理**：委託機關之**資通安全專責人員**應協助資通系統管理單位，確認資通系統維運作業確實依委託機關之資安管理措施落實辦理，例如登入維護、資料備份、效能調校、主機環境及系統版本更新等。
- ❖ 受託者應配置適當之**資通安全專責人員**：協助確認履約(執行)階段作業符合委託機關及受託者雙方之資安管理規範。
- ❖ 在**契約有效期間內之資安稽核作業**：
 - 得依資通系統籌獲案之規模及性質，要求受託者自辦資安稽核作業。
 - 資通系統防護需求等級為「高」者，應定期或不定期對受託者**辦理資安稽核**，為中者得視需求定期或不定期對受託者辦理資安稽核。
 - 發生重大資安事件時，委託機關應**辦理資安稽核**，並應將稽核結果送交資安主管機關。

68



~報告完畢，謝謝聆聽~