中央政府各醫院作業基金經營現況之探討

九、113 年度公立醫院整體資安通報事件係 109 年度之 2.48 倍，又部分醫院個人電腦作業系統及資安防護設備原廠已終止支援，恐生資安漏洞；另社交工程演練僅以比率為評估標準，恐有低估實際風險之虞

近年來醫院資安事件頻傳，顯示其資安防護機制議題值得重視，以確保病患資料及醫療體系安全。經查：

(一)113 年度中央政府轄管公立醫院整體資安通報事件係 109 年度之 2.48 倍，且嚴重等級較高之第 3 級資安事件占近四成；另近 5 年多來資安事件類型以非法入侵為主要發生原因

依行政院「國家關鍵基礎設施安全防護指導綱要」，醫院係八大關鍵基礎設施(Critical Infrastructure,CI)之一，而資通安全管理法於 108 年 1 月 1 日施行，並將該設施納管，此處關鍵基礎設施，係指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活等有重大影響之領域[1]，爰其資訊安全至關重要。為保障病患資訊、醫療系統運作，以及公共安全，醫院應落實資安防護。且依資通安全管理法第 14 條第 2 項規定，公務機關如發生資通安全事件，如系統、服務或網路狀態經鑑別後，顯示可能有違反資通安全政策或保護措施失效之情形，已影響資通系統機能運作，構成資通安全政策之威脅者，應通報主管機關；且依資通安全事件通報及應變辦法第 2 條規定，資通安全事件依嚴重程度可分為第 1 級至第 4 級，共 4 個等級[2]，由輕微至重大依序遞增。

---

[1] 資通安全管理法第 3 條。

[2] 依資通安全事件通報及應變辦法第 2 條第 2 項至第 5 項規定略以，**有下列情形之一者，為第一級資通安全事件**：1.非核心業務資訊遭輕微洩漏。2.非核心業務資訊或非核心資通系統遭輕微竄改。3.非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響。**有下列情形之一者，為第二級資通安全事件**：1.非核心業務資訊遭嚴重洩漏，或未涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。2.非核心業務資訊或非核心資通系統遭嚴重竄改，或未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕

根據 109 年度至 114 年 3 月底中央政府轄管公立醫院資安通報資料統計(詳表 3-9-1)，整體通報件數概呈上升趨勢，其中 113 年度通報件數達 57 件，為近年來最高，係 109 年度(23 件)之 2.48 倍，反映醫療機構在資訊化進程中，資安威脅呈現顯著上升趨勢。

表 3-9-1　109 年度至 114 年 3 月底醫院作業基金資安通報件數統計表

單位:件

中央主管醫院類別/年度	109	110	111	112	113	114.3	總計
教育部所屬醫院	6	11	26	20	35	3	101
退輔會所屬醫院	7	6	4	16	8	2	43
衛福部所屬醫院	10	13	24	14	14	5	80
整體合計	**23**	**30**	**54**	**50**	**57**	**10**	**224**

說　　明：國防部所屬醫院 109 年度至 114 年 3 月底無資安通報件數。
資料來源：教育部所屬各醫院作業基金、退輔會、衛福部提供；本中心整理。

另就資安事件等級觀察(詳表 3-9-2)，第 1 級事件雖自 112 年度開始下降，惟 113 年度仍達 19 件，114 年度截至 3 月底止亦已發生 9 件，顯示資安風險未顯著下降；而第 2 級事件則呈逐年上升之趨勢，從 109 年度 2 件增至 113 年度 16 件；另第 3 級事件更是於 113 年度顯著增加至 22 件，占當年度整體總資安通報件數(57 件)之 38.60%，近四成，由此可知，資安事件不僅在數量中增加，其資安威脅已由輕微異常逐步轉變為對醫療營

微竄改。3.非核心業務之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作，或未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，於可容忍中斷時間內回復正常運作。**有下列情形之一者，為第三級資通安全事件**：1.未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏。2.未涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭輕微竄改。3.未涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。**有下列情形之一者，為第四級資通安全事件**：1.一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏，或國家機密遭洩漏。2.一般公務機密、敏感資訊、涉及關鍵基礎設施維運之核心業務資訊或核心資通系統遭嚴重竄改，或國家機密遭竄改。3.涉及關鍵基礎設施維運之核心業務或核心資通系統之運作受影響或停頓，無法於可容忍中斷時間內回復正常運作。

運構成實質風險的事件型態。

表 3-9-2　109 年度至 114 年 3 月底醫院作業基金資安通報事件等級統計表

單位:件

資安通報事件等級	中央主管醫院類別/年度	109	110	111	112	113	114.3	合計
第1級	教育部所屬醫院	5	11	25	19	11	3	74
	退輔會所屬醫院	6	5	4	9	2	1	27
	衛福部所屬醫院	9	9	14	10	6	5	53
	合計	**20**	**25**	**43**	**38**	**19**	**9**	**154**
第2級	教育部所屬醫院	1	0	0	0	6	0	7
	退輔會所屬醫院	1	1	0	6	6	1	15
	衛福部所屬醫院	0	4	9	4	4	0	21
	合計	**2**	**5**	**9**	**10**	**16**	**1**	**43**
第3級	教育部所屬醫院	0	0	1	1	18	0	20
	退輔會所屬醫院	0	0	0	1	0	0	1
	衛福部所屬醫院	1	0	1	0	4	0	6
	合計	**1**	**0**	**2**	**2**	**22**	**0**	**27**
第4級	**無**							

說　　明：國防部所屬醫院 109 年度至 114 年 3 月底無資安通報件數。

資料來源：教育部所屬各醫院作業基金、退輔會、衛福部提供；本中心整理。

再就資安事件發生原因區分(詳表 3-9-3)，以「非法入侵」(75 件)、「資訊系統問題」(58 件)與「設備問題」(40 件)為主要類型，占整體通報總件數 224 件之大宗，恐有醫院常面臨外部駭侵、網站系統開發設計不夠完善及設備異常等潛在問題，鑒於醫院不僅肩負救死扶傷之責任，更是承載全國龐大個人健康資料與隱私資訊之核心單位，其系統一旦遭受攻擊或故障，不僅影響醫療作業運作，更可能造成民眾就醫延誤與社會信任動搖，允宜強化資安防護機制，俾使醫療體系建立更具韌性之資安防線。

表 3-9-3　109 年度至 114 年 3 月底醫院作業基金資安通報事件發生原因情形表

單位:件

資安通報事件發生原因	教育部所屬醫院	退輔會所屬醫院	衛福部所屬醫院	總計
設備問題	3	9	28	40

資安通報事件發生原因	教育部 所屬醫院	退輔會 所屬醫院	衛福部 所屬醫院	總計
軟體問題	5	10	1	16
非法入侵	33	17	25	75
僅存在內部對外連線行為	4	6	16	26
資訊系統問題	53	1	4	58
人為操作問題	0	0	2	2
其他	3	0	4	7
合計	101	43	80	224

說　　明：1.設備問題(包含伺服器或網路設備、電力或電信異常等硬體異常)。
2.軟體問題(包含系統軟體套件異常或程式等軟體漏洞)。
3.非法入侵(係指由外對內，如來自外部攻擊、植入惡意程式、帳號密碼外洩、挖礦、病毒等)。
4.僅存在內部對外連線行為(係指由內對外，如不確定原因但對外連線或同仁自行瀏覽假冒網頁、使用非法軟體等且無任何損害或竄改之情事)。
5.資訊系統問題(因資訊系統開發存在系統弱點漏洞被外部利用，如網站相關問題)。
6.人為操作問題(誤將含個資文件放置網頁上或人爲操作錯誤所致)。
7.其他。

資料來源：教育部所屬之各醫院作業基金、退輔會及衛福部提供；本中心整理。

(二)醫院之電腦作業系統及資安防護設備存有一定比例係原廠終止產品支援者，即無法獲得漏洞修補與更新，恐生資安漏洞

近年來，醫療院所資安事件頻傳，對於資訊安全的重視日益提升，而電腦作業系統及資安防護設備更在資訊安全架構中扮演著關鍵角色。且資訊科技發展日新月異，相關產品與系統之生命週期也隨著影響，一旦原廠終止產品支援或停止提供服務，即進入 EOS(End of support or service)狀態，此時系統將無法再獲得技術支援、安全性更新或漏洞修補等，也大幅提高資安風險，讓機敏資料有暴露之可能。

作業系統是電腦運作的核心，其安全性對於整體資訊系統穩定運作扮演著重要角色，依據各醫院作業基金提供醫院現行個人電腦作業系統安裝情形(詳表 3-9-4)，其中部分醫院仍使用

已終止支援[3]之作業系統，教育部所屬醫院1,637台，退輔會所屬醫院1,705台及衛福部所屬醫院550台，其終止支援占總電腦台數，分別為7.94%、8%及4.28%。雖部分醫院告知上開電腦，僅用於內部封閉網路或將於近期汰換等，惟其所採用之作業系統已不再獲得原廠提供安全性更新與漏洞修補，容顯潛在資安風險之存在。

表3-9-4　醫院作業基金之電腦作業系統已終止支援統計表

單位:台；%

中央主管醫院類別	總電腦台數 A	作業系統 已終止支援台數 B	終止支援占比 C=B/A
教育部所屬醫院	20,607	1,637	7.94
退輔會所屬醫院	21,319	1,705	8.00
衛福部部立醫院	12,860	550	4.28

說　　明：表內係截至114年3月底止之數據。國防部所屬醫院之電腦無作業系統已終止支援之情事。

資料來源：教育部所屬之各醫院作業基金、退輔會及衛福部提供；本中心整理。

另就資安防護設備進行檢視，所謂資安防護設備，係指防火牆、入侵檢測系統(IDS)和入侵防禦系統(IPS)及網頁應用程式防火牆(WAF)等，主要用於保護電腦系統、網路與資料，防範未經授權之存取，使用、洩露、破壞或修改之各種硬體及軟體設備，依據各醫院資安防護設備終止支援情形(詳表 3-9-5)顯示，其中退輔會所屬醫院共有54台已進入EOS狀態，占其總資安防護設備之10.53%，占比最高，另教育部所屬醫院及衛福部所屬醫院，則分別為9及2台，占比分別為0.76%及1.69%。

由上可知，醫院之電腦作業系統及資安防護設備存有一定比例已停止原廠支援，因無法獲得漏洞修補與更新，恐造成資安防護設備成為資安漏洞所在，或無法防護較新之攻擊樣態，潛藏資安風險，縱部分占比微小，惟資訊安全屬高敏感領域，

[3] 終止支援之作業系統係指Win 10以下版本。

即便僅有少數設備存有漏洞，亦可能成為駭客入侵系統之破口，影響整體資安防線，允宜加強資安風險評估、控管，及採行有效資安防禦措施，以確保整體資訊系統安全與運作穩定。

表 3-9-5　資安防護設備終止支援情形表　　單位:台；%

資安防護設備			
中央主管醫院類別	總台數 A	EOS 台數 B	EOS 占比 C=B/A
教育部所屬醫院	1,190	9	0.76
退輔會所屬醫院	513	54	10.53
衛福部部立醫院	118	2	1.69

說　　明：表內係截至 114 年 3 月底止之數據。國防部所屬醫院無資安防護設備終止支援之情事。

資料來源：教育部所屬之各醫院作業基金、退輔會及衛福部提供；本中心整理。

(三)近年來醫院社交工程演練結果雖符合設定之比率標準，惟宜同步納入違反規定之絕對人次指標值，以強化資安風險管控

依中央政府轄管公立醫院實施社交工程演練目標值，大部分係設定為測試郵件之開啟率[4]低於 10%及點閱率[5]低於 6%以下，雖此一比率標準，可作為風險指標之一，惟若僅以比率判定是否符合標準，而忽視實際開啟與點閱之人次規模，恐將低估機關實際面臨之資訊安全風險。

以退輔會所屬醫院為例，觀察其 113 年度社交工程演練結果(詳表 3-9-6)，總受測人次 20 萬 3,185 人次，開啟郵件 1,238 人次，開啟附件或點閱連結 708 人次，其開啟率及點閱率分別為 0.61%及 0.35%，雖形式上符合現行標準值，惟單一年度總開啟與點閱人次均已超過千人及百人情形，顯示該所屬醫院之實際暴露於潛在資安風險之人數不容忽視，仍有高度觀注之必要。

尤需強調的是，資訊安全風險之本質是「0 與 1 的問題」，即便僅有一人點擊惡意連結，也可能造成系統入侵、資料外洩

[4] 開啟率=(開啟郵件人次÷演練人次)×100%。

[5] 點閱率=(開啟附件或點閱連結人次÷演練人次)×100%。

等重大資安事件，故無論比例高低，絕對人次多寡即代表實際風險規模，不容忽視。尤其是醫療院所不同於一般機關，其資訊安全事件可能造成更嚴重之衝擊，主要包括如下：

1. 影響病患就醫安全：如系統遭受攻擊導致系統中斷，可能妨礙診療流程、急救資訊存取與處置時效等，嚴重恐影響病患生命安全。
2. 侵害個人隱私權：病歷、檢查報告、身份資訊等一旦洩露，將對病患造成難以彌補之損害，並可能衍生法律責任與社會信任危機。

是以，醫療機構資訊安全標準應高於一般標準，宜考量社交工程演練標準同步納入「開啟人次」與「開啟附件或點閱連結人次」絕對數值作為判斷標準，始能更精準掌握潛在風險規模，並據以持續強化資安教育，以降低實質風險暴露，並確保病患安全與資訊保護。

表 3-9-6　113 年度退輔會所屬醫院社交工程演練結果表

單位:人次；%

項目	113 年度
演練人次(a)	203,185
開啟郵件人次(b)	1,238
開啟附件或點閱連結人次(c)	708
開啟郵件人次比(開啟率)(b/a)	0.61
開啟附件或點閱連結人次比(點閱率)(c/a)	0.35

說　　明：以 113 年度退輔會所屬各醫院實際社交工程演練之結果加總，惟各醫院演練次數或有不一。

資料來源：退輔會提供；本中心整理。

（分機：1929 沈家榆）