宏洲纖維工業股份有限公司

資通安全治理暨風險評估報告

資料統計分析期間：2025 年 1 月～12 月

呈報單位：資安管理小組

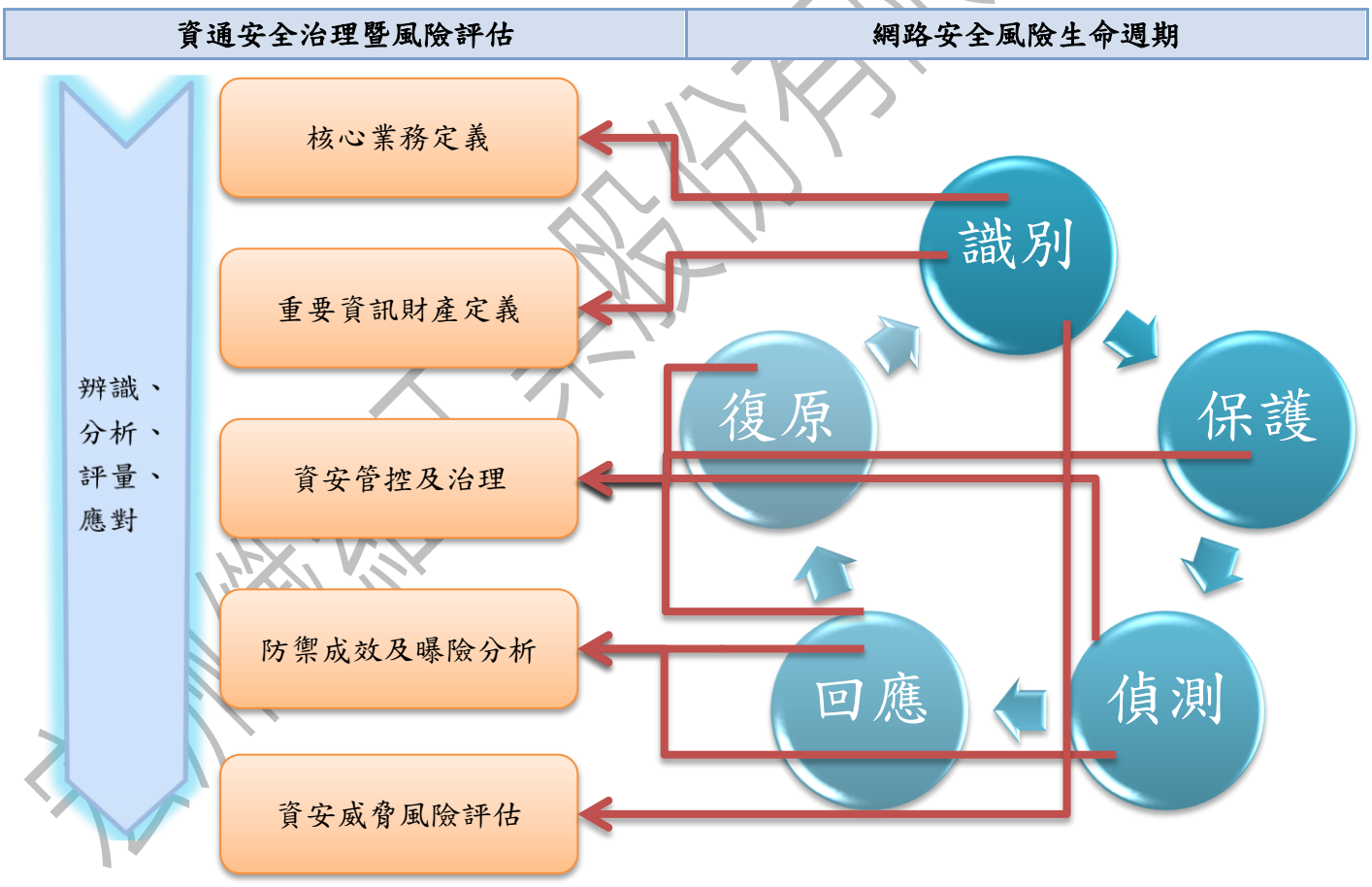
2026 年 3 月

宏洲纖維工業股份有限公司・資通安全治理暨風險評估

本公司有關資通安全管理事項之規劃、推動、評估及稽核，皆由「資安管理小組」統籌指揮，以確保各項資安政策之落實及資安措施之執行，協調各項資源分配，提升資訊安全之防禦能力及韌性，建立公司同仁正確的資訊安全作業觀念，降低整體資安威脅及降低風險，並每年定期向董事會提報資通作業之風險評估報告。

本公司的資通安全風險評估報告就核心業務及核心資通系統之重要資產，鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並檢視執行管理面或技術面的控制措施的成果；當中從資訊環境之端點、通訊閘道到網際網路三個作業層面剖析重要資訊財產可能面臨的威脅及風險，再從已導入的多層次資安管控措施或防禦設備，對於控制點所產生之數據，分析量化後綜合呈現其曝險趨勢，以使經營團隊對公司整體資訊作業的風險程度，能夠有具體的概念及警覺，並在面臨威脅事件時，能夠快速回應並即時採取適當防範處置，以維護公司資訊財產的安全性及完整性。

本公司資通安全治理暨風險評估報告架構以圖示表達如下圖說明：



報告內容以「識別和定義核心業務及重要資訊資產」、「資通訊安全之管控措施及成熟度自評結果」、「以定量分析評估資安的防禦成效及曝險程度」、「以定性分析評估資安威脅的未來風險」、「資安管控檢討，和未來的關注重點及因應策略」五大主題，分別說明評估過程及結果。

一、 核心業務及重要資訊財產

識別核心業務 ⇨ 定義重要資訊財產 ⇨ 重要資訊財產之價值量化

1-1. 本公司之重要及核心業務說明：

重要業務（◎核心業務）	資訊管理系統/資料	重要性	資訊環境失效對營運的影響程度	最大可容忍之中斷時間
◎原料採購	採購管理系統	公司營運必要業務	中/改紙本作業	1 週
◎生產製造	生產管理系統	公司生產必要業務	中/改紙本作業	1 週
◎產品銷售	銷售管理系統	公司營運必要業務	中/改紙本作業	1 週
料件庫存管理	料件庫存管理系統	公司生產必要業務	低/改紙本作業	1 週
◎財會出納	總帳管理系統	公司營運必要業務	中/改紙本作業	1 週
人力薪資管理	人力資源管理系統	公司營運必要業務	中/改紙本作業	3 週
產品品質檢驗	產品物性系統	公司生產必要業務	中/改紙本作業	1 週
文書資料管理	文管系統	公司治理必要業務	低/改紙本作業	2 週
空壓空調監控	公用監控管理系統	公司生產必要業務	低/改紙本作業	2 週
公司內部作業	內控制度管理	公司治理必要業務	低/改人工作業	3 週
資訊安全管理	資訊主機維護管理	確保資訊作業環境安全之必要業務	低/	2 週

[註 1]資訊環境失效對營運的影響程度：

高. 會影響多個作業單位，資訊作業延遲會影響帳款之結帳或資料申報的時限，或損害公司的聲譽、形象。

中. 會影響 1、2 個作業單位，資訊作業延遲雖降低帳款之結帳或資料申報的時效，但仍有替代方法可協助及時完成。

低. 不影響其它單位作業、帳款之結帳或資料申報的時間，但仍為日常管理或主管機關要求之重要執行事項。

1-2. 為維繫上述重要業務之持續運作，在各作業層面所需的重要資訊財產列示如下：

作業層面	資產名稱	功能失效對**業務**的影響程度/最大中斷時間之容忍值
內部網路/環境	伺服器(資訊軟體及資料庫)	高/5 天
	ERP 管理系統	高/2 天
	人事管理系統	低/7 天
	品質檢驗管理系統	中/5 天
	聚合管理系統	高/2 天
	生產監控管理系統	中/5 天
	檔案伺服器	中/5 天
	電子資料檔	中/5 天
	生產監控相關主機	中/5 天
	個人資訊主機	高/2 天
	網路交換器	高/2 天
	不斷電系統	中/5 天
	重要作業執行人員	中/5 天
	資訊機房溫控、消防設施	低/7 天
網路通訊閘道	防火牆	高/2 天
網際網路/外部	電子郵件伺服器	高/2 天
	公司網站	低/7 天
	連外網路設備	高/2 天
	資訊軟硬體支援服務廠商	中/5 天

[註 2]資訊設備功能失效對重要業務的影響程度：

高. 會影響資訊安全、作業的及時性或會使公司受到財務損失。

中. 不影響作業的及時性，但對營運流程或資訊安全仍有重大影響，具不確定風險。

低. 各項資訊作業仍能持續，為資訊或資安管理上所需，以避免突發事故衍生嚴重後果。

1-3. 為利於後續評估對資產將採取之風險因應方式及保護力道，上述重要資訊財產依 6-1. 資訊財產之價值估量表區分機密性、完整性及可用性，做較精細的價值(最高 12)估算如下：

資產名稱	與**核心業務**之依存關聯性	機密性(C)	完整性(I)	可用性(A)	資產價值(W)=C+I+A
伺服器(資訊軟體及資料庫	高提升效率、安全與競爭力	3	4	3	10
ERP 管理系統	高數據整合、提高決策效率	4	4	3	11
人事管理系統	中優化人力配置提升績效	4	2	1	7
品質檢驗管理系統	高確保產品穩定提升品質	3	3	2	8
聚合管理系統	中提升產品生產穩定性	3	3	2	8
生產監控管理系統	中確保產品質量、生產安全	2	2	2	6
個人資訊主機	高影響核心業務連續性	3	4	2	9
檔案伺服器	高確保資料存取與安全	4	4	2	10
電子資料檔案	高支持決策和營運優化	4	4	2	10
生產監控相關主機	中營運效率與即時管理	2	2	2	6
網路交換器	中數據傳輸穩定與業務通聯	2	3	2	7
不斷電系統	中機房運作穩定與業務連續	1	2	2	5
資訊機房溫控、消防設施	低設備安全與業務維持	3	1	1	5
重要作業執行人員	高執行各項重要作業	3	3	1	7
防火牆	高確保網路安全及業務資料	4	4	2	10
電子郵件伺服器	高確保溝通順暢，支援運作	4	4	2	10
公司網站	低提升形象，支援業務發展	1	2	2	5
連外網路設備	高通訊順暢，支援業務運行	2	4	2	8
資訊軟硬體支援服務廠商	高技術支援，確保業務運行	3	3	1	7

二、 資通安全管控及治理

資安管理分類 ⇨ 管控措施及執行說明 ⇨ 管控措施之成熟度執行

本公司對於資安風險之管控以公司內部控制制度為根基，參考外部實例或資訊廠商建議而持續改進，所採取之管控措施(如下表)乃衡量經營管理階層對營運宗旨與企業價值之共識，針對核心業務及重要工作之發展進程，依照 ISACA 國際電腦稽核協會台灣分會之「資通安全公司自我檢查表」的十個分類於每年定期進行自我評估及分析後，依據其中風險性較高的部分進行檢討及擬具改善措施，從系統面、技術面、程序面，對已知威脅採取適當之處理，對潛藏之威脅則盡可能予以事前分析及鑑別，以保護公司資訊財產的機密性、可用性及完整性，避免遭受各種威脅及降低可能的危害或損失，以提升本公司承受外部攻擊之防護能力及應變彈性，減緩衝擊等級及降低可能造成公司的損害，妥善因應各項風險。

項次	評估類別	風險評比(%)			重要管控措施
		低	中	高	
1	資訊安全政策	70	30	0	1. 定期審查、修訂資訊安全政策。 2. 內部稽核單位每年定期稽查管控措施。
2	建立資訊安全組織	73	27	0	1. 設資安管理小組及個人資料保護小組。 2. 訂立資安事件之緊急應變處理及回報程序。
3	人員安全與管理	10	90	0	1. 內部控制制度定義資訊人員、使用者之作業權限劃分，及人員異動、離職之作業準則。 2. 每年執行作業權限複核。 3. 每年定期普查個人電腦，防止公器私用。
4	資產分類與控管	33	67	0	1. 資訊類軟、硬體資產列冊管理。 2. 每年定期普查電腦，確認軟、硬體資產。
5	實體及環境安全管理	90	10	0	1. 專用電腦機房具溫度、電力自動控管。 2. 伺服器及重要職務之電腦，安裝防毒軟體，每日定時備份，其備份份數至少二代。 3. 營運資料庫資料每日壓縮後以磁帶儲存備份，每年定期模擬事故演練於廠商備援機房還原測試。

6	通訊與操作管理	64	36	0	1.電子郵件主機具自我防護及保存稽核之功能。 2.每日分析防火牆紀錄，並使用上網行為記錄器，即時防堵內、外部異常行為。 3.即時宣導資安事件、通告或案例，提升防護意識。 4.使用 Hinet 資安艦隊之防護方案，擴展防護廣度。
7	存取控制	76	24	0	1.電子檔資料依部門、個人設定存取權限。 2.對外連線作業申請需經部門主管及總經理同意。 3.電子郵件區分內、外部，不須對外連絡之人員僅能內部寄信。 4.人力資源系統於讀取個資時，自動記錄存取軌跡。
8	系統開發與維護	82	18	0	應用系統自行開發、維護，在規劃分析時主動將安全需求納入設計考量，防範外部的侵入篡改。
9	永續運作之計畫管理	73	27	0	1.營運資料庫每年定期演練、測試。 2.重要設備訂立緊急應變計劃，供發生重大資安事件時遵循及應變。
10	內部稽查及其它	50	50	0	1.每年電腦普查時告知公司軟體所授權之範圍，實際查核若有規範以外軟體則要求移除或提供授權證明；軟、硬體普查資料，隨時依資產狀況更新。 2.資訊單位每年定期自評資訊作業環境安全。 3.內部稽核人員每年定期稽查資訊控制作業。
總　　評（%）		68	32	0	1.舊版 Windows 個人電腦應汰換。 2.應加強機敏性資料的防護措施。

由於本公司的生產設備均為獨立運作，並未透過資訊系統(例如: MES 製造執行系統)及網路做資料集結和進一步之運用，且資訊管理系統僅限於公司區域網路執行，未開放透過網際網路之連線，自評中在機敏性資料的防護處理上較為不足,提高風險度,改善措施將汰換舊版電腦為 Windows 11，並擬請資安廠商進行外部偵測及稽核等相關服務，以加強資安防護之強度及增加風險評估之可信度，**總結整體之資安風險程度介於"低-中"之間，無重大營運風險**。

三、 資安之防禦成效及曝險分析(定量分析)

防禦數據統計 ⇨ 量化風險 ⇨ 歷史風險趨勢及重點說明 ⇨ 年度風險比較

3-1. 本公司自 2015 年 6 月陸續導入中華電信 Hinet 資安艦隊之防護解決方案，以便即時防堵網路作業的異常行為，其定期產生之防護報告均明確呈現已阻擋之各項威脅數目或風險程度，雖缺乏業界之整體指標做為比較，但經長期累積其統計數據，再以此為基礎資料依風險程度予以量化，轉換為資安的曝險程度指標，以表達對既有風險之管控成效，並作為公司日後改善措施之參考。

3-2. 風險量化的方式乃以資安防護紀錄之關鍵項目作為量化因子，依風險等級之高、中、低分別計算各月的平均數，再乘以不同權值後合計為風險值；各防護措施的風險量化因子，乃取自統計資料中對資安層面較能呈現威脅程度的項目，相關定義說明如下：

防護措施	功能說明	風險量化因子
端點防毒/防駭	運用 AVG AntiVirus Free 及 Malwarebytes，對公司個人電腦過濾郵件，防止使用者誤開帶有病毒之附件與惡意連結，管控員工聯外網路，防止連上危險網站，管控周邊設備，防止 USB、光碟資料的不當存取，鎖定機敏資料，防止意外或蓄意外洩。運用伺服器內建之自動及手動過濾機制阻擋 IP、郵址或域名之黑名單，並對企圖不明之長時偵測來源予以封鎖。	以被伺服器阻擋過濾的項目數為因子，依照風險等級分為高、中、低三級。
IPS 入侵防護	每日不定期數次更新病毒碼、防護特徵碼，更迅速準確的辨識駭客攻擊手法與行為模式，全面性偵測及防護中高風險的 CVE 漏洞，有效攔阻雙向惡意連線流量與網路病毒威脅，優化網路頻寬。	以被 Hinet 阻擋的攻擊防護次數為因子，依照風險等級區分為嚴重、高、中、低四級。
弱點偵測	以高度精確和極低的誤報率的掃瞄能力和功能，全面性掃描防火牆及郵件伺服器的所有網路通訊埠及系統上的弱點，也針對系統應用程式的安全漏洞，依照風險程度分類，提供修補建議與報告。	以被掃描的設備弱點項目數為因子，依照風險等級區分為高、中、低及資訊四個等級。
郵件伺服器防禦機制	利用郵件伺服器內建之掃毒器及垃圾郵件處理器，採用 ClamAV 掃毒引擎及 spamassassin 垃圾信評分機制，主動分析信件之安全性並給予垃圾信可疑度評分，再藉由下列多層式的偵測、過濾機制，研判複雜的電子郵件威脅，決定信件的處理流程，提供本公司電子郵件的安全防護。 1. 可調式的垃圾信評分鬆緊值和處理策略。 2. IP 攻擊自動阻斷。 3. 郵址或 Domain 之黑名單阻擋。 4. 可自定義的過濾條件。 5. 內建防火牆可對惡意登入偵測之 IP 進行封鎖。	以郵件系統每週統計阻擋的病毒、詐騙、冒名、廣告及垃圾郵件，過濾可疑信件為因子，分別予以高、中、低三種風險等級區分。

NGFW 防火牆	新世代防火牆服務，與傳統僅能依 IP 與埠位過濾設備不同，能夠在應用層進行深度封包檢測(DPI)，精準辨識並管控各類應用程式流量，其核心特色包括整合入侵防禦系統(IPS)、進階威脅防護(ATP)、惡意程式偵測與沙箱分析，能有效阻擋零時差攻擊與未知惡意程式。同時支援 SSL/TLS 解密與安全 VPN，並提供可視化的流量報表與使用者行為分析，協助公司在維持高效能的同時，強化邊界安全與合規管理。	以防火牆每日阻擋及防護的 Virus、Intrusions、Spyware、Botnets 等威脅項數及流量為因子，計算每月平均威脅值。

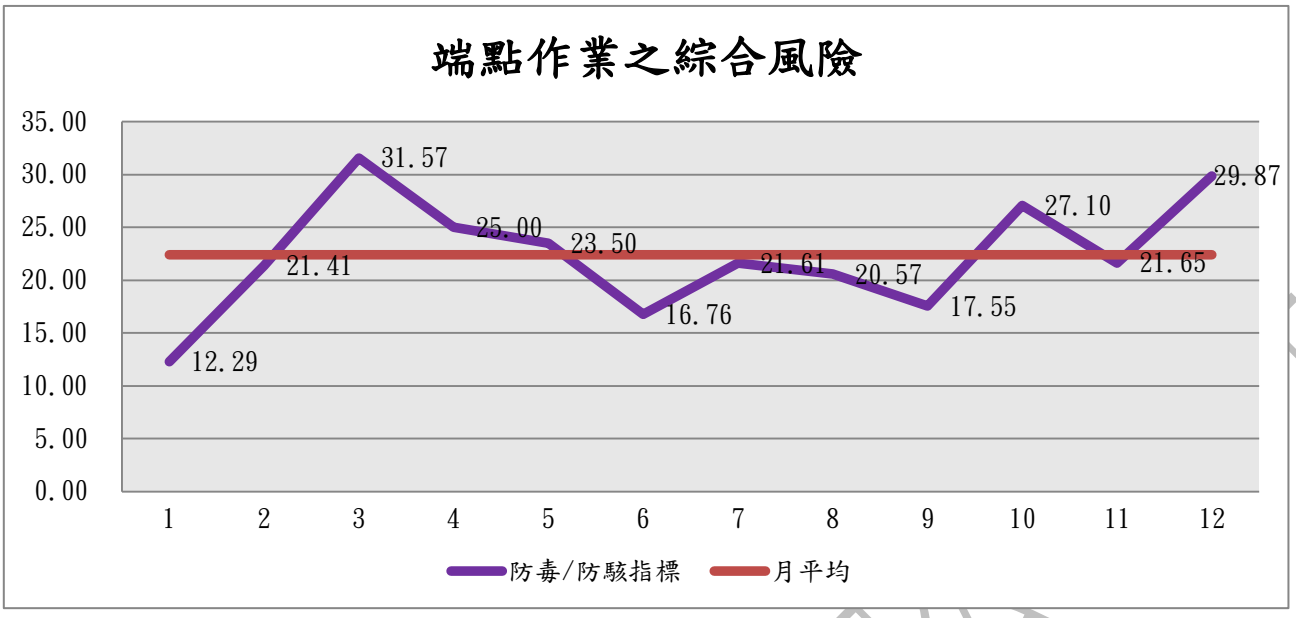
3-3. 月風險值=量化因子之（低風險數月平均值x1)＋(中風險數月平均值x2)＋(高風險數月平均值x3)［＋(嚴重風險數月平均值x4)］

依據2025年之統計數據(請參考6-6.資安防護措施之年度統計數據),依量化因子的風險等級之高、中、低予以轉換計算後匯整於下表，另將量化後的風險值，以折線圖呈現年度的曝險趨勢後。在此使用平均數及標準差，作為觀察風險量度的穩定性指標，當標準差數值越大，代表各月數值與平均數的落差起伏較大，處於較不穩定的環境，風險較高，當標準差數值越小，環境風險較為穩定，風險亦較小；就常態分配的機率分布觀察，若各月的數值比平均值高 1 個標準差之內的範圍，表示環境中有 34%的較高風險，若各月的數值比平均值低 1 個標準差之內的範圍，表示環境中有 34%的較低風險，以此衡量本公司資訊作業之曝險程度及防禦成效。

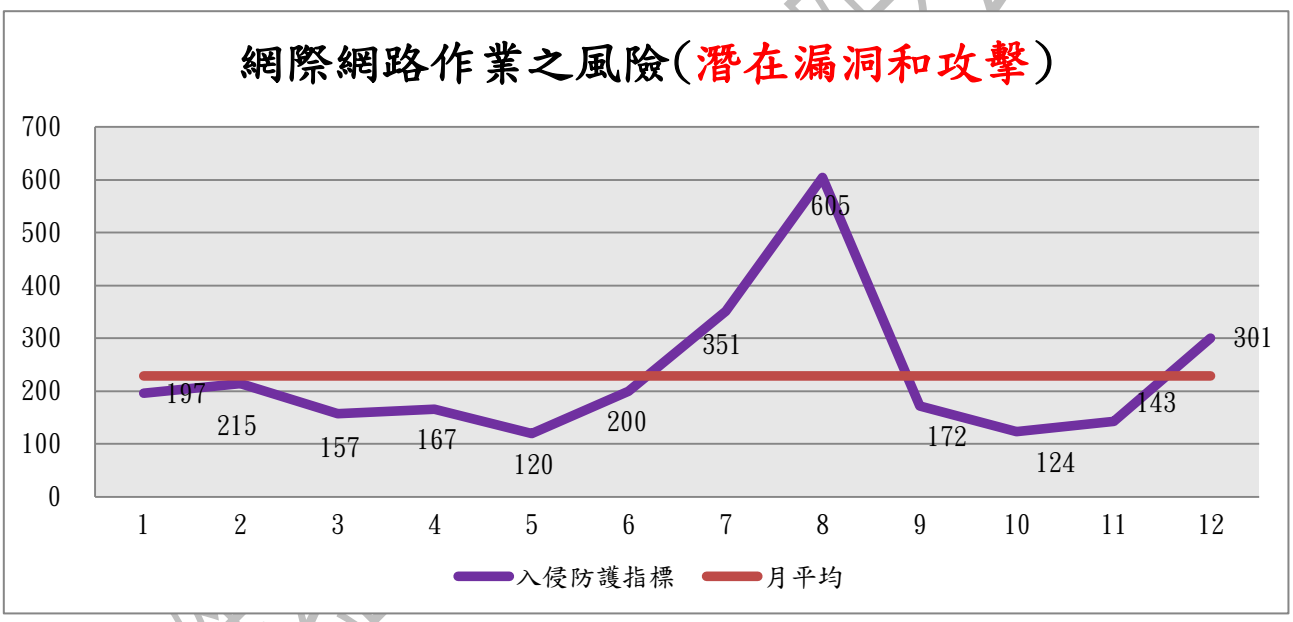
資料來源		端點防毒/防駭	HiNet 入侵防護	弱點掃瞄	郵件威脅	網路作業威脅指數
威脅值	2025 年平均值	22.41	229	11.63	142.70	11.67
	2025 年標準差	5.27	131	8.48	26.53	5.36
月份	一月	12.29	197	26.20	104.00	
	二月	21.41	215		156.75	
	三月	31.57	157	5.60	207.00	
	四月	25.00	167		162.50	
	五月	23.50	120		131.60	
	六月	16.76	200	8.50	123.50	21.10
	七月	21.61	351		160.25	17.00
	八月	20.57	605		145.20	8.60
	九月	17.55	172		121.75	6.82
	十月	27.10	124		130.00	6.28
	十一月	21.65	143	6.20	153.60	14.14
	十二月	29.87	301		116.25	7.74

[註]1.紅字為高於平均值，紅底紅字為高於一個標準差，綠底綠字為低於一個標準差。
2.網路作業威脅指數於更換防火牆後，從 6 月份開始統計。

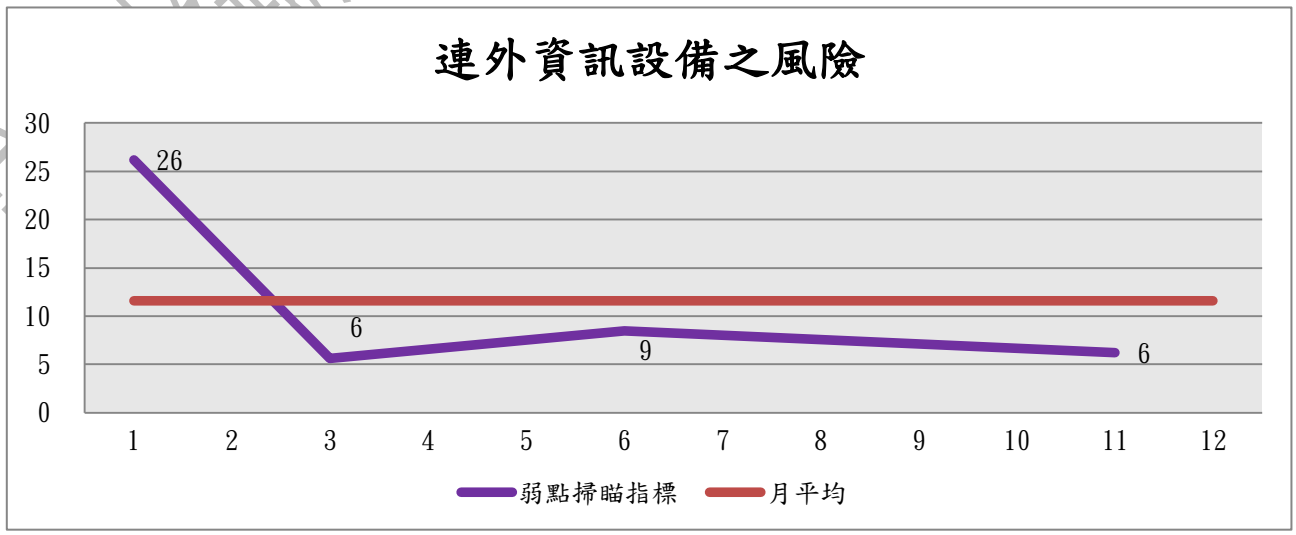
3-3-1. 端點防毒/防駭：阻擋 IP、郵址或域名之黑名單及企圖不明之長時偵測來源趨勢。



3-3-2. 入侵防護：在網際網路的連線風險趨勢。



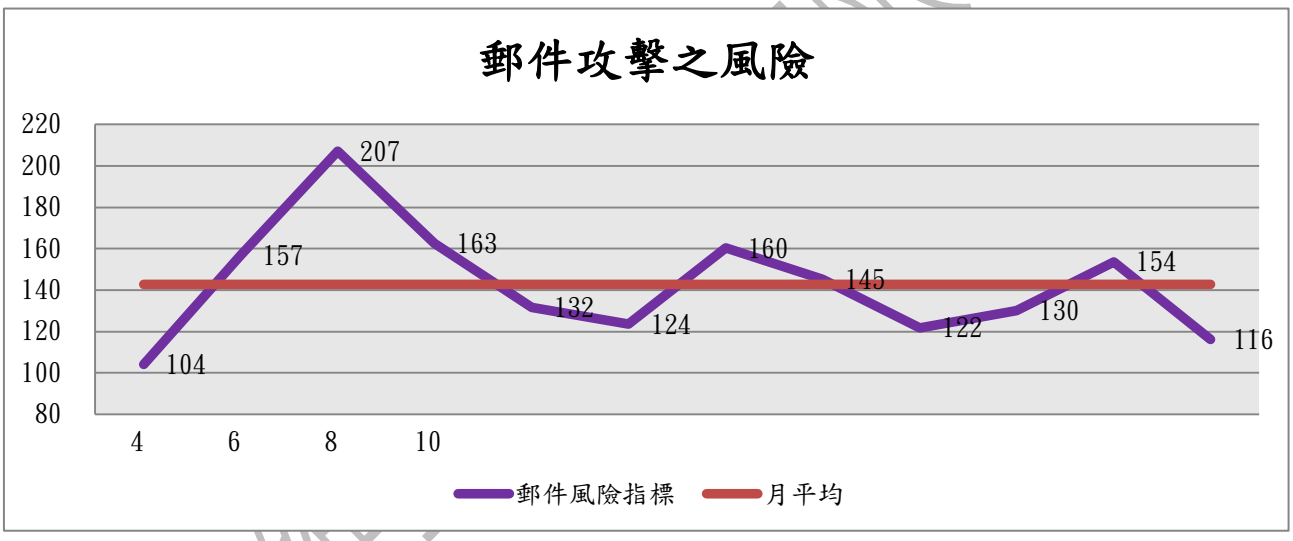
3-3-3. 弱點掃瞄：連外設備之弱點風險趨勢及威脅較高的弱點項目列示如下。



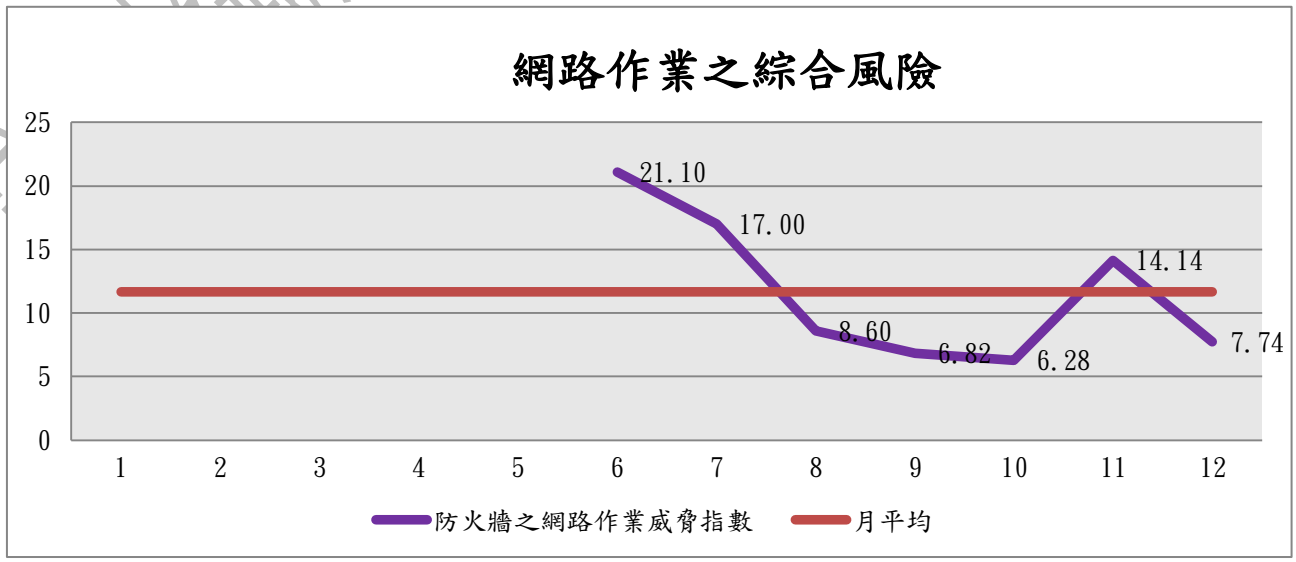
所列示之弱點，多為對外提供相關服務時，所必須開放的連接埠，為必須承擔之風險。

項次	弱點名稱	風險等級
1	SSL Version 2 and 3 Protocol Detection	高
2	SSL Medium Strength Cipher Suites Supported (SWEET32)	中
3	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	中
4	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	中
5	TLS Version 1.0 Protocol Detection	中
6	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	中
7	SSL Self-Signed Certificate	中
8	SSL Certificate Cannot Be Trusted	中
9	SSL Certificate Signed Using Weak Hashing Algorithm	中
10	HTTP TRACE / TRACK Methods Allowed	中

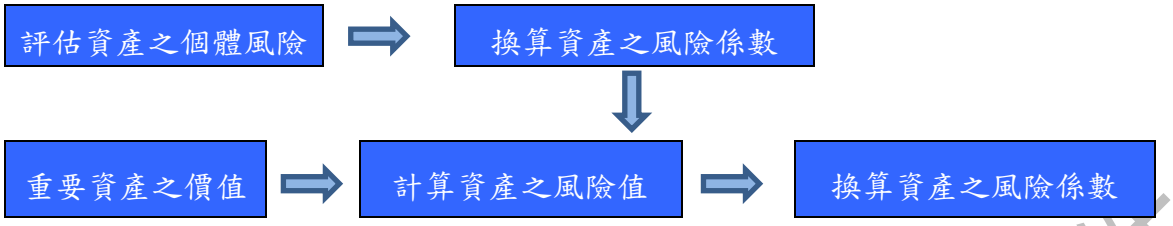
3-3-4.郵件伺服器防禦：電子郵件往來的作業風險趨勢。



3-3-5.防火牆(TZ-270)資安指標：各項應用程式於網路執行之綜合風險趨勢；於更換防火牆後，從六月份開始統計。



四、 資安威脅之風險評估(定性評估)



4-1. 對於未來的資通訊的安全風險分析，本公司乃針對資訊財產當遭受到威脅時，在考慮資訊環境經控管後，假設資產發生功能失效時，其脆弱性對公司營運上產生之風險水準評估；關於風險評估項目、計算公式及相關事項說明如下：

4-1-1. 資安風險評估乃考量資訊財產的價值、威脅-弱點事件之可能性及衝擊性等項目，資產價值之評估標準請參考 6-1. 資產價值評估量表，各威脅事件的可能性及衝擊性之評估標準請參考 6-2. 可能性及衝擊性評估量表。風險值(VaR：Value-at-Risk)乃依據威脅發生之可能性及衝擊性程度評估給分，所得風險值為已採取回應管控措施之後的殘留風險(Residual Risk)，而非資產之固有風險。

4-1-2. 進行評估之資訊財產，可能面臨之威脅-弱點事件分為下列五類，請參考 6-3. 威脅及弱點對應表；因各類資產之威脅事件項數不一致，在評估完 6-4. 單一資產的個體風險值(R_T)，需再除以資產所屬類別的總風險值(R)，換算為風險係數(R_C:Risk coefficient)，以取得相同的比較基礎，之後再計算風險等級。

資產類別之總風險值(R)＝威脅項數x可能性最高值 3x衝擊性最高值 3（如下表）
資產風險係數(R_C)＝該資產個體風險值(R_T)÷所屬資產類別之總風險值(R)

資產風險類別	說　　明	威脅項數	R.總風險值
H.實體資產風險 (Hardware risk)	包含缺少實體安控或環境監控不足等所產生之風險。	18	162
S.軟體資產風險 (Software risk)	包含系統設計、維護、操作不當等所產生之風險。	18	162
I.資訊資產風險 (Information data risk)	包含資料、文件之建立、維護、控管、傳遞不當等所產生之風險。	10	90
T.支援服務資產風險 (Technical support services risk)	包含容量不足或維護之不當等所產生之風險。	3	27
E.人員資產風險 (Employees risk)	包含因人員有意或無意行為、安全訓練不足等所產生之風險。	12	108

4-1-3. 資產價值(W)＝資產之機密性(C)＋完整性(I)＋可用性(A)，三個性質各區分四個等級給分，最高為 12 分，此資產價值已於第 1-3 節估算完成。

4-1-4. 資產風險值(AR)＝資產價值(W)×資產風險係數(R_C)

以資產風險值對照下列風險等級，當資產風險為高風險時，應填寫風險之因應或改善對策，並由資訊或相關單位於年度計畫中提報專案進行改善作業

風險等級(Risk Level)	低風險	中風險	高風險
資產風險值(Asset Risk)	**0.1~4**	**4.1~8**	**8.1~12**

4-1-5. 風險之應對策略分為下列四種方式，詳細說明請參考 6-5.風險應對策略。

Avoid.規避：迴避風險發生的可能性，以完全消除威脅。

Transfer.轉移：將風險由原資產轉嫁由第三方負責承擔，部分的風險仍需由己方承擔。

Mitigate.減輕：在執行前或執行中降低威脅發生的機率或影響，預防損失發生及降低損失的嚴重性。

Accept.接受：必須使用資產或無其他適合策略時，承擔不願或無法轉移的風險。

4-2. 依據上述評估方法，針對資訊財產進行分類及估算風險值於 6-4.資訊財產風險評估表，評估結果彙整如下表：

資產分類	資產名稱	資產價值/個體風險	風險係數/資產風險	風險等級/回應策略	因應/改善對策	處理順序
H.實體資產	伺服器(資訊軟體及資料庫	10/44	0.27/2.7	低/規避	建立異地備份及雲端虛擬主機。	優先
	個人資訊主機	9/27	0.17/1.5	低/轉移	提供遠端連線作業及雲端虛擬主機。	優先
	檔案伺服器	10/45	0.28/2.8	低/減輕	以備品因應。	高
	生產監控相關主機	6/40	0.25/1.5	低/減輕	以備品因應。	高
	網路交換器	7/39	0.24/1.7	低/減輕	以備品因應。	優先
	防火牆	10/47	0.29/2.9	低/減輕	以備品因應。	高
	電子郵件伺服器	10/51	0.31/3.1	低/規避	以鏡射硬碟或舊版郵件主機接替。	優先

	連外網路設備	8 / 49	0.30 / 2.4	低 / 規避	以備援網路因應。	優先
S. 軟體資產	ERP 管理系統	11 / 31	0.19 / 2.1	低 / 規避	從另一伺服器建立作業環境，回復資訊系統。	高
	人事管理系統	7 / 22	0.14 / 1.0	低 / 規避	以備份軟體還原因應。	高
	品質檢驗管理系統	8 / 40	0.25 / 2.0	低 / 減輕	以備品因應。	高
	聚合管理系統	8 / 26	0.16 / 1.3	低 / 減輕	以備品因應。	優先
	生產監控管理系統	6 / 23	0.14 / 0.9	低 / 減輕	以備品因應。	優先
	公司網站	5 / 25	0.15 / 0.8	低 / 轉移	租賃網頁主機暫代。	普通
I. 資訊資產	電子資料檔案	10 / 28	0.31 / 3.1	低 / 規避	將電子資料檔備份在 NAS 主機中，檔案遺失或損壞時皆從 NAS 還原。	優先
T. 支援服務資產	不斷電系統	5 / 6	0.22 / 1.1	低 / 轉移	將不斷電系統 By Pass，改時使用市電。	普通
	資訊機房溫控、消防設施	5 / 9	0.33 / 1.7	低 / 轉移	使用其他散熱設備(如電風扇、手持式滅火器)。	普通
	資訊軟硬體支援服務廠商	7 / 5	0.19 / 1.3	低 / 轉移	平日保持多廠商之採購政策，維繫服務關係，保持緊急聯絡之管道。	優先
E. 人員資產	重要作業執行人員	7 / 22	0.20 / 1.4	低 / 轉移	落實工作輪調及建立代理人制度，運用人力派遣。	高

五、 結論

5-1. 本公司於 2025 年度之重大資安事件統計如下，對業務及財務並未產生影響。

月份 統計項目	1	2	3	4	5	6	7	8	9	10	11	12	月平均
營業額 (單位：百萬元)	196	178	225	225	214	170	170	144	138	149	150	154	176
停工一日之損失營業額	6	6	7	8	7	6	5	5	5	5	5	5	6
發生重大事件次數	0	0	0	0	0	0	0	0	0	0	0	0	0
重大事件之損失天數	0	0	0	0	0	0	0	0	0	0	0	0	0
重大事件之損失金額	0	0	0	0	0	0	0	0	0	0	0	0	0
重大資安事件年度損失	$0												

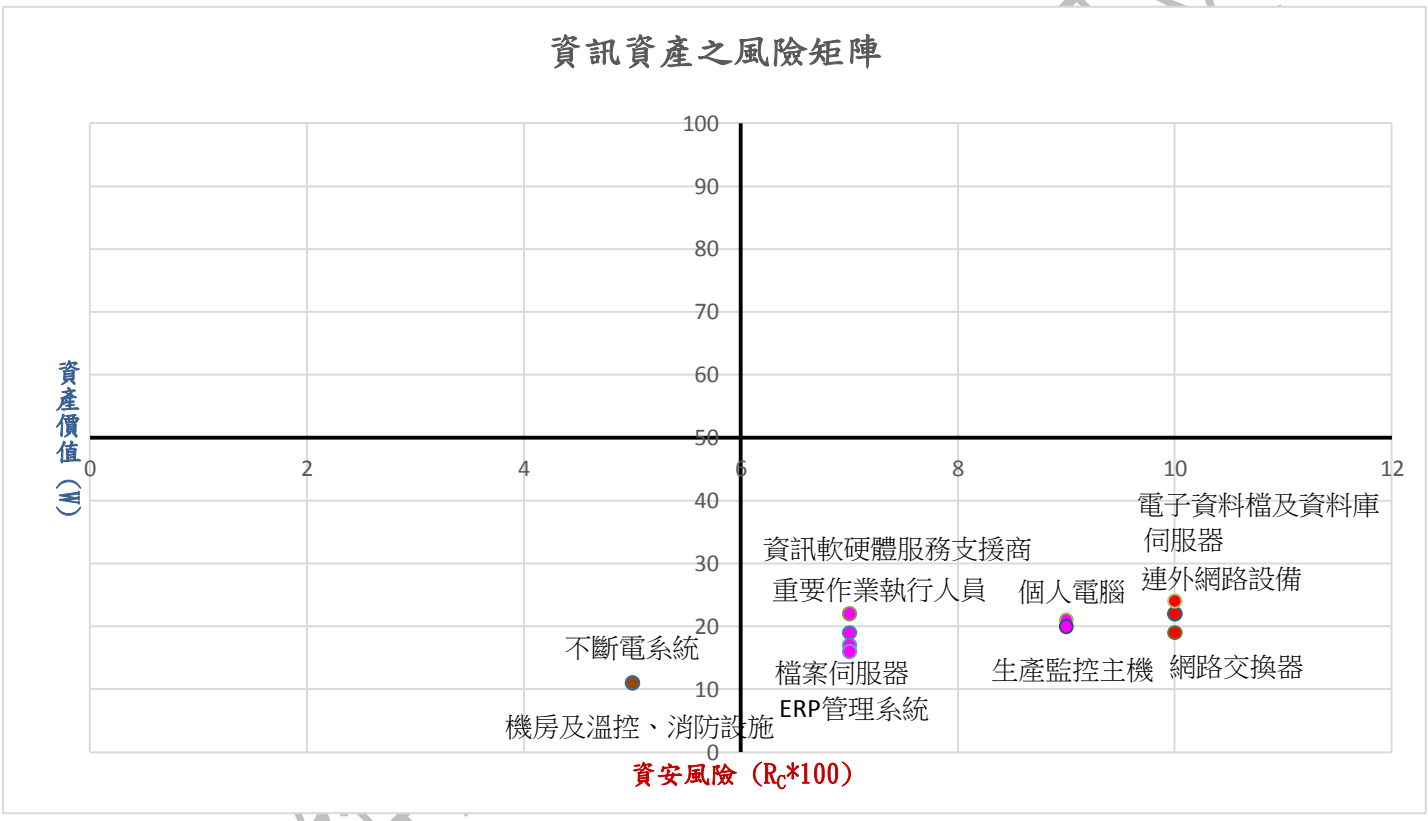
5-2. 從已採取的各項資安防護措施之 2025 年風險量化數據得知，本公司之資訊環境具一定程度之網路作業風險，各月份之風險值，除了在網際網路的連線風險逐月攀升和有少部份之偏離之外，其餘大多趨近於平均值，起伏多在一個標準差之內，表示外在的網路連線或網頁內容雖有越來越多的偽裝或未採用安全的設計技術，但各項防護措施均能發揮其功效，阻擋各種不當的網路作業，再加上內部控制上的各類管控作為，使整體風險控制在穩定的狀態；基於上述評估結果，認為本公司於 2025 年度在資訊安全維護效果、防禦措施之可靠性、資訊內部控制作業程序和方法之設計及執行係屬有效，其能確保資訊安全政策之落實。

5-3. 對於未來的資通安全風險，雖評估後整體資安處在低風險的位階，但對節節升高和變異精進的資安威脅，謹抱持”只有更好、沒有最好”的防禦心態，立即積極做好防範措施；以下從 6-4.資訊財產風險評估表，再個別分析發生可能性、影響性及資產風險相對偏高之項目如下，做為短期上應關注的焦點。

資產風險類別	發生可能性偏高的威脅	影響性偏高的威脅	風險偏高的資產
H.實體資產	1.地震 2.電力供給失能 3.技術失能	1.火災、破壞(含戰爭) 2.水災、偷竊 3.未授權存取資料、惡意破壞資料/檔案	1.電子郵件伺服器 2.連外網路設備 3.防火牆
S.軟體資產	1.誤傳或傳輸錯誤 2.作業人員或使用者錯誤	1.竄改或任意變更 2.未授權連線存取、入侵 3.技術失能、委外作業失能	1.品質檢驗管理系統 2. ERP 管理系統
I.資訊資產	1.未授權存取資料 2.作業人員或使用者錯誤 3.作業失能 4.社交工程	1.火災 2.未授權存取資料、作業失能 3.作業人員或使用者錯誤 4.委外作業失能、社交工程 5.冒充、破壞、偷竊	電子資料檔及資料庫

T.支援服務資產	1.中斷 2.誤用	1.中斷 2.誤用	資訊機房溫控、消防設施
E.人員資產	1.未授權軟體變更 2.社交工程	1.未授權存取資料、罷工 2.作業人員或使用者錯誤 3.使用盜版軟體、社交工程 4.詐欺、破壞、竄改或任意變更	重要作業執行人員

5-4. 從 4-2.各類資訊財產的價值及未來遭受之威脅風險分析，導出下列風險矩陣，對第四象限中價值及對比風險偏高的資產仍應投入高度的控管。



5-5. 美國國家標準與技術研究所(NIST)的網路安全框架(CSF: Cybersecurity Framework)明確定義網路安全風險生命周期為識別、保護、偵測、回應到復原，本公司從系統面建立符合實務之管控制度，從技術面導入可靠且實用之防禦方案，從程序面確實而穩健的監控查核，以落實資安政策之目標，期使資安的脈搏處在穩當且堅韌的頻率中，讓資安風險的生命周期維持良好循環；在面對錯綜複雜、難以預期的資安風險，既有因應方法絕非萬靈丹，但回應風險的策略和方法永遠不嫌多也不嫌晚，未來將加強異地備份機制，及投入評估「託管式偵測及回應」(MDR：Managed Detection and Response)，希望藉由資安委外服務的輔助，由資安的專家提供威脅追蹤及應變諮詢，協助監控網路、分析及回應各種資安事件，即時攔截、阻禦威脅，消除處理上的盲點，以使資安防護措施更加周全和即時。

六、 附件

6-1.資訊財產之價值估量表

6-1-1.機密性(C)量表

6-1-2.完整性(I)量表

6-1-3.可用性(A)量表

6-2.資安風險之可能性及衝擊性評估量表

6-2-1.可能性量表

6-2-2.衝擊性量表

6-3.資訊財產之威脅及弱點對應表

6-3-1.實體資產(Hardware)

6-3-2.軟體資產(Software)

6-3-3.資訊資產(Information data)

6-3-4.支援服務資產(Technical support services)

6-3-5.人員資產(Employees)- 重要作業人員、系統管理者、設備管理者、廠商工程師等。

6-4.資訊財產風險評估表

6-5.風險應對策略

6-6.資安防護措施之年度統計數據

6-6-1.防駭統計表

6-6-2.入侵防護統計表

6-6-3.弱點掃描統計表

6-6-4.郵件防護指標統計表

6-6-5.防火牆網路防護統計表