臺灣證券交易所109年度研究報告提要表			填表人：徐子浩 填表日期：109 年 12 月 28 日
研　究　項　目	封閉網路環境下之系統維運管理框架研究		
研　究　單　位 及　人　員	電腦作業部 徐子浩	研究 時間	自 109 年 1 月 1 日 至 109 年 12 月 1 日
報　告　內　容　提　要			

(一)研究內容重點

本文前半部將介紹封閉網路環境所面臨的維運管理困難及挑戰，及未能有效回應挑戰時將造成的資訊安全風險；後半部將針對各項維運挑戰擬定相關管理措施與規劃防護機制，並提出能強化資訊安全防禦措施同時兼顧維運管理彈性的方案。最終希望提高系統可用度、改善使用者操作經驗、縮短異常事件反應時間，更重要是透過封閉式網路環境，隔絕大部分的惡意攻擊，將有限資源配置在重要的防禦閘道，並持續針對內部環境合規性進行監控。

(二)結論與建議事項

封閉網路維運管理團隊最常遇到的挑戰，便是在現行架構的穩定與新興技術的便利之間拉鋸取捨，但對許多關鍵基礎設施單位而言，所面臨的威脅與所需的防護措施遠高於法令、法規的要求。可預見的是，引進新技術缺乏法源強制性，可能面臨內部使用者反彈或消極抵抗，抑或是管理階層對於引進新技術的必要性產生疑慮。本研究建議，各級單位如採用封閉網路架構保護關鍵基礎設施，除應滿足法令、法規及所屬行業別要求的安全標準外，更可將 NIST CSF 與 CIS CSC 的資安維運管理框架納入考量；實際措施可參考本研究第五章「封閉網路的安全維運管理關鍵控

制措施」所提及之內容：1.具備自動化資料檢疫與交換的實體隔離-透過單向網路、2.零信任安全架構、3.日誌分析、事件告警與報表系統、4.具備實體隔離特性的遠端訊息查看機制。

隨著資通安全法的實施，代表政府單位對資訊安全的重視與決心，臺灣證券交易所身為國家關鍵基礎建設的一環，更需持續研究新趨勢與新技術、逐步提升資訊安全能量，方能如同鴨子划水般從容面對各種未來風險及挑戰。

附註：一、報告內容提要應包括下列二部分：

(一) 研究內容重點

(二) 結論與建議事項

二、本提要表須附電子檔