壹、前言

隨著資訊科技的發展，網際網路的應用大幅改變人們的生活，而軟體系統已成爲我們每天經常接觸的事物之一，舉凡是收發郵件、訂購物品、資料搜尋等行爲，軟體系統的應用已經深入我們的生活當中，然而由於軟體系統特性的改變，再加上軟體系統環境的安全性不足以及駭客威脅日益增加，導致軟體系統的機密性、完整性以及可用性的安全性目標一再遭受到破壞，無論是企業的商譽、資產或是個人的隱私資料，隨時都有被破壞及竊取的可能性。

爲提升軟體系統的安全性，許多廠商開始從網路層的防護設備著手，包含防火牆、防毒牆、入侵偵測系統、入侵防禦系統等，都是設計用來解決可能面對的威脅，然而這些架設在網路層的防護措施，僅能針對 HTTP 的封包進行有限地監控及過濾，對於已加密的網路封包並無法探測其內容，因此對於因爲軟體系統本身的的弱點所產生的漏洞無法進行阻絕，導致資訊安全事件發生機率居高不下。

由於軟體系統的普遍性與現今網路設備防護的脆弱性，因此有學者及組織提出在軟體開發的過程中，將安全性的因素植入開發流程，採用安全軟體開發生命週期（Secure Software Development Life Cycle, SSDLC），從初始的需求階段到軟體維護階段，都加入安全性措施，以用來加強以及確保軟體系統能夠達到安全性目標，像是在執行階段使用的白箱（White-Box）測試方法，或是在測試階段使用的黑箱測試（Black-Box）等方法。就軟體成本開發成本考量，若能愈早修補軟體系統的弱點，所付出的開發成本將會相對降低。安全性問題的修正相當昂貴，而且會拖延研發的進度，修正軟體系統安全性弱點可能會產生的成本如表 1 所示（Howard、Leblanc、林正平，2006）。

表 1
軟體系統安全性弱點修正可能產生的成本

項次	可能產生的成本	項次	可能產生的成本
1	整合的成本	8	將程式公布到網站的成本
2	工程師發現問題程式碼的成本	9	撰寫支援文件的成本
3	測試人員修正程式碼的成本	10	處理不良公共關係的成本
4	測試人員測試修正程式的成本	11	失去生產力的機會成本
5	測試修正設定的成本	12	消費者運用修正程式的成本
6	建立並測試國際版本的成本	13	損失收益的潛在成本
7	修正程式的數位簽章成本	14	頻寬及下載的成本

圖 1 爲發現安全性漏洞的階段與修正漏洞之相對成本關係，由此圖可以清楚瞭解，在軟體系統維運階段所耗費的漏洞修補成本，將是需求及設計階段修補漏洞所需成本的百倍以上，表示在軟體開發生命週期中，愈早修正漏洞，所需的相對成本愈少（行政院研究發展考核委員會，2009；Goertzel, Winograd, McKinley, Holley, & Hamilton, 2006），而付出的成本愈少，軟體系統專案的成功率也能相對提升。

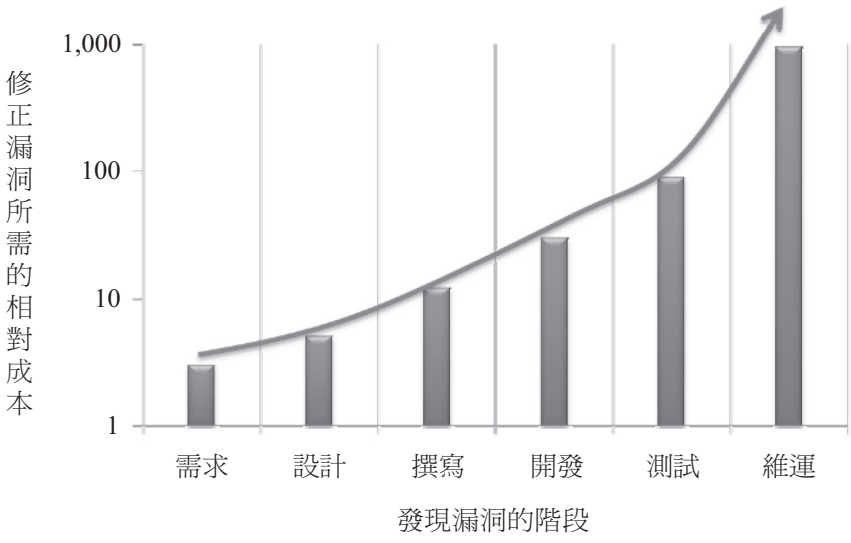

圖 1　發現並修正軟體漏洞之相對成本

有鑑於軟體系統的安全性以及成本開發與軟體系統導入軟體開發生命階段有相對應的關係，因此，本研究將探討目前常見的安全軟體開發生命週期最佳實務（best practices），並以風險管理的角度檢視及瞭解各個最佳實務設計階段所實施的安全性活動以及內容，藉以提出更具完整性的安全軟體開發生命週期之設計階段。

貳、文獻探討

一、軟體系統安全的目標

依據美國國家標準技術研究院（National Institute of Standards and Technology,