2014 數位科技與創新管理研討會
論文編號：76
資通安全組

以事件偵測機制改善電子商務個資安全之研究

賴森堂　羅翊萱　　實踐大學資訊科技與管理系

摘　　要

在網路與資訊的年代，日常各項活動都應與網路適度結合，透過電子商務(Electric Commerce) 進行的商業交易行為與活動更是熱絡。電子商務具備網路的優勢，提昇組織與企業許多效益及競爭力，卻也隱含許多待改善的問題和缺失，其中又以交易資訊與個人資料安全對於組織及利害關係人的影響最大。為改善電子商務系統個人資料的安全性，本文探討各種安全事件的防範與偵測方式，且剖析多項事件偵測方法的優劣。針對事件偵測方法的劣勢與不足，本文於電子商務系統環境與關鍵模組介面植入資料搜集器，規劃一套安全事件偵測機制(Security Event Detection Mechanism, SEDM)，SEDM 對於異常事件具備及時分析能力與處理效率，且以事件識別法則確認與判斷安全事件，適時提出安全事件補救措施，具體降低電子商務個人資料的安全風險。

關鍵字：電子商務、安全事件、事件偵測、個人資料安全、SEDM

2014 數位科技與創新管理研討會
論文編號：76
資通安全組

A Study on the Event Detection Mechanism for Reducing E-commerce Personal Data Risk

Sen-Tarng Lai, Yihsuan Lo

Department of Information Technology and Management, Shih Chien University

stlai@mail.usc.edu.tw, bonnie790308@gmail.com

Abstract

In the Internet and information times, the daily activities must be combined with the network, the business transactions and activities through e-commerce is carried more popular. E-commerce system has the advantage of network, enhance organizations or companies many effectiveness and competitiveness. However, it also existed several issues to be improved and deletions, which went transaction information and personal data security have high impaction for organizations and stakeholders. To improve the personal data security of e-commerce system, this paper discusses the methods of security events prevention and detection, and surveys the shortages of detection methods. For the shortages of event detection methods, the paper in the e-commerce system environment and module interface implanted data collection devices, planning the security event detection mechanism (Security Event Detection Mechanism, SEDM). For abnormal events, SEDM has timely analytical ability and efficiency, and to use the event detection rules to judgment the security events. Security events remedial measures can be timely proposed to reduce the security risk of e-commerce of personal data.

Keywords: e-commerce, security event, event detection, personal data security, SEDM

1.緒論

在網際網路與數位化的年代，促使各種追求高效率與高效益的活動都必須與網際網路適當的結合，如此才能在網路熱潮下提昇其競爭力以延續其生存空間，商業的各項行為與活動一直都是追求高效益與高利潤的先驅，因此，配合網際網路而改變的各種商業行為與活動，更是積極且快速的被開發與推動，凡是透過網路進行的商業活動都統稱電子商務(Electric Commerce; EC) [5,10]，根據「新網路時代電子商務發展計畫」之調查，如圖 1 顯示，2011 年我國 B2C 市場規模為新台幣 3,226 億元，預測至 2013 年可望達到新台幣 4,781 億元[19]。而依據研究調查機構 eMarketer 的調查數據顯示，全球電子商務銷售首度超越 1 兆美元，且預估 2013 年電子商務銷售將成長至 1.3 兆美元，其中亞太區銷售額將超越北美。不過，在 Gartner 的研究報告指出，由於消費者擔心安全上的問題，使得電子商務的銷售額因而短少 20 億美元之多[24]。從以上的研究報告中，可以得知電子商務銷售額將持續的成長，而影響銷售額成長的關鍵因素就是電子商務的安全性。

圖 1　2008-2013 年台灣 B2C 市場規模

電子商務具備了網路的優勢，在各式各樣商業行為與活動中，提昇許多的效益與競爭力，不過，卻也隱含了許多急需改善的問題和缺失，包括執行效率、網路交易安全、系統運作的特性及配合環境調整與異動的維護能力等問題，所涉及的因素非常多，其中又以個人資料與交易隱私資訊的安全對於組織及利害關係人的影響最大，其衝擊已經超越功能與效能的需求，Pew Research Center 調查顯示，有 18%的美國民眾曾遭遇個資外洩，包括社會安全碼、信用卡資訊，或是銀行帳號資訊，美國最近這半年的資料外洩事件頻傳，例如零售業者 Target 在去年底傳出有 1.1 億筆的客戶資料外洩，精品百貨 Nieman Marcus 也有 110 萬筆的客戶資料外洩[14]。另外，知名專賣女妝產品網購平台「86 小舖」，疑似個資外流，造成一個月內有 83 名消費者遭到歹徒以取消分期付款手法詐騙得逞，估計總共財損金額約 300 多萬元，電子商務個人資料安全性是一項必須重視的議題。

電子商務出現重大的安全事件幾乎都非主動發現的，大部份異常事件屬於被告知後才發現的，因此，一旦確認系統被入侵或個人資料外洩等事件，對組織所造成的損失以及對用戶所形成的衝擊，是難以評估與預期的，即使後續採取耗費人力與成本的修補作業或改善措施，也無法有效彌補，為此，本文針對如何有效偵測安全事件，以提昇電子商務個人資料的安全性進行探討，於電子商務安全事件發生後，主動偵測安全事件且即時提出後續的補救措施，以「主動偵測且立即處理」的概念，來降低電子商務安全事件的重大損失。

本文共分成五節，第二節將探討電子商務與個人資料的關係及電子商務系統的安全議題及其特質。第三節說明提升電子商務多層式安全防範措施，從電子商務開發作業、例行檢測作業與偵測作業三個方面進行探討。第四節將本文提出的安全事件偵測機制(Security Event Detection Mechanism; SEDM)包括蒐集系統關鍵介面的存取資料，訂定存取資料為基礎之事件識別法則，最後進行安全事件的確認與補救措施，用以及時發現安全事件且透過補救措施。第五章針對本文所提出的安全事件偵測機制(SEDM)進行評估與剖析。第六節將彙整電子商務安全事件偵測方法在降低電子商務安全風險的貢獻，且針對本主題作個結論。

2.電子商務與個人資料的安全

2.1.個人資料保護法的源起及影響力

近年來詐騙案件層出不窮，手法也不斷翻新，不僅造成民眾財產的損失，擾亂民眾正常之作息，甚且威脅到民眾生命之安全。個人資料保護法民國 100 年頒布且於 101 年 10 月實施，主要是為了規範個人資料之蒐集、處理及利用，其目的是為了避免人格權受侵害，並促進個人資料合理利用。而所謂的個人資料，依據全國法規資料庫個資法第一章第二條第一項：「指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料」[16]。

網路與資訊科技日新月異，透過網路作為資料傳輸主要管道日益增加的情況之下，對於各種商業活動與行為都已導入網路資訊化，不過，近年來駭客入侵、間諜軟體、木馬程式、社交工程與釣魚網站等惡意攻擊日漸猖獗，對於網路與資訊環境下的個人資料造成極大的威脅，如何善盡個人資料的保護，更是遭遇相當大的挑戰[17]，觸犯個資法若是足以損害於他人者，可處二年以下有期徒刑、拘役或併科新臺幣二十萬元以下罰金；且有意圖營利者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金[16]。

2.2 電子商務系統與個人資料之關係

網路環境改變了商業交易方式，為電子商務系統帶來許多商機，卻也隱含了難以預期的安全危機。然而，電子商務的各項活動或行為都會涉及關鍵的個人資料與交易資訊，這些重要的資訊成為電子商務安全性的一大隱憂。電子商務系統被駭客入侵，且導致個人資料外洩事件，不僅要接受刑法處分，還可能要賠償用戶隱私權的損失。根據 104 市調中心對於網路購物的安全性及影響調查的結果顯示，有 84%的民眾，擔心使用網路購物而導致「個人資料外洩」，如圖 2 所示，然而，也有 42%的民眾發生過「個資外洩」或遇到「詐騙事件」。近年來，個資外洩以及交易安全的問題更是越來越頻繁，表 1 為個人資料外洩之相關案例及所形成的衝擊，造成個人資料外洩的原因大致為駭客入侵、系統本身安全漏洞與內部人員所為。因此，各大公司無不採取各種方法以避免客戶個人資料因駭客入侵或系統的漏洞而外洩。其中，除了透過防火牆(Firewall)、網路偵防系統(Intrusion Detection and Prevention, IDP)等硬體設備加強網路安全防護外[34,17]，還應該採取弱點掃描工具與滲透測試技術檢測軟體系統與應用程式的安全漏洞與缺失，事先完成修補作業，以降低被駭客

入侵的風險。

圖 2 84%的民眾擔心網路購物個人資料外洩

表 1　個人資料外洩的相關案例

個人資料外洩的企業或組織	個資外洩案例的原因與損失
Adobe	(1) 外洩原因：駭客利用其產品代碼上存在的安全漏洞，進行複雜精密的網路攻擊。 (2) 造成的損失：290 萬名用戶的個資外洩。
美國線上交易付款服務公司 Global Payments	(1) 外洩原因：遭不明駭客入侵。 (2) 造成的損失：上千萬筆 Visa、萬事達、美國運通與 Discover 持卡人的個資外洩甚至遭人盜刷。
南韓爆發國內史上最大信用卡個資外洩	(1) 外洩原因：從事個人信用評等的韓國信用評價公司(Korea Credit Bureau)旗下員工所為。 (2) 造成的損失：超過 1 億筆個資遭到竊取轉賣，受害者多達 2000 萬人以上，連總統朴槿惠、聯合國秘書長潘基文的個資也全都外洩。
內政部網站	(1) 外洩原因：內部作業疏失。 (2) 造成的損失：將志工的個人資料外洩。
中國信託網路銀行	(1) 外洩原因：網路銀行功能未正常運作。 (2) 造成的損失：多達五萬筆個資外洩。

3 提升電子商務多層式安全防範措施

從電子商務開發作業、例行檢測作業與偵測作業三個方面進行探討。

3.1 電子商務的安全需求

當企業或組織規劃的電子商務系統未能注意到安全上的議題時，不但會讓使用者對於該企業或組織所提供的系統產生安全上的質疑，而且，還會大幅降低對於該單位或組織的信任度與系統的使用意願。因此，電子商務系統必須在開發前，就擬訂一套完善的安全需求，以強化系統的安全性[5,10,29]。Holcombe 認為任何電子商務系統都必須滿足四個安全需求[26](如圖 3 所示)：

1. 授權(Authorization)：對於電子商務驗證完成的使用者，須確認該使用者的功能權限。
2. 完整性(Integrity)：在電子商務資料交換的過程中，須確保資訊不會遭到變更或篡改，以確定資訊內容的完整性。
3. 隱私性(Privacy)：在電子商務資料交換的過程中，須避免未經授權人員的接觸及參與，以善加保護用戶的個人資料與交易資訊。

4. 不可否認性(Non-Reputation)：各種電子商務的交易行為中，均能夠具體證明且記錄交易雙方都已經確實收到對方的交換資訊，以達到不可否認性。

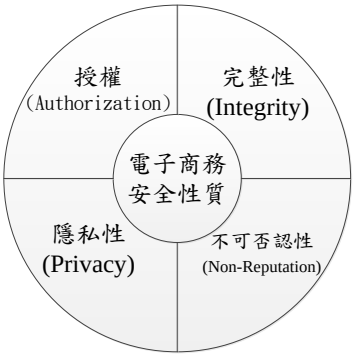

圖 3 電子商務四項不可分割的安全性質

3.2 電子商務的例行檢測作業

電子商務系統必須擬訂一套例行性的安全測試作業在安全事件未發生前，即時修補安全漏洞，以確保電子商務能夠在安全的環境中正常運作，安全測試作業大致分成弱點掃描、滲透測試以及人工檢視三種方式[11]：

1. 弱點掃描(Vulnerability Scan)：屬於系統內部安全漏洞與缺失的檢測作業，可交由電子商務軟體系統維護人員執行，至少應半年執行一次，利用弱點掃描工具的協助找出電子商務軟體系統的安全漏洞與缺失，再由維護人員進行後續的修補作業，免費或開放原始碼的掃描工具包括 NetCat、NIKTO、Paros Proxy 等。由於弱點掃描只能針對程式碼可能存在的安全缺失與漏洞進行檢視，無法達成全面性的安全環境測試作業，能夠處理的範圍與改善的能力較為有限，此外免費的弱點掃描工具出現誤判率過高的狀況，也造成安全漏洞修補人員的一大困擾。為了彌補弱點掃描的缺陷，滲透測試成為安全防範措施不可缺少的重要作業[12,11,27]。

2. 滲透測試(Penetration Test)：是一項正式的安全漏洞與缺失的檢測作業，它是模擬惡意攻擊者的攻擊手法，來去評估整個系統的安全性，而滲透測試一般都委託顧問公司且由專業人員來執行，測試的時間與檢視項目的多寡有關，且至少需要五個工作天以上，完成的滲透測試報告，除了詳述測試的執行過程外，最重要的是完整記錄發現的安全漏洞與缺失，若經費預算之許可，更可以交由顧問公司協助企業或組織進行後續的安全改善措施[11,27]。

3. 人工檢視：使用弱點掃描及滲透測試等檢測作業，或多或少還是會有小部分的漏洞與缺失是沒辦法找出來的，所以，最後需依靠人工針對所列舉出來的電子商務安全清單一一去做審核的工作。Racquel 針對電子商務的安全性提出了人工檢視的清單，其目的是幫助企業或組織提供一個安全且可靠的環境給使用該電子商務軟體系統的客戶，使企業或組織的系統與網站的信任度能夠提升[11]。最後，將弱點掃描、滲透測試及人工檢視針對其特性整理如下表(如表 2 所示)，但是，無論採取何種方式都無法避免誤判或漏判的狀況發生。

表 2 安全測試方法相關特性比較表

測試方法 / 特性	弱點掃描	滲透測試	人工檢視
執行頻率	三個月或半年	半年或一年	依需求
執行時間	短	長	長
成本	低	高	中等
執行人員	維護人員	專業技術人員	維護人員
改善方式	自行改善	顧問公司協助完成	自行改善

3.3 安全事件的偵測作業

資訊系統的軟、硬體設備都是以日誌紀錄(Log)來掌控事件的發生原因。日誌記錄(Log)管理須考量的問題，包含日誌記錄的有效性及正確性、涵蓋範圍、保存期間、產生日誌記錄的原始用途以及企業營運與日誌記錄之間的相關性及必要性[28]。過去，記錄是分散在各個設備，並用不同的形式儲存(大部分為電腦檔案)，而非必要的時候，很少人會去時常查閱日誌記錄檔案，只有在事件發生後，需要知道來龍去脈時，日誌記錄就成為有效的證據來源，協助找出問題的根源，用以還原事件的始末並且找到事件發生的原因；此外還可以判斷異常的行為，進行修訂與調整，防範未然。

電子商務系統應該透過日誌記錄及監測(Log and Monitoring)的方式來保護使用的個人資料。美國國家標準技術研究所(National Institute of Standards and Technology，NIST)電腦安全日誌管理指南提到，日誌記錄管理的基礎架構通常包括三個層次：日誌記錄的產生、日誌記錄分析和儲存及日誌記錄監測[29]。事件日誌記錄用於監測電腦系統及網路環境的運作安全與執行效能，對於資訊系統的安全性與網路資源的效能掌控越來越重要[33,31]。市面上有很多協助事件日誌記錄管理的商品化工具，如 GFI Event Management、Manage Engine Event Log Analyzer、Event Log Explorer、Event Log Viewer、EventLog Analyzer 等，其中，Manage Engine Event Log Analyzer 的分析功能佳，但處理時效性卻較低。這些事件日誌記錄工具主要都在協助使用者進行事件的收集、分析、管理、查詢等功能，由於受到電腦硬體資源的限制，大部分的工具無法達到即時判定異常事件[31]。網路管理系統(Network Management System) 是以「網路設備即時發生的實際事件」為管理基礎，才能準確地了解網路環境的真實狀況，並且有效地建立與其他相關層面的相互關聯性，達到以服務為導向之管理系統[9]。目前有多種的網路管理系統，其中最多企業及校園常使用的商用網路管理系統包含：HP Open-View、Java SunNet Manager、IBM Tivoli NetView 等。現今的日誌記錄及監測(Log and Monitoring,簡稱 L&M)機制大多用來協助找出異常事件，原因為主要受到電腦環境資源的限制，一般 L&M 機制無法達到即時判定異常事件，而網路管理系統是以網路的流量來判斷異常事件，因此可以即時處理異常的狀況，但是它的誤判率相對較高。入侵預防系統（Intrusion Prevention System, IPS）常被當作安全檢查哨，IPS 並不會逐一檢查每個潛在的安全威脅，而是尋找已知的問題與明顯可疑的行徑。表 3 根據現有的安全偵測作業的特性做比較，Log 機制雖然資料收集的很齊全，但是資料量太多，會造成系統處理上的負擔，處理的時間相對於會較長；網路管理系統只

能針對流量判斷，達到即時防範的功效，所以誤判的機率高；然而，入侵預防系統對於設備上的防範，由於它的建置成本偏高，一般的小型機構較少去使用它。安全偵測作業的缺失必須具體的改善，電子商務個人資料安全風險才能有效降低。

表 3 安全偵測作業相關特性比較表

偵測作業 / 特性	Log 機制	網路管理系統	入侵預防系統
優點	資料收集完整	能達到即時防範的功能	即時偵測主動防禦
缺點	收集資料量過多	誤判率高,只針對流量判斷	建置的成本高、不會逐一檢查每個潛在的安全威脅
效率	低	高	中

4.安全事件偵測機制與運作流程

4.1 事件偵測機制的特性

系統幾乎很難避免不發生安全事件，因此，如何及時發現電子商務安全事件且快速採取應變措施，才能有效降低事件造成電子商務的衝擊。用戶個人資料、商品資料、交易過程資訊及交易完成資訊都必須進行完整的備份，當資料遭到破壞或竄改時，可以透過備份機制還原資料與各項交易活動的記錄，才能盡快恢復電子商務的正常運作。運行中的電子商務，最重要的是偵測安全事件，才能有效降低事件的衝擊，為了提昇電子商務系統個人資料的安全性，本節規劃一套安全事件偵測機制(Security Event Detection Mechanism; SEDM)，識別安全事件、確認事件的嚴重性以協助採取後續補救措施。安全事件偵測機制應具備適時的事件分析能力與及時處理效率，為此本文提出的事件偵測機制應包括蒐集系統關鍵介面的存取資料，訂定存取資料為基礎之事件識別法則，最後進行安全事件的確認與補救措施，用以及時發現安全事件且透過補救措施，有效阻止事件持續擴大，適時降低電子商務利害關係人的損失。SEDM 應該具備下面五項特性(參閱圖 4 所示)：

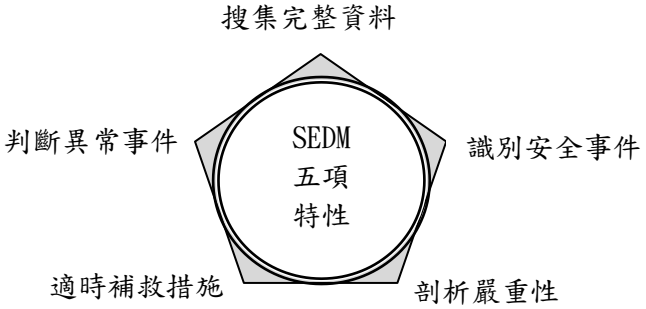

圖 4. SEDM 應具備的五項特性

(1) 能夠即時搜集到完整且關鍵的資料：在電子商務系統環境架構中，剖析出關鍵子系統資料存取介面，植入資料蒐集器(參閱圖 5 所示)，且在電子商務系統功能架構中，剖析出關鍵模組功能資料存取介面，植入資料蒐集器，可以即時蒐集到完整且關鍵的資料。

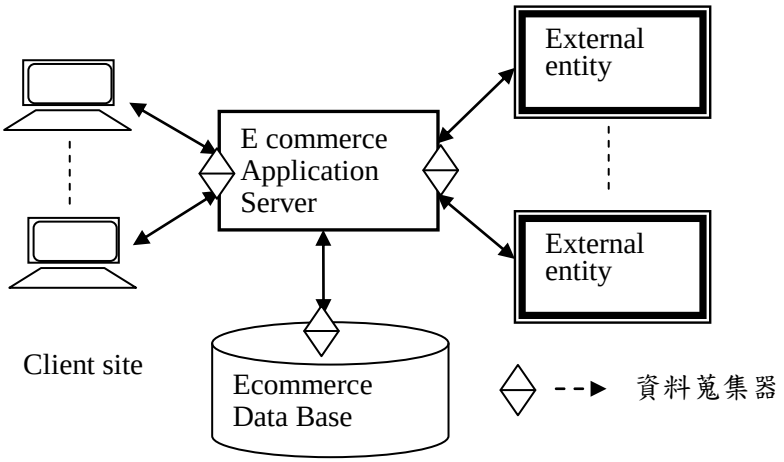

圖 5 電子商務系統關鍵介面示意圖

(2) 及時的判斷異常的交易或作業行為：異常的交易或處理行為很難全面性的考量，導致無法及時判斷，為此，本文採取排除法方式，事先錄製正常的交易行為與維運作業行為，再以排除法找出與正常交易與作業行為互斥的異常行為。

(3) 異常的交易或作業行為識別出安全事件：

(4) 剖析安全事件的嚴重性：依事件影響的範圍與數量確定安全事件的嚴重性。

(5) 採取適時的補救措施：進行安全事件的確認與補救措施，用以及時發現安全事件且透過補救措施，有效阻止事件持續擴大，適時降低電子商務利害關係人的損失。

4.2 事件偵測機制的運作流程

SEDM 為了減少大量資料的蒐集以提昇事件識別與判斷的效率，必須標示電子商務系統的關鍵介面，且插入資料搜集器，於電子商務系統運作過程中，及時收蒐集相關活動與交易資訊，以適時協助安全事件的偵測作業，本文規劃的 SEDM 主要涵蓋三個作業階段(參閱圖 6. SEDM 運作流程)，說明如下：

(1) 資料搜集與事件識別階段：Log 機制涵蓋的類型包含六個層面，有營運流程層面、應用系統層面、資料庫管理層面、作業系統層面、網路環境層面及實體環境層面[6]，其中以應用系統層面、資料庫管理層面與網路環境層面等 Log 紀錄與安全事件的關係較為密切。不過，Log 記錄的資料太多且複雜，不利於及時識別事件。電子商務運作過程中，所有的交易活動或處理行為必須通過關鍵的系統或模組介面，對於每一項交易活動或行為，資料記錄(Data log)將詳細記載且儲存資料存取的人員、行為、時間及項目等內容[29]，為了保存所有的交易活動，資料記錄需要大量的儲存裝置用來儲存與管理蒐集到的資料，同時也需要高效率的查詢能力與高效益的管理能力，才能及時的識別安全事件，且協助後續的補救措施。為此，本階段作業透過關鍵介面蒐集交易活動或處理行為的存取資料，且事先記錄各種正常交易活動與處理行為，以排除法識別

異常的安全事件。

(2) 安全事件確認與判斷階段：事件識別階段已針對蒐集資料進行篩選作業，排除大部分屬於正常狀況或合法行為的資料記錄，為了提高後續事件判斷的效率，應該對於可能是異常狀況或非法行為所留下的資料記錄，則必須進一步採取剖析與分類作業。透過已完成分類的資料記錄及事先規劃的安全事件確認法則，可以有效且快速完成安全事件的確認。本文彙整安全事件的歷史資料與數據、引用安全專家的事件判斷經驗，以及近年來各種個人資料外洩的案例，並參考 OWASP Top Ten 2013[35]，制定出安全事件的確認法則，本文歸類出五類安全事件判定法則：存取量異常、Log 檔案異常、交易行為異常、非法使用者、銀行與客戶通報。

(3) 安全事件判斷與補救階段：確認安全事件後，應該彙集更完整的資料記錄進行進一步判斷作業，用以排除誤判的安全事件且針對安全事件衝擊的狀況及影響的範圍進行判別，能夠具體的區分安全事件的嚴重等級，才能有效地協助後續的補救措施。對於輕微或個別的安全事件，應盡快通知受害以避免使用者遭受更大的損失。對於較嚴重的安全事件，應採取適當補救與因應措施，避免事件持續擴大。若屬於範圍很大且很嚴重的安全事件，應考量暫停電子商務系統的運作，以減低安全事件損失擴大。本階段作業是確認安全事件的嚴重等級，且針對安全事件採取適當的補救措施，有效降低且減少電子商務安全事件對個人資料安全的衝擊。

5.SEDM 之效益評估

本文探討各種安全事件的防範與偵測方式，且剖析多項事件偵測方法的優劣。針對事件偵測方法的劣勢與不足，本文於電子商務系統環境與關鍵模組介面植入資料搜集器，規劃一套 SEDM，對於異常事件 SEDM 具備及時分析能力與處理效率，且以事件識別法則確認與判斷安全事件，適時提出安全事件補救措施，有效阻止事件損失持續擴大，本文所規劃的 SEDM 具備四項優勢，說明如下：

(1) 適時性：本文剖析出關鍵子系統資料存取介面，植入資料蒐集器(參閱圖 5 所示)，且在電子商務系統功能架構中，剖析出關鍵模組功能資料存取介面，植入資料蒐集器，可以即時蒐集到完整且關鍵的交易與活動資料，協助適時識別、確認且判斷安全事件的嚴重性。

(2) 高度調整彈性：近年來，由於個人資料的外洩的比例層出不窮，安全事件更是難以預期，因此，此方法能根據當下安全事件進行調整。

(3) 減少誤判率：SEDM 以排除法進行異常事件識別，再以安全事件確認法則確認安全事件，可以大幅降低電子商務安全事件的誤判率。

(4) 降低安全事件的損失：確認安全事件的嚴重等級，且針對安全事件採取適當的補救措施，有效降低且減少電子商務安全事件對個人資料安全的衝擊。

SEDM 屬於進行中的計畫研究，仍有許待加強的內容，SEDM 後續有兩項需要在不斷進行改善的工作，如下：

(1) 安全事件的誤判率與漏判：依據每年安全事件的歷史資料與數據、安全專家的事件判

斷經驗，及近年各種個人資料外洩的案例不斷更新與調整，以幫助降低 SEDM 誤判率與漏判之情形。

(2) 安全事件確認法則的調整：由於個資外洩的案例越來越多，法則上的制定能夠依當下的狀況作調整。

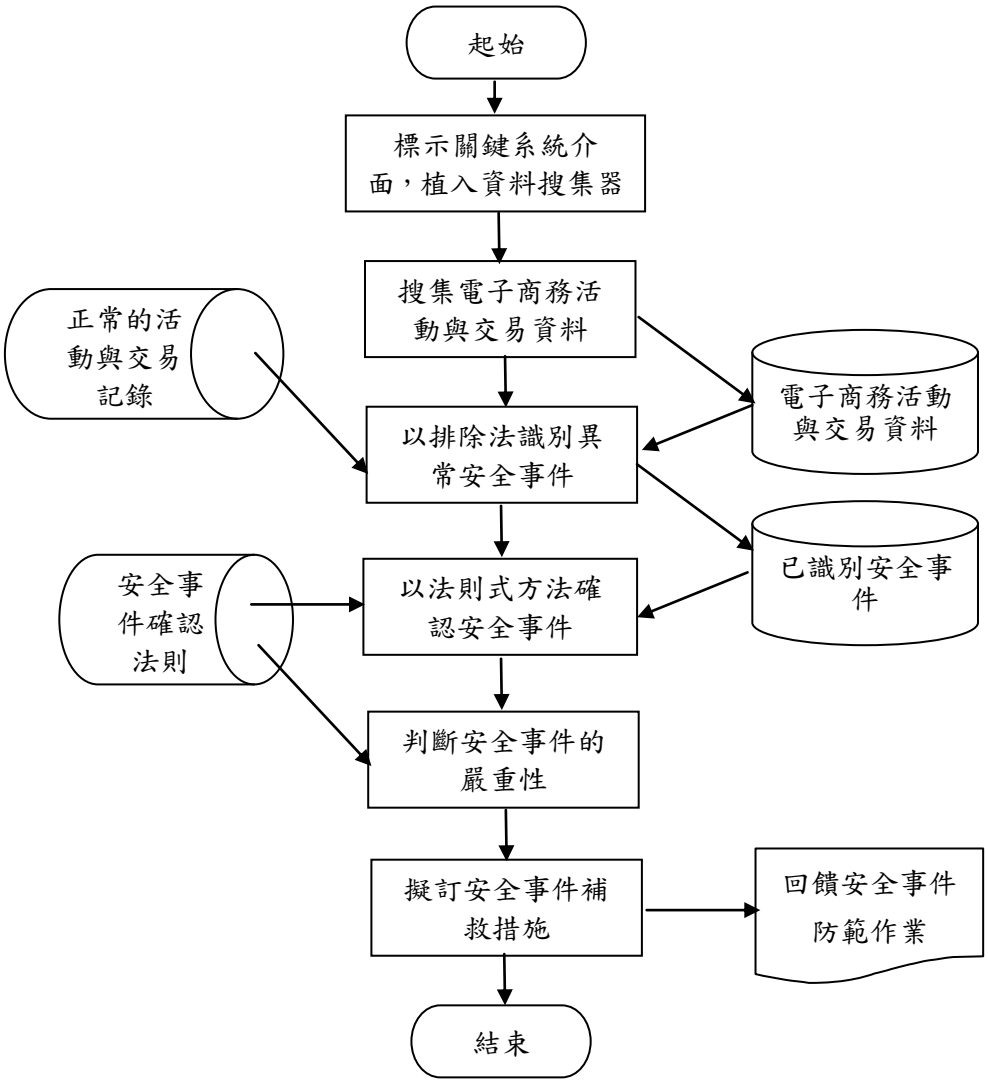

圖 6. SEDM 運作流程圖

6.結論

網路與資訊科技日新月異，的交易行為及金額更是逐年持續增加，人們的日常生活幾乎無法擺脫電子商務的應用範疇，也因此電子商務個人資料的安全性成為一項值得深入探討與重視的議題。本文探討多層面電子商務系統安全性改善方法，其中安全事件偵測作業存在許多缺失，包括蒐集的資料非常龐大，不僅浪費資源且無法適時判斷事件，缺乏一套識別與判斷法則，不易評估事件嚴重性，誤判率太高，影響後續補救措施。為了改善偵測作業缺失，以提昇電子商務個人資料的安全性，本文規劃一套安全事件偵測機制(SEDM)，識別電子商務安全事件、確認事件的嚴重性以協助採取後續補救措施。SEDM

達成的下面三項優勢：

1. 透過關鍵介面的資料蒐集器，可以及時掌控重要的交易與活動資訊，適時發現電子商務的異常狀況。
2. 以法則式方法進行事件識別、剖析與判斷等步驟，具體降低安全事件的誤判率。
3. 可以依安全事件的嚴重性，協助採取後續補救措施。

參考文獻

1. 王立柏、張世元、藍俊哲，個資法上路-IT 部門的衝擊與因應，中華技術，第 97 期，第 134-141 頁(2013)。
2. 呂崇富，網路規劃與管理實務，學貫行銷股份有限公司(2009)。
3. 陳翔，網路安全事典書，商翼資訊股份有限公司(2001)
4. 陳政龍，軟體開發之資訊安全管理問題探討，資通安全專論(2008)。
5. 梁定澎，電子商務理論與實務，華泰文化事業公司(2000)。
6. 葉威廷，軌跡資料儲存技術簡介，漢昕科技(2013)
7. 劉文良，電子商務概論特訓教材，基峰資訊股份有限公司(2004)。
8. 劉若芬，認識個人資料保護法，國立台灣大學計算機及資訊網路中心電子報 http://www.cc.ntu.edu.tw/chinese/epaper/0023/20121220_2304.html(2012)
9. 鄭進興、翁嘉誠，OpenNMS 網路管理實務，上奇資訊股份有限公司(2013)。
10. 賴森堂，「電子商務軟體品質量測模式」，企業管理學報，第 53 期，53-72 頁，國立臺北大學企業管理學系(2002)。
11. 賴森堂，「以弱點掃描結合修補函數提昇 Web App 安全品質」，電腦稽核，第 25 期，158-168 頁(2012)。
12. 蔡明成，「結合弱點掃描的入侵偵測系統」，逢甲大學資訊工程碩士班碩士論文(2004)。
13. iThome，做好 Log 管理，勢在必行：你有做 Log 檔管理嗎？，iThome online。 http://www.ithome.com.tw/privacylaw/article/77107(2012)
14. 陳曉莉，Pew 調查：18%的美國民眾曾遭遇資料外洩，iThome online。 http://www.ithome.com.tw/news/86745(2014)
15. 八成民眾，擔心網路購物遇到【詐騙事件】(2010)，104 市調中心。 http://www.104survey.com/faces/newportal/viewPointCtx.xhtml;jsessionid=70AFB339F7F99D2503FBD40CBF199DD4.svyweb202?researchId=254
16. 全國法規資料庫-個人資料保護法 http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021
17. 黃于珊(2012)，[觀點] 惡魔藏在細節中-- 個資外洩的四大漏洞，網路資訊雜誌 http://news.networkmagazine.com.tw/magazine/2012/08/14/42204/
18. 臺灣個人資料保護與管理制度，http://www.tpipas.org.tw/index.aspx
19. 2012 中華民國電子商務年鑑(2012)

http://ecommercetaiwan.blogspot.tw/2012/10/blog-post_29.html

20. Aprill,A.(2010), A simple guide to creating a knowledge base, Dev Logic Pty Ltd.
21. Colin, H.(2007), Advanced Guide to e-Commerce, LitLangs Publishing.
22. Efraim, T., David, K. & Judy, L (2011), Introduction to electronic commerce, 3rd ed., New Jersey: Prentice-Hall.
23. Efraim, T., David, K., Jae, L., Tin g, P. L. & Deborrah, T. (2012), Electronic commerce 2012 : a managerial and social networks perspective, 7th ed., New Jersey: Prentice-Hall.
24. Evan, S.(2006)," Gartner: $2 Billion in E-Commerce Sales Lost Because of Security Fears", PC Magzine , http://www.pcmag.com/article2/0,2817,2064021,00.asp
25. Gary, M.(2004), "Software Security", IEEE Security & Privacy, vol. 2, no.2, pp. 80–83.
26. Holcombe, C.(2007),Advanced Guide to eCommerce, LitLangs Publishing.
27. John Barchie (2011),Penetration Testing vs. Vulnerability Scanning, http://www.tns.com/PenTestvsVScan.asp
28. Justin, M.(2010), A Dynamically Configurable Log-based Distributed Security Event Detection Methodology using Simple Event Correlator, AIR FORCE INSTITUTE OF TECHNOLOGY, Wright-Patterson Air Force Base, Ohio.
29. Kent, K. & Souppaya, M.(2006), "Guide to Computer Security Log Management.", National Institute of Standards and Technology (NIST) Publication 800-92. , Retrieved from http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
30. Racquel.(2013), 15 Point e-Commerce Security Checklist
https://www.swipehq.com/blog/post/15-point-e-commerce-security-checklist/1395
31. Sabah, A, F. & Fahad, M.,(2012), "Events Classification in Log Audit", International Journal of Network Security & Its Applications (IJNSA), vol. 2, no.2,pp.58-73.
32. SANS Consensus Project, (2007) "Information system audit logging requirements", SANS Institute, http://www.sans.org/resources/policies/info_sys_audit.pdf
33. Sunil, G.(2012), "Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment", SANS Institute InfoSec Reading Room
34. Theresa, K. & Ratika, K.(2009), E-Commerce Security, Washington DC.
35. OWASP Top 10(2013):
https://www.owasp.org/index.php/Top_10_2013-Table_of_Contents
36. Security Issues in E-Commerce (2010):
http://webscience.ie/blog/2010/security-issues-in-e-commerce/