國立交通大學

管理學院（資訊管理學程）碩士班

碩　士　論　文

導入資料外洩防護系統關鍵影響因素之多重個案研究

Critical Factors Affecting the Implementation of Data Loss Prevention System: A Multiple Case Study

研究生：洪彬益

指導教授：楊千教授

中 華 民 國 103 年 5 月

導入資料外洩防護系統關鍵影響因素之多重個案研究

Critical Factors Affecting the Implementation of Data Loss Prevention System: A Multiple Case Study

研究生：洪彬益　　Student：Pin-I Hung

指導教授：楊千　　Advisor：Dr.ChyanYang

國立交通大學

管理學院(資訊管理學程)碩士班

碩士論文

A Thesis

Submitted to Institute of Information Management

College of Management

National Chiao Tung University

In Partial Fulfillment of the Requirements

For the Degree of Master

in

Information Management

May 2014

Hsin-Chu, Taiwan, Republic of China

中 華 民 國　103 年　5 月

導入資料外洩防護系統關鍵影響因素之多重個案研究

研究生：洪彬益　　指導教授：楊千博士

國立交通大學管理學院（資訊管理學程）碩士班

摘要

隨著資訊科技的蓬勃發展，電子商務以及社群媒體的興起，讓資訊的流通更加容易，但也使得傳遞管道變得複雜，導致企業難以控管及防護，造成了不少個人資料外洩的事件發生。而當台灣個資法通過後，如何保護重要個人或者客戶資料，在企業中變得相形重要，因此導入資料外洩防護系統開始受到重視，也是企業未來重要策略之一。

目前導入資料外洩防護系統在台灣仍是少數，所以本研究依據相關研究系統導入成功因素的文獻，並以科技－組織－環境架構為基礎，歸納出「組織」、「專案」、「科技」以及「環境」做為本研究主要架構，並透過多重個案研究法去了解影響導入資料外洩防護系統的關鍵因素，在兩家不同產業類型的本土公司進行個案研究，並以半結構方式深入訪談。而後進行訪談資料的內容分析與歸納，再根據各項證據內容，找出主要影響資料外洩防護系統導入的關鍵成功因素，提供給未來欲導入系統的企業參考。

本研究從二個不同個案，透過訪談系統導入專案相關成員，經資料分析後發現，在組織構面中高階主管支持、資源的取得、內部使用者的參與程度、對資訊政策的了解，是主要影響導入的關鍵成功因素，而專案構面和科技構面中，成員的專業知識、責任的分配、系統品質則是影響導入後系統產出結果是否符合預期效益，而環境構面中，產業相關法規、產業的競爭程度則是影響高階主管制定導入系統決策的積極度。

關鍵字：資料外洩、關鍵成功因素、多重個案研究、科技－組織－環境架構

Critical Factors Affecting the Implementation of Data Loss Prevention System: A Multiple Case Study

Student：Pin-I Hung　　Advisor：Dr.ChyanYang

Master Program of Institute of Information Management
College of Management
National Chiao Tung University

Abstract

With the rapid development of information technology, e-commerce and the rise of social media, are making the flow of information much easier. However, the messaging channel is more complicated in such a situation. It caused a lot of personal data leakage incident and let the enterprises difficult to control and protection for personal data. When the Personal Information Protection Act of Taiwan passed, how to protect important personal or customer information in companies becomes a critical issue. Therefore implement the Data Loss Prevention system began to be one of the important strategic in information security technology.

In the past, implement Data Loss Prevention system in Taiwan is not crucial in many enterprises. So this study bases on information system implement success model and Technology -Organization -Environment architecture to summarize the "Organization", "Project", "Technology" and "Environment" as the main framework of this study, and through multiple case study to understand the key success factors affecting implement Data Loss Prevention system. We use in-depth interviews for two companies which are in different industries. This study applies semi-structured interviews to collect data. Then we conduct the content analysis of interviews, and summarize the results to present the major critical success factors affecting implement Data Loss Prevention system.

Keywords:DLP、Data Loss Prevention、 Critical Factors 、Multiple Case Study、 Technology-Organization-Environment Framework

誌　　謝

從入學開始，就知道在這二年的學業裡有個重要的事要做，能不能拿文憑也是得看它臉色，這件重要的事，就是寫論文，而它也可能會是我這一輩子寫的第一本書。當讀者在閱讀文章的同時，我已經完成它了，所以在這過程中有不少幫助過我的人，希望藉由這短短的幾段字表達我的感謝。

當然首先最要感謝的，我的指導老師－楊千教授。其擁有廣博豐富學問，與精彩的人生歷練和業界多年經驗的傳授，一個字一句話，都能啟發學生的思考，讓我終生受益。還有每個月不辭辛勞，新竹台北往返跑的耿杰學長，在學長的協助指導下，讓我順利的完成了論文的寫作，也使我在論文上能做出小小貢獻。

還有特別感謝在論文中幫助我完成最重要的個案分析章節，受訪個案公司的相關人員們，撥空接受冗長的訪談，並在過程中不吝嗇的分享您們的導入經驗和過程，以及提供相關所需的文件資料，您們的知識以及經驗分享，讓我可以在論文中做出貢獻，讓未來想要導入DLP的公司，了解有哪些必須克服的障礙及會遭遇到的困難點，使其可以順利的執行這重要的資訊安全政策。

另外要感謝的是在一起打拼二年的同學們，尤其是我們KM Labs的成員們，馥玉、凱軒、佳偉，在求學期間互相學習勉勵，讓我在寫作的過程中不孤單。我常覺得唸專班有個大的優點是，除了課業上的學習以外，最重要的就是能認識許多在業界優秀的人，從他們身上學習到不同的思考方式，簡報技巧，生活態度等，這些都是寶貴的人生資源。

最後感謝家人的支持，在口試的前夕，假日和平常日都需努力到很晚，無法抽出時間來陪你們，但也因有你們的支持，讓我無後顧之憂，才能專心的完成這人生重要的著作。而中國人對父母的情感一向表達得很少，在此特別謝謝你們！

目錄

表目錄

圖目錄

第一章　緒論

1.1 研究背景與動機

台灣在 101 年 10 月 1 日通過個人資料保護法後，其求償金額以及刑度都相對提高，個人以及客戶資料的保護成了各大企業的重要議題，特別是牽涉到擁有龐大客戶資料的企業尤其重視，並且首當其衝，所以資料外洩防護系統也開始引起大家的注意，即使這已不是一個新的概念。更不是最近才有的系統。

所以對企業或組織而言，避免資料外洩所引發的連帶成本，就是在第一時間防止資料外洩。所謂資料外洩成本涵蓋法律、調查、管理支出等，以及客戶的流失、商機的喪失、商譽損害，以及資訊熱線及信用偵測等相關成本。因為機密資料不只存在企業內部，因此企業需要部署全面且長期的資料安全策略。於是資料外洩防護（Data Leakage Prevention, DLP）就被視為是未來企業資訊安全規畫的重要系統之一，且在主流大廠大力敲鑼打鼓後，相關資料保護應用的安全業者也開始一一加入此戰局。

根據國外專業研究機構 Ponemon Institute 研究發表的 2013 年全球資料外洩成本調查報告(2013 Cost of Data Breach Study:Global Analysis)指出在 2012 年的資料外洩事件中，有三分之二是肇因於人為疏失與系統故障或損壞，而且跟以往相比更將每筆外洩資料的平均成本推升到 136 美元。在工業科技大國：如德國與美國每筆資料外洩的成本更來到了 199 美元與 188 美元，其中，醫療、金融及製藥等高度嚴格規範的產業，其資料外洩的成本較其他產業高出七成。

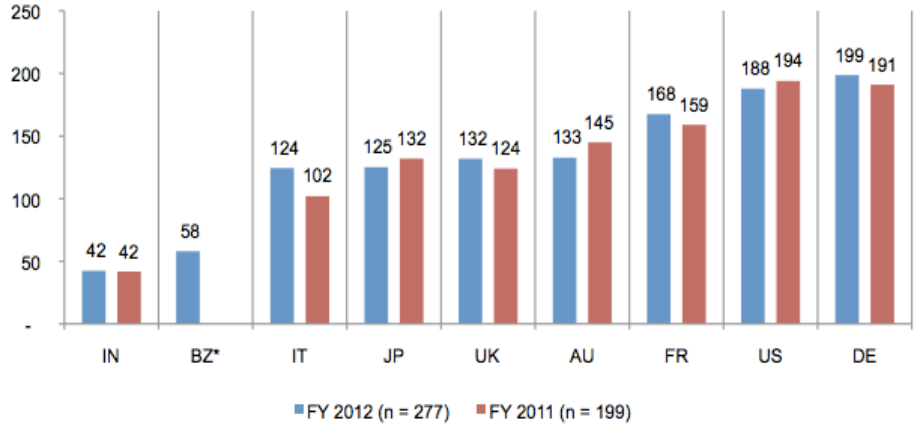

圖 1 過去二年每筆資料外洩的平均成本(美元)

資料來源：2013 Cost of Data Breach Study: Global Analysis

另外報告中也提到，人為的疏失與系統出錯是資料外洩的主要原因。其結果顯示，64%的資料外洩皆肇因於人為疏失和系統錯誤，先前的研究報告則顯示，62%的員工認為在公司以外的場合使用公司資料是合理的，而且大多數員工使用完畢後也從來不會刪除電腦中的資料，這些都有可能是日後資料外洩的主要因素。其研究顯示大部分資料外洩事件有可能是企業內部員工所造成。另外惡意程式(Malware)和網路入侵對全球大部企業造成的損失為最高。其調查結果顯示，有 37%的資料外洩是因為惡意程式與網路攻擊所造成的。

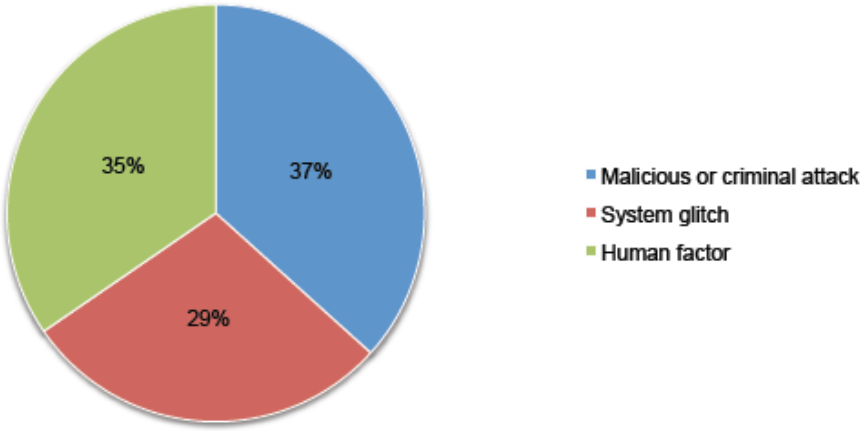

圖 2 資料外洩的主要來源分布圖

資料來源：2013Cost of Data Breach Study : Global Analysis

有鑑於此有不少企業開始重視此問題，也愈來愈願意在預算及經費上投資在資料外洩防護系統上，但由於此建置費用並不低，操作上及使用上也有一定程度上的複雜性。也因為目前導入企業尚未普及，導入成功需要由哪些因素配合，以及要如何評估系統等，這些都是有意導入的企業需要了解的。目前國內尚無研究主要探討 DLP 系統如何導入以及評估、主要影響的關鍵因素的研究，基於以上原因加上作者在資安界的多年經驗，欲透過對客戶的面對面深入訪談來探究此系統現今在組織及企業的應用情況以及所遇到的問題和導入成功因素為何。

1.2 研究目的與研究問題

基於上述研究動機，本研究選擇了二個個案公司，分別屬於二個不同的產業型態，其營業項目產品、獲利模式都截然不同，透過這二個不同的個案訪談及資料分析，來探究企業導入 DLP 的主原因及動機為何？以及主要導入的關鍵成功因素和執行過程中所遭遇到的困難點,和管理決策和導入成效是不是相互影響等問題,一一剖析和了解現象，提供將來需要導入 DLP 系統的企業或組織作為參考。

為達上述研究之目的，本論文以個案研究的方式探討以下問題：

1. 企業對資料外洩防護系統是否建置的主要因素為何？
2. 不同產業的以及企業文化是否會對系統的認知有差別？
3. DLP 系統導入策略是否會影響效益？
4. 高階主管的支持以及專案人員的程度與 DLP 資料外洩防護系統導入的關係？
5. 政策執行力以及全體員工是否有共識，對於系統導入是否有關鍵性的影響？
6. 不同的影響因素是否有相對應的關係？
7. 企業如何評估 DLP 系統導入效益？

1.3 研究流程

本研究之研究流程首先主要了解在資料外洩系統導入時，有哪些情況會影響導入的成效以及阻礙，並欲了解其關鍵成功因素等，而提出問題，再透過相關資訊系統導入的文獻收集與分析，分別建立關鍵成功因素之構面與釐清個別構面的決策因素，確認並設計相關訪談問題，而後利用深度訪談資料，以個案分析法來了解，進而確立資料外洩防護系統導入的關鍵成功因素，最後根據數據合理的分析與討論研究意涵，最後做出研究結論，並根據本研究結果，給未來欲導入資料外洩防護系統之企業或者組織建議，而本研究整體流程請參圖 3。

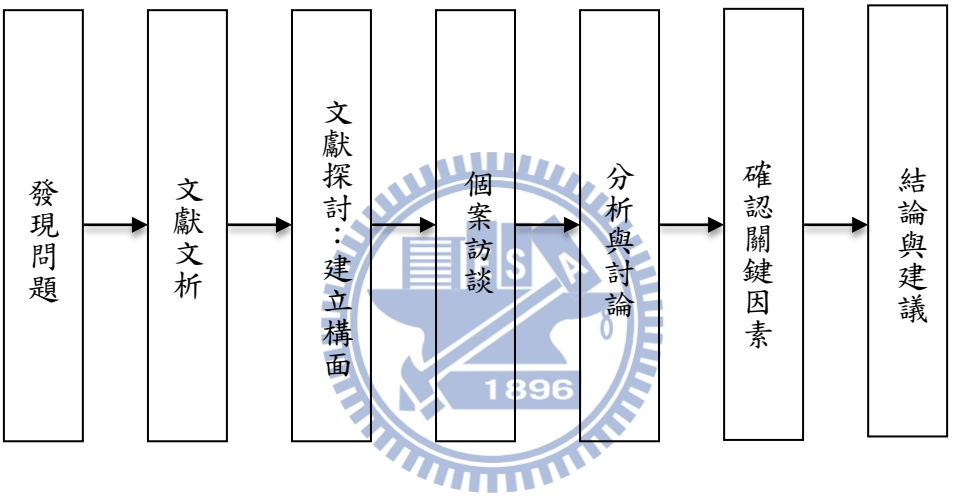

圖 3 研究流程圖

資料來源：本研究整理

第二章　文獻探討

本研究主要在探討 DLP 資料外洩防護系統在企業應用的情況，所以文獻探討的部份，將以資訊安全管理的角度來解釋，其 DLP 資料外洩防護系統在企業是屬於其資訊安全管理範疇，另外資料外洩牽涉到個人隱私以及資訊安全法規，所以本章也會提及目前個人資料保護法的國內外實施情形。而本研究欲了解 DLP 資料外洩防護系統導入影響的關鍵因素，所以針對在資訊系統導入相關研究領域的重要文獻模型理論，做整理說明以及探究，以作為本研究在 DLP 外洩防護系統導入關鍵因素研究架構的理論基礎。

2.1 資訊安全管理

資訊安全的定義：電腦在處理資訊系統的使用者之非授權行為的預防與發現（Gollmann, 1999）。而任何電腦安全政策的廣義目的，其需能保護儲存於資訊系統中資料之機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），即所謂「C.I.A.」(Schultz et al,2001;林鈴玉,2001)。其整體來說，三者所想要達成的目標分別為：

1. 機密性：確保「資訊」只能被經過授權的人，才能存取。
2. 完整性：保證「資訊」和其「處理方法」的準確性與完整性。
3. 可用性：確保經過授權的使用者，當需要時就能存取「資訊」，並使用相關「資訊資產」。

所以資訊安全就是保護任何與電腦有關的事務之安全，將管理程序與安全防護技術運用在硬體、軟體與資料之中（黃亮宇,1992）。對組織和企業而言，資訊是一種具有價值的重要商業資產，需妥善加以保護，以免受到各種威脅攻擊，而維持組織營運的持續性，並使業務可能發生損失降至最低。

Von Solms ,(1994)認為資訊安全的範疇包括：資訊安全政策、風險分析、風險管理、權變規劃（Contingency Planning）及災害復原（Disaster Recovery）等。運用可施行於資訊資源（硬體、軟體及資料）上之技術性防護方法及管理程序，期使組織所擁有的資產及個人隱私，均能受到保護（樊國楨與楊晉寧，1996）。

而有關資訊安全管理的文獻中，以 ISO / IEC 17799 及行政院參照 BS7799-1 制定的資訊安全管理規範，對資訊安全管理範疇的界定較為完整，茲整理如下：

（一）資訊安全政策制定及評估

（二）資訊安全組織及權責
（三）人員安全管理及教育訓練
（四）系統安全管理 電腦系統作業程序及責任、系統規劃、電腦病毒及惡意軟體之防範與控制、軟體複製的控制、個人資料之保護、日常作業與媒體之安全管理、資料及軟體交換之安全管理。
（五）網路安全管理網路安全規劃與管理、全球資訊網與電子郵件之安全管理、網路安全稽核、憑證機構之安全管理。
（六）系統存取控制 資訊系統存取控制與責任、網路存取之安全控制、電腦系統之存取控制、應用系統之存取控制、系統存取及應用之監督、組織外部人員存取資訊之安全管理、系統稽核規劃。
（七）系統發展及維護之安全管理

根據文獻定義來看，DLP 資料外洩防護系統是屬於資訊安全管理策略的一項，而「資訊」（Information）是企業的重要資產之一，對組織或企業而言，是具絕對價值的，因此，必須妥善的加以保護。而資訊安全的日趨重要，係由於資訊系統的環境大幅度的改變，在網際網路的環境中，隨時都有為數可觀來自世界各地的非授權使用者，可能去存取或變更、竊取企業的資訊，使組織的資訊系統面臨空前的威脅；因此，資訊安全也是當今任何組織為達成有效管理的重要關鍵之一，也是組織的核心業務之一（Schultz,2001）。

2.2 導入 DLP 資料外洩防護系統的動機

從上一節資訊安全的角度來看，現今科技發展迅速，已從傳統對隱私權的保障漸漸轉為以電子資料保護為重的機制（廖緯民,1996），目的為了就是要確保在網際網路普及的今日可以保障使用者的隱私權，以面對種種資訊科技、技術上或是人為上可能產生的漏洞。所以資料外洩防護（Data Leak Prevention 或 Data Lost Prevention，DLP），在企業或個人重要資訊外洩頻傳的今日，已經被許多高科技產業或金融業列為一定要考量的資訊安全項目，在 IDC(2013)預測，DLP 將會是企業的最重要資安需求之一，在國外已有很多企業開始採用，在台灣個資法通過後，確實市場上 DLP 的詢問度相對的提高。現今各大組織以及企業，無論資料儲存為何種形式，這些有形的資產既然有儲存的必要性，相同地也會有遺失的情形出現，而在 IT 應用的領域，我們會用備份、相互備援的概念來解決資料意外損毀及遺失的問題，但是對於有心人士的竊取、外洩，則必需採取資訊安全解決方案來防護。(戴燊,2013)

在台灣由於個資法等資安法規的推動，加上近年來不景氣下許多高科技與中小企業裁員所連帶產生可能的資料外露風險，讓企業開始擔心影響公司存亡的機密及重要業務或客戶資料，會因擁有存取資料權限的主管或員工離職而外洩至企業內部以外，而法規中提到，企業需要提供相關的資料外洩證據(全國法規資料庫，2010)，而 DLP 系統具備

儲存鑑定時所需的資訊（Kim, Y., 2011），因此企業對採購 DLP 的意願比以往增加許多，即使內部 IT 預算縮減，導入 DLP 仍是現在與未來在資安防護上勢在必行的做法。

戴燊(2013)指出目前資訊安全系統發展的情況角度而言，在早期大家所普遍採取的防禦思考方式，主要在於阻止病毒入侵、避免系統運作與所存放的資料受到影響而癱瘓，後來隨著駭客入侵的行為越來越嚴重，動機也逐漸從炫耀技術變成盜竊、販賣重要資料來牟利的違法行為，所有人越來越清楚自己所要保護的最重要資產，就是資料。系統壞了，可以重新建置，如果資料沒了，或許還可以從備份系統中還原，但一些重要的機密、營業用或者個人敏感資料如果外洩出去，被其他人濫用、冒用，後果就不是我們能控制的。

另外企業導入 DLP 的原因，除了本身對於機密資料的保護需求之外，來自外部的法規要求也是主要的一個原因，而目前的 DLP 產品至少對於幾種常見的法規，像是金融業常用的 PCI-DSS，及專為醫療業者量身打造的 HIPPA 等，皆提供可以直接套用的範本，也是吸引企業考慮建置的原因。(戴燊,2013)

2.3 導入資訊系統關鍵成功因素

關鍵成功因素(CriticalSuccessFactor，CSF)，關鍵成功因素最早概念始於J.R.Commons(1934)所提出的限制因子(Limited Factor)想法，並將其運用在管理及談判運作。近期的學者 Jorge(1988)認為關鍵成功因素是指每一產業中，有些因素數或工作和組織績效間有特別的相依關係，企業想要獲得較佳的競爭優勢條件，就必須在這些因素或工作中比他們的競爭者成功。

而在資訊系統成功因素研究方面 Kown & Zmud(1987) 認為影響資訊系統施行的關鍵因素有五個層面，包括：(1)組織結構構面，高階主管的支持態度、專案團隊選擇(2)使用者構面，如員工資訊認知、接受度或抗拒程度、部門特性(3)專案構面，如專案進度掌握、目標制定、工作範圍(4)資訊技術構面如系統相容性、優勢(5)企業管理構面如流程再造、工作分配、責任授權等。(Kown & Zmud,1987)

綜合以上學者的研究，其關鍵因素泛指在企業營運的過程中，對於企業政策或系統的導入有正面影響效果的因素或工作項目，並可提升企業的競爭能力。然而，在不同的時間及產業環境下，企業所要求的關鍵成功因素也不盡相同。有些學者探討的角度有「管理資訊系統」，「策略管理」，「組織設計」等，但不論是從何種角度，雖然有一些差異性存在，但其主要觀念是一致的。

一般企業採用資訊系統在策略、組織結構或是管理決策上，都會造成相當大的影響。尤其在運用資訊科技強調整合，以取得競爭優勢。欲成功導入任何資訊系統在組織中達到效益，過程中充滿複雜的問題與挑戰，若導入後效益不彰，嚴重者造成系統棄置不用，導致組織資源成本浪費，更可能影響企業的營運。因此，瞭解導入資訊系統的關鍵成功因素，進而檢視企業本身的目標與需求，選擇與企業適配的資訊系統，以增加成功的機率。

2.4 資訊系統導入理論探討

由於資訊科技之導入對於組織而言，將會產生一定程度的的變化與影響，因此為了使困難及問題降至最低，探討資訊科技導入之關鍵成功因素實屬必要，因此本節將針對過去其他相關資訊系統導入理論之相關文獻彙整說明之。

2.4.1 IS 成功模式

DeLone & McLean (1993) 分析了一百多篇文章後，提出資訊系統成功模式，認為不同的系統應與使用對象，會產生不同的的使用效益與認知。不過因為應新的電子商務時代的來臨，先前相關研究也已經不適用，許多學者對原本模式有諸多探討與批評，所以 DeLone & McLean 於 2003 年提出新的資訊系統成功模式。其主要將資訊系統成功模式並歸納為六大構面：系統品質、資訊品質、服務品質、系統使用、使用者滿意度及系統使用效益。

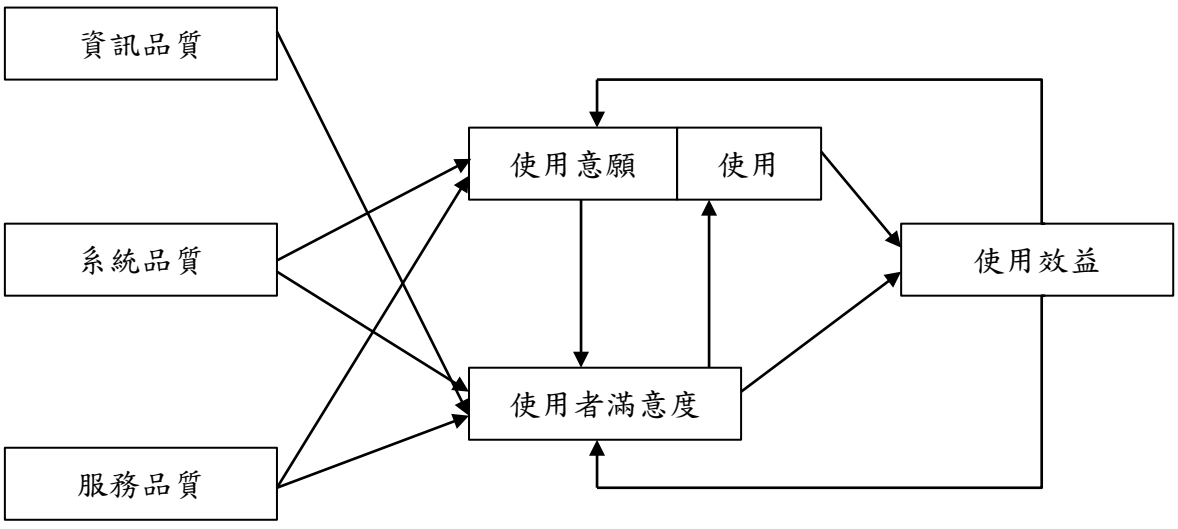

圖 4 修正後 IS 資訊系統成功模式

資料來源：(DeLone & McLean,2003)

各構面簡述如下：

1. 資訊品質－對資訊系統產出的衡量，包含完整性、可了解性、關聯性、資料正確性、嚴謹性、簡單性、及流通性、即時性等。

2. 系統品質－對資訊系統本身的品質衡量，包含存取便利性、效能處理、功能性、資訊完整性、一致性、操作簡單易用性、學習簡單性、穩定度與擴充彈性等。

3. 服務品質－其能系統能提供確實性、體貼性與快速回應等。

4. 使用意願－衡量系是否讓使用者有使用意願，包含使用系統、操作系統、取，主要評估是否方便使用、導引程度、與系統使用次數等。

5. 使用者滿意度－使用者對系統產出後以及使用後的感覺，包含決策滿意度、硬體滿意、軟體滿意、整體滿意度、資訊滿意與介面滿意度等。

6. 系統使用效益－評估新的系統對個人、客戶、產業、經濟、組織、社會，其所產生的正反面影響，包含是否能提升服務品質、工作效率、溝通便利、或能有效的節省資源以及降低營運成本等。

2.4.2 TOE 架構

一般在研究組織採用創新資訊科技的文章中，大部份皆會採用 Tornatzky 及 Fleischer(1990)所發展的科技-組織-環境架構(Technology - Organization - Environment Framework, TOE Framework)，其非常適合用來協助企業或者組織辨視是否採取新的資訊科技系統的評估架構之一。其主要研究架構包含三個構面：科技構面(Technology)、組織構面(Organization)，和環境構面(Environment)。TOE 架構指出企業在取得新的資訊科技決策上，會遇到那些狀況與障礙，其主要貢獻是幫助企業在面對與制定資訊科技創新的決策上提供參考哪些為導入的成功因素(Tornatzky and Fleischer, 1990)。

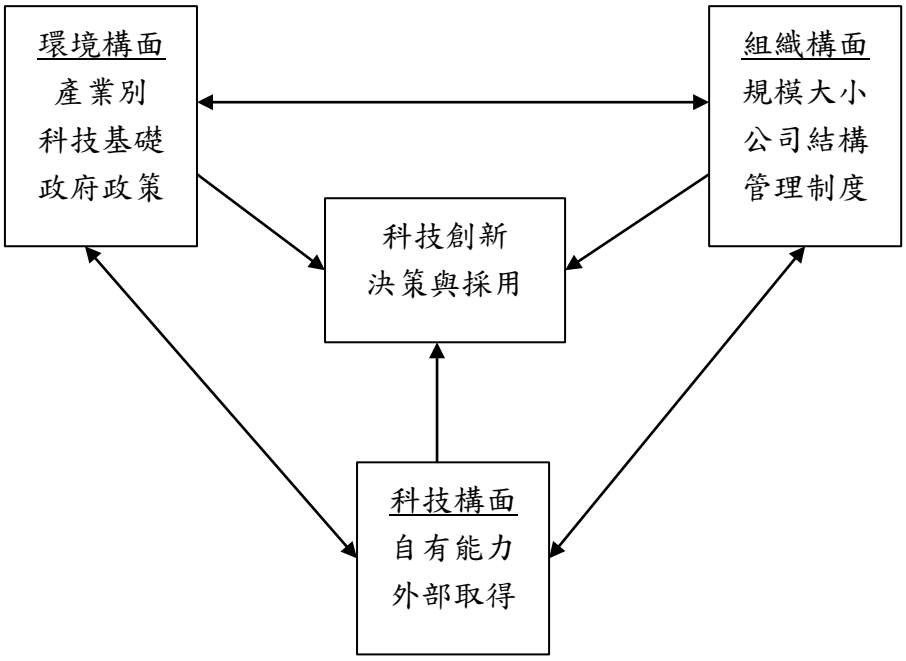

圖 5 TOE 架構

資料來源：(Tornatzky and Fleischer, 1990)

TOE 架構中，主要提出三個重要的構面影響組織在新的資訊科技導入時決定是否採用的因素，各構面定義分述如下：

1. 科技構面：指組織內部目前擁有的資訊科技以及外部可獲得之資訊技術。
2. 組織構面：組織的大小及規模、其管理制度集權化、正式化或者者管理結構的複雜度以及內部閒置資源等等。
3. 環境構面：組織所面對的外在環境特性，包括其所屬的產業別生態、主要競爭對手及政府政策等(Tornatzky and Fleischer, 1990)。研究指出如果環境不確定性對組織則具有相當顯著之影響，更有可能產生各種額外的成本。

2.4.3 TAM 科技接受模型

Davis(1989) 根據理性行為理論 (Theory of Reasoned Action, TRA) 和計畫行為理論 (Theory of Planned Behavior, TPB)，提出科技接受模式 (Technology Acceptance Model, TAM)。特別針對人的科技使用行為而發展，從使用者的認知與情感因素，探討使用者與科技使用之問的關係，其中指出合理的理性行為理論可以用二個面向解釋個人的行為狀態：人類行為表現是在自己意志下且合乎理性；人們採取某些行為的意向為該行為發生與否的決定因素，並以使用行為態度、主觀認知規範、認知行為控制等三項因素表示人的行為影響 。(Davis,1989)

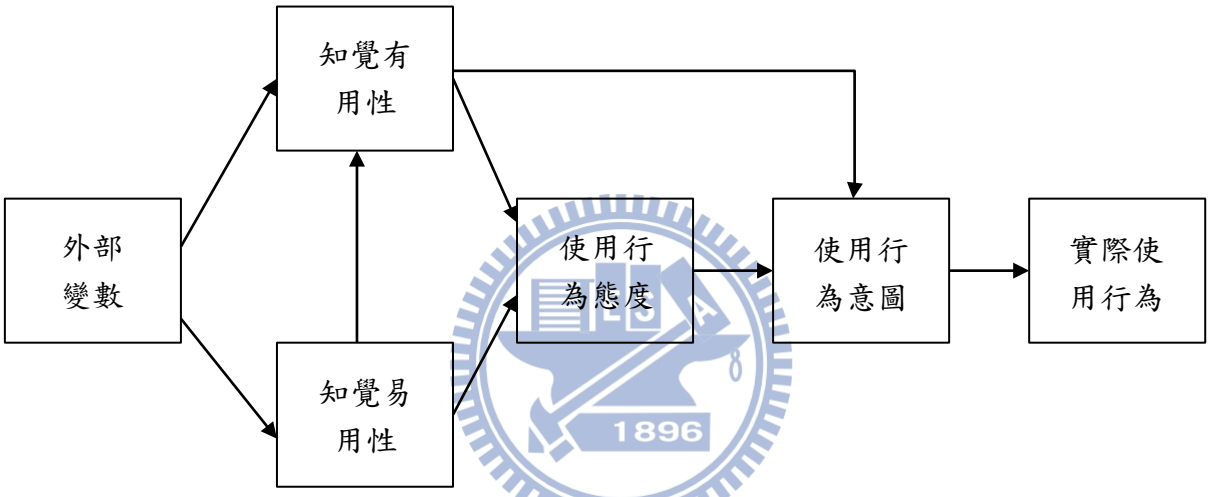

圖 6 科技接受模式（TAM）

資料來源：(Davis,1989)

科技接受模式主要以認知有用性 (Perceived Usefulness) 與認知易用性 (Perceived Ease of Use) 等兩概念組成，用以解釋、診斷、與預測使用者面對新資訊科技時的行為。科技接受模式有三個階段目的，包括發展階段：了解使用者想法加以改進系統；導入階段：診斷使用者接受程度因應導入策略；評估階段：系統是否成功的參考指標。(Davis,1989)

科技接受模式是現今研究中最常用於探討使用者對新的資訊科技接受度的理論模型，主要包括五個主要構面：外部變數、認知有用性、認知易用性、使用行為態度、和使用行為意圖。 Davis(1989)指出：科技接受模式的外部變數會影響使用者的內部變數，包括認知有用性和認知易用性。認知有用性主要說明：使用者相信資訊系統能加強工作或表現程度；認知易用性則是：使用者相信資訊系統能減少學習時間，減低操作的難度程度。認知有用性和認知易用性會影響使用行為態度、使用行為意圖和實際的使用行為。

2.4.4 Wixom and Watson 資訊系統導入成功因素

Wixom 與 Watson (2001)，在 MIS Quarterly 發表了一篇研究，其主要探討建置一個資料倉儲系統的成功的關鍵因素，二位學者針對北美地區已成功導入資料倉儲系統廠商進行研究調查，其研究成果顯示資料倉儲系統建置的相關影響因素包括發現高階主管的支持、組織相關單位支持、足夠的資源、使用者參與、純熟的技術、開發團隊技能、資料來源系統等因素，均有助於資料倉儲系統之順利建置。並提出影響資訊系統導入的成功與否，則應從三個層面來討論，分別為組織層面、專案層面與技術層面，參閱圖 7。

在組織構面中，除了高階主管的支持在系統導入的成功佔了很大的因素以外，其中也談到一個系統的導入成功與否，在於該系統的效益(產出)是否為組織所接受，並且與工作流程相互結合。因為一個重要的資訊系統的導入可能引起重大的組織變化，使得員工偏向抗拒系統的導入。另外隨著系統導入而產生的組織變化範圍與強度，也會使組織內部對系統導入的抗拒也會增強。因為新的系統導入，有可能改變了資料的使用與存取方式，同時也改變了組織成員的工作方式，進而影響企業的整體流程。

專案構面，其說明資訊系統專案通常包括一個複雜的任務內容，以及專案所需的人員。而任何一個資訊系統專案特別皆需要不同的專業能力以及知識和管理制度良好的合作團隊，而該團隊並且能夠克服專案中所面臨的一些議題專案團隊必須著重於關鍵目標與適當的議題，避免預料外且導致整體風險升高的事情發生。滿足了這些目標的專案團隊，將能成功導入一個專案並能提供高品質的資訊系統產出和功能。

科技構面，任何資訊系統在其科技技術上都有其複雜度，所以在技術上可能發生的問題可在很多地方發生，例如：新的技術必須適用於現存的資訊基礎架構。在現有應用上是否已經成熟。這些技術問題可能使得專案團隊無法創造一個有高品質的資訊系統專案導入，而如果不合用或者不穩定的系統也可能無法達到組織所需求的系統功能，或系統的整合度也未達要求如此一來將嚴重影響專案的成功。

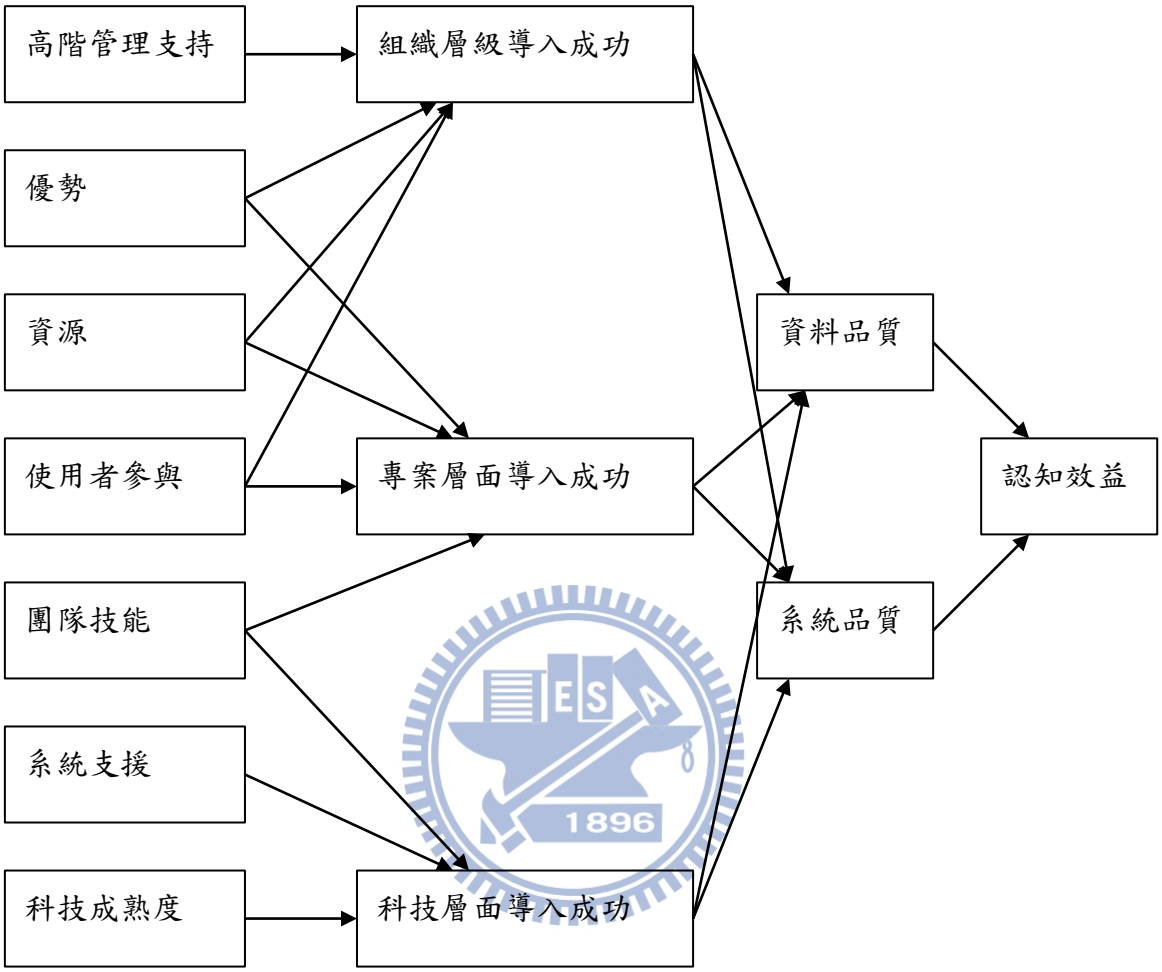

圖 7 Wixom and Watson 資料倉儲研究模型

資料來源：(Wixom & Watson,2001)

2.4.5 理論整理

本小節歸納上述有關資訊系統導入關鍵因素之文獻，整理如下，參見表 1

表 1 相關理論整理表

理論	*論點*	*構面整理*
IS 資訊系統導入成功模型(DeLone & McLean,2003)	將系統導入使用效益分為個人效益與組織效益兩方面探討。個人效益係指系統產出的資訊能否改變資訊接受者的行為或認知；至於組織效益則以企業利潤、成本等議題為主要考量	1. 系統品質 2. 資訊品質 3. 服務品質 4. 系統使用 5. 使用者滿意度 6. 系統使用效益
TAM 科技接受模型(Davis,1989)	在研究個人使用資訊科技的行為模式與接受程度時，用以探討態度、使用意願、使用認知及外部變數間的關係，進而解釋並預測使用者的使用行為。	1. 知覺易用性 2. 知覺有用性 3. 使用態度 4. 使用意圖 5. 實際使用
TOE 理論(Tornatzky and Fleischer, 1990)	資訊因素提出科技的特色與優勢是影響企業採用 IT 的主因，而組織因素則包括組織策略、組織結構、管理流程和人事，例如資本、專業人力資源，其中財務資源是許多企業採用新科技的阻礙。 環境因素則是指出企業所營運的外部環境與一些會影響企業行為的相關因素。	1. 科技構面 2. 組織構面 3. 環境構面
Wixom & Watson (2001)	將系統導入成功分為三大構面：組織構面、專案構面、科技構面，其中認為高階主管的強力支持與導入資訊系統的優勢和人員的參與程度是主要影響系統導入成功的主要關鍵因素，	1. 高階主管支持 2. 優勢 3. 資源 4. 參與度 5. 團隊技能 6. 系統支援 7. 科技成熟度

資料來源：本研究整理

新的資訊系統能否在有限的預算、時間、及人力資源前提下，圓滿達成使用者的業務需求，讓資訊系統能順利運轉，都仰賴企業在這些相關因素上的配合。雖然探討這類資訊系統成功的關鍵因素文獻很多，不過目前研究 DLP 資料外洩防護系統導入的相文獻並少之又少，所以在本研究遂將多位學者論述的系統關鍵成功因素架構整理後，來作為研究導入 DLP 資料外洩防護系統關鍵影響因素的基礎架構。

2.5 台灣個人資料保護法探討

台灣「電腦處理個人資料保護法」因為時代變遷，已經諸多不宜，逐漸產生許多問題，於管理層面、稽核層面也都缺乏足夠配套措施。所以政府也已經在 101 年完成台灣個人資料保護法。

何謂個資法，台灣早在民國 84 年時，就已公佈施行《電腦處理個人資料保護法》，但部分內容早已無法因應現今社會實際資料利用現況，所以在民國 99 年完成修法，並更名為《個人資料保護法》， 其立法目的為規範個人資料之蒐集、處理及利用，個資法的核心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，根據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」其中，個資法特別把醫療、基因、性生活、健康檢查、犯罪前科等資料歸納於特種資料範圍內，明令此類資料除非特殊情形，不得蒐集、處理或利用。（全國法規資料庫，2010 ）

個資法主要從蒐集、處理和利用等三個層面，來規範個人資料的合理利用，新個資法所保護的資料型態，也從原本的電腦處理之個人資料，延伸到無論是電腦處理的數位個人資料，或是紙本的個人資料，皆適用於直接或間接識別之個人資料中。在以往，若發生個資遭到不法蒐集、處理、利用等糾紛時，受害者必須親自舉證，獨自進行訴訟，新的個資法規定，不但舉證責任歸屬於被告機關的責任，也建立團體訴訟機制，可由公益團體出面代表所有受害者進行訴訟，發揮民間團體之力量，保護受害者。除此之外，更提高相關刑事與民事責任，落實保護個人資料制度。（全國法規資料庫，2010 ）

底下則說明新版個人資料保護法的修法重點：

（一）個資法規範對象：擴及各產業，除了公務機關、法人和自然人受約束外，包含各種團體。

（二）必須保護的個人資料：個人資料：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。

（三）求償金額最高 2 億元，企業主最多 5 年刑責個資法提供權益受損客戶可透過團體訴訟向企業求償。若無法估算損害金額時，每人每件可求償 500－20,000 元。

- 相同原因造成事件總求償金額最高 2 億元。

- 若違反個資法造成他人損失時，相關人員還會加重為 5 年刑期、拘提或併科 1 百萬元罰金。
- 當事人可向主管機關投訴企業違反個資法，經由主管機關派員稽查企業法規遵循情況，若發現企業有違反個資法，限期改善無效後，主管機關會對企業處以行政罰鍰，依違法罰款 2 萬－50 萬元不等。

（四）企業必須自行舉證沒有違反個資（SOP，DBAuditor，EmailAuditor etc.）

（五）只要擁有 1 筆個資就得遵循新法

日本個資法只管 5,000 筆以上的資料。但台灣新法未來實施後，企業只要擁有 1 筆個資就需遵循個資法規範。

（六）個資蒐集或利用前須告知當事人

- 在使用行為規範，個資法從蒐集、處理和利用三面向來要求個資法使用範圍。
- 企業直接向客戶蒐集個資時，需盡到告知義務（蒐集目的、企業名稱、資料類別、資料利用期間、方式、當事人權益）。
- 企業委託第三方機構向客戶蒐集個資，委託機構作為視同企業，所以也需告知當事人。
- 在法規實施之前企業已擁擠個資，企業如果是向當事人取得個資，且使用沒有超過當初告知目的，就不用依據 54 條規定再次通知當事人。但企業若不是直接向當事人蒐集（透過委託機構），企業需在新法實施一年內告知，在未告知當事人前，企業無法使用個資。（全國法規資料庫，2010 ）

2.6 國外相關法律探討

在國外以美國為例，到目前為止，共有 12 個州有資訊自由、資料外洩的相關法律，以及集中式的統計報告；有 34 個州有資訊自由、資料外洩的相關法律，但沒有集中式的統計報告；其餘不到 5 個州則是只有資訊自由的相關法律。 以美國紐約州為例，該州有 649 個跟資訊安全相關的法源，也有資訊自由、資料外洩的 相關法律，以及集中式的統計報告。紐約州的資料外洩法律概述如下：「如果有任何紐約居民有資料外洩的情形發生，該人或企業應通知該國總檢察長、消費者保護委員會或是國家辦事處之網絡安全管理者，並儘速通知大致受影響的人其內容及過程，上述通知應不拖延通知受影響的紐約居民。」由此可知，紐約已相當重視個人（企業）資料外洩的問題，並在第一時間作出處理及告知義務，將人民的權益擺在最前面。

美國目前已有「美國隱私法」、「健康保險流通與責任法案」、「美國金融服務現 代

化法」，英國也有「資料保護法」、「官方機密法」，而目前台灣在個資法通過前，在民國九十四年十二月，為建立政府資訊公開制度，便利人民共用及公平利用政府資訊，保障人民知的權利，增進人民對公共事務之瞭解、信賴及監督，並促進民主參與，便於公布施行「政府資訊公開法」(立法院圖書館，2010)。

而在日本，政府認為近年來電子科技日益精進，在邁向網路資訊化社會之同時，電腦處理個人資料之保護更形重要，於是在 2003 年制定「個人資料保護法」，其衡量個人資料電子化雖促成社會繁榮進步，但個人資料之處理亦攸關個人權益，應於尊重個人人格之理念下慎重處理。

隨著電腦處理資料技術的發達,攸關個人隱私等資訊或資料,可簡單利用電腦儲存、流通、加工、編輯，且因網路普及，個人資料可瞬間傳遞至全世界，如能善用電腦處理個人資料，有助提升行政效率，甚至促進經濟發展。但個人資料經電腦處理後，因可輕易彙整獲悉個人資料全貌，如遭濫用或不當利用，有侵害個人權益之虞，若處理不當，導致個人資料外洩，即使未對個人造成實質傷害，亦可能引發個人對其個人資料保管、使用之疑慮,所以上述原因遂促使日本政府成立個人資料保護法。(立法院圖書館,2010)

在德國其名為 聯邦資料保護法 (Bundesdatenschutzgesetz)主要是為保障個人權益不致因儲存、傳遞、更正及刪除等資料處理過程而受損，所以德國於一九七七年一月二十七日即制定「資料處理個人資料濫用防制法」（Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung），簡稱「聯邦資料保護法」（Bundesdatenschutzgesetz），且已行之有年。之後因為歐洲聯盟成立，為轉置歐盟指令、保障個人資料及資訊自由流通，而於 2001 年修正其內容。主要修法目的旨在保障個人資料自主權，並落實歐盟有關建立共同資料保護標準之指令(立法院圖書館，2010)。

第三章　資料外洩防護系統介紹

目前針對企業內部或外部的威脅所引起的資料外洩之防範措施並不儘相同，以目前資訊安全產品的技術應用可分為幾種，(1)標準的安全施:例如入侵偵測 IPS、防毒產品 Anti-Virus。(2)強化型的安全產品：例如檔案加密、存取控制等。(3)專有的資料外洩防護系統,例如 DLP 資料防外洩系統、E-DRM 等主要以資料內容來管控的產品(Phua,2009)。所以就目前國內外市場上針對資料防外洩相關法規防範所推出的產品中，本章就以比較多企業採用的資料外洩防護(Date Loss Prevention)和企業數位版權管理(E-DRM)二種。做進一步的說明。

3.1　企業數位版權管理(E-DRM)

DRM 是一種保護數位內容使用的管理機制，強調在數位內容生命週期內(從產生到銷毀)，不論其處理、利用過程中是否被複製到它處，仍然可以持續追蹤並管控數位內容之使用方式可以便符合安全政策上之要求。傳統的 DRM 技術最常為娛樂產業採用，這包括了電影或音樂產業，近年來為了因應娛樂業數位化趨勢，線上音樂商店和電子圖書發行商也採用 DRM 技術，而一般的企業組織為了防止重要的企業內部文件檔案在企業網路內任何位置均不會被未經授權存取，因此也開始應用了 DRM 技術來控制企業文件之使用稱為企業數位權利管理，或稱為資訊版權管理 (Information Rights Management；IRM)。其與一般存取控制不同點在於限制檔案文件的開啟、修改、列印、轉寄或其他相關存取行為，不論檔案在何處這些限制原則都會保持不變。(工業技術研究院，2008)

E-DRM 的基本運作主要是依賴加密系統來保護文件內容，以及驗證系統來確保只有經由授權的使用者可以解開加密的文件，換言之，當保護的文件產生時，DRM 將加密資料而讓資料在無正確的解密金鑰時將無法被任何入讀取，另一方面，現代的 E-DRM 系統允許企業組織透過政策(policy)為基礎的設計來來定義、落實並稽核資料的存取與使用，而政策可以定義允許誰在何時與何處對資料執行何種操作，且政策為持續、動態並可稽核。(工業技術研究院，2008)

實務上而言，企業數位版權管理乃是用來持續控管企業內部檔案與文件使用權限的加密技術，因此對於不同 DRM 廠商如何加解密、以及有無檔案備援機制、支援保護的檔案類型、目前網路架構是否相容均應列為導入時之重要考量。此外，E-DRM 的部署架構通常複雜，因為通常需要管理伺服器、帳戶伺服器 (Active Directory)、資料庫及額外部署用戶端軟體。(周世雄,2010)

3.2 DLP 資料外洩防護系統定義

『資料外洩防護 (Data loss/leak prevention)』簡稱 DLP 是目前資訊安全產品市場上防範資料外洩的技術和產品，按照 SANS 機構有關於 DLP 的定義：『其採用中央控管的政策，利用深層資料分析，能夠辨識資料內容並執行監控和保護在資料儲存端、用戶端點以及網路傳輸中的資料』，而根據 NSS Labs 的定義，DLP 是一種特殊設計的系統，能夠從時間的角度偵測潛在資料外洩突發事件，並且預防它們發生。

而 Gartner Inc(2013)則定義，資料外洩防護（DLP）的技術，主要的核心功能應包括，進行內容檢查資料的流向在靜止或移動中，並可以執行的回應，例如從簡單的通知，主動攔截，或者依策略設置動作。而企業在採用時必須考慮到，產品必須支援先進的內容檢測辨視技術，超越簡單的關鍵字比對和正則表達式，(Gartner Inc,2013)。

Shabta & Rokach (2012)在其文章中提到，即使資料處於不同存取狀態，DLP 系統應能掌握資料，包含使用中（Data in Use，端點正在存取資料）、傳輸中（Data in Motion，資料透過網路傳輸）、存放中（Data at Rest，資料儲存在固定的位置），能夠預防敏感資訊的意外散播，而這些相關產品所用的方式，是透過控制資料進出網路與端點系統的關鍵位置，並且藉由內容檢查來監控資料的狀態。而資料外洩防護三個主要個層面的涵義以及作法如表 2 敘述：

表 2 DLP 資料外洩防護主要層面

資料傳輸中 (Data in motion)	防範資料經由網路傳輸途徑而導致外洩，這類技術用以偵測與阻擋任何企圖透過網路來外洩資料的手法，通常的做法是需要在企業網路連出的周邊部署一部流量必經的閘道器來檢查封包中是否有違反公司政策的敏感性或私密性資料(個資)正在傳送。
資料使用中 (Data in use)	此類型為端點安全性的的解決方案，此種端點安全性技術利用代理程式監控終端使用者電腦或筆電監控是否有任何資料經由行動設備 (如軟碟、CD、USB)被拷貝離開或攜出，此外，也可以提供敏感性資料被列印的稽核。
資料儲存中 (data at rest)	用以辨識儲存中的資料是否有問題以避免外洩，傳統上敏感性資料被存放在儲存裝置內的目錄檔案或資料庫內，因此為了確保資料來源端的安全，這一類型的解決方案通常需要掃瞄網路的伺服器、資料庫或其它存放區，查看是否有敏感性的資料被儲存在不適當的地方或位置。

資源來源：(Shabta & Rokach,2012)

Liu & Kuhn,(2010)指出 DLP 系統為了防護上述三個狀態層面的資料外洩發生，且能達成自動辨識並保護敏感性／機密性的資料之目的，一個設計良好且完善的 DLP 系統需一般需要包含下列四個主要功能元件：

1. 管理元件(Management)：

用以建立並管理執行 DLP 系統的各項政策，包括定義敏感性資料的類型與行為待徵，以及敏感資料允許執行那些操作，一旦辨識元件發現了敏感性資料，保護元件應該如何回應處理。

2. 機密資料學習(Discovery):

學習重要機密資料，建立、管理機密資料儲存位置，並可以依照設計自動找出企業內部重要資料存在不同的狀態的使用情況。

3. 辨識元件(Identification)：

根據管理元件所定義的政策規則以及事學習特徵來偵測發現敏感性資料的移動，通常利用統計方法來判斷是否存在敏感性資料，因此會存在有誤判(false positive)和漏報(false negatives)的問題。

4. 保護元件(Protection)：

一旦 DLP 辨識元件發現到敏感性資料，將由保護元件執行政策所要求的動作，封鎖或加密是最常件的二項動作。例如有人正在拷貝敏感資料到 USB 行動碟時，保護元件將攔截並禁止這項資料的拷貝與傳送，假如授權的使用者企圖儲存敏感性資料，保護元件可能會在儲存前先予以先加密。(Liu & Kuhn, 2010)

底下圖 8 則說明一套 DLP 資料外洩防護系統應該能保護來自不同的對像將什麼樣的資料或者資訊傳送到什麼地方，透過哪種管道離開企業或者系統。

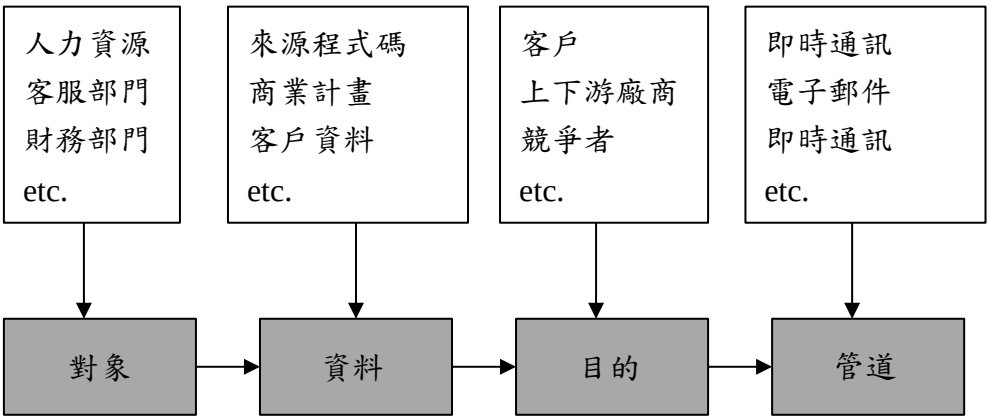

圖 8 DLP 資料外洩防護系統概念示意圖

資料來源：本研究整理

3.3 DLP 機密資料辨識技術

在 Mogull & Securosis, (2007) 的文獻中指出，DLP 資料外洩防護系統的機密資料辨視技術而言，其方式主要是透過檔案格式比對、關鍵字及正規表示式過濾，和特徵辨識等 3 種方式，來檢查檔案本身是否包含需要受到保護的機密內容。

1. 檔案格式比對

就檔案的主要副檔名特徵，例如 AutoCAD 的.DWG 檔，及可能含有機密文字的檔格式，來比對政策中是否有不允許的機密檔案，一般來說不同應用程式所產出的檔案格式皆不相同，所以就算使用者經過加密，或者修改過副檔名的情況下，技術上還是可以辨識、分析其中內容。如果無法辨視時，有些產品在功能上，可以做到禁止無法分析內容的檔案傳送，或者限制使用者不能傳送可以帶有機密資料的檔案格式。

2. 關鍵字過濾

關鍵字過濾一般分為自定關鍵字及特殊關鍵字等 2 種。自訂關鍵字指的是使用者可以指定一個或一組以上的文字或符號給系統做資料外洩時的偵測依據。而特殊關鍵字指的是信用卡卡號、身分證字號或者地址格式等採用特定規則所組成的字串，及程式碼之類具有固定格式的文字內容，一般來說都由系統內建提供。不過許多原廠都在歐美地區，針對國外才具有較完整的支援度，如果範本中沒有提供所需的特別格式，就通常必須利用正規表示式（Regular Expression）圖 9 手動來定義規則，才能過濾客制化的規則的資料；不過目前支援亞洲地區的範本也愈來愈齊全，現在用戶可以在設定介面選取已經內建好的規則，就可以很輕易地過濾使用者傳送的資料當中，是否含有本身所需的規則範本。

```
^(?:(?<Visa>4\d{3})|(?<Mastercard>5[1-5]\d{2})|(?
<Discover>6011)|(?<DinersClub>(?:3[68]\d{2})|(?
:30[0-5]\d))|(?<AmericanExpress>3[47]\d{2}))([
-]?)(?(DinersClub)(?:\d{6}\1\d{4})|(?(AmericanExpr
ess)(?:\d{6}\1\d{5})|(?:\d{4}\1\d{4}\1\d{4})))$
```

圖 9 信用卡號碼的正規表式示

資料來源：(Mogull, R., & Securosis, L. L. C. ,2007)

3. 特徵辨識

特徵辨識是不同的 DLP 產品主要要的偵測技術，也是最關鍵的核心技術。目前 DLP 產品採用的特徵辨識技術可分為 2 種，一種是指紋（Fingerprint）特徵，其次則是利用標記（Tag）的方式加以識別，DLP 產品在技術上大多支援其中一種，不過也有少數較為特別，同時採用兩者。指紋特徵的概念，類似於用來過濾垃圾郵件的貝氏（Bayes）演算法，同樣是必須提供範本檔案供產品分析、產生指紋檔，以相似度的高低，判定檔案是否為機密資料。(Mogull & Securosis,2007)

3.4 DLP 資料外洩防護系統類型

Lawton G,(2008)在 IEEE 發表的文章中提到,DLP 目前在架構設計上可以分為兩種，主機型(Host based)以及網路型(Network based)，做法上的差別顧名思義就在於其佈署與管制的運用位置是在主機端點上或是網路層面(通常在閘道端),兩者沒有絕對的優缺點，端看企業的資料重要性與實際需求決定。而也有廠商提出要防範資料外洩最好的方法就是從資料本身著手，若能從源頭就進行加密管制方可達到最高的安全要求。此看法立意甚好，不過須注意有加密後勢必就會有解密的需求，可能會牽涉到系統資源的消耗、延遲到讀取的速度，甚至可能會大幅增加資訊系統的複雜程度，因此並非所有的系統或資訊都適用，企業在選擇解決方案時須詳加確認比較，以挑選到最適合的解決方案。(Lawton, G,2008)

以上兩種架構雙管齊下則是目前 DLP 的趨勢，網路型 DLP 的好處在於，可以在不需要更動內部原有環境的前提下設置產品，同時由於它是採過濾流量的方式控管機密資料的外洩，因此只要是可以連接網路的任何裝置都必須接受管理，至於缺點則是無法控管機密資料在內部的流動狀況、不提供離線保護的功能，欲即時封鎖機密資料透過網路傳輸時，大多必須再整合第 3 方的閘道器產品，無法靠產品本身來完成(Lawton, G,2008)。

主機型產品則剛好相反，由於是採代理程式的方式安裝在使用者的個人端電腦，因此可以和欲監控的平臺達到最緊密的整合，管理者可以透過代理程式封鎖機密資料的傳輸，同時可以搜尋個人端電腦上是否有需要控管的機密資料存在，不過此一類型產品的保護對象以 Windows 平臺的個人端電腦為主，無法管理異質平臺的主機，同時，由於是在個人端電腦上安裝軟體做管理，因此需留意代理程式與現有應用程式間的相容性問題，此外，在 DLP 搜尋電腦內部是否有機密資料時，會佔用到較多的系統資源。(Lawton, G,2008)

3.5 DLP 資料外洩防護解決方案

3.5.1 Symantec DLP

賽門鐵克公司在 2007 年併購資安廠商 Vontu 之後,就開始推出自己的 DLP 產品線，本研究編寫時，其主要系統版本為 Data Loss Prevention 9.0（以下簡稱為 DLP 9.0），是該公司在最近所推出的最新版本。和前一版本相比，DLP 9.0 的代理程式具備了更多功能，可以偵測使用者對於資料剪貼、複製的重製行為，同時能針對更多的資料傳輸管道

提供保護，另外，產品本身還可以和 Blue Coat 的 ProxySG，及 McAfee 的 Web Gateway（Webwasher）等第 3 方的 Proxy 閘道器產品相整合，在網路出口攔截欲傳送出去的機密資料。(Symantec,2013)

其能提供多種不同功能的防護元件,DLP 9.0 產品,早期是架構單純的網路型 DLP，不過後來也提供代理程式的元件，因此同時具備了主機型 DLP 的功能，可以隨著需求不同，而彈性調整 DLP 的部署架構。DLP 9.0 的計價方式隨著企業採購的模組不同，及使用者授權數的多寡而有差異，它的伺服器套件為軟體，可安裝在符合硬體需求 Windows 伺服器上運作。

另外布署 DLP 9.0 的伺服器元件，除了最基本的 Enforcer（管理伺服器）角色外，還有 Network Monitor（DLP 閘道器）、Discover or Protect（資料庫防護伺服器）、Email Prevent（郵件防護伺服器）、Web Prevent（網頁防護伺服器），及 Endpoint Server（用戶端防護伺服器）等幾種模式可供選擇，在人數較少的環境下，使用者可以在一臺伺服器上同時啟用多種角色。

和其他廠商相同的 DLP 產品一樣，DLP 9.0 也具備了指紋辨識的能力，做法上是採 Hash 的方式產生資料的指紋特徵。管理者可以透過掃描本機、遠端主機的共享資料夾，及 SharePoint 等應用程式伺服器的方式，分析檔案範本。在架構上，製作完成的指紋特徵除了會放置一份於管理伺服器之外，在前面提到的幾種防護伺服器上也會同樣放置一份，因此在這些伺服器與管理伺服器失去連線的情況下，仍然可以發揮作用。

而在端點防護部份，除了派送 DLP 9.0 的代理程式，其可以透過 Windows AD 的 Logon Script、微軟的 System Center Configuration Manager（SCCM）等第 3 方的套件伺服器，及 Symantec 自家的 Altiris 平臺派送，安裝完成之後，代理程式會以偽裝的方式，在系統的背景程式中執行，除了在洩密事件發生時可以秀出警告訊息之外，在一般狀態下，使用者很難查覺到它的存在。

除了派送軟體的功能之外，DLP 9.0 也可以透過該系統的管理介面，偵測、收集代理程式的狀態訊息，透過單一平台就可以了解同廠牌產品的運作情況，使得安全管理的工作更加方便。另外不同於能針對資料庫內容提供防護，DLP 9.0 並不會將指紋特徵的資料庫派送到個人端電腦，當資料被複製到 DLP 閘道器，或者使用者透過自己的電腦將資料傳送出去時，可以利用指紋特徵，針對檔案內容做深層分析。

對於存放在資料庫裡的機密資料，DLP 9.0 提供了相當不錯的的防護功能，使用者可以透過 ODBC，或者匯入文字等 2 種方式，讓 DLP 能夠過濾出儲放在資料表裡的文字內容。以上 2 種設定方式中，ODBC 的操作較為複雜，實際操作時，必需將內含所有

機密資料的文字檔，上傳到 DLP 9.0 的管理介面，就可以設定由系統直接套用文字檔的欄位資料，使得資料的匯入更加方便，此後管理者可以設定僅選用資料表當中的某幾個欄位，做為比對機密資料的依據，適時的觸發 DLP 的控管政策。

在即時通訊的控管方面， DLP 9.0 目前僅支援微軟的 MSN，至於 Skype 的管理，則必須透過 Windows AD 的群組原則等其他方式，限制一部份的功能，降低洩密事件的發生機率。而周邊裝置的管理上，DLP 9.0 可以搭配 Symantec 本身另一個套件的 Endpoint Protection 防毒軟體，或者其他的周邊控管產品，提供企業所要求的 USB 儲存裝置的白名單功能。

在政策範本部份，該系統能提供了幾種常見的資安法規，事先內建好相關的範本，可以直接套用，控管企業內部的機密資料流動。依產品部署的架構做區分，這套 DLP 記錄所得的事件可以分為網路及本機等 2 種，查詢單一筆的記錄時，除了可以看到使用者傳送出去的完整資料內容，所觸發的控管政策之外，報表也一併列出相同事件在過去一段時間曾經發生過的頻率，協助管理者判斷這是否為蓄意發生的洩密事件。

3.5.2 Websense DLP

Websense 公司的 DataSecuritySuite（DSS），是該公司在 2006 年收購資安廠商 PortAuthority，利用其技術推出的資安產品。本研究的二個個案皆是使用導入 Websense 系統。其具備了主機型和網路型 DLP 的能力。能整合多種網路伺服器提供保護。其模組提供以下 4 個功能：(Websense Inc,2013)

1. Data Monitor

稽核使用，可增加機密資料使用行為的透明度。在網路上偵測可疑的洩密行為，涵蓋 HTTP/HTTPS(HTTPS 需結合 WebsenseContentGateway),SMTP,FTPandIM 等。電子郵件的偵測(含：身分證字號，客戶名稱…等，透過電子郵件方式寄出，將會記錄)

2. Data Endpoint

管理使用者在端點使用機密文件的行為。可依據政策，自動化控管疑似洩密行為，涵蓋 USB、Printscreen、localprinter、IM 等。IM 偵測(如：MSN、Yahoo…等)

3. Data Protect

稽核兼阻擋功能。除上述功能外，可依據政策，自動化進行阻擋、緩送、記錄、提醒通知、加密等。

4. Data Discover 盤點查核企業內機密資料，主動掃描公司網路相關的機密資料，並紀錄造冊分類等。

在架構上，DSS 主要是由 DSS Management Server（管理伺服器）、DSS Protector（DLP 閘道器），及代理程式（Agent）等 3 者所組成。其中管理伺服器是安裝在 Windows 平臺的軟體套件，至於閘道器則是整合 Linux 環境的系統套件。DSS Protector 的部署上，包含旁聽的方式的建置，也能以 In-Line 的架構部署在內部的骨幹網路，即時過濾進出的流量中是否帶有機密資料。

除了採用本身套件外，DSS 對於其他的網路應用伺服器也具有良好的整合性，像是微軟的 Internet Security and Acceleration（ISA）、ExchangeServer，及 Websense 公司推出的 EmailSecurity 相關產品等，在這些伺服器上安裝外掛程式後，就可使其兼任 DLP 閘道器的角色。另外 DSS 在架構上，也可以和 BlueCoat 的 ProxySG 等支援 ICAP 的第 3 方閘道器產品搭配，當系統偵測到洩密事件發生時，即由前者阻斷流量的傳輸。

機密資料學習方式，可透過多種方式產生指紋特徵，PreciseID 是 Websense 的指紋特徵技術，它從檔案內容擷取特徵的方式，和趨勢 LeakProof 的 Data DNA 相類似，兩者都是在去除內容的無效字元後，再根據字詞間的相關性，重新組合成多道特徵，由相似度的高低，辨別資料的真實屬性。

所以機密資料範本的來源，可由 DSS 的管理伺服器從內部網路的共享資料夾，及微軟的 Share Point Server 等途徑，將檔案的文字內容傳送回本機運算，最後才會產生指紋特徵。在架構上，DSS 的閘道器本身也具備指紋特徵的資料庫，因此不必透過管理伺服器的分析，也能得知是否為機密資料。如此一來，當閘道器與管理伺服器間的連線中斷時，資料的過濾服務還是可以正常運作。除了學習機制以外，DSS 也同樣有內建完整的通用政策範本，操作各項功能的設定之前，使用者可以透過精靈模式，先以地區、產業別的方式，篩選出適合套用的範本，最後再調整 DLP 的過濾功能設定，就這點來說，和其他款 DLP 產品較為不同。

另外 DSS 的代理程式的派送，可以透過 WindowsAD 及其他第 3 方的套件伺服器來執行，產品本身提供了一支打包工具的程式，我們可以在此預先完成代理程式的功能設定，然後再產生安裝檔，使得軟體部署的工作變得更加容易。常見的 I/O 控管，其也能針對周邊控管能力予以加強 DSS 對於資料庫提供了相當良好的防護功能，它和 Symantec 的 DLP9.0 一樣，都可以透過 ODBC 及匯入文字檔等 2 種方式加以保護。可以在 DSS 管理伺服器的設定介面，透過 Windows 的 ODBC 連線設定，連結測試環境中的 SQL Server，並且手動選取資料表當中想要防護的欄位加以分析；當系統判斷某一欄位的內容重複性太高（例如居住縣市），這時會在分析結果中，以紅字做為標示，提醒用戶修

改設定，整個設定流程相當容易，可以在簡短的幾個個步驟之內快速完成。

以上做法的好處是，可以完全避免員工傳送個人資料時，因為重複輸入造成 DLP 的誤判，同時，它也可以做到當所有欄位資料皆為同一人所有時，才會觸發 DLP 的控管政策。以個人端電腦上開放使用的幾種服務來說，DSS 皆能有效予以過濾，當機密資料傳送時，DSS 的代理程式會顯示目前正在掃描資料的動作訊息，接著則是出現洩密事件的警告訊息，並且加以封鎖。

這款產品的報表事件相當詳細，可顯示資料是由何人，透過什麼樣的管道所外洩，又是因為什麼樣的原因被 DLP 所攔截，而傳送出去的資料，被攔住之後，會留存一份副本於管理伺服器上，做為日後舉發洩密事件的證據。除了透過報表介面查閱記錄外，也可以和這次我們所測試的一些其他款 DLP 一樣，在事件發生時，可以依照員工在企業的組織層級，透過郵件方式通知主管處理。

3.5.3 趨勢 LeakProof

它原本是資安廠商 Provilla 推出的 DLP 產品，2007 年底趨勢併購該公司之後，使其成為旗下產品。相較於先前的版本，最近推出的 LeakProof 5.0 在功能上的主要不同之處，在於採用體積更小的指紋特徵檔，提高比對資料內容的速度，其次，則是具備繁體中文的操作介面，並提供更加完整的法規範本，因此使得產品的部署變得愈加容易。

特色是能提供可安裝在虛擬平臺的管理伺服器套件，能降低產品的部署費用，而 LeakProof 原本只有主機型的 DLP 產品，需由一臺專用的管理伺服器硬體，搭配代理程式所組成，不過，從新版產品開始，趨勢也提供可以安裝在 VMware 虛擬平臺的管理伺服器套件，在採用後者部署的前提下，產品只需要依使用者授權人數的多寡計價，而不需要負擔額外購買硬體設備的費用。

趨勢目前已將 DLP 的功能模組移植到現有的 Threat Discovery Appliance（TDA），這款網路病毒的防護設備，使它能兼任 DLP 閘道器的角色，TDA 也是採用鏡射方式設置在企業內部的網路骨幹，檢查進出的流量當中，是否有需要受到保護的機密資料存在。

透過 Remote Crawler，可在遠端的檔案伺服器本機分析檔案內容，製作指紋特徵，而 Data DNA 是 LeakProof 的機密資料辨視技術，用來學習機密資料的 LeakProof 5.0 將單一檔案擷取出來的指紋特徵體積，縮小到只有 128Bytes，在不影響辨識率的前提下，加快檢查檔案內容的速度。除了透過共享資料夾將檔案取回管理伺服器分析之外，LeakProof 也能透過 HTTP 連接微軟的 SharePoint 伺服器，利用後者的知識庫，產生機

密資料的指紋特徵。

Remote Crawler 是 LeakProof 5.0 的新功能，透過它可以在不需要開啟資料夾共享的情況下，直接在檔案伺服器本機分析機密資料的內容，最後將製作出來的指紋特徵傳回到管理伺服器，如此一來，可以減少 DLP 傳送資料時所使用到的網路頻寬（當資料在單一伺服器、多點管理的跨廣域網路架構下，影響較為明顯），及管理伺服器分析檔案內容時的硬體消耗。另外可以從管理伺服器的網頁介面，下載約 70MB 大小的 Remote Crawler 主程式，安裝在 Windows 平台的檔案伺服器。開啟 Remote Crawler 的應用程式介面，在此可以設定供 LeakProof 分析內容的本機資料夾路徑。除此之外還可整合代理程式即時阻攔洩密訊息

LeakProof 的主機端代理程式可以透過 Windows AD 的 Logon Script 等多種方式安裝到使用者電腦，程式執行時，系統列預設不會出現常駐圖示，同時也會在背景程式的清單當中自行隱藏，避免使用者將其關閉，而影響防護效果。產品對於洩密事件的預設處理動作為僅作記錄，然後放行通過，管理者可以修改 DLP 的控管設定，改採即時阻攔的方式加以管理，此外，也可以將有問題的檔案複製一份儲存於管理伺服器，做為日後備查之用，或者由使用者在代理程式顯示出來的詢問畫面，填寫資料的攜出原因之後，才會解除封鎖。

LeakProof 能辨識 300 種以上的檔案格式，在此之後，和其他這次所測試的 DLP 產品一樣，可以透過關鍵字（包含身分證字號一類的特殊關鍵字），及指紋辨識兩道程序，檢查使用者傳送出去的資料是否需要控管。對於 SQL 伺服器存放的個人資料，我們可以透過關鍵字過濾的方式來做防護，LeakProof 採用的做法和 McAfee 的 DLP 產品一樣，可以設定當傳送出去的資料大於一定筆數時，才會觸發 DLP 的防護動作，範圍之內的資料則視為正常動作。

另外如果以郵件嘗試傳送機密資料，LeakProof 的代理程式會主動刪除郵件附檔，僅允許不含機密內容的郵件本文傳送出去，如果試圖將檔案的內容複製起來，貼至郵件內文傳送時，在按下「Ctrl+C」的快速鍵時，就會觸發 DLP 的防護動作，禁止文字轉貼。在即時通訊的洩密預防上，除了各家 DLP 產品皆支援的 MSN 之外，LeakProof 也支援具有加密能力的 Skype，可防止使用者透過文字訊息，或者是傳送檔案的方式傳送機密資料。

周邊裝置的控管方面，LeakProof 在功能上相當彈性，不僅可以完整封鎖連接埠的使用，對於隨身碟一類的 USB 儲存裝置，則可以設定白名單，允許特定的裝置連接個人端電腦。為了方便設定，LeakProof 提供了一支工具程式，從管理伺服器下載執行之後，程式會將結果輸出於網頁，以便收集裝置的相關資訊。

LeakProof 5.0 較前版產品易於部署及管理，在外觀上，除了將設定介面的語系全面中文化，同時也提供了流程圖形式的設定介面，讓使用者不需要多花時間研究產品的設定邏輯，只要按照流程圖所要求的 5 個步驟，完成各項設定，很輕易地就可以完成政策的制定與派送。此外，產品本身也內建 5 個可以直接套用的法規範本，因此也不用像其較早期的版產品一樣，要手動設定法規範本的稽核項目。網頁介面首頁提供了儀表板式的事件圖表，因此管理者能夠快速瀏覽違規事件的摘要統計，另外 LeakProof 5.0 在功能上，強化了與 Windows AD 之間的整合，因此可以透過產品所提供的報表，得知目前有那些人違反了企業的管理政策。(趨勢科技,2013)

3.5.4 McAfee Host Data Loss Prevention 3.0

McAfee Host Data Loss Prevention（簡稱為 HDLP） 3.0，主要提供 DLP 及周邊控管的功能。它也是 McAfee Total Protection for Data 功能的一部分，這套最高階的資料防護產品同時具備 DLP、周邊控管及目錄檔案的加密等 3 項功能。McAfee 的 DLP 技術，主要來自於 2006 年被該公司併購的資安廠商 Onigma。(Mcafee,2012)

就架構而言，HDLP 是一款主機型的 DLP 產品。它和同廠牌的許多資安產品一樣，都是架構在 McAfee 行之有年的 ePolicy Orchestrator（ePO）。透過 ePO 的管理介面，使用者可以設定 HDLP 的控管政策、閱覽報表，及派送 DLP 的代理程式。就計價方式來說，由於這套產品有版本的差異，因此它主要是以用戶所採購的功能模組不同，再以使用者授權數量的方式決定價格。

McAfee 的 HDLP 目前在技術上可以同時支援標籤及指紋特徵等 2 種技術， 在設定上，可以根據檔案的存放路徑，及特定應用程式所產生的檔案等 2 種方式，將辨識所需的標籤加入，貼上檔案，但有別於採用同類型技術的 DLP 產品，HDLP 在做法上並不會針對檔案本身執行任何的寫入動作。舉例來說，當資料從定義為機密存放路徑的共享資料夾，複製到個人端電腦後，HDLP 會將標籤寫入到一個資料庫檔案，而不是檔案本身，因此不會對於內容造成任何改變，造成企業管理上的疑慮。

McAfee HDLP 的指紋特徵在做法上，是採用字詞方式比對檔案間的相似度，做法上，與前述的 Websense DSS 及趨勢 LeakProof 等 2 款產品較為類似。使用者可以指定讓 HDLP 分析共享資料夾的檔案，後續可透過排程方式定期掃描，維持指紋庫的完整性。

而 HDLP 的代理程式在使用上，必須在個人端電腦已經安裝 ePO 代理程式的前提下，才能透過前者的管理介面主動派送。完成安裝之後，雖然代理程式會在系統列顯示

一個常駐圖示，不過使用者無法透過手動方式關閉它，以規避 DLP 的檢查。此外，它的代理程式在電腦無法連線到 DLP 管理伺服器的離線狀態下，仍然可以針對使用者傳送機密檔案的行為加以控管。

另外對於存放在 SQL Server 資料庫裡的個資，HDLP 可以採取特殊關鍵字的方式加以過濾；信用卡的部份，可以直接套用內建在 HDLP 的規則做檢查；至於臺灣使用者環境才獨有的身分證字號，目前仍然必須透過手動方式設定規則後，才能加以檢測。如果使用 SMTP、Webmail 等 2 類郵件，HDLP 可以在使用者寄信過程中，當完成夾檔，準備傳送時，就中斷資料的傳送，同時透過代理程式秀出警告訊息。至於將機密文字內容貼在郵件本文傳送出去的方式，則可設定 HDLP 禁止使用者針對機密檔案的內文剪貼、複製；啟動這項功能之後，轉貼過去的內文將會變成 DLP 的警告文字。

針對即時通訊的控管，HDLP 在功能上可以支援 2 種即時通訊軟體，當使用者透過即時通訊軟體傳送被 DLP 界定為機密資料的檔案時，MSN 和 Skype 會立即離線，中斷所有訊息的傳輸，同時電腦桌面的右下角也會出現警告訊息，提示使用者須重新啟動即時通訊軟體的主程式後，才能繼續使用。

在稽核部份，可透過 ePO 平臺閱覽 DLP 的完整事件報表，切換閱覽 DLP 的狀態儀表板，可快速了解機密資料的控管狀況，監控的所有記錄所得的事件皆條列在此，可使用設定篩選器，選取管理者所需要的事件加以閱覽，HDLP 針對事件提供了相當完整的記錄，除了一般的違規原因，及查閱傳送出去的原始檔案之外，也一併列出欲傳送的目的地，便於日後舉證。

McAfee 除了主機型的 DLP 產品之外，也有採硬體型式推出的 DLP 閘道器設備，兩者在架構上是各自獨立運作的產品。早期的 DLP 閘道器，是從該公司的 Secure Internet Gateway（SIG）硬體閘道器所修改而來，可用來檢測使用者透過網路的方式傳送機密資料的行為。不過，隨著 McAfee 在 2008 年併購了另外一家網路型 DLP 廠商 Reconnex 後，前述的設備便為新款的產品所取代。因此，目前 McAfee 的 DLP 閘道器分為 Network DLP Discover、Network DLP Monitor、Network DLP Manager，及 Network DLP Prevent 等 4 種，前身皆為 Reconnex 所推出的硬體閘道器設備。

這些設備的差異主要是功能。就像 Network DLP Discover 是一款稽核設備，它可以透過網路掃描的方式，檢查內部端點是否有可能造成資料外洩的漏洞存在；Network DLP Monitor 的運作方式和其他廠商推出的 DLP 閘道器相同，都是以鏡射方式收集進出網路的流量；Network DLP Prevent 則是能夠和自有的 Web Gateway 等第 3 方閘道器產品相整合的設備，攔截透過網路傳送的機密資料；至於 Network DLP Manager 則是用來管理前述 3 種設備的管理伺服器硬體。

3.6 DLP 資料外洩防護系統導入策略

DLP 系統的導入，不同的企業有著不同的基礎架構，各廠牌的系統也皆有其不同的導入方式，圖 10 是系統建置概念圖，但一般來說會依循基本步驟及防護概念來導入，簡單來說會將 DLP 的導入大致分為以下四個階段：1.文件分類，2.建立機密資料，3.政策佈署，4.告警及紀錄分析。(Websense ,2013)

階段一：文件分類,政策制定

一般企業均無法掌控他們的機密資料，因機密資料的辨識、存取以及轉移並未整合至他們的整體作業程序中，同時也可能分散在不同的部門。所以開始導入時，則必須請相關單位配合，將各部門的機密資或者資料庫資料位置，提供給 DLP 系統來學習，以及分級並確定套用適當的規定。例如財務部門的資料可以傳輸到會計師事務所，但不能在傳送到網路硬碟等行為,這些規定與程序定義了這些公司資料的保護方式。如此一來，員工與主管便都負有責任，來確保公司的重要資料不會外洩。

階段二：建立機密資料的指紋(Fingerprint)

透過產品專屬的管理伺服器，提供集中化的檢視及政策設定，從定義為機密文件內容當中擷取資訊，各家不同的的演算法能從內容當中擷取資訊，為每一份文件製作出獨一無二的檔案特徵序列，也就是所謂的「指紋」。這些「指紋」就能讓端點裝置在上線或離線時，或閘道器強制實行保護措施。

階段三：政策部署到用戶端以及閘道器

界定好以及學習完機密資料的指紋特徵後，透過管理伺服器把政策布署到用戶端以及閘道器，用戶端透過自動與管理伺服器溝通來收取政策與更新資料，並且將違規事件回報給管理伺服器。 端點裝置上安裝了用戶端驅動程式來監控網路流量、I/O、應用程式操作。部份產品可以在在敏感資訊離開公司之前將資訊加密以防止外洩。用戶端代理程式也包含分析引擎可以利用先前步驟所建立的指紋、規則表達式 (regular expression)、關鍵字及中繼資料 (metadata) 提供即時過濾。

階段四：告警以及記錄供辨識分析之日誌

一旦搜尋端點裝置 (如筆記型電腦、桌上型電腦及伺服器)，或者網路閘道器上偵測到政策所制定未獲允的機密資料。其互動式的「告警」讓 IT 管理員定義內容感知對話方塊，直接顯示在員工的電腦畫面上。 這些對話方塊內含自訂的 URL 連結，可藉此教育員工如何正確處理機密資訊。 未獲授權的資料傳輸將被攔截，這些偵測到洩密行為時的內容都必須一一紀錄，提供日後做為分析以及鑑識。

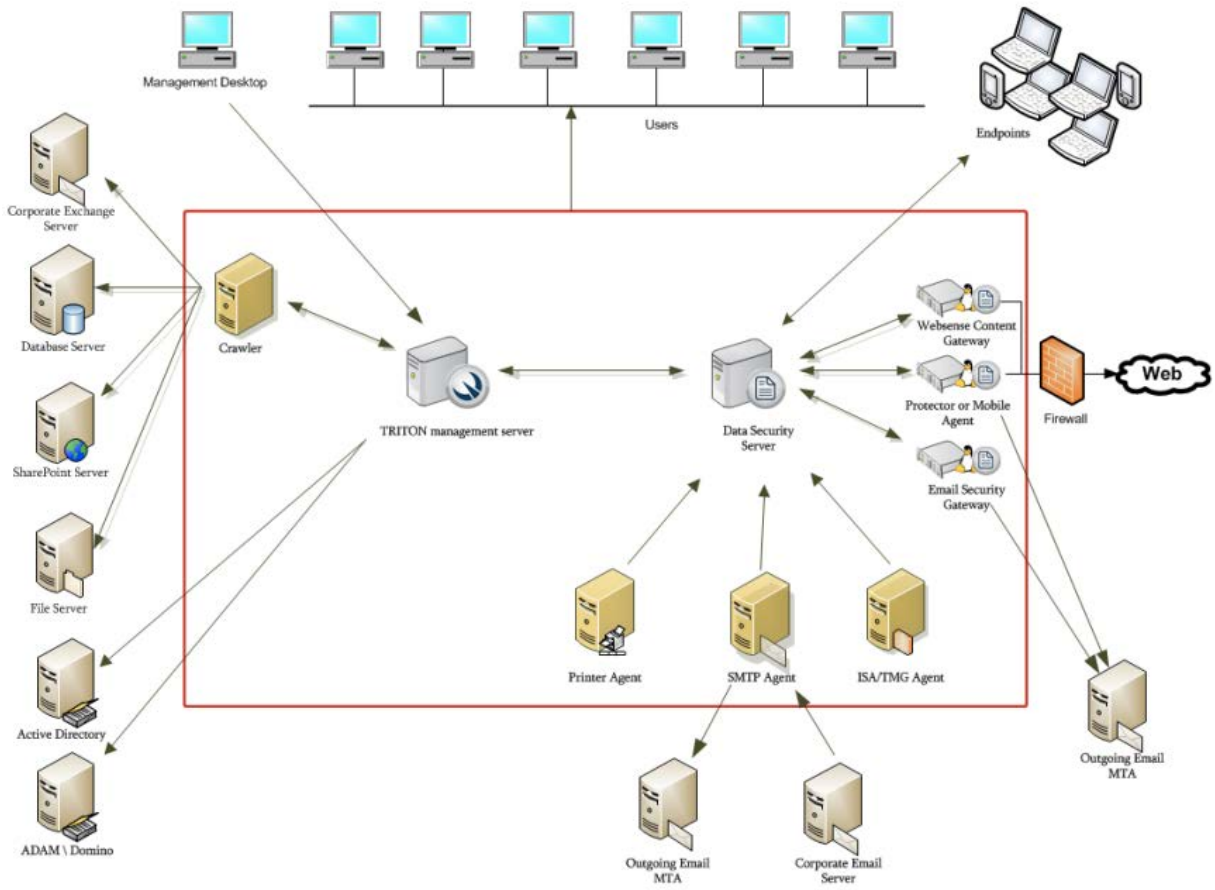

圖 10 DLP 導入架構示意圖

資料來源：(Websense Inc,2013)

第四章　研究架構與方法

4.1 研究方法選擇

質性研究是利用質性的資料來解釋(Explain)或瞭解(Understand)特定的社會現象，而目前主要社會科學的研究方法，主要包括實驗調查法(Experiment)、調查報告(Survey)、檔案紀錄分析(Archival Analysis)、歷史研究(History)及個案研究(CaseStudy)等，每個研究策略都有其優點及缺點。

另外在相關文獻中 Yin（1994）認為研究方法的選擇需視以下幾種情形而定：研究問題的類型、研究者在實際事件上所做的操控、以及研究重點在當代或是歷史的現象。如表 3 所示。由於本研究針對 A 與 B 公司現階段導入 DLP 資料外洩防護系統，探討其在同樣導入 DLP 資料外洩防護系統在不同公司建置上，為什麼企業需要此系統，如何導入，而影響導入成功原因又是什麼，二者導入後結果是否相同？符合「是什麼」與「如何」的研究問題形式，與 Yin 所提出的這三種情況不謀而合，因此本研究將會採用個案研究方法來進行。

表 3 不同研究策略矩陣

研究策略	研究問題形式	是否需要在行為事件上操控	是否著重在當時的事件上
實驗法	如何、為什麼	是	是
調查研究	什麼人，是什麼，在哪裡，有多少	否	是
檔案紀錄分析	什麼人，是什麼，在哪裡，有多少	否	是／否
歷史研究法	如何、為什麼	否	否
個案研究法	如何、為什麼	否	是

資料來源：Yin,1994

4.2 研究設計類型

依學者(Herriott and Firestin,1983)指出，普遍來談說由多重個案研究得到的證據較為穩健而且有力，也因此整個研究常被認為是較為值得參考。其缺點方面，多重個案研究通常無法滿足採用單一個案設計的原因，一些特殊的個案(例外或少見的個案、關鍵性個案等)就不適用多重個案法，而且多重個案研究需要更大量的資源和時間。

根據 Yin(1994)個案研究中提出，個案研究法其包含單一個案研究與多重個案研究，分析項目也存在單一分析與多重分析兩者不同類型，因此可組成四種設計類型：如所表 4 示：

表 4 個案研究設計類型

	單一個案設計	多重個案設計
單一分析單元（整體性）	類型一	類型二
多重分析單元（嵌入性）	類型三	類型四

資料來源：Yin,1994.

故本研究適用於多重個案單一分析單元的設計，因為是以「A 和 B 公司」作為研究個案，在二家不同公司上分析 DLP 資料外洩防護系統導入影響的關鍵因素為何。

4.3 資料蒐集方法

一般質性資料來源包括初級資料以及次級資料，而蒐集初級資料的方式包括：深入訪談法、德菲爾法、直接觀察法等；另外在(Malhotra,1993)認為深度訪談法是由面談者使用非結構性、直接的方式與受訪者接觸，是一種單獨的、個人的互動方式，用來發現受訪談個案基本的動機、行為、方式等。

依據上述原則，故本研究的資料蒐集方式主要是以訪談、直接觀察與實際接觸、並參閱個案所提供書面文件與相關資訊和記錄為主，其目的在於蒐集並記錄有關於個案公司的所有跟研究相關有用資訊與資料。本研究的資料蒐集來源以初級資料為主，次級資料為輔助。在初級資料方面，是採用深度訪談與實際參與的方式，並採半結構性的問題來進行訪談，以確保掌握訪問重點與研究相關。而在次級資料方面，舉凡與個案公司相關的研究或資料、個案公司所提供的相關書面文件以及公司檔案資料與紀錄均列為蒐集範圍，並由不同資料來源與受訪者內容互相去驗證，之後以歸納出研究發現與相關建議。

根茲依據本研究所述所引用文獻探討中所引用之資訊系統導入之應用理論架構設計出主要訪談題綱，並針對個案 A 和個案 B 公司進行如表 5 所列項目訪談：

表 5 訪談題綱

構面	因素	訪談題綱
組織	高階主管支持	1. 是否獲得高階主管支持 2. 決定採購的關鍵？預算？成效？法規？ 3. 導入 DLP 系統主要考量哪些項目，這些項目對公司有何影響？ 4. 風險評估？
	資源	1. 專案獲得資源與權限、執行程度。 2. 部門配合程度？ 3. 跨部門溝通協調？
	優勢	1. 改善程度 2. 系統導入的(量化)成效？ 3. 與現有系統的相較帶來的效益？
專案	參與度	1. 使用者行為是否改變？ 2. 使用者配合程度，被 audit，側錄？ 3. 員工對導入系統的接受與抗拒程度？
	專案團隊	1. 專案團隊程度？如何遴選？ 2. 導入流程 Step 為何？ 3. 導入策略、責任分工，主導程度？
環境	科技基礎	1. 與原有系統的整合度？ 2. 目前基礎資訊安全建設為何？ 3. 公司文化(產業)問題？(例:傳統產業與科技業對隱私保護的認知) 4. 相關政策影響範圍？
	產業環境	
科技	系統支援	1. 建置系統相容性？學習文件來源取得？最大的阻礙點？ 2. 導入後情況？符合需求？正確(誤判)、安全、方便？ 3. 建置時程複雜度與系統易用性？效能問題？和既有系統相容性？ 4. 教育訓練 5. 產品是否成熟足以帶來效益？
	系統品質	
	科技成熟度	1. 原廠顧問服務與技術支援性，產品在市場成熟度？ 2. 客制化需求能力

4.4 研究個案選擇

個案公司選擇方面，由於目前導入 DLP 資料外洩防護系統的公司尚未普及，所以主要以方便性、能夠實際接觸、以及能配合深度訪談，是選擇個案的主要標準。另外為求研究資訊的正確性及豐富性並達研究目的，本研究的個案選擇對象符合下列條件：

1.所選取個案公司近期內成功建置完成 DLP 資料外洩防護系統。
2.所選取的個案公司規模在百人以上，且有中等程度的資訊系統建置。
3.所選取的個案公司在該產業領域裡，居優秀地位並具有競爭力。
4.所選取的個案公司配合意願高，並可提供相關資訊以及可驗證之有用資料。

除此外為了了解不同產業的公司文化是否也是影響導入的因素，並增加研究的信度，所以本研究依據上述條件，選擇二家規模大小相同，但不同產業，不同公司文化之個案公司為研究對象，其個案背景及介紹如第四章節所述。本研究之訪談對象以個案公司資訊主管或 DLP 系統專案建置負責人或其相關成員為主要的訪談對象，而公司內部其它單位的主管亦為資料蒐集的輔助訪談對象，以便獲得更完整的資訊。

4.5 研究架構

本研究根據文獻所探討之相關資訊系統導入成功因素之理論如表 6，並參考文獻中所探討的相關模型架構，以及針對文獻中所提出的影響資訊系統導入的研究構面，歸納出以下「組織」、「專案」「科技」以及「環境」做文本研究架構的主要四個構面做為本研究架構如圖 11 所示，並定義出下列幾個重要的關鍵因素作為本研究主要的分析因子，並依據四個構面十個主要因素設計訪談題綱，用來確立 DLP 系統導入成功與否的參分析要素。

組織構面包含的因素有「高階主管支持」、「資源」、「優勢」3 個衡量項目。專案構面包含的因數有「參與」、「團隊技能」2 個衡量項目，環境構面則為「科技基礎」、「產業環境」2 個衡量項目，而科技構面則為「科技成熟度」、「系統資源」、「系統品質」3 個衡量項目。在經過文獻整理以及本研究之概念性模式的提出後，總共有 4 個構面，10 個主因素，以下將對各因素分別解釋。

(1). 組織構面

正面的組織特性可以幫助資訊科技的成功導入。對於組織而言，需要耗費的資源甚

多，且內容上的規劃也很複雜。同時在建置過程中，權力轉移以及使用者抗拒的壓力將會接踵而來，因此計劃得到高階主管的認同與支持，或是影響建置的組織資源是否充足皆是很重要的(Grover and Goslar,1993)，以組織規模的大小皆是重要的考慮因素之一（Palviaetal,1994）。在建置過程中考慮組織的因素，將可減少組織所形成的限制與阻礙。

i. 高階主管支持

管理者的態度對於資訊科技的實施是相當重要的（Drury and Farhoomand,1996）。組織在資訊化及資訊應用上的好壞，決定於高階主管對資訊科技的認知程度及支持度，其中認知程度愈高，高階主管越會將資訊科技視為組織發展策略的一部份（Premkumar and Roberts,1999），如總經理或資訊長的態度以及高層主管支持與認知，如此公司對資訊系統的要求與配合才會有效率。再者除了同意專案的進行，高階主管還必須將其主動且熱心的支持讓組織所有階層的工作人員都能明白感受到(Grover and Goslar, 1993)。Zmud(1987)提到，沒有高階主管的支持，創新科技不太可能被組織或企業所採用。

ii. 資源

Kwon and Zmud（1987）指出成功的資訊系統必須要有足夠的組織資源，包括足夠的發展和使用時間、足夠的基金，還有足夠的科技技術，在導入新系統或事物通常都需要資源與經費，包括讓新系統在組織內部正常運作所需。因此表示組織內部充足的資源越多，那麼這個組織就會有更多的技術、訓練、資金可以運用並支援創新。

iii. 優勢

企業組織需要先評估創新資訊科技的效益 才能決定是否採用，其中必須要先評估創新 科技相對於舊科技的相對優勢(Premkumar and Roberts, 1999)。任何新的資訊系統能否提供未導入前所沒有的優勢，新系統其所帶來的效益可能包含有減少作業時間、較好服務品質並可減少成本，和獲得即時性的資訊等。所以在導入資料外洩防護系統後，是否可提供公司重要資料的保護，並減少機密資料外洩所造成的營業或者商譽損失等，這些都是在建置系統所必須考慮到的。

(2). 專案構面

i. 參與度

公司與新導入新系統的相關人員，其執行力和參與配合程度，都會影響專案導入的品質，以本研究之資料外洩防護系統而言，在機密資料界並不是資訊部門能決定，其必需跨部門協調以及配合，才能獲取不同單位的機密資料來源，另外在端點的防護系統安佈署上，也需全公司的相關作業人員配合才能順利導入，以往的研究指出，參與使用者對新系統的使用有直接的影響，良好的團隊必須評估新的系統對最終使用者的影響力，如此才能減低參與系統使用者的排斥阻力。

ii. 團隊技能

導入新系統的團隊中扮演重要角色的人員應該由具有專業知識的個人和專業紀律，並有相關的背景知識。此外該團隊成員需具有一定的經驗，包含建置廠商，內部使用者等，並了解相關的管理和維護知識，這部份是影響系統品質及以及是否成功相當重要的因素。

(3). 環境構面

i. 科技基礎

導入新科技資訊系統時，不同產業所擁有的科技基礎架構皆不相同，所以在新系統導入時，配合不同的組織環境與資訊化程度，對任何一個新的科技系統建置成功與否有很大的影響。

ii. 產業環境

在不同產業環境裡可能會有不同的相關知識以及資訊科技需求，在政府法規上也有著不相同法規(Tornatzky and Fleischer, 1990)約束情況，都是有可能影響新資訊科技系統導入是否成功的原因。

(4). 科技構面

i. 系統支援

建置資訊系統時，資訊科技所能影響的範圍包含相容性、複雜性，以及相對優勢（Reich and Benbasat,1990）。學者(Tornatzky and Klein,1982)在彙整 75 個研究中發現相容性、複雜性，以及相對優勢與擴散行為有一定的影響性。因此在建置新的系統時，能考慮這方面的議題，對於成功的建置會有很大的幫助。

ii. 系統品質

前面文獻提到 DeLone 和 McLean(2003)根據在提出一個成功的資訊系統所指標，要衡量資訊系統作業是否能夠成功，很重要的一個因素是資訊系統本身的所能提供的品質特性(即系統品質)、資訊系統產出的品質(即資訊品質)、資訊系統產出的消費(即使用)等。

iii. 科技成熟度

任何一個導入企業的科技專案，其資訊系統成熟度，意義為該系統在各層面應用上是否已具有相當的正面回饋，以及發展的過程中，已達到成熟及穩定性的程度，使其資訊系統能跟企業策略得以緊密配合

表 6 資訊系統導入關鍵成功因素整理

關鍵成功因素	*描述*	*相關文獻*
高階主管者支持	高階管理階層對於專案的支持程度為何。	Wixom & Watson,(2001) Tornatzky & Fleischer ,（1990）
可獲得相關資源	可供專案使用之預算、時間、人力為何，權限，以及相關的所有資源。	Wixom & Watson,(2001) Tornatzky & Fleischer ,（1990）
優勢	新導入之創新資訊科技是比現有或以前的科技擁有更多的效益以及優勢。	Wixom & Watson,(2001) Tornatzky & Fleischer ,（1990）
使用者參與程度	相關參與專案時之合作與配合情形與投入程度，以及組織全體對於建置系統之目標認知	Wixom & Watson,(2001) Davis,(1989) Tornatzky & Fleischer ,（1990）
專案團隊能力	專案團隊成員的技術能力與認知和跨部門的溝通協調能力	Wixom & Watson,(2001) Tornatzky & Fleischer ,（1990）
科技基礎	企業本身的科技基礎建設以及相關導入系統所需的科技知識	Tornatzky & Fleischer ,（1990）
產業環境	產業環境特色、相關政府法令、競爭對手。	Tornatzky & Fleischer ,（1990）
系統資源	提供相關資料或資訊或資源整合或者導入新系統所需之資源品質優劣。	Wixom & Watson,(2001) Tornatzky & Fleischer ,（1990）
系統品質	對系統本身的品質衡量，包含效能、功能性、易用性、擴充彈性、輸出正確性。	DeLone McLean,(2003) Davis,(1989)
科技成熟度	建置一系統時，對於硬體、軟體、相關方法，科技技術與可行方案間的成熟程度。	Tornatzky & Fleischer ,（1990） Wixom & Watson,(2001) DeLone McLean,(2003) Davis,(1989)

資料來源：本研究整理

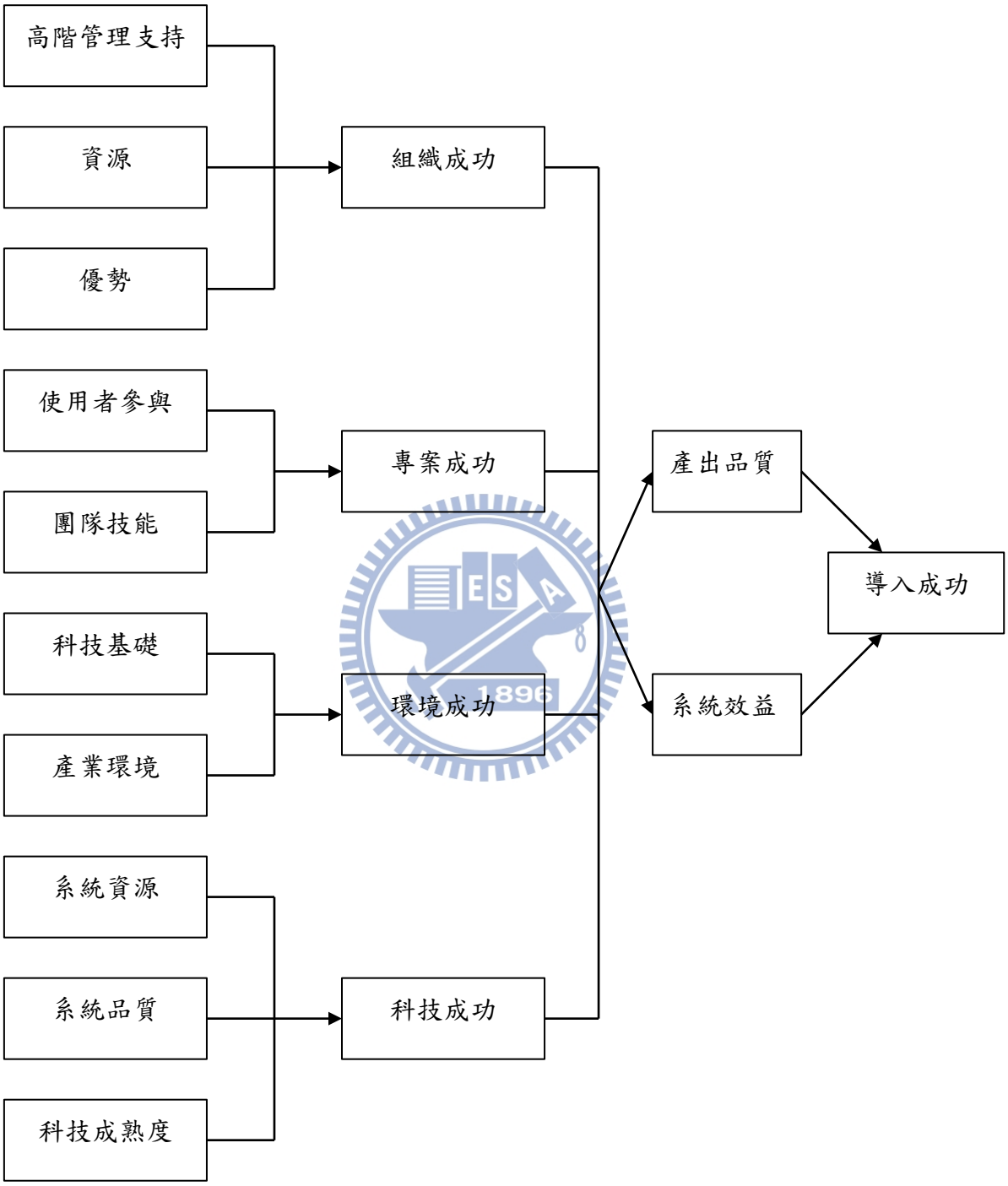

圖 11 研究架構

資料來源：本研究整理

第五章　個案討論與分析結果

本研究談訪談了二家不同型態及產業的企業，根據訪談及相關資料，仔細且客觀的分析不同的受訪者在訪談過程中所描述的資訊，並且由此訪談內容去思考和發現有意義且與本論文的研究問題相關的決策以及行為模式，透過這樣直接面對面的訪談，嘗試去了解，不同產業及不同背景的公司在內部的重要資料保護是用何種方式去應對，以及採取怎樣的策略以及考量的因素有哪些。

5.1 個案 A 公司

5.1.1　公司簡介

A 公司，其員工數為 200 人，資本額為 2 億 4990 萬，主要以提供生前契約及禮儀服務為主的公司，該公司經營理念為：「落實環保理念，改革殯葬文化」為己任，把傳統繁複的喪葬禮節去蕪存菁，稟持「簡明、莊嚴、尊貴、專業」四大理念精心策劃出兼具市場性、時代性、正統性之一元化喪葬禮儀服務，期以創造生命昇華之價值，為人生旅程畫下完美句點。

A 公司的集團由往生事業起家，歷經二十多年陸續成立福座開發、禮儀服務、北海福座墓園、服務行銷；轉投資休閒事業的西湖渡假村、水立方時尚館；其也長期投入社會弱勢關懷公益服務，並成立社會福利慈善事業基金會、以及松崗資產等企業。期以近、中、遠的規劃，促使企業經營商品多元化、事業領域多角化。

A 公司從民國 82 年成立迄今，服務案件數已有數萬件，其企業標榜擁有國內服務經驗豐富的團隊，目前是頗具規模的禮儀服務公司，現今全省各地均已設立連鎖服務網，以下為其主要商品及服務項目：

- 喪葬用品代理與買賣
- 代辦喪葬事宜業務
- 鮮花及禮儀禮品之買賣業務
- 前各項有關產品之進出口
- 國內廠商向金融機構提供消息或媒介之顧問業務（不包括辦理融資保證等授信業務）
- 花卉批發業
- 花卉零售業
- 祭祀用品批發業

- 祭祀用品零售業
- 圖書批發業
- 書籍、文具零售業
- 國際貿易業
- 投資顧問業
- 殯葬禮儀服務業
- 仲介服務業
- 殯葬場所開發租售業
- 不動產仲介經紀業
- 其他批發業
- 除許可業務外，得經營法令非禁止或限制之業務

5.1.2 產業現況及發展概述

殯葬禮儀服務業在台灣現況產業生態中，根據內政部殯葬資訊網所提供的資訊，主要以經營服務地理範疇區分可分為「單體區域性經營」及「連鎖全區性經營」兩類，若以服務對象來源區分可分為「期約客源型」及「現用客源型」兩類

如果將前述分類綜合區分則現今殯葬禮儀服務業約可區分為三大類：

I. 大型連鎖業：其經營範疇遍及全國，各縣市均有其服務據點，且服務對象來自各大醫院或特定團體。(例如：萬安、台灣人本…...)
II. 品牌財團業：其經營範疇遍及全國，各縣市均有其服務據點，但服務對象來自「生前契約」或其他期約方式。(例如：國寶、龍巖…..)
III. 傳統經營業：其經營範疇局限於特定區域，甚少有其他服務據點，服務對象來自介紹或自來客。

其中「大型連鎖業」及「品牌財團業」，以其規模經濟及財力資源，目前囊括服務市場量一半以上，且因人力資源充沛財力充足，不但建立起「社會品牌形象」，且幾乎在為殯葬禮儀服務建立「服務產品規格」，此一狀況不斷在萎縮「傳統經營業」的生存空間，以家數而言傳統經營業幾佔 95%，但卻只能在日漸被壓縮的市場中經營。

5.1.3 導入動機(需求)分析

A 公司目前有將近 40 萬的客戶資料，根據訪談內容，其中有將近 20 萬筆是目前機會客戶（已購買契約但尚未執行合約內容之客戶）資料，他們又稱為 Active Customer，這些客戶為有潛力機會做其它的產品行銷，依描述在民國 98 年首次發現有不少重要客戶資料在其它地方流通，經常被客戶投訴個人資料遭受盜用，遂請資訊單位著手調查採取相關資訊系統工具防止重要的客戶資料外洩，以及公司重要營業機密被竊取。

根據訪談，該公司之後遂請資訊單位規劃長期、中期、短期資訊安全計畫，如表格 4.5.6 所提內容，A 公司曾經在 99 年導入相似的資料外洩防護產品 IPGuard，就前面文獻所述，該產品設計屬於週邊控管以及檔案控管的階段，其週邊控管是由中央控管所有終端電腦的儲存裝置，以及 USB 隨身碟、外接式硬碟、燒錄機或印表機等輸出入裝置，需由資訊人員陪同或認可才能使用；缺點是不夠人性化，易造成人員作業上諸多不便。而且會「改變原本單位內同仁的使用習慣」，並有可能犧牲電腦部份的使用功能，其造成相關業人員怨聲載道以以作業上的不方便，另外在外勤人員部份也常常因為這樣而無法帶回家加班，即時的完成工作或者存取相關資料。

其中資訊處長表示：「為了作業方便，公司終端裝置與網路其實是採開放性的管理方式，也就是並不想設限員工使用行為，但又必須要能夠針對這些重要機密資料進行管制，因此格外需要 DLP 這類解決方案來協助控管。」訪談中也談到，重要資料大多會因為不同作業行為而流動於各員工的終端設備，而開放網路與行動裝置存取也讓資料控管更加困難。

針對該系統客戶目前主要遇到以下問題：

1. 無法防範檔案的建立者機密資料外洩：文件的建立者（或者擁更大編輯權限的使用者），如果將內容複製到 Email 外洩，即可將機密文件傳送到公司以外。

2. 保護的檔案格式更限：檔案控管以及加密的系統皆會針會針對檔案的格式設計，但所以每一個不同的應用軟體（每一個版本）都必開發一個特定的 plug-in 分析程式，因此受限於 Microsoft Office、Acrobat PDF 等眾多不同的文件應用程式檔案格式。

3. 需要改變員工以及使用的習慣：譬如作者需手動設定權限，文件才受保護。

4. 需要犧牲電腦的使用功能：限制週邊儲存裝置、輸入出裝置、網路、Email、MSN 的使用功能，譬如限制使用者無法使用 USB 隨身碟、MSN 不能傳送檔案等。

5. 需要改變原有的資訊管理的制度以及流程：譬如需要制定不同單位的權限政策、進行文件的分級、整合其他權限控管系統如 LDAP、ActiveDirectory 等等。

表 7 個案 A 公司短期目標(99 年)：資訊機房安全鞏固

建置項目	功能說明
IPGuard	資訊安全與稽核
McAfeeIPS	入侵防禦管理
AnchivaWeb	安全閘道管理
McAfee 防毒	防毒管理
SSLVPN	禮儀服務同仁、聖恩工作夥伴遠端登入公司網路安全閘道

資料來源：A 公司提供

表 8 個案 A 公司中期目標(100 年)：一般使用者管理

建置項目	年度計畫	說明
人員帳號管理	➢ AD&Excahnge 重建	1. 人員帳號中央管理機制
存取控制管理	1. AD&Excahnge 重建 2. 機房備份強化–DPM 機制	➢ 檔案伺服器權限管理 ➢ 防止人為誤刪檔案
資料外洩防護	(1). 資訊安全–WensenseDLP (2). 網路設備–Router、Switch	➢ 過濾、記錄公司機密資料 ➢ 加強網路監控，分析 ➢ 監控使用者 PC 上作業
網路負載管理	➢ 資訊安全–SonicWALL 防火牆	1. 確保防火牆不會因單點的故障，造成服務中斷。
電子郵件安全	➢ AD&Excahnge 重建 ➢ 資訊安全–CiscoIronport	1. 將進入之郵件作一份副本儲存，利用圖形化工具查詢，以共日後稽核之用。

資料來源：A 公司提供

表 9 個案 A 公司長期目標(101 年)：強化短、中期工作目標

建置第 2 階段防止資料外洩：
1. DataProtect：「稽核」、「阻擋」公司機密資料外洩
2. DataDiscover：盤點查核企業內機密資料。
3. 配合個資法暨施行細則，持續調整國寶資訊安全政策

資料來源：A 公司提供

5.1.4 導入過程

在此以前，其實 A 公司已經導入 IP Guard 周邊控管類型的防護產品，在主要功能上，雖然可以防止其他使用者不當存取檔案，但是對於擁有完整讀寫權限的人來說，可說是防不勝防，以至於後者則是僅能封鎖一部分的資料傳輸管道。

此次 A 公司所採用的是 Websense 公司的 DataSecuritySuite(DSS)，是該公司在 2006 年收購資安廠商 PortAuthority，利用其技術推出的資安產品。其具備了主機型和網路型 DLP 的能力，能整合多種網路伺服器提供保護。

A 公司是先以網路閘道來部署，其部署在台北以及三芝 2 個據點的網路出口，採旁聽（側錄）的方式來監測，檢查流量當中是否含有機密資料。待偵測以及設備效能上沒有狀況，才更進一步提升供的控管需求，爾後才會考慮在個人端電腦上安裝代理程式。A 公司在安裝代理程式的做法，是先以資訊部門的員工做為測試對象，即使產生問題也不會造成太嚴重的影響，直到測試確認不會和企業現有的應用程式相衝突之後，再擴大部署範圍。目前他們一共部署了 2 台 DLP 的閘道器，及 1 台管理伺服器。他們目前所界定為機密資料的檔案，主要是微軟的 Office 文件、客戶資料庫 SQLServer，供應商管理系統資料庫，以及業務和訂單系統等 5 種。

階段一：界定機密資料範本

DLP 在功能特性上，是一種內容學習以及過濾型式的資安系統，因此必須提供機密資料的來源檔，供系統分析，產生特徵檔，才能以相似度高低的方式，辨識資料的真實屬性。就來源來說，除了一般最常見的檔案伺服器之外，像是 SQL Server 資料庫、Share Point Server 這類的知識平臺，乃至於員工儲存在郵件伺服器的郵件，都有可能在其中儲存了需要保護的資料或機密內容。所以客戶導入 DLP 是採分階段的方式做建置，以免影響到現有運作中的環境。所以第一步必須先知道機密資料的來源以及種類，才能有效避免產品導入後，仍不斷有外洩事件的發生。

由於同一企業的不同部門，被界定為機密資料的檔案也不盡相同，因此 A 公司在界定機密資料，以先做跨部門協調，並請各部份主管與會以及相關接觸重要資料行政人員，明確指定那些檔案，資料庫，為機密檔案，並提供可能擺放的來源位置以和授與相關存取權限之後，提供範本檔，而不是先直接針對放有資料的整臺伺服器做掃描分析，如貿然作業，可能會增加 DLP 的導入難度。

另外 A 公司是屬於服務業類型，客戶資料庫中也有基本的常用訊息，所以初期除了

由各部門提供相關機密資料訊息外，也針對系統本身所內建的範本來保護相關資料，如信用卡法規 PCI-DSS，台灣地址、身份證號碼等相關的組合，如在不合法系統政策上被偵測，也會做相同的阻擋策略。

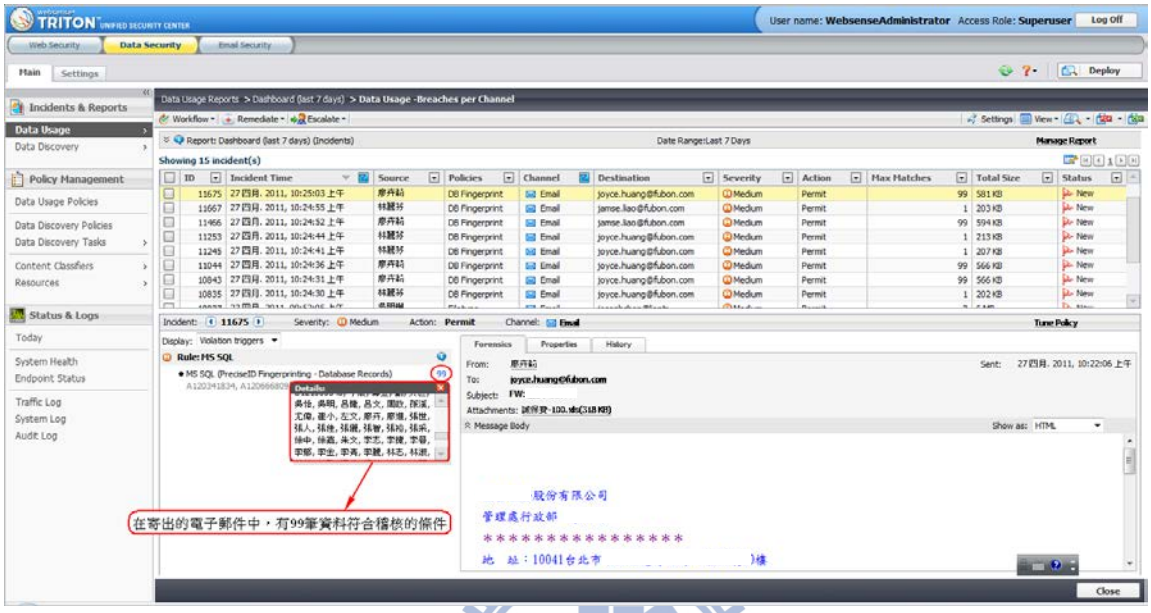

圖 12 A 公司啟用資料庫學習模式所偵測洩密情況

資料來源：A 公司提供

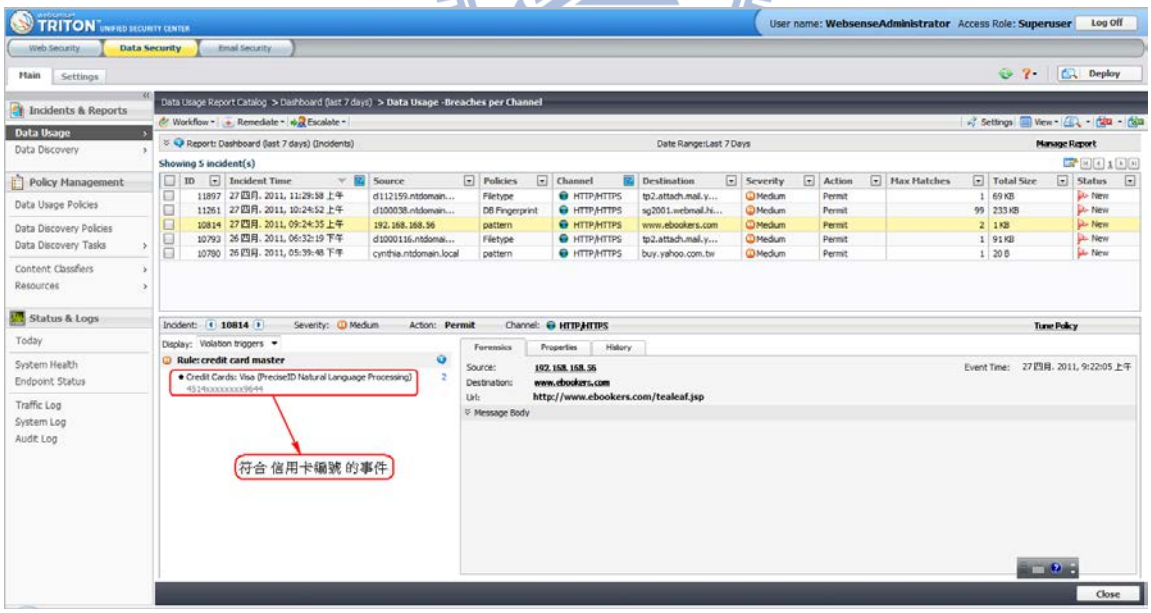

圖 13 A 公司啟用內建信用卡法規範本所偵測洩密情況

資料來源：A 公司提供

階段二：資料分析

由於此 DLP 所記錄下來的，大多是 A 公司內部的機密資料，對於資訊部門來說，並不一定有能力稽核這些事件是否為誤判，所以該單位採取的方式是交由各部門內專責資安的資訊人員來稽核這些記錄，主要是透過郵件通知的方式，所以在告警設定上以及報表的管理方面，目前他們的做法是由各部門主管要求閱覽報表，當洩密事件發生時，DLP 會寄發郵件告知資訊部門，再由資訊部門轉告該單位的主管處理，讓該部門負責人去了解內部員工，機密資料外流事件如何發生，以及指出哪些資料為誤判的狀況。由於 DLP 能提供事件的即時阻擋紀錄，同時也是洩密事件發生時的重要舉證工具，因此對於報表功能的提供的資訊的完整性，也是 A 公司在導入階段時特別注意的部份。

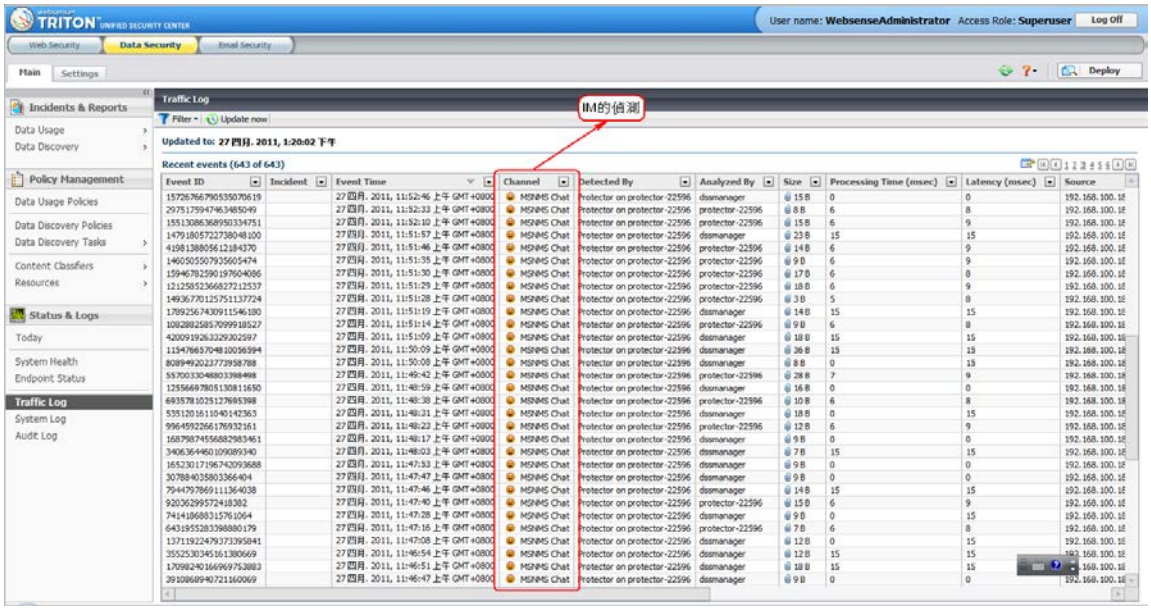

圖 14 A 公司在系統上線後所偵測 IM 洩密日誌

資料來源：A 公司提供

5.1.5 導入結果

1. 對公司資料流有效管理與監控：

A 個案公司原有資安系統並無法針對機密或者重要資料的流向做有效的監控和深入的管理，經由 DLP 系統的導入，原本各部門重要資料只有他們知道，統一管理上有其難度，導入後將其重要的資料納入系統，不但讓重要機密資料能有效保護，也能讓這些資料統一的被管理和監控，協助管理當局更為有效的整合與相關重要機密資訊和流向，還能將作業模式作更細緻的管理、搜尋使用行為與確認使用者身分等等，進行較為精細嚴謹的控管機制。

2. 預期系統效益達成：

訪談過程中客戶提到，在資料外洩的偵測上，在建置以來其監控到外洩的情形比想像中來得多，也直接表示原本公司這些會因為人為的蓄意或者意外所洩漏出去的重要機密資料，在系統導入後受到保護，與原本使用者預期上線後所能提供的訊息要來得多，這些訊息也意外的讓專案小組了解到公司員工們使用公司電子資訊上的行為，因為這些結果符合原本公司導入的能提供的效益，所以也讓高階管理者更加重視此資訊系統。

3. 部門間資訊安全認知提高：

其組織扁平化提供良好的基礎，並隨著資訊流通及導入流程透明化，部門間溝通的品質提高，也了解公司資訊安全政策，專案小組的跨部門溝通以及適時的給部門員工了解 DLP 在公司扮演重要的資安角色，也讓他們知道不當的行為會危害公司營運，個人的行為也會受檢視，導正員工的資訊系統使用認知，並提高員工處理敏感文件的警覺性。

4. 防止人為的疏失：

對 A 公司而言，導入前希望可藉由 DLP 改善員工的意外作業疏失，例如以電子郵件寄送機密文件時，DLP 即可攔截並會提醒寄件者，確認行為妥當與否，或將此寄送行為報知企業內部 IT 人員，進而控管資訊流向並加以規範。進而降低企業的資料外洩案件的機率。而導入 DLP 系統後透過監控日誌中直接證實，有不少事件是公司機密資料透過郵件和 IM 流出的紀錄，在布署系統之前這樣的行為可能會為公司帶來不少營業損害，也難以避免人為的意外疏失所導致的資料外洩。

5. 不影響使用者行為

A 公司原本的 IP Guard 端點防護系統，由於不是針對資料的內容去做控管，是需要犧牲電腦的使用模式：如限制週邊儲存裝置、輸入出裝置、網路、Email、MSN 的使用功能，或限制使用者無法使用 USB 隨身碟、MSN 不能傳送檔案等。導入 DLP 系統後，

公司提供的機密資料學習，可以有效的針對傳輸內容做偵測，而不是針對檔案去加密，功能之限制來達到目的，解決公司內部員工使用電腦的不便，同時又能做到重要機密資料的保護何存取，降低使用者對資訊安全系統的抗拒。

5.1.6 深度訪談資料分析

本研究所選取個案 A 公司，其深度訪談對象主要針對實際參與 DLP 系統導入專案團隊成員，作為個案研究深入訪談受訪者，訪談內容具有可靠性與真實性。在各個部門主要參與此專案人員，從不同職務角色以及不同的參與程度觀點作為本研究個案分析的依據。各部門的主要工作內容如下:

(1)資訊技術部門:主要負責公司資訊專案管理、資訊技術評估、系統開發。

(2)系統維運部門:主要負責工作為公司各部門與資訊單位的協調者、線上系統維運，以及協力廠商溝通。

(3)網路管理部份:主要負責公司內部網路基礎建設規畫和伺服器設備維運。
此外，由於系統最終會涉及採購行為，為了增加訪談的真實性，特別加入了採購部門處長參與訪談，以提供更多相關意見。本研究受訪者的背景資料如表 10 所示:

表 10 A 公司受訪者背景資料

部門	職稱	年資	訪談日期
資訊技術	處長	12 年	2014.3.18
系統維運	課長	8 年	2014.3.18
網路管理	資深技顧問、工程師	5～8 年	2014.3.18
採購部	處長	10 年	2014.3.24

資料來源：本研究整理

根據訪談所歸納出導入結果資料分析可知，A 個案公司在 DLP 資料外洩防護系統導入專案是成功的。為探究其專案導入成功之關鍵因素，茲將關鍵成功要素結合本研究所建立的構面所定義出的 10 項關鍵成功要素，透過實地訪談及彙整分析所有資料後，，A 個案公司 DLP 資料外洩防護系統導入成功之關鍵因素分析如下：

(1). 組織構面分析

在 A 公司中高階主管支持佔了很大的原因，該專案成員提到，因為該公司是服務業，主要的的利潤都是來自於客戶，所以其客戶個人資料以及營業上的機密資料保護對公司有營運及未來的發展有重大的影響，這些資料是公司的營運及未來發展命脈，經過資訊部門的評估及衡量，在陳述其系統在公司經營上佔有重要角色，另外在訪談過程中，也提到 A 公司在資訊系統的建置上有相當的重視，在建置 DLP 資料防外洩系統前，資訊部門已經著手計畫五年內的資訊安全系統規畫，其中就有將資料外洩防護系統納為重點，所以在此次專案上，獲得各大部門及資訊長的高度支持以配合，也在財務方面予以適當的支援。在另外一部份，個人資料保護法的通過，讓高管理階層對公司內部資料流出造成客戶傷害，以及法令的規定其龐大賠償金額會對公司造成莫大損失，更有可能影響商譽的重視。

1. 高階主管重視：

- 由於導入系統會短暫的造成部份使用者行為改變，及系統使用的磨合期，有可能造成營業上的損失，或者其它存在的風險，所以 A 公司在專案導入前，的起始會議（kick off meeting）由資訊長親自主持，對總經理及相關主管說明此資安系統在公司的重要性，以及其如何影響公司作業和營運。
- 負責專案的資訊經理每星期定期提出導入情況報告給資訊長，若有進度落後，或導入期間遇到困難，資訊長則會要求專案小組將原因整理出來。必要的話，他會直接下達指令，要求相關部門互相配合解決問題。
- 總經理積極參與 DLP 系統軟體評選過程，並要求需系統規劃、建立專案團隊、規劃軟硬體配置。
- 資訊長公布專案導入項目，讓各部門使用者，了解所需配合項目，請大家配合，相關建置需求，並改變部份系統使用習慣。
- 最高管理當局意識到系統導入的重要性，召開多次高階管理會議。會議中一再強調 DLP 系統導入的重性，並要求各部門主管宣達及強力要求各部門員工，務必確保系統導入順利成功。

2. 相關資源取得：

- 導入系統之前，資訊長就已決定將公司 IT 資源優先分配給 DLP 專案，並在所有資

訊專案中優先將相關資源分配給 DLP 系統，並決定上線後每年依需求編列預算用於系統維護。

- 由於 DLP 所需學習之機密和重要資料來自各部門的高級管理者，所以總經理下達命令，給需配合該專案人員，人力規範、並賦與專案成員相關所需權限以及資源。

3. 優勢

- 在訪談過程中 A 個案公司提到，因為公司先前有客戶資料外洩的情形，所以本次的 DLP 資料外洩防護系統導入專案列為公司重要的營運策略之一，所以在導入前已有做過相關的評估項目，包含整合與原有的 IPGuard 系統，以及部份的資訊安全系統，這些事前的規畫以及效益評估都是針對提升公司在未來營運以及資訊科技的優勢上有加分的作用。
- 訪談中也提到，目前在同競爭對手中，他們是最先評估也是最先導入的公司，能在科技的策略上以及優勢上比同業再往前一大步，所以其認知在系統導入後，在未來的產業競爭以及重要客戶資料保護上都能領先其它公司，也因為系統能帶來如此的優勢，所以影響了本次的專案讓高層主管的特別的重視。

(2). 專案構面分析

1. 參與度

- 該公司在導入任何資訊專案時，只要會影響使用者或者重大系統上線時皆會公告，更由於此系統會監測所有進出公司的網路行為，所以牽涉到同仁們的部份隱私，勢必會造成某部份的排斥，所以特別通知相關主管配合及說明。
- 個案公司內部組織編制較扁平化，公司在文化上，同仁也樂於溝通協調，有任何作業模式屬於跨部門問題時，專案單位會邀集各相關單位，討論如何進行或解決相關議題，因為個案公司具有這種文化，部門間溝通協調並無太大問題。
- 專案導入過程及上線後，雖有非常多跨模組及跨部門間溝通協調的問題，但都能經由個案公司這種跨部門合作的組織文化解決。
- 由於導入後，在上網及檔案的使用行為上需做改變，公司不同部門單位人員主動與專案小組人員會不定期舉行工作溝通與協調會議，針對各項會影作業流程之問題，共同討論研究解決及應便之道。
- 另外安裝端點防護代理程式(Agent)，若影響原本系統造成問題，專案管理人員除會與各部門使用者一起溝通協調外，也會將無法解決的問題請原廠顧問協助解決。
- 此 DLP 專案系統上線後，會保留所有內部使用者對外傳輸資料的紀錄，以及郵件相關內容，以備日後稽核查詢，專案成員在會議針上會對各種有可能造成使用者隱私行為疑慮狀況公開討論，並取得各部門主管認同，以減低系統導入難度，提高使

用者配合程度。

- 安裝裝端點防護代理程式(Agent)，會影響使用者線上作業，所以專案成員在導入前已規畫不同部門的執行時程，並先以資訊部門做前期導入的對像，並做測試，讓營業上的不便減到最低。

2. 專案成員

- 專案總負責人由資訊長擔任，負責系統導入成敗。專案主管由資訊科技處長擔任，負責設定時程目標及建立專案組織。
- 資安系統所需相關知識較複雜，專案人員組成的部份，該專案納入系統部門員，主要因為該部門對公司系統和使用者電腦最了解，也有一定的經驗，減低因不熟悉所造成出錯的機率，另外也整合網路部門最資深的工程師，和同部門的資訊安全領域的成員，
- 由於系統的作業模式及特性，就個案公司而言初期可能會有比較大的問題產生，所以初期由原廠提供必要技術上的協助和問題解決。
- 導入策略上，所有的特性以及功能，都先行資訊部門做先導測試，正試導入後，先針對影響使用者較小的部份來導入，其方式是先布置網路閘道代理伺服器(Proxy)監測網路流量，爾後再導入對影響使用者較大的端點代理程式。
- 在導入過程中需要知道公司的重要資料位置（如系統無法得知將減少導入效果），就前面所述，高階主管下達命令給予相關的權限，專案成員事先協調各單位主管把機密資料界定導入工作，分權給該單位輸入，並督促其執行程度。

(3). 環境構面分析

1. 科技基礎

- 雖然 A 公司是傳統產業，但很早就將作業流程資訊系統化，其資訊基礎設已相當完善，包含相關資安設備，所以這次的專案中，其整合度以及配合相關的網路設備以及操作基本知識皆已相當充足，並沒有因為本身的科技落後而導致建置上額外增加難度。

2. 產業環境

- 因為其所屬產業是寡佔市場，競爭上並不是那麼激烈，之前發生客戶資料外洩到其它公司時，著實讓公司擔心之後再發生同樣的事情，不但會使商譽受損，也會失去不少商機，這都讓公司希望系統早日建置完成。
- 原本在個人資料保護法通過前，在系統導入的積極性上並沒有時間表，由於法規的通過迫使公司定出了專案時間表，而間接影響專案必須導入成功的使命。

(4). 科技構面分析

1. 系統資源

- 選擇對的系統，公司高層對於系統選擇完全尊重專業，並充分授權，系統能符合 A 個案公司需要。
- 由於 DLP 在建置上不同的產品難易度不一，在採購前該專案成員，事先彙整及評估各項產品與作業需求以建置布署上的差異分析，並依據評估結果決定選用何種 DLP 產品，是較適合公司以及專案成員較熟的技術。
- 另外此 DLP 系統管理上是採用成員們較熟悉之微軟系統，在操作上減低其難度，在伺服器的整合上也因內部都是相同的作業系統，這部也較少阻力和不相容或需客制化的程度。
- 建置開後初期先採用系統內建法規範本，起初偵測到太多不相關資料，其成員根據此狀況調整臨介值及參數，以降低誤判的機率，減少使用者的報怨。
- 另外由於該系統是採用資料指紋辨視的方式來監控資料，其學習文件都來自於各部門所提供的資料，減少其因誤判所造成的作業中斷。
- 由於得到財務上的支持，系統所建置之主機，皆全新採購，規格上由專案成員提出，全部以效能及高可用性，以及穩定性考量，並無預算不足之慮。

2. 科技成熟度

- 該 DLP 防護系統在台灣有不少的建置經驗，此專案在初期有要求原廠加入顧問群，提供相關的除錯及建置經驗，減少失敗的因素。
- 在完整系統上線前要求廠商確實做好各項教育訓練，並在初期提供 5X8 的線上支援，資訊長要求專案成員需將所有作業程序文件編製完成，以及相關應變措失 SOP。
- 由於產品成熟度，其問題修正在每週都會提供相關訊息，另外客制化需求在 A 公司並沒有特別的需求，在相容性上問題較少。

3. 系統品質

- 在系統導入後其產出的品質，對 A 公司的使用者而言是大部份符合需求的，除了在初期系統尚未學習完公司機密文件特徵時，採用內建範本發生不少誤判情形以外，之後針對公司的資料流出有不錯的偵測率。
- 在功能上，客戶非常重視的法規需求範本以及稽核報表，該系統皆能提供並能準確的偵測，也能針對之前其它資安產品，只能限制使用，而不能由內容來控制行為的需求，另外也通過稽核部門對日誌保存和資訊安全的要求。

- 操作使用上，由於是英文界面，易用性較一般資訊系統上較差，專案人員反應在未熟悉系統前，在設定組態上以及系統邏輯並不是很好操作和了解，這部份初期將由廠商來負責教導以及協助，其大大減低了使用上困難度的疑慮。

表 11 A 公司各構面影響導入結果整理表

主要構面	關鍵因素	影響導入的結果
組織	高階主管重視	• 專案依序進行，定期會議的召開與追綜，讓專案在時呈內完成 • 減低跨部門溝通時的阻力
	資源取得	• 得充份授權，獲得所需資源並取得財務上的支持
	優勢	• 補齊原有的 IP Guard 檔案防護系統不足的地方，在整個資訊安全系統上，增加防護範圍，達到加乘的效果。
專案	參與度	• 部門間資訊安全認知度提高 • 使用者了解後，其不影響使用者行為大大的減低在系統導入上的抗拒程度
	專案成員	• 專業能力，減低在系統建置時的狀況以及錯誤 • 責任的分配，讓成員們在專案中可以做好自己的角色，而沒有推卸的情況 • 在溝通學習上，有較積極的態度
環境	科技基礎	• 完備的資訊基礎建設，增加系統導入的速度，與成功的機率，減少無法配合而需額外支援的其它設備經費
	產業環境	• 增加在產業上的競爭力、提高客戶的信賴度，以及本身的商譽 • 達到法規的要求，減少其它法律上的風險
科技	系統資源 (相容性)	• 穩定性、整合度高 • 與現在的設備相容性和使用習慣程度高，減少建置時的困難度
	科技成熟度	• 操作的易用性，減低人為的錯誤 • 良好的教育訓練以及廠商支援，增加使用者的信心
	系統品質	• 對公司資料流有效管理與監控 • 預期系統的效益達到公司原的要求 • 防止人為的疏失

資料來源：本研究整理

5.2 個案 B 公司

5.2.1 公司簡介

B 公司目前員工數為 260 人，資本額為 2 億，是國內一家也是華人世界較早成立的網路書店。其網路書店於 2000 年初創立，該公司目前與數千家以上的出版社合作，至今已成為國內前幾名的網路書店。並以「華文世界的知識入口」為目標，強調為廣大中文知識需求人口提供豐富完整的服務。 其經營理念強調：「提供誠實、品質、快速、專業、創新的服務平台，打造消費者完美使用經驗。」成為電子商務服務平台的領導品牌，並以『使用者滿意度』為經營指標，以持續開發符合會員多元選擇的商品屬性及數量，設計更簡易、更貼心的購物介面及流程，挑戰更快的出貨速度及更好的客戶服務品質，期待邁向更安全、更便利、無障礙的電子商務服務平台。

B 公司現今擁有超過二十萬類的書籍在網路上販售，可說是國內藏書量極豐富的線上書店，消費者透過網路 SSL 保密連線，可安全地上網購買書本，加上憑藉著豐富的電子商務經驗，搭配完善的物流管理制度，出書便捷，大大提昇經營效率。 B 公司最大的優點就是與全省上千家的便利商店合作，提供免付運費取貨付現服務，以提供網友最安全、多樣、方便的服務，享受更優惠的購物樂趣。另外，B 公司也與其它中文入口網策略聯盟，推出圖書、雜誌與音樂的線上購物服務。

B 公司像是個大型的圖書館，採用先進的全文檢索功能，在茫茫書海當中不僅可以搜尋到最新、最熱門的書籍，亦能找到已從書架上下架的書籍。除了提供書本的銷售外，該公司也提供多樣的書籍資訊，包括完整的介紹、封面及書摘，甚至開放空間讓使用者互相交流。同時，所發行的 e-page 電子報，提供即時的出版及閱讀資訊。 B 公司亦開發電子書這塊市場，採用國內數位版權管理系統供應商優碩系統「eBook 版權管理系統」，與優碩資訊做為技術夥伴，推出付費電子書下載服務。

5.2.2 產業現況及發展概述

網路書店，以書籍本身具備某些特質適合在網路上販售。書籍之產品品質差異性不大，書籍之規格性也不會因人而異。配銷方面，書籍易於運送，也不需要繁複的包裝，運送過程中無須擔心腐敗、摔破等問題。甚至可以以數位化檔案的方式傳遞，由這些特性可以發現書籍成為網路購物熱門商品的原因。所以至今網路購物中，成立許多家的網路書店。台灣近年來至少已經成立了十五家的網路書店，如：HOT、OpenTech、三民、天下、念慈、金石堂、高點、常春藤、晨星、博客來、舒讀、華文、搜主義、誠品、聯

經…等。由蕃薯藤網路行為大調查發現，網路購物行為的產品中的第一名便是書籍雜誌出版品。

臺灣網路書店發展至今，已走向多元化虛實整合的階段，對於經營虛擬書店這一部份已有成熟的技術與經驗。為了讓網友間能夠透過交流產生情感上的連結，網路書店建制了許多開放式的平台，如：部落格、個人書店、討論區、留言版，當今這樣的方式十分的普遍，也代表網路書店的經營者試圖建立一種社群關係。

以近幾年台灣網路書店的發展，無論是在網站功能、產品內容、服務提供等方面，都已發展至一定水準，雖未臻完備，尚且為目前消費者所接受。網路書店的基本功能不外乎書籍齊全、檢索引擎、書籍介紹與試閱等功能，並具備付款簡便、取貨容易等特質。隨著網站技術、機制的成熟，網路書店可以有多元化的發展。而從網站內容建置及發展特色來看，則顯見業者對於網路書店業務的積極作為。「綜合型網路商城」即是發展特色之一。

5.2.3 導入動機(需求)分析

B 公司目前的網路會員數超過 100 萬，其重要的客戶資料是公司主要的行銷來源，也是其經營的重要命脈，由於網路購物其特有的經營模式是以虛擬商店的方式來交易，對消費者來說，許多研究指出，在網路交易的安全性及個人資訊的保護機制，是主要影響消費者網路購物意願的關鍵因素。B 公司在有鑑於相同產業及類型的電子商物網站個資外洩案例層出不窮，不但影響消費者購物的疑慮和商譽的受損，長期以來都在找尋相對應的資訊安全解決方案，據訪談在 2010 年時，該公司在單位重新編組下，成立了資訊安全單位，並商請有相關驗的資訊安全顧問加入讓資訊團隊。

B 公司導入 DLP 資料外洩訪護系統專案，主要起因是在台灣 101 年通過個資法後，其公司開始規畫如何避免客戶和公司的機密資料發生外洩的狀況, 在購買 DLP 以前，B 公司也已經導入了 IBM ISS xForce DRM 的系統來保護公司內部的機密資料，不過後來因為 DRM 在功能上沒有辦法符合需求，該產品主要是採取檔案加密的方式來防止資料被不當存取，並加入權限控管，其主要缺點是需改變使用者原有的操作習慣，另外加密伺服器的備份也是一大問題，再加上加密檔案的類型也受廠商設計的影響，並不是每一種的檔案的格式都能被分析並加密。在擁有權限的作者身上也很難掌握資料的流向，在稽核上也是一個很大的問題，所以 B 公司的資安團隊開始規畫並找尋適合公司的資料外洩解決方案，因此他們將評估的重點轉為採購 DLP,來保護公司重要的機密資料。

依 B 公司描述，之前公司內部已有採用 Websense 的上網過濾產品，經考量在整合

生上以及偵測技術層都屬最適合該公司目前的需求，且該產品在維護運作上及界面熟悉度上有同仁們已有相當一定程度的了解，另外在價格及原廠的支持度上也得到正面的回饋，所以在評估的過程中並無花太多的時間做不同產品的測試及評估，就決定採用 Websense 的 DLP 資料外洩防護解決方案。

5.2.4 導入過程

B 公司其導入方式與 A 公司不同，在佈署系統方面是以網路閘道來監控為主，並採取（旁聽）的方式來布署，在端點(使用者電腦)系統方面，其因 AD 架構導入並不完全，所以並沒有規畫在個人端電腦上安裝代理程式。現階段前他們一共部署了 1 台 DLP 的閘道器，及 1 台管理伺服器。

階段一：系統穩定性評估

B 公司在初期導入系統並不是以全公司為主要範圍，為了解產品的穩定性以及與現存系統的相容性,在一開始是以資訊單位做為導入的主要範圍,導入評估期間為二個月，由於公司在網路閘道上布署了 IPS 與防毒閘道與和上網行為管理等產品，在相容性風險評估之前並不會冒然的將系統上線以避免影響正常的業務運作。

階段二：使用機密資料範本來源

在初期評估結束後，開始正式導入公司所有的網路流量到 DLP 系統，並做監控，但由於在專案成立之初，相關部門主管並無下達命令到各部門，所以資訊部門當中也無法得知，也無法界定各單位機密資料的檔案來源位置，因此他們在界定機密資料，並無執行跨部門協調，所以無法明確指定那些檔案，資料庫，為機密檔案。且由於檔案伺服器的資料量相當龐大，不容易透過網路掃描，並產生所有的機密資料的指紋特徵，所以初期其主要監控以及準備界定學習的機密資料檔案，為微軟的 Office 文件、以及系統上所提供的政策範本，包含身份證信用卡號以及 PCI-DSS 相關與電子商務法規，現階段並無考慮與該會員資料庫做結合與學習。

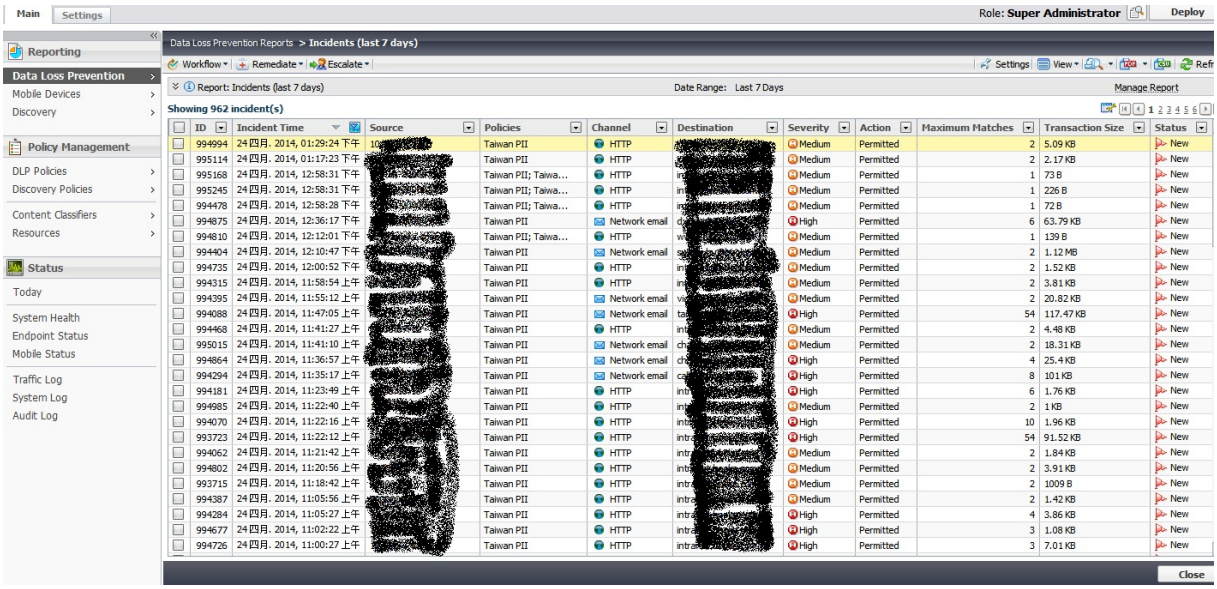

圖 15 B 公司在系統上線後由內建範本所偵測到的洩密日誌

資料來源：B 公司提供

階段三：資料分析與修正

由於 B 公司的機密資料定義方式是採用系統所提供的範本，相對的在偵測的準確度較差，所以在偵測到洩密資料發生時，並無設定通知相關部門主管，只有透過郵件的方式通知系統管理者，因為對於資訊部門來說，系統提供的範本誤判較高，需經過研究才能得知是否為洩密事件，所以該單位採取的方式是由負責該系統的資訊人員來稽核這些記錄， 針對有問題的洩密事件人員進行訪談及確認，如發現為有問題的事件才會通知主管進行處理，如果為誤判則進行系統的偵測做設定上的調整，反覆的動作來將 DLP 系統政策調校到符合公司的需求為止。

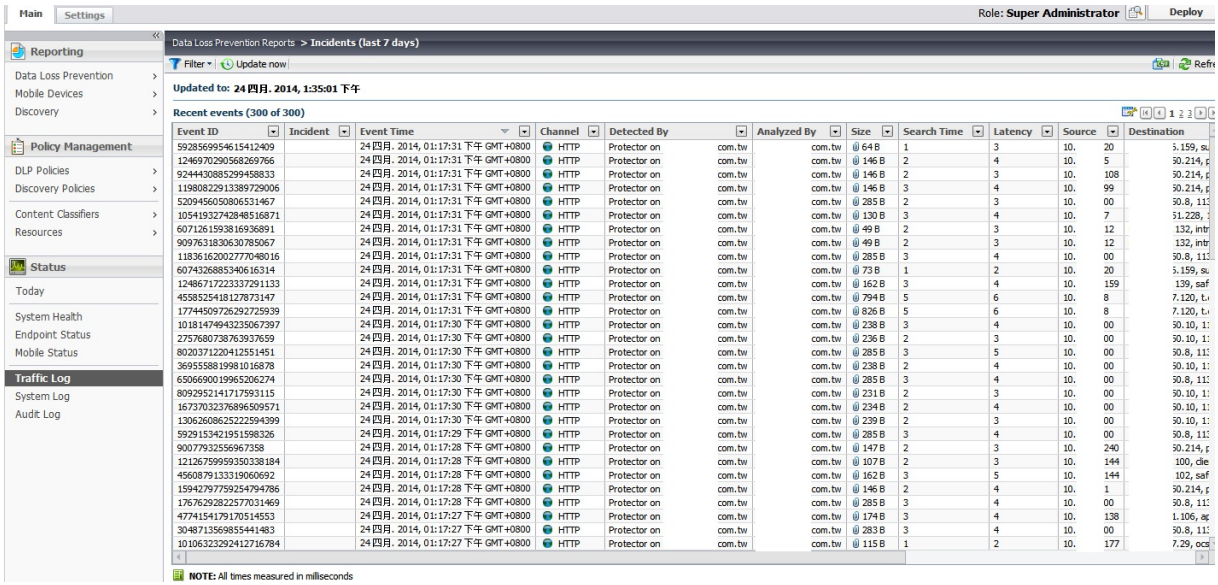

圖 16 B 公司在系統上線後在閘道上所監控到洩密日誌

資料來源：B 公司提供

5.2.5 導入結果

1．導入時間過長：

個案公司高層對此系統導入後對公司影響並沒有特別的重視，所以並無成立專案小組，如此一來所有的建置時程都仰賴資訊人員的時間分配，因為沒有壓力，資訊單位建置人員皆將 DLP 系統工作安排在其它主要工作排程之後，當系安裝失敗或者前導測試不成功，則往後延期重新再按排時間及重建作業係統，如果遇到問題再請廠商及顧問開會協助以及判斷問題所在，其建置期間長達三個月。

2．誤判率高

政策無法下達至各部門，其它部門並無接到上層命令，需主動協助建置 DLP 系統建置及佈署，導致資訊人員無法得知並定義各部門機密資來源及位置，再加上沒得到充份授權，在跨部門溝通協調取得相關系統需求資料時時遇到不少阻礙，如客戶資料庫無法取得權限，檔案伺服器路徑位置等。系統建置人員只能從系統上所提供之政範本以及一般用用法規來做為洩密資料偵測的依據，由於內容屬於通用型，並不是針對公司內部資料及檔案去設定，所以依照監測日誌來看，都是沒有意義的洩密資料監控。

3．內部參與程度太低

公司內部層級扁平化不足，上對下的政策難以傳達到各單位部門，往往是一道資安政策下來，最後因人員支持與參與度低而導致系統成效不彰，建置後放置不用，系統佔用資源，浪費人力物力。沒有成立專案小組，上層與下層參與人員少，只有負責安裝人員接觸，其它人皆無法得知狀況，同仁們甚至不知有此系統。

4．建置人員對系統熟悉度差

由於人員沒有分工以及執行權責劃分，不時有責任推托的情況，導致在使用以及學習方面，因責任不清，同仁們都不認為是自已負責，影響教育訓練學習態度，最後人員無法完全熟悉以及接手系統。由於對系統認知及熟悉度差，使用率及應用程度上就明顯下降

5．執行力不足

在訪談過程中提到，公司文化對 DLP 系統入成效有顯著的影響，該公司文化在資訊系統的使用上是以內部使用者感受及作業順暢為優先考量，各單位部門主管也怕影響使用者作業及原有的操作習慣，也怕侵害使用者隱私所造成的人員不安，所以在政策執行上就採取消極的態度，如果上級無強力要求則不主動接觸系統和配合相關的佈置作業，如此一來，造成系統布署的失敗。

6．系統變成測控設備使用

由於上述幾點原因，目前系統單純套用內建範本，沒有定義符合公司內部機密資料的內容，所以因誤判率高最後只做流量監控，並沒有做告警處理，現今設備只做消極的內部稽核時使用，或者有需要查詢某部單位的資料時才會產出報表做為依據，或在因應法規上，政府要求出示個人資料洩漏時，所需證據提供相關資料時提出佐證，在一般情況下系統變成側錄設備在使用。

5.2.6 深度訪談資料分析與結果

本研究選取 B 公司實際參與 DLP 系統導入相關專案成員，作為 B 個案研究深入訪談受訪者，訪談內容具有可靠性與真實性。在各個部門主要參與此專案人員，從不同職務角色以及不同的參與程度觀點作為研究 B 個案分析的依據。各部門的主要工作內容如下：

(1)總經理室特助：主要負責總經理相關政策命令佈達，以協助處理公司行政與外部溝通事務，由於特助在該公司曾經帶領過資訊單位，在此專案中為顧問角色，因為在此次訪談中特別在管理面的部份與特助詳談採購原因及其想法。

(2)IT 維運部門及系統維運：主要工作為負責公司的資訊基礎建設的系統維運，包含確保內部員工所使用的電腦正常運作以及維護廠商的溝通。

(3)網路管理部份:主要負責公司電子商務以及主要伺服器維運，包含郵件、網站、資訊安全設備、異地備援等重要的設備。

表 12 B 公司受訪者背景資料

部門	職稱	年資	訪談日期
總經理室	特助	8	2014.4.23
IT 維運部門	經理	2 年	2014.4.23
系統維運	資深工程師	5 年	2014.4.23
網路管理	資安技術顧問	1 年	2014.4.24

資料來源：本研究整理

從導入結果資料分析可知，B 個案公司在 DLP 資料外洩防護系統導入專案中，其最後的結果是不符合原本的預期效益的，所以專案並不算成功。透過訪談導入系統相關負責人員後，了解 B 個案公司在 DLP 資料外洩防護系統導入專案中失敗的關鍵因素，並將其導入失敗的原因將其訪談資料分析彙總後，其關鍵因素彙總分析如下：

(1). 組織構面分析

B 個案公司在高階主管支持部份，在此系統的導入過程中扮演的角色是屬於比較被動，起因主要是來自於個資法的通過，為了新法規制度，其洩漏一筆個資的巨額的罰鍰，才遂請資訊部門開始執行系統的導入與評估，這期間都由剛加入的網路部門的資安顧問來做統一處理與協調。

1. 高階主管支持：

- 高階主管決定導入 DLP 系統的原因，主要是為個因應人資料保護法規的通過，才請資訊部門以現有的硬體和相關系統去規畫需要額外採購的解決方案，其並沒有視為公司重要資訊政策，在命令下達後就比較少主動去關心目前導入情況和進度。
- 期間沒有強制其必需定期將導入情況給報告給相關的主管，主要進度都掌握在資訊部門的身上，最後變成一個封閉式的作業。
- 在導入過程中資訊部門的上級單位曾有人事異動與輪調，異動過程中原有的責任並沒有徹底同步與交接，遂造成有些主管不清楚有此系統的存在。
- 訪談過程中提到，其公司在主管在部門溝通上一直有很大的問題，命令通常都無法由上而下的貫執行，使得資訊單位人員無所是從。

2. 相關資源取得：

- 因為此次的系統導入並沒有受到重視，所以在相關資源分配上沒有特別的優先權，由於高階主管授權不足，在系統需要跨部門支援以及合作時遇到不少阻礙，例如，各部門的機密資料以及客戶的資料取得都存在不同部門，因為沒有特別命令要相關單位配合，使得資訊人員在溝通時遇到很大的問題與質疑，也直接造成系統無法直接學習重要的資料。
- 高階主管雖主雖然沒有特別針對專案去注視，但在財務面上的支援是尊重業的，所以在系統所建置之主機，或者相關的需求，如專案成員提出，是可以獲得財務上的資支持。

3. 優勢：

- 在策略上，DLP 資料外洩防護系統如果建置成功，是能給公司帶來正面的效益，因

為 B 個案公司是屬於電子商務的經營模式，也算是服務業的一種，會員數的量是公司相當 重視的一環，如果能保護其現有客戶資料，不但對其企業發展有良好的幫助，在商譽部份則有良好的形象加分。此因素在訪談的過程中曾被提及是導入 DLP 系統的原因之一，並且有所期望的效益之一，但也因為如此，最後在系統的導入效益評估以及產出品質在其它因素的影響下不如預期時，使資訊部門成員在衡量導入成效時感到失望。

- 另外需求分析提到，B 個案公司原本是採用 IBM xForce 的系統，其成員們擔心會有相容性以及功能重複性的問題，可能會影響原系統的穩定以及效能，在這部份他們選擇，棄置原本的 xForce，所以在功能的加乘效果上效低，沒有增加其系統上的優勢。

(2). 專案構面分析

1. 參與度

- 由於 DLP 系統會監測所有進出公司的網路行為，所以 B 個案公司的高階主管在做決策時，會擔心系統導入後會影響使用者的線上作業並改變原有的使用習慣，以及操作行為，且 DLP 系統的監控日誌內容會涉及到員工的隱私，因此認為有可能會遭員工抗拒，或者造成某部份的反彈，所以在導入的過程中並沒有公告給全體員工，因為以上原因，也間接的影響成員的認知與參與程度。由於 DLP 系統是屬於資訊安全的一環，在一些情況下任何的資訊安全防護系統都有其不足的地方，除了本身系統能做的功能項目外，人員對資訊安全的認知也是非常重要的，公司成員如果能都了解以及參與，對系統的導入是有加倍的效果。
- B 個案公司在本次導入系統的過程中，資訊單位沒有特別公告其需要同仁配合的項目，所以安裝端點防護代理程式(Agent)方面，因怕影響使用者線上作業，也擔心系統有可能不相容而造成問題，再加上 AD 導入不完全，在派送代理程式時需要很大的人力，最終沒有導入，這部份也使用用者無法參與。

2. 專案成員

- 在專案的規畫過程中，訪談時成員們提到所有計畫以及評估都是由到公司不久的資安顧問來執行，也因為如此，很多事情其並沒有那麼熟悉，評估過程中也沒有透過會議與資訊人員協調，有如黑箱作業，很容易造成主觀意識以及資訊不對稱的評估過程，進而影響高階主管部份決策，與資訊人員對系統認知上的落差。
- B 公司在此的的 DLP 系統導入專案中，並沒有特別成立專案小組，也沒有指定負責專案負責人，只有指派資訊部份人員去負責建置，所以沒有人去負責主導系統導入的規畫以及成敗。這是一個很大的問題，成員們不知自己在這次導入資料外洩防

護系統的角色是什麼，也不道自己要負責什麼樣的工作任務，其影響是會有責任推托情況，直接造成建置品質和系統品質的產品變差。

- DLP 系統所需相關知識較複雜，B 公司這部份有資訊安全專長的人員，所以在對產品的整個概念性上有一定程度上的認知，雖沒有成立專案來執行，但其資訊單位部門在各領域中都有不錯的相關經驗和知識，這點在這次的 DLP 系統導入中有相當的幫助。
- 不過其中一個主要的問題是，由於成員們沒有工作項目上的分配，也因為如此在責任上的認定模糊，造成執行效率上的問題，最明顯的部份是在心態上以及系統導入後的學習上較 A 公司為差，因為不知道系統上線後由誰來維護以及操作，再加上原本資訊部們的工作項目就已經非常繁多，多一事不如少一事的心態，導致後來部份成員們在系統的操作上以及遇到問題的解決能力上不夠熟悉，進而在某些部份產品生排斥效應，也因為如此造成初期系統上線有不穩定的情況，影響到部份系統所能提供的功能效益上減低。
- 另外 B 公司的 IT 部門在部份文化上屬於比較不善處理跨部門溝通，就前面所述，因為沒有得到高階主管的相關權力資源，再加上公司沒有額外的公告或者發布任何的資訊訊給需要配合系統的部分主管或者員工，以致系統在不同部門的政策制定上以及機密資料學習的設置如果需要跨部門協調時遇到不少阻疑，這也是後來系統產出品質不如預期的主要原因之一。

(3). 環境構面分析

1. 科技基礎

- 然 B 公司是資訊科技產業，其作業流程以及資訊系統已相常的先進，資訊基礎設施的軟體架構皆相當完善，包含與本次導入 DLP 系統需整合的相關資安設備，所以這次的專案中，其整合性和相關的網路設備以及皆沒有影響系統導入的品質，在這方面有加分的效果。

2. 產業環境

- 因為其所屬產業是競爭市場，之前同業發生客戶個人資料外洩的事件層出不窮，跟 A 個案公司相同，公司也擔會發生同樣的事情，但不同的事，公司是擔心個人資料在法規通過後，其洩密一筆個人資料罰金提高的部份，而不是在站在公司營運面去考量，所以在環境構面上法規是促使公司被動導入的因素，但由於是被動，也是影響前面高階主管的支援態度。

(4). 科技構面分析

1. 系統支援

- 由於 B 個案公司之前就有採用過 Websense 公司的產品，在產品特性以有相當的理解，所以 DLP 在建置上會遇到的相容性問題，在採購前有做部份的評估，雖有小狀況，但在本次的專案並沒有遇到重大的問題。
- Websense 產品的特性，其主要都是 Windows Base 的元件，其相關安裝建置步驟以及複雜程度上較其它產品來得低，在導入系統過程中大部份成員都有能力協助。
- 比較大的問題是，因為沒有事先的政策計畫，再上在機密資料的位置上分布於各部門，如果採用資料指紋辨視的方式來學習，造成其極大的困難，最後政策面的設置也因為如此，採用較不精確的通用範本來偵測外洩事件，也是導致後來系統效益不符合預期的主因。

2. 科技成熟度

- B 公司先前已有接觸過 Websense 其它產品線的資安系統(URL Filter)，和原廠及廠商也非常的熟悉，並知道該 DLP 防護系統在市場上有一定領導地位，並具有相當的成熟度。系統相當的穩定，這部份對導入過程中有加分的效果。
- 在顧問以及產品相關的應用，在導入前有做部份的前導測試，以資訊部門為對象，在系統的穩定性和功能有一定效果，這部份在訪談過程中，B 公司提到 Websense 目前所提供的 DLP 系統是符合其需求的。

3. 系統品質

- 該公司有著特殊的文化，就是在導入任何資訊系統專案時，如果遇到會影響使用者作業或者需改變其行為時，就會先以使用者的立場考量，改變系統原有的功能，儘量避免並以能減少使用者報怨為主，以 DLP 系統而言，是有可能牽涉到同仁們的部份隱私，主管擔心某些情況可能會造成使用者的反彈，於是更改原有的功能，將偵測到的洩密資料只做紀錄，並沒有阻擋，這也直接造成系統導入系統效益與原本的預期有落差。
- 由於無法取得正確的機密資料讓系統去學習以及辨視，最後只能採用系統上所提供的法規政策範本，又因為是通用範本，有可能不一定符合公司內部的文件或者機密資料型態，所以其造成偵測情況誤判率過高（產出的品質），也是讓系統後來不被重視的原因，由於辨視機密資料外洩是系統最重要提供的效益，誤判率過高，是最後系統導入失敗的重要因素。
- 由於權責沒有劃分，責任上不屬於任個一個資訊人員，資訊人員在學習態度上變得較差，且因為在操作上不熟悉，這也使得資訊同仁們開始排斥操作，間接使系統利

用率降低，而無法有效利用系統，來達其預期所能帶來的效益。

表 13 B 公司各構面影響導入結果整理表

主要構面	關鍵因素	影響導入的結果
組織	高階主管重視	• 沒有專案規畫以及任務追綜，導致建置時程過長 • 政策無法確實執行到各部門，執行力不足
	資源取得	• 沒有得充份授權，造成部門溝通時的阻力大 • 在系統導入時無法取得重要的系統配合項目(機密資料)，導致後來的系統產出品質低落
	優勢	• 取代既有的 xForce 系統，但新系統又無法在時程內上線以及提供相對的效益，導入後無法取得比舊有系統更好的優勢
專案	參與度	• 內部參與程度太低，系統導入完整度不足(無法完整布署端點監控 Agent) • 使用者不了解系統，使其系統導入上因不了解而造成某些程度上的抗拒
	專案成員	• 沒有專案小組來主導，成員們自行決定，群龍無首 • 工作分配不當、責任分散，不時有責任推托的情況，導致在使用以及學習方面效果差。
環境	科技基礎	• 資訊基礎建設完善，有益系統導入的進行
	產業環境	• 無法增加在產業上的競爭力、保護客戶的重要機密資料 • 系統最後無法提供法規的資料稽核要求，增加其法律上的風險
科技	系統資源(相容性)	• 事前只有部份相容性評估，其穩定性、整合度較 A 公司差，但沒有增加其建置時的難度
	科技成熟度	• 產品穩定性高，使用者也使用過該公司產品，但因為學習心態較差，教育訓練效果不佳 • 所以在部份狀況需要廠商高度配合，而無法完全自行管理
	系統品質	• 操作的雖有易用性界面，但因資訊人員沒有工作指派，並沒有主動學習，使其無法完全的熟悉並管理 • 監控效果差，誤判率高，達不到公司預期的系統的效益 • 最後變成監控設備使用、失去原本導入的目的

資料來源：本研究整理

5.3 個案公司分析結果彙整

在本研究深入訪談後，茲依上述使用研究架構所列影響資訊系統導入之分析，其如何影響二個個案公司 DLP 資料外洩防護系統的導入，比較其成功與失敗的原因，彙整如表 14：

表 14 DLP 影響導入因素彙整表

關鍵因素	A 公司(影響導入的原因)	B 公司(影響導入的原因)
高階主管重視	重視且主動參與，並大力支持 追綜進度、專案會議召開	被動支持，重視程度較少 執行力差、命令無法傳達
資源取得	充份授權，並給予資訊部門系統執行的優先權	授權不足、溝通正面回饋少
優勢	補強原有的 IP Guard 檔案防護系統不足的地方，增加原有系統功能的範圍，來達到加乘的效果。	主要取代原有的 xForce 系統，而不是整合，優勢完全依賴新系統的上線。
參與度	公告，並請各單位主管配合說明，已有建置完善的 AD 架構，完整的導入端點程式到各部門。	同仁不知有導入此系統，共識以及參與度極低。且導入端點代理程式不完整。
專案成員	對系統認知及專業程度高	專業程度高，但對系統的認知與責任感較低
科技基礎	完善的資訊系統以及相關資訊安全設備	完善的資訊系統以及相關資訊安全設備
產業環境	傳統產業，擁有龐大的客戶資料庫，擔心客戶流失，且因為個資法規通過，擔心受罰遂主動積極導入。	科技產業，擁有龐客戶資料庫，競爭者多，受個資法規以及金融法規約束，被動積極導入。
系統資源(相容性)	備有系統專用硬體，事先做過相容測試，減低不相容的情形，並提供一切所需的建置的完整軟硬體資源，以確保系統執行穩定性。	備有系統專用硬體，只有做部份的系統需求與內部架構相容性評估，在導入時遇到一些相容性的問題。
科技成熟度	系統在市場上及應用面都有良好的正面回饋，其顧問人員以及服務廠商都有相當程度	系統在市場上及應用面都有良好的正面回饋，其顧問人員以及服務廠商都有相當程度的指導，與 A 公

	的指導，也有完整的教育訓練。	司不同的是，因為權責劃不清，系統學習態度效果差。
系統品質	事先了解功能以及能提供原有系統上的加倍效果。組態上在初期不熟悉的部份，初期由廠商協助。另外由於能獲大部份的機密資料資訊，使用導入後產品的結果與品質與預期相符。	組態上較不熟悉，再加上無法獲取大部份的機密資料來源以及位置，而導致只能使用通用範本的方式來監控，其最後產出的資訊品質與預期有落差。
導入結果	成功	失敗

資料來源：本研究整理

根據上述十個因素分析整理後，個案 A 與個案 B 公司影響 DLP 系統導入的主要關鍵因素可以整理成表 15：

表 15 導入 DLP 系統主要影響關鍵因素

個案 A 公司	*個案 B 公司*
1. 高階主管的全力支持。	1. 高階主管被動支持
2. 資源取得程度高	2. 相關資源無法取得或授權不足
3. 使用者參與程度高	3. 使用者參與配合程度低
4. 專案團隊認知與責任感	4. 專案團隊權責無法劃分
5. 系統產出品質與效益符合預益	5. 系統產出品質差
6. 產業環境(法令)使其更加積極	

資料來源：本研究整理

依表 15 所整理，可說明在 DLP 資料外洩防護系統導入成功的主要關鍵因素，在組織構面高階主管以及相關資源的取得和內部使用者的參與度及對資訊政策的了解，是主要影響導入的關鍵成功因素，而專案構面和科技構面中，成員的專業知識以及責任的分配跟系統品質則是可能造成導入後系統產出品質是否符合預期效益的原因，而環境構面中，產業相關法規和產業的競爭程度則是影響高階主管制定導入系統決策的積極度。

5.4 命題發展

由於本研究欲了解主要影響企業導入 DLP 資料外洩防護系統的因素為何，故本節將依據受訪資料證據，以及個案彙總結果，分別針對研究目的中所提出的研究問題進行分析，目的在於歸納發展出具有意義的命題。其中，部份命題所提出的觀點是針對目前尚未有研究而加以觀察或發現的現象進行探索；另外，有部份的命題或主張是出現與先前文獻所提出之研究理論有不同的結果。

1. 主要導入 DLP 資料外洩防護系統原因是由因為其企業本身擁有的重要資料，且這些資料會影響整體公司的營運(如客戶資料、業務資料等)，另外一部份是因為個人資料保護通過，以及其罰鍰金額的提高。

2. 企業文化會造成 DLP 資料外洩防護系統導入過程中產生抗拒以及接受的程度，但不同產業別對系統的認知並沒有直接的影響，以本個案研究而言，B 公司是屬於科技業，但其員工的接受度以及認知程度相較於 A 公司傳統產業較差，因此，由訪談分析得知其主要取決於公司高階主管對資訊政策的執行力以及宣導績效。

3. 不同的導入策略會直接影響系統導入是否成功，其主要影響導入後的系統產出品質，就 B 個案而言，因 AD 架構不完整所以沒有布署端點代理程式，並因為擔心使用者的抗拒而將偵測到的洩密行為只做紀錄而不阻擋，且又因為過程中無法得知機密資料的來源位置，而使用通用的範本，導入誤判率高，最後導致系統所帶來的效益不如預期，最後影響 DLP 資料外洩防護系統導的成效。

4. 依訪談分析結果，高階主管的支持以及認知程度是主要影響系統導入成敗的關鍵因素，因為在資源的取得以及政策執行力在導入時扮演者重要的角色。而專案人員的程度則是必須，且責任上的分配以及適當的授權在導入過程中也有次要的影響力。

5. DLP 系統導入時，政策命令的傳達有直接的影響，在 B 個案公司中，由於高階主管較被動，其上對下的命令常常無法傳達，進而使資訊人員在與部門協調時除了沒有得到相關授權資源外，由於命令沒有傳達，各部門都不了解也不清楚該資訊政策，使得在溝通時遇到許多阻礙，這也讓系統後來誤判率提高，系統品質降低，而系統品質是影響導入成功的主要因素之一。

6. 不同因素有前後的關係，環境構面中的產業環境促使高階主管決策，而高階主

管的支持與資源取得程度影響使用者的參與度，而參與程度和系統優勢及系統相容性、科技成熟度、專案成員會影響系統品質，而系統品質會影響最後的導入效益，也是 DLP 系統導入的重要關鍵成功因素。

7. 企業透過系統產出品質來評估導入成效，DLP 資料外洩防護系統主要是保護企業的機密資料不會外洩，而評估方式就是從系統上所偵測到的外洩事以及正確率來和與現有系統的整合度來評斷，一但無法取得機密資料來源以及誤判率高，或無法整合現有的系統，以致建置不完全，無法偵測部份機密資料，就會失去保護公司重要機密資料的目的。

第六章　結論與未來研究方向

本研究主要是透過個案的訪談，深入了解 DLP 資料外洩防護系統導入的過程，以及 DLP 資料外洩防護系統導入的成功與否的關鍵因素，希望能藉由本研究所整理出的因素分析及企業導入 DLP 資料外洩防護系統的實際經驗，了解導入 DLP 系統時必須克服的障礙及其導入的困難處，以協助現今有意導入 DLP 系統的企業管理者夠掌握這些關鍵要素，順利執行 DLP 資料外洩防護系統專案。

6.1 研究發現

本研究引用多位學者的理論，並根據第五章的的訪談分析歸納出之導入 DLP 資料外洩防護系統導入的關鍵因素如下：

1. 組織層面因素：

在高階主管支持，在此次的訪談中了解到高階主管的重視是影響整個系統導入成敗的主要因素之一，原因是 DLP 資料外洩防護系統對於公司而言，是需要員工全面性的參與和了解，公司的各項重要機密資料或者客戶資料，都有可能在透過任何一個員工而洩漏出去，對公司而言是相當重要的政策，如果政策命令無法由上到下，就有可能導致員工無法配合，或者不了解而產生抗拒導致整體性的失敗。

由於 DLP 資料外洩防護系統導入需要事先定義機密資料來源的位置，專案小組在布署系統時需事先知道，如果沒有得到上級的授權或者相關資源的給予，可能會造成在跨部門溝通時遇到某種程度上的阻疑，B 公司就是在這部分遇到其它使用單位因為對系統的不了解，也沒接到政策命令，而發生不配合的情況，無法獲重要資料位置讓系統做學習，直接影響了 DLP 資料外洩防護系統的產出效益，對整個專案而言佔有很大的影響層面。

其它間接的影響，如高階主管沒有重視或者支持，可能無法給專案成員在時程上的壓力或者責任，雖不一定會導致失敗，但會因為沒有定期的專案進度或者回報，在專案建置時程上可能會有所延誤，專案成員們如沒有責任的分配或者定期的提供進度壓力，有可能會造成責任推卸的情況，或者在建置以及系統操作學習上的心態及熟悉度降低，導致上線目前標以及預期效益上莫大的落差。

另外特別發現公司文化也會間接影響導入的成敗，在任何一個資訊安全專案中，或多或少都會影響或者接觸到員工的個人隱私，在此次的 B 公司個案中，由於上層主管對系統導入後的員工反應和公司資訊政策相較之下，是比較在意使用者的抗拒程度的，最後將部份功能變關閉或者與原應用的架構做異動，之後的結果就變成 DLP 系統導入的不完全，與原來的預期目標不符。

2. 專案層面因素：

由於資訊安全系統的導入在技術以及專案面都是屬於較進階的，其需要有一定程度的知識和經驗，所以對參與專案成員的遴選，必須是嫻熟於有實際接觸的資深工程或者專案經理，且最好能在專案期間做好權責分配。因為這樣人員才能真正熟悉作業過程及實際問題所在，全力協助專案之進行。

本研究所訪談的二個個案公司在專案成員方面都有不錯的知識以及對產品的認知，所配合的廠商以及顧問團隊都是相同的，唯一不同的是責任上的分配，與對 DLP 系統導入的成敗對公司未來發展影響的認知上有很大的差別，在 A 個案公司有成立專案團隊，有清楚的共同的目標，不但分工也有責任上的分配，在整個建置過程中與系統學習上的態度都對其建置的成功有極大的幫助。而對 B 公司的參與成員來說，此次的導入專案與一般的系統無異，其心態上與責任感就有很大的差別。再者專案會議的規畫也很重要，有計畫的排定與廠商和原廠開會，可以定期檢視進度以及提出目當前遇到的問題，是否需要協助或者客制化應用等，都會影響專案建置時程以及妥善程度。

另外成員們的溝通能力上也會有所影響，前文所述，在導入系統時，在某些情況下是需要跨部門協助的，A 公司是屬於傳統產業，不但一般員工很信任資訊單位，且其文化上也是活潑親切，樂於相互了解，這點對於系統導入的協助與溝通上有很大的助幫助，而 B 公司是科技產業，員工門在資訊科技上的認知較為深入，也因為如此對資訊單位的態度上就較 A 公司為差，所以在配合程度上需要花費成員們很大的努力來說服或者上級的授權才能達成共識，這也是後來 B 公司導入失敗的一個重要的因素。

3. 科技構面因素

硬體需求量和部署步驟和難度，是判斷 DLP 產品成熟度的一個關鍵指標。一台設備和一台伺服器即可構成一個完整的方案，並允許加裝額外設備以提供延展性。理想狀況下，一個 DLP 方案應可以當成一個整合式的方案進行部署，而非採用諸多點方案組合而成。而容易使用是許多資訊系統導入成功的主要因素，複雜的的產品設計會使資訊人員效率減低，例如需要多個複雜的設定和管理步驟，以及難以理解的界面，不僅增加成本而且提高人為錯誤的可能性。設計良好的的產品應該可以透過一個整合性的友善

GUI 介面執行所有管理和政策設定工作，達到簡化管理，減少系統作業的所需時間，以及降低人為不當的操作，而導至成效不彰。

所以在科技構面來說，本研究個案公司所導入的 DLP 資料外洩防護系統產品 Websense 公司，在相關技術上以及產成熟度都是屬於世界級的領導者，其系統的支援度上非常的完整，其相容性以及在本次訪的個案公司軟硬體上的整合度都沒有出現太大的問題以及阻礙。在教育訓練上的提供以及經驗上也都非常的豐富，針對客戶的客制化需求也有提供付費的服務，所以這方面並沒有影響二個個案公司導入的問題。

其次由於本次專案建置，採用 Websense 提供的 DLP 資料外洩防護系統，其所要求的軟硬體規格並不高，以目前企業的資訊基礎建設皆能符合，所以在本研究的二個個案公司當中並沒有發生影響導入的狀況，系統的穩定度上也都非常良好。唯一需要考量的是專案建置人員對企業內部系統的了解程度以及資訊安全方面的認知度。

在科技構面，其系統品質因素是影響導入成功的重要因素之一，DLP 資料外洩防護系統其主要的作用就是幫公司保護重要的資料或者資訊外洩，在個案 A 公司當中，其較成員較 B 公司成員熟悉操作，在政策制定以及流程都有方案，且因有事先公告所以參與成員的配合度高，所以無論是閘道器端的監控以及端點的布署都很完整，最終在系統應用程度上有不同的結果，當然在預期資料外洩防護的成效上就符合預期。

而 B 公司在，因為公司文化的差異，公司員工在抗拒程度上，以及執行面和策規畫上都沒有一套標準，又加上布署 DLP 資料外洩防護系統的完整度較 A 公司差，因為無法取得重要機密資料，只能套用通用政策範本，最後導致誤判率過高，輸出品質不符合預期效益，高階管理者也害怕因為誤判率高，如果冒然的採用嚴謹的政策，有可能會影響使用者的線上作業,更因為沒有責任劃分,所以更加沒有人願意去承擔出錯時的風險，由於準確率的問題，無法有效偵測事件，最後導致系統閒置，只當成事件發生和稽核記錄的工具，終究使系統導入失敗

4. 環境構面因素

在本次的研究個案訪談當中，環境構面的因素並沒有直接影響 DLP 資料外洩防護系統導入的成敗，但會直接推動企業導入系統的積極度，例如個資法的通過，由於罰金的提升以及比以往的法規多了舉證的義務等，如果目前企業沒有類以的資安系統，勢必會造成其對 DLP 資料外洩防護系統的迫切性需求。

在科技基礎上，其複雜度及使用流程上並不像 CRM 或者 ERP 等系統，牽涉範圍那麼廣大，以及對公司的營運和效率甚至是獲利上有著重大的影響，因為 DLP 資料外洩

防護系統，在分類上並不屬於公司的獲利策略之一。除了上述不同點外，其同樣的是，成員們在這些特定的的領域裡一定要非常的熟悉，很多時候一件專案的成敗都是來自於對事物的不了解以及忽視而導導失敗。

這次的訪談中 B 公司在 Windows AD 的基礎建設上較 A 公司為差，有間接影響在 DLP 系統在建置完整度的不同，因為 AD 沒有完全應用在公司上，最後無法透過統一的派送機制把 DLP 資料外洩防護系統所提供的端點代理程式安裝在使用者的電腦上，造成部份功能喪失。這也是日後要導入 DLP 資料外洩防護系統需求在事先規畫產品以及建置策略需要特別留意的部份，另外不同公司所提供的產品建置需求有所不同，所以在產品評估階段，建議把公司目前的科技基礎狀況與專業顧問做妥善的討論。

6.2 研究建議

本論文根據科技－組織－環境基礎架構為本研究之主要理論基礎，將導入 DLP 資料外洩防護系統之公司以科技構面、專案構面、組織構面和環境構面進行分析與探討。其中發現科技構面中的系統品質，與組織構面中高階主管支持，以及專案構面的專案成員以及參與度等因素均為導入 DLP 資料外洩防護系統成功的主要因素。

然而由於過去 DLP 資料外洩防護系統導入企業尚不普及，使得有意導入該系統的企業裹足不前。隨著個人資料保護法的通過，以及對 DLP 資料外洩防護系統的認知愈來愈重視，也視為企業經營的重要策略之一。本研究針對之後欲導入 DLP 資料外洩防護系統的公司提出以下建議：

1. 明確的目標：
   除了高階主管本身對系統導入有高度認知與支持之外，建立明確的目標，並確實執行以確保命令傳達到各單位上，才能使員工能更加的重視以及貫徹，另外成立專案團隊，在必要時給予適當的權限以及資源，並建立一套標準的作業程序以及訂定導入時間表，適時的讓高階主管了解目標達成率。

2. 專案團隊設計：
   專案團隊在根據系統所需的相關知識以及經驗人員建立後，應適當的給予責任上的分配，並了解內部員工的作業習慣，以及在導入 DLP 外洩防護系統的前後做適當的資訊安全教以及宣導，可以提高員工的配合程度以及專案認知。其次專案負責人亦有責任提供足夠的資料以及相關資訊，爭取高階主管的認同及參考，並定期召開專案會議回報目前執行狀況和進度，適時的讓高階主管可以獲得清楚而正確的決策資訊。

3. 政策面的實施：
另外 DLP 外洩防護系統導入的專案的成敗，是由各層構面一層一層由上而下影響而來，最後影響系統的品質輸出，DLP 是一個特殊的系統，當輸出的結果不能替企業防止資料外洩，那麼其效益趨近於零。

4. 導入評估計畫：
DLP 資料外洩防護系統是一套需要有相當知識以及經驗才能導入順利的系統，所以其教育訓練定以及相關知識需要及早了解以及安排，另外顧問及廠商應從旁協助提供練習的機會；尤其是資訊人員以及主要關鍵管理者，以減少日後的錯誤發生，或者不熟悉導致系統發生錯誤的風險。另外導入 DLP 方案時需評估目前現有環境的整合性，並了解建置所需軟硬體資源，需要多少伺服器才能建置完成，才能產生企業層級的成效，才不會耗費數星期或甚至數個月的部署時間。

6.3 研究限制

由於研究過程中可能發生的誤差以及資源、時間的有限性，仍有下列的研究限制：

1. 受訪主觀意識的談話可能造成的影響，在個案訪談的過程中，被訪者有可能因為在整個專案中立場的不同，和職位角度不同，而無法以客觀的態度來提出看法與回答，另外與訪談者的熟悉度也會造成不同受訪者提供訊息上的程度落差，影響其對訪談問題的結果。所以在針對問題進行歸納分析時，亦會因為上述之因素，影響本研究結論。

2. 由於研究時間有限，且 DLP 資料外洩防護系統市面上也有多種類似產品，導入個案公司選擇無法完全代表整體已導入或者未導入之公司，所以在取樣上無法完全代表整體的研究對象，因此將研究結果推測到其它不同產業以及不同公司規模和導入不同性質產品的專案有其限制性。

3. 本篇研究採用個案分析法，所以並沒有使用量化的方法來進行一連串合理的推論。在研究建議方面，由於時間及客觀環境的條件下，本研究只針對已導入 DLP 資料外洩防護系統的公司進行訪談，未來研究可以增加未導入或正進行導入 DLP 資料外洩防護系統的公司，了解其影響導入的關鍵因素以增加研究深度。也可使用不同模型理論做進一步探究，進一步擴大了解在不同層面影響原因，建議未來欲研究相關議題者，可採用問卷的方式來獲取實際量化數字來進行資料分析。

參考文獻-中文部份

1. IT Home, . (2011). "資料外洩防護產品." http://online.ithome.com.tw/001/20100324/
2. 工業技術研究院.(2008)"數位版權管理技術" http://www.itri.org.tw/chi/tech-transfer/04.asp?RootNodeId=040&NodeId=041&id=3323
3. 立法院圖書館. (2010). "國外個人資料保護法案." http://npl.ly.gov.tw/
4. 全國法規資料庫. (2010). "個人資料保護法" http://law.moj.gov.tw/LawClass/
5. 周世雄. (2010). 資料外洩防護導入實務經驗談. 資訊安全通訊, 16(4), 159-172.
6. 林鈴玉. (2001). 國內網路銀行現況發展及交易安全之研究, 國立交通大學管理學院(資訊管理學程) 碩士論文.
7. 黃亮宇. (1992). 資訊安全規劃與管理. 松崗電圖書資料股份有限公司, 民國 82 年, 8.
8. 廖緯民(1996).論資訊時代的隱私權保護－以「資訊隱私權」為中心。資訊法務透析，1996(11)，22。
9. 樊國楨, & 楊晉寧. (1996). 互連網 (Internet) 電子信息交換安全-以電子公文交換作業安全為本.
10. 戴燊. (2013). 台灣企業資訊安全預防管理之現況, 方法與趨勢. 資訊安全通訊, 19(1), 75-81.
11. 趨勢科技(2013),” MIS 如何導入適合企業的 DLP-趨勢科技資料外洩防護方案” http://www.trendmicro.com.tw/micro/TMLP/TMLP_microsite_mis.html#mis01

參考文獻-英文部份

1. Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. Management science, 35(8), 982-1003.

2. Delone, W. H. (2003). The DeLone and McLean model of information systems success: a ten-year update. Journal of management information systems, 19(4), 9-30.

3. Drury, D. H., & Farhoomand, A. (1996). Innovation adoption of EDI. Information Resources Management Journal (IRMJ), 9(3), 5-14.

4. Gartner (2013). "Content-aware data loss prevention (DLP)." http://www.gartner.com/it-glossary/content-aware-data-loss-prevention-dlp

5. Grover, V., & Goslar, M. D. (1993). The initiation, adoption, and implementation of telecommunications technologies in US organizations. Journal of Management Information Systems, 10(1), 141-163.

6. Herriott, R. E., & Firestone, W. A. (1983). Multisite qualitative policy research: Optimizing description and generalizability. Educational researcher, 14-19.

7. Kim, Y., Park, N., & Hong, D. (2011). Enterprise data loss prevention system having a function of coping with civil suits. In Computers, Networks, Systems, and Industrial Engineering 2011 (pp. 201-208). Springer Berlin Heidelberg.

8. Kwon, T. H., & Zmud, R. W. (1987, April). Unifying the fragmented models of information systems implementation. In Critical issues in information systems research (pp. 227-251). John Wiley & Sons, Inc..

9. Lawton, G. (2008). New technology prevents data leakage. Computer, 41(9), 14-17.

10. Liu, S., & Kuhn, R. (2010). Data loss prevention. IT professional, 12(2), 10-13.

11. Malhotra, N. K. (1993). Marketing research: An applied orientation. Englewood Cliffs, NJ: Prentice Hall.

12. Mcafee(2012).“Mcafee total protection for data loss prevention” http://www.mcafee.com/us/resources/solution-briefs/sb-total-protection-for-dlp.pdf

13. Mogull, R., & Securosis, L. L. C. (2007). Understanding and selecting a data loss prevention solution. Technicalreport, SANS Institute.

14. Phua, C. (2009). Protecting organisations from personal data breaches. Computer Fraud & Security, 2009(1), 13-18.

15. Premkumar, G., & Roberts, M. (1999). Adoption of new information technologies in rural small businesses. Omega, 27(4), 467-484.

16. Reich, B. H., & Benbasat, I. (1990). An empirical investigation of factors influencing the success of customer-oriented strategic systems. Information Systems Research, 1(3), 325-347.

17. SANS Institute . (2010). "Understanding and Selecting a Data Loss Prevention Solution." http://sans.org

18. Schultz, E. E., Proctor, R. W., Lien, M. C., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. Computers & Security, 20(7), 620-634.

19. Shabtai, A., Elovici, Y., & Rokach, L. (2012). A taxonomy of data leakage prevention solutions. In A Survey of Data Leakage Detection and Prevention Solutions (pp. 11-15). Springer US.

20. Symentec(2013).” Symantec data loss prevention for endpoint” http://www.symantec.com/content/en/us/enterprise/fact sheets/b-dlp for endpoint DS 21189146.en-us.pdf

21. Tornatzky, L. G. and K. J. Klein (1982). "Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings." Engineering Management, IEEE Transactions on(1): 28-45.

22. Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). Processes of technological innovation.

23. Von Solms, R. (1996). Information security management: the second generation. Computers & Security, 15(4), 281-288.on

24. von Solms, R., van der Haar, H., von Solms, S. H., & Caelli, W. J. (1994). A framework for information security evaluation. Information & Management, 26(3), 143-153.

25. Websense(2013),” The shortest path to prevention and risk eduction”http://www.websense.com/assets/white-papers/white-paper-dlp-path-prevention-en-june-2013.pdf & http://www.websense.com/content/support/library/data/v78/deploy/deploy_dss.pdf

26. Wixom, B. H. and H. J. Watson (2001). "An empirical investigation of the factors affecting data warehousing success." MIS quarterly 25(1): 17-32.

27. Yin, R. K. (2009). Case study research: Design and methods, sage.