縱深防禦策略應用於資訊外洩防制之探討

作者／國防大學理工學院電機系博士生 周兆龍少校・副教授 劉江龍上校・教授 婁德權上校

提要

一、縱深防禦策略（Defense-in-Depth, DiD）為實踐資訊確保（Information Assurance, IA）的主要核心策略，針對各個資訊系統與網路採取層層防護的機制，以全方位的防護機制，確保核心資訊的安全。

二、隨著通信與資訊科技的快速發展，無論企業或個人對於資訊化與網路化的依賴程度愈來愈高，相對面臨資訊外洩的情況也愈來愈嚴重。

三、本文針對可能發生資訊外洩的管道及途徑，運用縱深防禦策略，提出能有效防制資訊外洩的具體作法，可供國軍資訊安全政策發展之參考。

關鍵詞：縱深防禦策略、資訊確保、資訊外洩防制

壹、前言

2007 年 10 月，英國發生一起嚴重的個人資料外洩事件，儲存近 2 千 5 百萬筆英國民眾的光碟，在郵寄過程中遺失。這個事件將造成英國近半數人口的銀行資料可能外洩，並且遭到盜用、盜領的風險[1]。事隔不久，英國皇家海軍一名軍官的筆記型電腦失竊，裡面儲存近 60 萬名入伍士兵的個人資訊，包括住址、電話、護照、駕照、保險號碼、家庭狀況，甚至銀行帳戶等資料，這些外洩的資料將可能讓這些士兵遭受財產與人身安全的威脅[2]。

類似的情況同樣發生在你我周遭，香港知名藝人因為電腦故障送修，電腦硬碟內儲存的私密照片被有心人士竊取並故意散播；誠品網路書店將 40 萬名會員的交易資料與紀錄外洩到詐騙集團手裡[3]；大約 500 萬個人所得稅網路申報的明細資料可以透過 FOXY 軟體搜尋到[4]；31 萬基測考生基本資料疑似遭外洩給補教業者[5]…等等。

從上述幾個案例可以發現，資訊外洩（Information Leakage）是一個日益嚴重的問題，隨著資訊化程度的增加，資訊外洩事件發生的機率也愈來愈高，小

1 蔡學鏞，「資訊安全最弱的一環」，2007 年 12 月 12 日，http://www.ithome.com.tw/itadm/article.php?c=46698。
2 「英國資料外洩又一樁 60 萬士兵個資遭竊」，資安人科技網，2008 年 1 月 21 日，http://www.inormationsecurity.com.tw.
3 「漢光、誠品資料外流 資安事件層出不窮」，資安人科技網，2008 年 3 月 10 日，http://www.inormationsecurity.com.tw.
4 「網路報稅 500 萬個資恐不保」，壹蘋果網路，2008 年 5 月 5 日，http://1-apple.com.tw。
5 「基測個資外洩？ 教育部：已展開調查」，資安之眼，2008 年 6 月 13 日，http://www.itis.tw/node/1867。

從個人隨手列印的一張文件，大到政府資料庫系統內儲存的資料，都有可能發生資訊外洩。

國軍在資訊系統發展的推動上不遺餘力，許多傳統業務都已仰賴資訊系統的運作，例如電子公文資訊系統、人事資訊系統、財務資訊系統、聯合後勤資訊系統...等等。由於國軍將逐漸實施募兵制，國軍人力勢必縮減，而隨著通信、資訊、電子環境的逐漸複雜化與多元化，國軍對於資訊系統只會更加依賴。

由於國軍在國家安全扮演絕對重要性的角色，因此在防範資訊外洩的議題上更應受到重視。近來國軍層出不窮的資安事件，例如國防部某單位因重要文件未遵照規定與標準程序銷毀，導致機密資訊外流；國軍同仁因使用家用個人電腦不慎遭到駭客植入木馬程式，致演習機密檔案遭到竊取...等等，已非單純靠資安技術「加密」就可以防範，而是與資訊系統有關的「人」或「程序」出了問題，這種現象值得我們警惕。

本文借鏡了美軍在 90 年代發展資訊作戰期間，所提出的縱深防禦（Defense-in-Depth, DiD）的概念，其原理係指在核心資訊之外，建立層層的防護機制，使得外部若想探悉內部資訊，必須通過層層關卡，無形之中確保了核心資訊的安全。

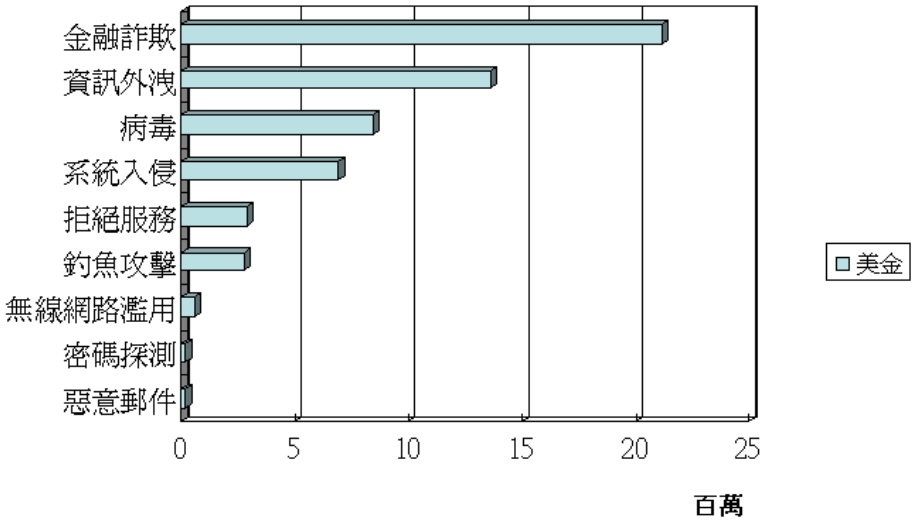
貳、本文

隨著資訊科技（Information Technology, IT）的快速發展，現今不論軍事、商業、科技、醫療、政府機構或家庭個人，日常生活中對於各種電子、資訊、通信系統依賴程度已到了不可或缺的程度。例如個人必備的手機通訊、學校推展網路化的遠距教學、企業運用網路進行商業交易活動、政府機構強調網路作業的便民、其他如金融股市交易系統、國家運輸系統（如航空機場、鐵路、高速公路等）、重要能源設施（如核能電廠、水庫、油庫）...等等，我們可以發現生活周遭都離不開電腦資訊系統。電腦與網路給人們帶來了便利，但在愈來愈複雜的電子化環境之下，各種軟體、硬體、資料庫、電腦系統、網路...等等，實際上面臨了各式各樣的威脅。

以個人來說，因為身份證被盜用、信用卡被盜刷、住址、電話、醫療紀錄、財務狀況、家庭生活細節等私人資訊外洩，將可能造成財物損失、名譽受損、隱私權受損、生活干擾、心理壓力...等等不良影響。

以企業來說，因為軟體、設計藍圖、專利技術、業務計畫、交易紀錄、客戶資料等商業機密資料外洩事件，除了龐大的利益損失，還可能造成罰鍰、訴訟、企業形象受損、失去消費者信心等負面影響。

不論是個人或企業，資料外洩都可能造成昂貴的代價。根據 2007 年美國電腦安全協會（Computer Security Institute, CSI）對網路犯罪與資訊安全的最新調查[6]，常見的電腦犯罪手段以非法存取網路（59%）、病毒感染（52%）及竊取移動式裝置（50%）的比例最高，超過半數以上的受訪企業都曾發生類似的案例。而 2007 年統計電腦犯罪對造成企業的財產損失，因機密資訊遭竊及內賊所造成的損失金額共計 1,360 萬美元，排名第二，僅次於金融詐欺（2,112 萬美元），並且已超過因病毒、蠕蟲、間諜程式（839 萬美元）及系統遭外界入侵（687 萬美元）所造成的損失[7]（如圖一所示）。



圖一 2007 年電腦犯罪損失金額統計表[6]（作者繪製）

國軍對於資訊安全的發展不遺餘力，從集控式防毒系統、系統修補更新、檔案加解密軟體、電腦輸出入埠管制、AD 網域建置、CERT 監控機制、移動式儲存媒體管制...等作法，顯見國軍資訊整體戰力已有顯著的提昇。惟近來國軍仍發生多起資訊洩密事件，不僅影響軍譽，也對國軍戰力造成了嚴重的影響，歸納其發生原因如下：

一、過於著重資訊科技的運用，而忽略其他資訊外洩可能的管道。

二、人員教育訓練成效不彰，缺乏危機意識。

三、資訊技術停滯未更新，無法應付新興的威脅。

四、缺乏良好的風險管理與監控機制。

五、資源不足（缺乏專業資訊人力、技術）。

6 R. Richardson, "2007 CSI Computer Crime and Security Survey," Computer Security Institute, 2007, http://www.gocsi.com/.

7 「善用資料外洩防禦技術保護企業重要資產」, Trend Micro Inc., Jan 2008, http://tw.trendmicro.com/tw/products/enterprise/leakproof/white-paper/index.html.

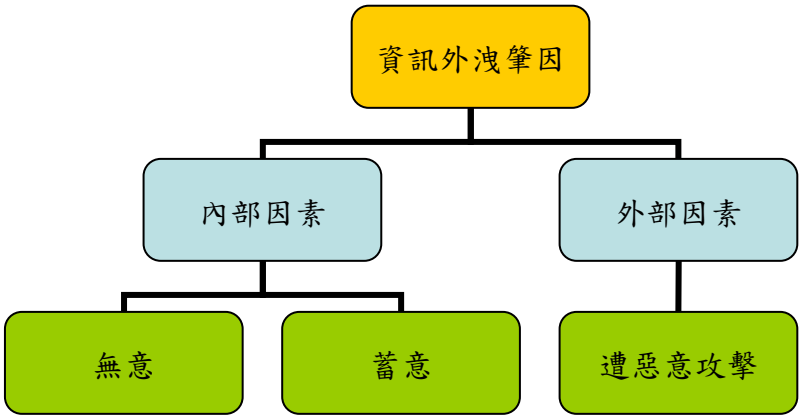
資料外洩的肇因廣義來看可以概分為「內部因素」及「外部因素」兩大類[8]（如圖二所示）：

一、內部因素

通常泛指因內部人員「無意」或「蓄意」所造成。例如員工寄送電子郵件時，未仔細檢查收件人名單，而不慎將內部機敏資料寄給外部人員，這類屬於無意事件；若內部員工因貪圖利益，知悉違反工作職責，仍將內部資料竊取或複製販賣給外部人士，這類即屬於蓄意事件。

二、外部因素

指遭內部以外的「惡意攻擊」所造成。例如遭駭客入侵資訊系統，竊取內部機密資料檔案；或者合約商或競爭者以非正式手段，竊取內部商業機密文件，這類均屬於外部因素。



圖二 資料外洩肇因分類示意圖（作者繪製）

資訊外洩的管道大致可以分為「實體裝置」、「虛擬通道」及「人員」三大管道[9]（如圖三所示）：

一、實體裝置

係指透過例如電腦、筆記型電腦、PDA、USB 儲存裝置、CD/DVD、iPod、數位相機、照相手機、印表機、傳真機...等等實體裝置。

二、虛擬通道

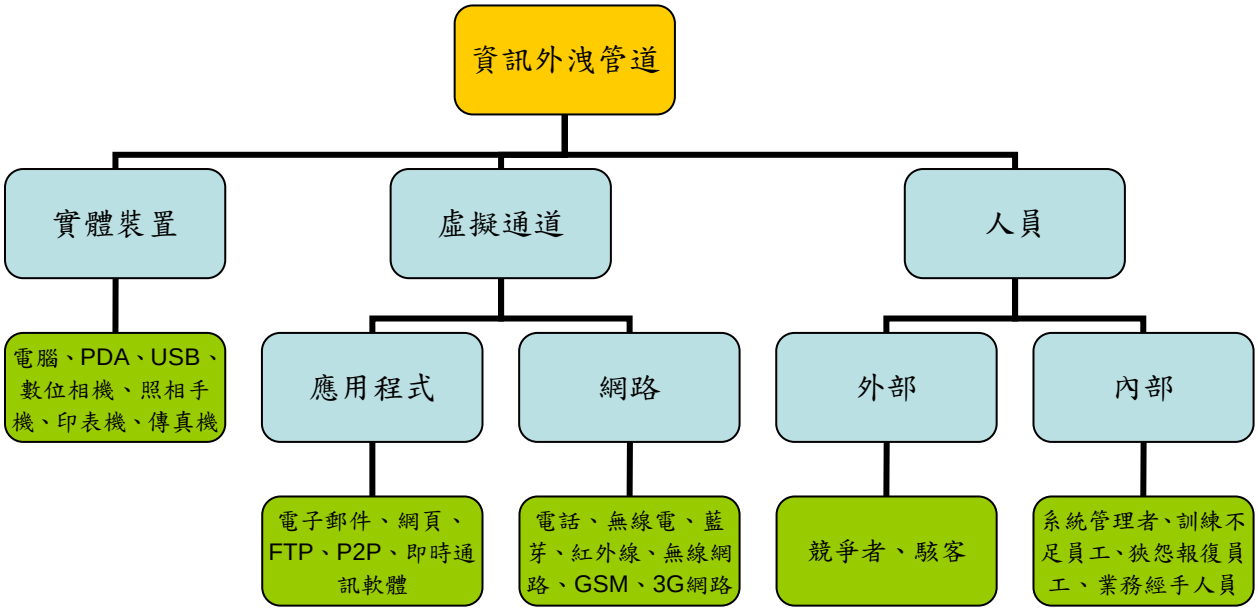
指透過應用程式或網路傳輸方式。應用程式的部分例如電子郵件、網頁、FTP、即時通訊軟體、P2P 分享軟體...等等；而網路傳輸方式則例如電話、無線電、藍芽、紅外線、無線網路、GSM、3G 網路...等等。

三、人員

8 “Information Leak Prevention Accuracy and Security Tests”, Percept Technology Labs, Inc. 2006 http://www.websense.com/docs/whitepapers/wp0106-0506_perceptlabs.pdf.

9 「防制企業資料外洩實務方案」，資安人雜誌，2007 年 7 月。

包括內部與外部的人員。外部人員如競爭者或駭客；內部人員則可能是具有系統管理權限的人員、訓練不足的員工、重要業務經手的員工、狹怨報復的員工...等等，都可能成為資訊外洩的管道。



圖三 資料外洩原因分類示意圖（作者繪製）

由於無線網路、通訊系統及行動裝置的普及化，再加上資訊技術的不斷推陳出新，大大提昇了資料交換或分享的便利性，但無形之中在現今如此複雜的資訊環境下，資訊外洩的風險也跟著大幅增加。

防制資訊外洩並非一股腦將所有可能外洩的通道完全封堵，這種作法不但不切實際而且成本太高。比較有效的方式，仍必須從資訊外洩事件發生的根本原因來分析，究竟是因為內部或外部因素？是透過何種裝置？是因為系統設計錯誤？是因為網路管控不當？還是遭受駭客的惡意攻擊？惟有找出原因，才能對症下藥，解決問題。本文將進一步探討如何利用縱深防禦的概念，來有效落實資訊外洩防制。

參、縱深防禦策略

美軍在 90 年代開始推動所謂的軍事事務革新，箇中原因就是在波灣戰爭後，美國開始洞察到資訊科技的快速發展，對傳統軍隊的結構、編制體制、作戰思想和軍事訓練都產生深遠的影響。這波軍事事務革新係以發展光電、自動控制、通信、電腦資訊、網路、人工智慧等核心與關鍵的創新科技，以優化指揮、管制效能，提昇部隊戰力。

美軍在「2010 年聯戰願景」中明確宣示，將運用「優勢機動、精確接戰、

聚焦後勤及全方位防護」等創新作戰構想，確保資訊優勢（Information Superiority），快速掌握戰場的全貌，以獲致最終的勝利[10]。

美軍具體的發展策略是從資訊基礎建設開始，建立所謂的全球資訊網路架構（Global Information Grid, GIG），嘗試將網路上的資源全面連結、互通，建立一個強大具感測（sensor）能力、協同合作（collaboration）的軍事資訊網絡，而在其基礎之上發展資訊戰（Information Operation, IO）及網狀化作戰（Network-Centric Warfare, NCW）等未來型態作戰，以確保資訊優勢[11]。其目標是透過資訊優勢建立決策優勢（Decision Superiority），並最終獲致作戰的全方面優勢（Full-spectrum Dominance）（如圖四所示）。

圖四 美軍軍事網格架構示意圖

（資料來源：陸儀斌，「走向資訊網格時代」，94 年國軍資電優勢研討會。）

由於資訊戰與網狀化作戰對於資訊系統與網路的依賴程度極高，相對的安全需求亦極高，因此為了確保資訊戰與網狀化作戰運作順遂，美國國防部與國安局共同制訂了一套資訊確保技術架構[12]（Information Assurance Technical Framework, IATF），對資訊系統與網路提供防護、偵測、應變與復原等能力，其五個核心要素如下：

一、有效性（Availability）

為了確保資訊服務品質，必須預防因為外部攻擊或系統本身的錯誤，造成資料無法被合法存取使用。

二、鑑別性（Identification and Authentication）

對於資源的存取者要求某種程度的身份識別，並且針對不同機敏等級的資料必須進行權限管控，以防止未經授權存取資訊。

10 “Joint Vision 2010”, http://www.dtic.mil/jv2010/jv2010.pdf.
11 陸儀斌，「走向資訊網格時代」，94 年國軍資電優勢研討會，中正理工學院，桃園，pp.37。
12 「確保資訊安全之技術與架構」，陸軍軍事譯粹選輯第十二輯，pp.207-228。

三、機密性（Confidentiality）

當資料遭到未經授權存取或非法竊取時，可以透過加密方式進行保護，以防止資料內容被窺探。

四、完整性（Integrity）

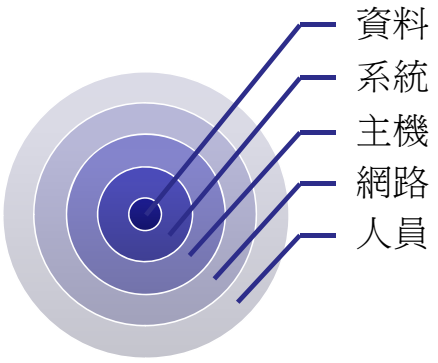
當資料在傳輸或使用的過程中，防止資料被未經授權的竄改、偽冒或刪除，以確保資料與原始來源相同。

五、不可否認性（Non-repudiation）

當資料在交換的過程中，可以透過數位簽章的方式，避免因偽冒或其他原因，使得傳送者或接收者的任何一方，否認已傳送或接收的資料。

美軍資訊確保架構的主要核心就是縱深防禦策略。縱深防禦的觀念可以應用在各種資訊系統及網路，其基本原則是對機密資料所存放的系統或網路...等各個層級中，都採取多層式的防護（Layered Defense），當某一層級的防護機制被突穿時，其他層級的防護機制就會取而代之提供備援防護功能。

一般的資訊系統環境由內而外依序可以區分為資料、系統、主機、網路、作業人員等各種不同層級[13]（如圖五所示）。資料通常被儲存在最核心的部分，多層式防護的觀念係指當人員欲存取內部資料時，須由外而內依序透過人員、網路、主機、系統等層層防護，才能取得最終的核心資料。如果網路防禦層級遭突穿時，主機層級的防禦機制則提供進一步的防護機制；主機防禦層級遭突穿時，則由系統防禦機制繼續提供防護，以此類推。



圖五 縱深防禦多層防禦示意圖（作者繪製）

美軍資訊確保技術架構中將縱深防禦概念區分「人員」、「科技」及「作業程序」三大主軸[14,15]，其要點如下：

13 P. Rubel, C. Payne, M. Ihde, S.Harp, and M. Atighetchi, “Generating Policies for Defense in Depth”, IAnewsletter Vol.9 No.3 2006.
14 B. K. Ashley, L. Jackson, “Defense in Depth”, IAnewsletter Vol.3 No.2 1999.
15 “Information Assurance Through Defense in Depth”, 2000, http://handle.dtic.mil/100.2/ADA377569.

一、人員

是縱深防禦概念中的核心元素，依據安全管理政策及權責區分，包含高階管理者、安全管理人員、作業員工等，負責的項目包括安全管理政策制訂、資源分配、風險評估、系統設計、系統建置、系統管理、作業維持...等重要工作。因此人員的教育訓練、實務經驗、專業知識與安全認知都是不可或缺的條件，尤其重要的是必須挑選出值得信賴的人員負責各層級的工作，才能確保核心安全。

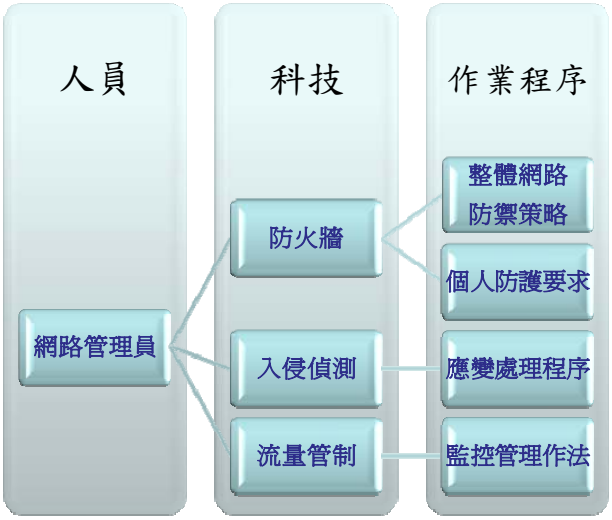
二、科技

科技發展日新月異，良好的科技必須配合適當的控管，應用在適當的位置，才能發揮最大的效益。因此科技的運用係依據系統架構與安全政策，評估各層級的安全係數，進行風險評估後，選擇適合的安全防禦技術（例如針對網路採用防毒系統、入侵偵測系統或防火牆；針對資料則採用加解密、電子簽章），將其部署在各層級節點。

三、作業程序

指與安全防禦有關的整體策略、管理目標、作業準則、執行細節...等相關作業程序，涵蓋範圍十分廣泛，包括認證、授權、金鑰管理、安全評估、偵測、預警、應變、復原、重建...等程序，為了能有效防禦新的安全威脅，必須隨時檢視相關安全政策與作業程序，適時予以修正。

依據縱深防禦策略中多層式防護的概念，在每個層級的防禦機制中，「人員」、「科技」及「作業程序」三者之間應該緊密結合。以網路防護層級為例（示意圖如圖六所示），人員的部分代表單位應具備專業的管理人員（如網路專業人員）；科技的部分則代表需要採用的技術（如防火牆、入侵偵測、流量管制...等）；而作業程序的部分則代表有關網路層級的整體策略、作業程序與管理辦法（如整體防禦策略、緊急應變程序、監控管理作法...等）。



圖六 縱深防禦策略:以網路層級為例（作者繪製）

綜合上述特點可以發現，縱深防禦策略的多層式防護概念象徵著「縱向防護」，而人員、科技及作業程序等三大主軸則象徵著「橫向防護」，當縱向與橫向的密切整合，便能建構一個完善的整體防禦機制。

肆、防制資料外洩實務作法

一、縱深防禦策略原則

應用縱深防禦策略來探討資料外洩防制時，有幾個值得注意的重要原則[16]：

(一)必須防禦關鍵位置

應同時針對內部、外部，各個關鍵點部署足夠的防禦機制，以防範可能的資料外洩風險。例如資料管理人員、主機 I/O 連接埠、應用系統管理介面、網路的通訊埠...等，通常是資料傳輸的必經之路，也是常見的資料外洩管道，因此應視為關鍵點加強防禦。

(二)必須採取多層式防禦

再好的防禦技術都有可能具有弱點或被破解的時候，每個層級所面臨的威脅也不同，例如網路層級依賴較多的資訊防禦技術，而人員層級則仰賴嚴謹的管理辦法與作業程序，因此採取多層次的防禦機制，以面對不同特性的威脅，建構整體防禦機制。

(三)必須防護資訊作業環境

除了部署多重防禦機制之外，與資訊作業有關的各個環節，例如主機、伺服器、應用系統、內部網路、外部網路、作業人員...等，都必須分別採取適當的防護措施，以確保各個環節的安全，消弭可能的資安疑慮。

(四)完整的安全機制

良好的安全機制，必須透過完善的整體防禦策略與作業管理程序，並且結合適當的資訊技術與專業人員，從整體的安全架構進行分析與評估，隨時調整、應變，以適應各種新興的威脅。

二、資訊外洩防制實務作法

依據縱深防禦策略的原則，資訊外洩防制的實務作法，由內而外分層說明如下（如圖七所示）：

(一)資料層級

1.資料分級制度：資料依據重要性應加以分級，並訂定人員存取權限，如有運用需求，可針對特定檔案類型或機敏等級進行管控。

16 同註 12。

2.制訂資訊運用政策：資料在製作、交換、儲存、運用等各階段，都應明確規範相關作業範疇或產生稽核紀錄（Access Log），以確保資訊不會因為壓縮、檔案格式轉換、檔案名稱變更等作業，而造成資訊外洩。

3.運用加密技術：資料本身可以運用加密技術，以確保資料遺失或遭竊時可將傷害減至最低。

(二)系統層級

1.訂定存取權限：系統應設定帳號權限及認證機制，依據不同等級存取適當資源，並進行認證，以避免帳號遭盜用或非法存取機密資料。

2.建立稽核機制：當實體裝置連結至系統或主機時，應主動進行偵測，以避免不當濫用。

3.完善構型管理：針對系統可能具備的弱點應持續改善或監控，並進行構型管理，以瞭解系統整體防護能力。

(三)主機層級

1.訂定資產管理政策：明確律定出禁用或管制使用的裝置，例如禁止使用USB、照相手機、數位相機、MP3 隨身聽等高風險的行動儲存裝置；而對筆記型電腦、印表機、傳真機的使用加強管控。

2.加強實體裝置的監控：當實體裝置單獨使用或連結至系統或主機時，應適時予以管制並主動進行偵測，以避免不當濫用。

3.裝置加密：當實體裝置確有使用必要時，可以運用加密機制，以確保若裝置遭竊或遺失時資訊不致外流。

(四)網路層級

1.防毒系統：防毒是最基本的網路防禦，避免因外部人士透過病毒、蠕蟲或木馬程式，進入網路內部竊取機密資料。

2.傳輸管道監控：網路應用十分廣泛，如電子郵件、FTP、即時通訊、網頁、P2P…等，這些通道都應該進行嚴格的管控，在正常的日常作業中，如發現可疑情況則應立刻採取警告、隔離、鎖定等措施。

3.防火牆管控：依據網路管理的整體策略進行防火牆設定，並針對特定的威脅進一步加以管控，減少網路遭外人入侵的機會。

4.無線網路安全機制：無論是採用紅外線、藍芽或寬頻網路，無線網路是未來不可阻擋的趨勢。針對無線網路的特性需要採取嚴謹的安全防護機制，包括認證、加密、專屬設備…等，以確保無線網路安全。

(五)人員層級

1.教育訓練：平常即應建立良好的危機意識，一般人員對於作業程序中可能

發生的威脅要具備基本的辨識能力，專業資訊人員則應針對各項安全防護機制有深入的瞭解。

2.作業準則：為了預防資料外洩事件肇生，完善的作業準則可有效達到預期的效能，例如風險評估作業、緊急應變程序、備援機制...等。

3.人員管理：人員是資訊外洩防制中最難執行風險管控的對象，尤其是內部具有權限的人員，常是造成資訊外洩的主要因素。內部人員背景過濾與稽核是必要加強的部分；另外可以利用法規罰則或切結的方式嚇阻有心人士。

圖七 資訊外洩防制實務作法（作者整理繪製）

伍、未來發展趨勢

2008 年 4 月在美國舊金山舉辦的「RSA 國際資訊安全研討會」中，將資訊外洩防制（Data Leak Prevention, DLP）選為 2008 年最受企業重視的安全技術之一[17]。同年 5 月在國內所舉辦的「2008 電子商務資訊安全研討會」上，國內電子商務業者也開始著手致力防範因資料外洩所造成的金融詐騙事件[18]。綜合目前國內外對於資訊外洩防制技術的研究，有幾項技術發展趨勢值得注意[19,20]：

一、集中式管控

17 「RSA 資安會議：DLP、NAC 與身份認證為今年焦點」，資安之眼，http://www.itis.tw/node/1731。

18 「電子商務業者今年加強防範資料外洩」，資安之眼，http://www.itis.tw/node/1751.

19 S. Besser, “Stopping Information Leaks: Why Traditional Content Filtering is no Longer enough”, PortAuthority Technologies, http://www.websense.com/docs/whitepapers/PA_contentfiltering.pdf.

20 R. Layland, “Data Leak Prevention: Coming Soon to a Business Near You”, Business Communications Review, May 2007, pp.44-49.

從美軍發展軍事網格的策略來看，看似分散的實體資訊架構，實際上是朝向虛擬整合的目標來發展。因為過於鬆散的資訊架構環境，容易造成不易管理的缺點，也相對增加了資訊外洩的機率。透過相同的資訊架構與管理機制，才能有效整合運用所有的資源（人員、裝備、知識），並提昇速度、分享資訊、協同合作，相對才能有效監控並防制資訊外洩的情事發生。

國軍因應人員精減的趨勢，資訊作業環境必須逐漸朝向集中架構發展，以降低人員與技術成本。首要工作就是降低資訊作業環境的複雜度，提高資訊透明度與資源分享的程度，並且逐漸朝向共通的資訊作業環境發展，進行虛擬整合，以達到集中管控，防制資訊外洩的目標。

二、內容過濾（Content Filter）

傳統的資料外洩防制系統會採用關鍵字搜尋的技術來防止機密外洩，例如掃瞄檔案名稱或電子郵件主旨中是否含有機密資料的字眼，但這種方式常因為檔案名稱被更改或資料格式轉換後，發生較高的誤判率。因此為了確保機密資料的安全性，新一代的監測系統將改採內容（Content）搜尋的方式