各國資訊安全政策初探

王貴珠

目　次

壹、前言
貳、資訊安全問題與對策
參、國內外資訊安全政策與措施
　一、 資訊安全問題
　二、 資訊安全防制對策
　三、 報案與危機處理機制
肆、資訊安全未來之展望
伍、結論

摘要

隨著資訊與網路的發展，世界各國已邁入電子資訊時代，尤其近來電腦犯罪與入侵案例頻傳，顯示出資訊與通信安全已是非常重要的課題。從政府的角度來看，資訊安全是攸關國家安全全局的問題；從企業的角度來看，資訊安全是維繫生計的利潤；而以人民的角度來看，資訊安全是保證公民基本權利的重要措施。因此我們可以從組織層面訂定資訊安全方針，從結構層面訂定資訊安全對策，從應用層面訂定資訊安全技術，全面來防範可能的入侵行為。

然而造成系統面臨危機的原因，並不只有人為的因素而已，尚包括自然災害、機器損壞等等，所以我們並沒辦法保證任何系統是絕對安全的，基於網路系統的安全問題隨時都有可能發生，就如同發生意外災害一樣，政府需要全民來正視此一問題，建立緊急應變程序及危機處理模式，將傷害降至最低。因此，本文提出在政策上從國家資訊安全的戰略思維、建立資訊安全管理標準、架構資訊安全規範、創設隱私權標章制度暨發展電腦密碼鑑識科技等概念性作法，期盼將來有助於提升我國對資訊安全的處理能力。

關鍵字：資訊安全、資訊安全規範、隱私權標章制度、密碼學

壹、前言

二十一世紀新科技的發展使人類透過電腦網路，交往日益緊密、頻繁與便捷，改變了大家的生活與價值觀，卻也開啟了犯罪的新紀元，電腦犯罪與入侵案例包括電腦病毒、網路蠕蟲、軟體木馬、系統暗門、邏輯引線、晶片嵌入、微型機械，矽晶噬菌、電子干擾、及電磁脈衝等，藉由毀害資料以達劫奪資訊系統所控制的實體，如使銀行帳目不正確、工廠生產設備停頓、病人維生設備失靈、交通儀空大亂、飛機失事、核電溫控異常等重大危害社會非法行為。然而資料所依附的軀殼是軟體系統，如同槍砲是利用彈藥的瞬間爆炸力破壞人類藉以隱蔽的建築防護體，資訊武器則是設法破壞資料軀殼，我們可將其分為四步驟：軟體缺陷利用—邏輯失控—劫奪控制—引爆（瞬間殺掉大量資料）[1]。

資訊已成為國家安全總體戰略目標重要工具，也成為當代政府及企業經濟活動的資產，亦是個人生活上處理事務最重要的工具，資訊犯罪在瞬間能穿越數國國境，也能於瞬間將犯罪證據消失於無形，各國間若未能採取更明確的合作方式，恐難對抗層出不窮的犯罪技術。因此要積極地防止他人侵入的危害，強化資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，保障民眾權益，此即為資訊安全；而採取的各項措施有網路安全防護技術、身份認證技術、防火牆技術、資料加密技術、資料備份技術、入侵檢測技術、防病毒技術等。本文從如何因應資訊安全等迫切需要的議題，藉由各國相關政策與他人過去的經驗，期盼「他山之石可以攻錯」，用以減少自己資訊安全的風險。

貳、資訊安全問題與對策

由於近幾年來電腦與網路的快速發展，電腦及網路有關的犯罪案件也日趨增多，其進行方式從最常見的系統入侵與電腦病毒破壞，到甚至於恐怖份子透過電腦網路來進行入侵與破壞行動(參考表一)，蛻變衍生出許許多多的資訊安全議題。而傳統犯罪如詐欺、洗錢等亦因電腦與網路的興起，更有了新的樣貌[2]。

表一　電腦犯罪威脅表

分類	入侵者	目的
國家安全	敵軍	窄化敵方決策空間，擾亂、侵害行為，取得戰略上優勢
	情報員	蒐集軍事、政經情報
共同危害	恐怖份子	示威、宣傳、擾亂、顛覆政權
	產業間諜	脅迫行為、取得競爭優勢
	組織犯罪	復仇、經濟利益、改變產結構
局部損害	職業駭客	金錢、刺激、挑戰、名譽
	業餘駭客	追求刺激、挑戰

資料來源：美國重要基礎保障局部(CIAO)1999 年

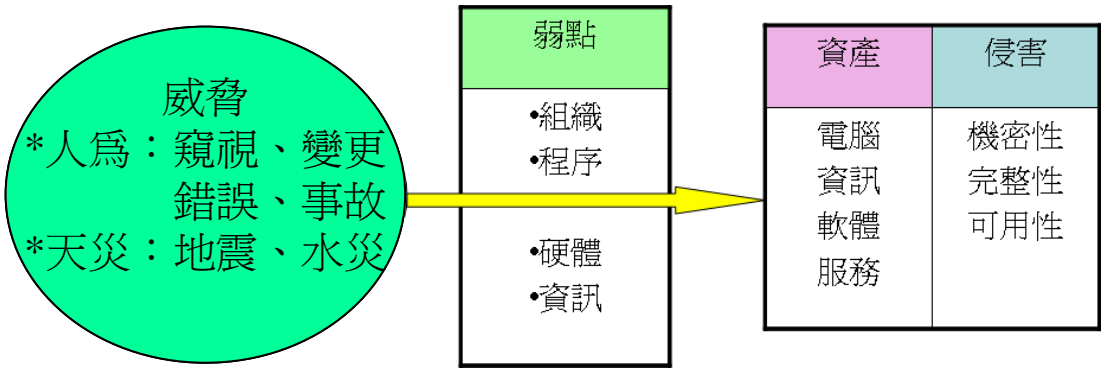
1陳年興，「網路安全與危機處理」，資訊安全通訊第六卷第二期，2000 年 3 月，頁 105~111。

[2] 高大宇著，「資訊安全」，臺北博碩文化，2003 年 6 月。

當人與電子資料互動的時侯，如何在擷取、分配、儲存及管理電子文件流程的過程中，提供適當的安全措施來確保電子社會中電子文件面對竄改、竊取、延滯、冒名傳送、否認已傳送等問題，而建置一個可以信賴的電子文明民主作業環境，奠定資訊社會的基石，已是眾所矚目的焦點，首先從資訊安全問題、資訊安全防制對策及報案與危機處理機制提出簡略的看法：

一、資訊安全問題

資訊安全基礎建設發展涵蓋範圍廣泛，舉凡政治、心理、經濟、科技和軍事等各領域，均為敵方運用資訊技術手段爭奪資訊優勢的目標，為確實掌握我國政府機關（機構）及重要民間業者之資訊及網路系統，免遭受破壞或不當使用等緊急事故發生時，能迅速作必要之應變處置並在最短時間內回復正常運作，以降低該事故可能帶來之損害[3]；基本上資訊犯罪多利用資訊安全結構上的疏漏(參考圖一)，來抓取電腦密碼比對器（Password Cracker），侵入系統根本談不上破解密碼，只是執行系統缺陷運用程式（就像盜賊所用的瓦斯焊槍、電鋸），以尋找系統保護結構的漏洞，因此難以破解的門鎖固然是安全的第一步，房屋的健全結構更重要。攻擊的重點在於「尋隙」，這是從蒐集未知的人事地物的安全切身資料，如所使用系統的版本、網路服務種類、網路結構、內部人員的使用習性、防衛設施、與安全策略等，而往往攻擊的一方比被攻擊單位的內部人員更能掌握整體系統的缺陷。因為雙方的角色與責任不同。攻擊者只要挖一塊小牆腳，就能癱瘓整個系統，後者人員卻要應付繁重的日常維護需求與所有角落的補強工作。如圖二所示為攻擊趨勢、程序與安全防衛的簡要說明。



圖一　威脅、弱點、侵害圖

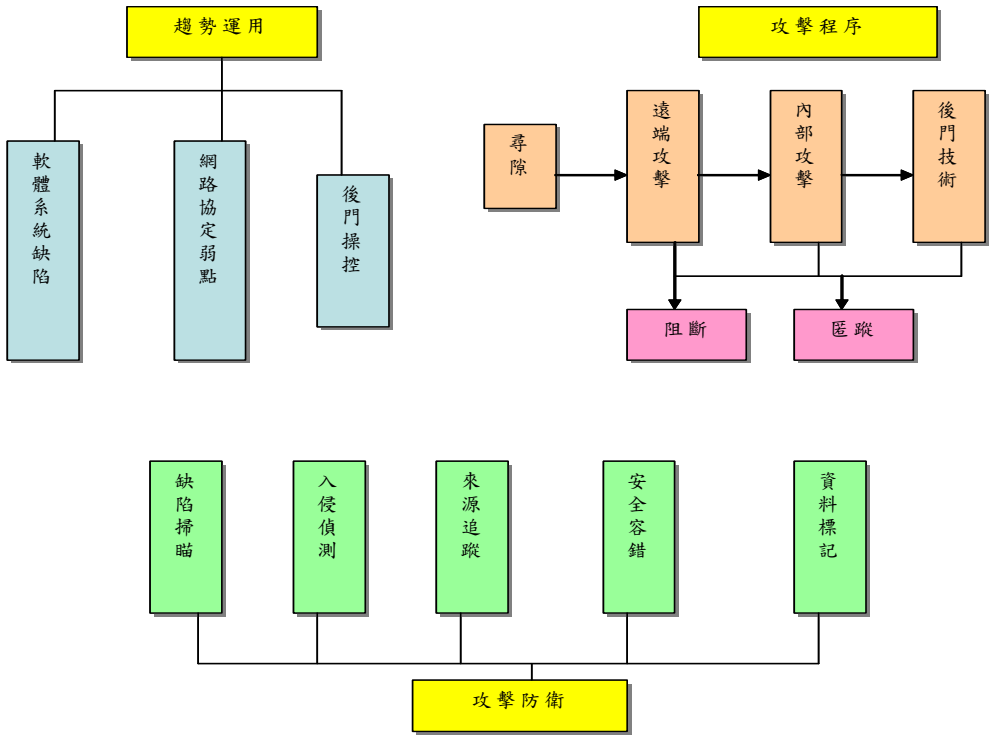
資料來源：GMITS-18.2，1999 年

二、資訊安全防制對策

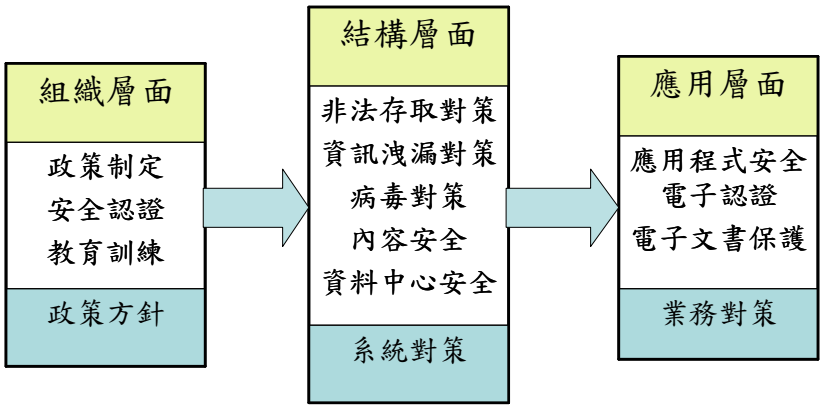
從統計資料我們得知，大部分入侵事件的發生，是由於系統管理者與使用者的錯誤設定所造成，亦即主要的問題是由「人」所產生的，因此著重人為因素的

[3]行政院 NICI 小組，「建立我國通資訊基礎建設安全機制計畫」，91 年 6 月，http://www.moj.gov.tw/chinese/c_rule_sys_point0-3.aspx

補強，並輔以資訊安全技術，是維護網路安全十分重要的觀念。因此，同時在制定政策時，亦要以組織、結構、應用等層面加以思考，建立整體性的資訊安全防制對策(參考圖三)，用以推動技術人員認證、網路安全軟體認證、網路保全服務、資訊存活管理，便能將技術與管理整合，進而阻止入侵的行為[4]。



圖二　資訊犯罪攻擊趨勢、程序與安全防衛圖



圖三　資訊安全階層思考圖

1、　技術人員認證：隨著全球網路市場的蓬勃發展，需要大量有關的專業人才來管理與維護網路系統安全，然而資訊安全的技術如何才值得信賴？而系統

[4]沈碧容譯, Richard H. Baker, “Network Security – How to Plan for it and Achive for it.” (中譯:網路安全手冊-個人應用篇), 1996 年。

管理者又該如何評定自我的身價？因此經由「技術人員認證」，諸如：Miscrosoft 的 MCSE(Microsoft Certified Systems Engineer)，NOVELL 的 CNE (Certified NetWare Engineer)及 Cisco 的 CCIE(Cisco Certified Inter-network Expert)等可以提供我們一個評判的標準來解決這些問題。

2、 網路安全軟體認證：目前國內似乎並無相關的主管機關或單位，執行網路安全相關產品的認證服務。然而隨著網際網路的迅速發展以及電子商務的推行，我們有必要對於自己的網路安全產品建立認證制度，諸如：運用密碼模組與密碼技術，藉由訊息加密(encryption)、數位簽章(digital signature)、訊息摘要(hash function)、鑑別(authentication)等功能，有助於在訊息傳遞、儲存、與處理時確保達到資訊處理之隱密性(secrecy)、完整性(integrity)、與不可否認性(non-repudiation)[5]。如美國 ICSA 成立的宗旨一樣，網路安全產品的認證制度是希望能提供給消費者採買網路安全相關產品時的參考，減低網路安全上的風險，避免購買到安全沒保障的產品[6]。

3、 網路保全服務：現今的生活中，假如有歹徒侵入住家，這時若有保全裝置（如：防火牆、入侵偵測、缺陷掃瞄），保全公司將採取迅速的反應，以避免顧客遭受危險或損失。而網路保全服務的性質，類似於現今的保全公司，亦即在入侵攻擊事件發生時，透過此機制能迅速處理並降低損害。

4、 資訊存活管理：是假設系統已被攻入的情況下，如何減低損失、迅速復原，並能追查（甚至反擊），這在軍事戰略上是必備的，在戰場上打敗仗之後必須能安全撤退，在安全管理上，則希望能做到安全容錯（安全危害容許），根據攻擊強度調整安全策略，採行適當的自保措施[7]。

三、報案與危機處理機制

網際網路將電腦串連起來成為龐大的系統，因而若有攻擊或入侵的行為產生，這些危害可能迅速就會蔓延開來，所以為了因應遭受網路攻擊可能造成的危害，應建立國家層級之通資訊安全指揮機制，並結合內政、外交、國防、財政、教育、法務、經濟、交通等部會及國家安全局，針對電力、電信、金融、交通等國家基礎建設之安全防護，共同研析相關因應作為，為此特協調各部會積極規劃建立國家通資訊系統通報及應變機制，以為我國通資訊安全提供最佳之保障。我們從緊急連線管制處理、建立網路報案系統以及建立資訊安全之處理機制，分述如后：

1、緊急連線管制處理：當我國遭受到國外資訊戰的攻擊，若能迅速由對外網路連線出口做緊急處理，切斷國外連線，或拒絕國外攻擊位置的連線要

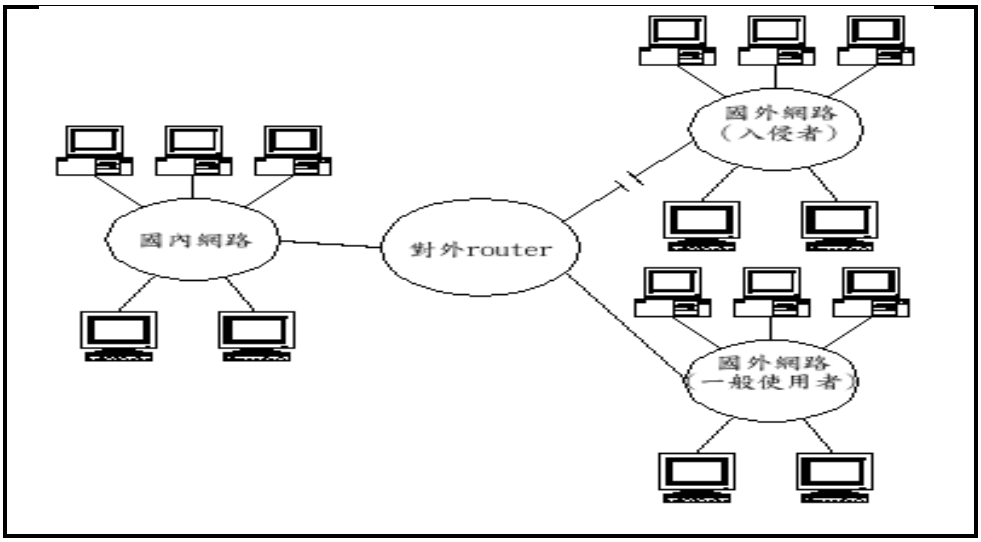
[5]林祝興，「密碼模組管理、驗證與應用-管理機制」，資訊安全通訊第六卷第二期，89 年 3 月，頁 86~90。

[6] ICSA 提供之防火牆軟體認證方式，除了技術的測試外，是針對操作手冊的認證。ICSA Product Certification, http://www.icsa.net/services/product_cert/

[7]Special Issues: Defensive Information Warfare, Communications of the ACM, Vol. 42, No. 7, 1999, pp.30-75.

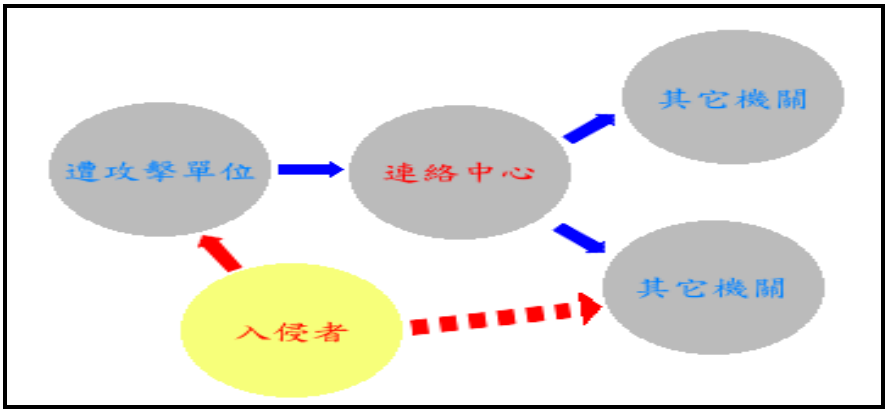
求，將可爭取應變時間，減低傷害與損失，例如：2002 年 8 月的「政府網站資料篡改事件」為例，此次攻擊者的來源皆為中國大陸的 IP 位址，故若迅速從管制國外封包進入的 Router 上阻擋中國大陸部份 IP 位址，將可防止對方騷擾，如**錯誤! 找不到參照來源。**所示。

2、建立網路報案系統：當網路系統遭到入侵，系統管理者可能不知道入侵者來自何方，亦沒有人知道入侵者的下一個目標會是哪裡，然而一旦攻擊行動蔓延開來，可能造成驚人的損失，因此政府應建立網路報案系統，成立一個緊急連絡網，以便迅速對入侵事件做出因應行動，其主要的功能分為入侵通報、追蹤入侵者以及入侵記錄等三點：



圖四　緊急連線管制處理圖

(1) 入侵通報：一個入侵者是無法同時攻擊所有的主機，所以當某一網站發現攻擊動作或是已被入侵，若能透過連絡網，告知其他管理者相關的訊息以做為防備，將有助於防止災害的擴大其基本的架構，應有一連絡中心以負責接受回報與執行並分派連絡工作，如圖五所示。



圖五　入侵通報圖

(2) 追蹤入侵者：當發現入侵者位置來自國內，可透過「網路報案系統」的機制，請該來源位置的管理者協助追蹤入侵者身分，以防制電腦犯罪事

件。

(3) 入侵記錄與分析：我們可以將每一個入侵事件的資料記錄起來加以檢討，有助於了解入侵者的手法，並提供電腦犯罪的分析，以協助電腦犯罪案件的偵查。

3、網路安全防衛體系：此一防衛體系於平時提供技術諮詢與入侵事件求助和系統安全資料的發送，當機關遭攻擊時，可以迅速蒐集資料，並提出緊急處置方案與協助處理系統安全問題，諸如：台灣電腦網路危機處理中心(TWCERT)於本次「政府網站資料篡改事件」中，能提出迅速應變處理之方法，發揮防止危害繼續擴大的功能。

4、政府應從政策面、市場面以及教育訓練上著手，除了宣導網路安全的重要性、訓練相關人員的技能之外，也要強化網路安全相關體系的建立、加強網路安全服務組織(例如：TWCERT)的功能與運作、宣導正確面對入侵事件的態度，如此才能落實資訊安全的危機處理。

參、國內外資訊安全政策與措施

二十一世紀的新科技開啟了犯罪的新紀元，除了傳統犯罪資訊化外，利用新科技犯罪更是層出不窮，不斷地更新，由於在電腦與網路系統中，傳送的資訊是光電訊號或電磁波、媒體是電纜線、光纖或大氣層並儲存在磁性物質的磁化狀態或半導體物質的電子狀態中；因此，不法人員很容易在資訊使用的環境裡加以竄改、變造、重演或冒名傳送而不留下痕跡[8]。而能在瞬間穿越數國國境，也能於瞬間將犯罪證據消失於無形，因此各國皆致力於建立資訊安全管理標準，採取更明確對抗資訊犯罪的合作方式，現以國際上資訊安全 ISO 認證、非法存取行為禁止法及隱私權標章等作法，分述如后：

一、資訊安全管理準則 GMITS(Guidelines for the Management of Security)：是日本從 1996 年起逐步發行的 ISO/IEC13335TR(技術報告)，為概念性的提出安全管理架構與過程的方針，性質為技術性報告，如字面所示為「方針」，並非有強制力之「國際規格」，分別說明其內容如下[9]：

1、 資訊安全的概念與模型：針對資訊安全負責部署之上級管理者，說明資訊安全概念與模型有關的資訊安全管理。

2、 資訊安全的管理與計畫：針對負責採購、設計、執行、運用資訊系統的資訊處理管理負責人，說明有關資訊安全的管理與企畫的各種活動與組織內的職務與責任。

3、 資訊安全的管理技術：針對資訊安全管理與實施部門的負責人，說明資訊安全的管理技術，為設計、維持資訊安全標準的安全要求事項，風險評價之技術說明。

4、 安全守衛的選擇：針對依據安全對策(安全守衛)實施時的概要、選擇

[8]樊國楨，「型式認證在台灣社會可信賴的資訊使用環境中所面臨的問題與挑戰」，透析資料庫

[9]岸田明著/林雯譯，「學資訊安全的第一本書」，臺北博碩文化，2003 年 10 月，頁 216~227。

程序、基本水準手法(Base-line-Approach)適用與否來選擇對策。閱讀對象設定為安全管理者。

5、 對外部連結的安全守衛：針對安全管理者，說明保護外部連結、服務、IT 系統免於威脅、風險、減少弱點之安全守衛的選擇。

二、資訊安全管理程序體系 ISO/IEC17799：

英國在 1995 年編訂管理規章 **BS7799**「資訊安全管理實施準則(Code of practice for Information security management)」，作為資訊安全之最適當具體範例；於 1999 年改訂 BS7799，分為實務慣例(第一部)與管理說明書(第二部)二部所構成，至 200O 年 8 月以 ISO 的身份成立，通過成為國際標準。

三、國際標準 ISO/IEC15408：

美國、加拿大、荷蘭、德國、法國於 1993 年組織了共同標準(Common Criteria，簡稱 CC)制定計畫，組成的編輯委員會於 1994 年開始訂定資訊安全評價標準，幾經修改與改組為共同標準實行委員會後，至 200O 年 8 月方成為國際標準，其主要目的是針對資訊系統及其構成機器、軟體(包含 OS)，以全部安全功能、決定安全標準的評價標準為基礎加以評估，並對其結果執行認證動作。具體來說是對產品、系統所預設威脅之妥當性、對抗該威脅的對策是否足以面對威脅、為實現對策的安全方法之妥當性、該方法的執行能保證到何種程度(安全品質)，進行客觀評價的結構；分為導論與一般模型(ISO/IEC15408-1)、安全功能要件(ISO/IEC15408-2)及安全保障要件(ISO/IEC15408-3)。

四、韓國：

主導資訊安全政策的最高單位是屬於「資訊暨通訊部（Ministry of Information and Communication, MIC）」的「資訊安全局（Korea Information Security Agency, KISA）」，成立於 1996 年。在 KISA 下有三個目標分別針對 Research & Education Community、Secure Administration、Security Vendors 三種單位。在 Secure Administration 下於 1996 年成立 Consortium of CERTs 簡稱 CONCERT，目前有 150 多個會員，負責安全事件處理協調 (Incident Response)、針對系統管理者的安全教育訓練。另外也成立 CERTCC-KR 負責 CONCERT 的運作，其擔負的任務與目前的 TWCERT 類似。CERTCC-KR 24 小時運作，更有十多名專職人員，是常設的政府單位。

五、「非法存取行為禁止法」及「隱私權標章」：

為日本自 2000 年 2 月起施行，為禁止非法存取的法律，其定義是「在擁有存取控制功能的特定電腦上，經由通訊線路，輸入他人的識別符號，使之啟動，利用該電腦之存取控制功能，獲得被限制使用之特定資源之行為」，內容可分為禁止、處罰與防禦兩大類[10]。隱私權標章的目的為「對企業家自主的限制與努力給予獎勵，對資訊主體的個人提供可容易判斷民間企業個人資訊處理適切與否的標誌」，其相關法律可溯自 1980 年開始通過「保護隱私與個人資料流通方針之理

[10]日本「非法存取行為禁止法」第條規定：禁止方面包括「任何人皆不可從事非法存取」與「助長非法存取之行為」，如禁止販售他人的帳號、密碼等。防禦方面，訂定「存取管理者、網路管理者防護措施之必要」，為公安委員會應加以支援、援助的內容。

事會勸告」有關保護個人隱私的法令，1988 年制定「行政機關持有電腦處理之個人資訊保護法」則是以行政組織為對象；1989 年提出「民間部門個人資訊保護方針」，當作指導民間部門的基礎，並配合各種外國法令修訂，於 1997 年 3 月公布「民間部門電腦處理之個人資訊保護方針」，為使之普及而創設隱私權標章制度。

六、我國資訊安全現況及未來方向：

1999 年春季起意識到通資訊基礎建設安全對國家的重要性，隨即著手規劃「我國通資訊基礎建設安全機制」；但由於我國現有之通資訊安全措施均侷限於局部性，並無整體防護、識別及回復能力等，為爭取時效及達成總統的指示，行政院國家資訊通信基本建設專案推動（簡稱 NII(National Information Infrastructure)）小組研討相關規劃作業；經審慎研擬，於 2001 年 1 月 31 日召開「國家資通安全會報」第一次會議，期以 4 年的時間，完成「建立我國資通基礎建設安全機制計畫」[11]，分成四種等級規劃資訊安全不同模組(參考表二、表三)，資訊安全的範圍包括(1)管理制度、(2)作業流程、(3)人員、(4)軟體、(5)應用系統、(6)電腦作業系統、(7)硬體、(8)通訊設備、(9)資料、文件、媒體的儲存及(10)實體設施等[12]，交由各所屬機關並要求切實配合辦理，正式開啟了我國資訊安全發展的新頁。會報下設立綜合業務工作組、危機通報工作組、技術服務中心、網路犯罪工作組、資料蒐集工作組、稽核服務工作組與標準規範工作組等七個組，負責推動國家資通安全基礎建設之各項工作，其中標準規範工作組是由經濟部為主要負責單位，而研考會、國防部、交通部、財政部則配合協辦，主要職掌陳述如下：

1.訂定資通安全技術標準。

2.訂定各機關辦理資通安全有關作業規範。

3.規劃建置資通安全檢測技術。

4.規劃建置資通安全驗證方法。

5.規劃建置資通安全認證程序。

另外，我國制定「電腦處理個人資料保護法」以來，即將屆滿十年。隨著電腦網路科技進步快速，各種資訊化服務以及其他電子通訊工具的普及，實務運用的層面也越來廣泛，社會大眾確實享受到許多資訊化社會所帶來的便利。然而，在享受便利的同時，資訊的大量流通，可能因管理不當或犯罪意圖，使個人資訊有被洩漏或遭受濫用之虞，進而侵害個人的權益。為配合科學技術發展與社會環境的變化，近來法務部積極推動個人資訊的保護，將原「電腦處理個人資料保護法」修正為「個人資料保護法（草案）」，保護範圍將不限於「電腦處理之個人資料」，進一步擴大保護適用範圍，使本法內容的影響更為深遠[13]。

表二　密碼模組安全等級適用範圍示意

[11]行政院資訊與通信基本建設專案推動(National Information Infrastructure，簡稱NII)小組(2001)國家資通安全會報第一次會議(會議資料)，行政院資訊與通信基本建設專案推動小組。

[12] 行政院及所屬各機關資訊安全管理規範，88 年 11 月 16 日公發布。

[13]鄧曉芳，「最新科技法律透析內容簡介 93.04」，http://stlc.iii.org.tw/stlc_c.htm。

安全等級	適用範圍
1	提供最少防護的資訊安全使用環境 (例：個人、便利商店等)
2	提供一般防護的資訊安全使用環境 (例：郵購、商業文件傳遞等)
3	提供正規防護的資訊安全使用環境 (例：電子商務、金融服務等)
4	提供特別防護的資訊安全使用環境 (例：中央銀行、中央政府等)

表三　安全等級需求驗證標準

等級領域	安全等級 1	安全等級 2	安全等級 3	安全等級 4
密碼模組	密碼模組與邊界規格。密碼模組規格描述包括所有硬體、軟體、韌體(firmware)等組件。必須陳述模組安全策略(module security policy)。			
模組介面	必須及備選介面。必須要有所有介面與所有內部資料路徑(data path)規格。	重要安全參數之資料阜(data ports)應該在實體上與其他資料阜分開。		
角色與服務	必須及備選角色與服務應在邏輯上分開。	角色基(role_based) 操作者鑑別(authentication)。	身分基(identity_based)操作者鑑別。	
有限狀態機	有限狀態機模型規格。必須狀態與備選狀態。狀態轉移圖(state transition diagram) 與狀態轉移規格。			
實體安全	製造等級(production grade)設備。	上鎖或篡改證據記錄	篡改偵測與開蓋及開門反應(response for covers and doors)。	篡改偵測與開封反應(response envelope)。
實體安全之環境失敗保	無需求。	溫度與電壓。		

護/測試				
軟體安全	軟體設計規格。軟體以有限狀態機模型模擬過。	高階語言實作。	正規模型 (Formal model)。	
作業系統安全	可執行碼。鑑別機制。單機、單使用者。	控制下之存取保護 (C2 等級)。	標示保護(B1 等)。可信賴的通訊路徑。	結構化保護 (B2 等級)。
金鑰管理	FIPS 通過之產生/分配技術。	以加密形式進/出金鑰或以分開知識程序 (split knowledge) 直接進/出。		
密碼演算法	FIPS 通過之保護非機密資訊密碼演算法。			
EMI/EMC	FCC Part 15,Subpart J, Class A (商業用)。可用之 FCC 需求 (voice 用)。	FCC Part 15,Subpart J,Class B (家庭用)。		
自我測試	開機測試 (Power-up tests) 與條件測試 (conditional tests)。			

資料來源：行政院資訊與通信基本建設專案推動小組，2001 年

肆、資訊安全未來之展望

未來資訊化社會面臨的最大挑戰是來自於人為蓄意的破壞攻擊，其影響有如慢性疾病或是隨時可觸發系統失序的危機，一般大眾若能瞭解自己使用系統的缺陷及可能遭致的危險，將可以提昇自身保護能力；維繫治安的警察若清楚破壞手法，將能掌握危害者舉動，維繫電子商務交易與保障網路社會秩序。同樣的，在國家安全保障上，資訊化部隊的最大威脅將來自於資訊戰爭中的軟體武器，瞭解攻擊將幫助國防單位建立軍事網路危機意識[14]，現由建立國家資訊安全的戰略思維、建立資訊安全管理標準、架構資訊安全規範、創設隱私權標章制度暨發展電腦鑑識科技等方面，提供參考如後：

[14]黃世昆，「電腦網路危機處理機制—從防震及 Y2K 應變 談網路安全存活管理政策」資訊安全通訊第六卷第二期，2000 年 3 月，頁 86~101。

國家資訊安全的戰略思維

維護資訊安全的政策與措施也必須以國家資訊安全戰略思維來考量，諸如：資訊化發展與安全的同步協調推進、結合平時網路支援戰時的應變、全國預警與綜合決策的資訊安全的應變指揮、強化法制制約下的資訊安全、政府資訊安全部門的協調與整合、建制資訊安全的國際標準、資訊安全服務的社會化、資訊安全與國防產業鏈的建立、資訊安全評估體系的建設、資訊戰集中體系與分佈主體的結合策略等，美俄在這方面的策略不僅強調以防護手段維護資訊安全，而且重視以進攻手段達到目的，所以重視法規、資金、技術。法規是基礎，資金是保障，技術是關鍵[15]，用以達成國家資訊安全戰略目標。

一、建立資訊安全管理標準：採用國際標準作為方針，將之本土化，借鑒國際先進經驗，深入探索在資訊安全涉及到安全策略、安全法規、安全管理、安全人材、安全技術、安全產業、安全基礎設施等諸多領域中，遇到的那些問題、難處、關鍵和敏感點，尋求科學處理這些問題的正確思路，以便引導資訊安全進入一個更理性、更科學、更實際、更符合我國特色的資訊安全管理標準。

二、架構資訊安全規範：資訊安全的核心在於「人」的作用，目標管理標準就是在群體中進行人的規範，資訊安全管理標準的有效實施，可以避免內部的許多漏洞，也可以避免許多未授權檢索和濫用，有力地保證資訊的保密性、完整性和可用性。在資訊安全管理標準的實施中，人的安全意識是會起重要作用的，有了良好的安全意識，就可以自覺地遵守標準。對於所有的國際資訊安全標準和發達國家的標準，我們應該以求實求真的態度去評估，在形成全面認知的基礎上，建立資訊安全的組織文化。

三、編制安全專業部門：我們已經瞭解資訊安全的必要性，如何落實此具體活動，需編制專門部門實行，因其業務範圍廣泛，功能需加以區分為管理作業、技術對應、偶發事件對應、檢查功能等，必須集合各式各樣的人才，通力合作才能達成任務(參考表四)。而在此種意義下，安全的權限是集中的；為避免這種情況，檢查功能需分開組成以分散權力，或必須另行以運作牽制功能。

表四　編制安全專業部門功能表

管理作業	資訊安全委員會的事務 資訊安全政策相關資訊發報與維持 網路管理、新系統/連結的認定 帳號/密碼等認證系統的管理 教育、啟發活動 外部連結點的管理
技術對應、偶發事件對	外部連結點的監視及狀況的內部宣導

[15]嚴亞平，「美俄維護資訊安全的觀點和舉措」，中國國際關係學院學報 2001 年第 1 期。

應	公司內網路的監視及狀況的內部宣導 安全偶發事件的對應及狀況的內部宣導 各種安全資訊的看守及狀況的內部宣導 安全技術等技術指導與資訊發報 新系統、首頁、公司內伺服器等的安全檢查(定期、隨時)
檢查功能	評價新系統的安全政策 檢查(資訊、資訊系統)安全政策實施狀況

四、創設隱私權標章制度：資訊社會對於個人、企業、政府在網際網路中，進行通訊、連結與交易，應建立在使用正當的方法與程序，架構互信的協定，才能有效保障我們的資訊安全。從另一方面來說，網路上的良性互動行為是基於雙方互信的原則，使用者「相信」通訊網路不曾洩露通信者的秘密，而網站管理者也「信任」使用者會遵循既定的規範來使用網站所提供的服務，達成資訊化的進步與發展。

五、發展電腦密碼鑑識科技：資訊安全機制的核心技術「密碼學」，包括「明文」、「密文」、「金鑰」、「加密函數」與 「解密函數」等模組的組合，在具「秘密性」、「鑑定性」、「完整性」與「不可否認性」等要求下，能使得資料的安全機制得以運用。另藉由數位證據的呈現方式，可作為法院訴訟程序上的證據參考，在國外美、英、法、日等跨國組織在 Ontrack、Vogon、New Technologies -TSW(The Seanless Website)提供保護電腦資料資產方法及諮詢服務，對於數位證據處理程序、採集要領與完備手續以增加採證過程中，發現 (復原)被刪除或隱藏檔案及復原密碼保護檔案的機會，並減少資料遺失、毀壞或產生未具證據能力資料的遺憾。身為警察工作者不僅可以作為學習的對象，亦可刺激我們研發更新穎、更便捷的軟體程式來採集數位證據，使電腦犯罪相關案件的法院訴訟程序更為完備與完善。

伍、結論

隨著微電子、電腦網路及其相關技術的發展，人類開始進入資訊社會，資訊逐步成為維持經濟活動、生產活動和社會活動的重要資源，成為政治、經濟、軍事，乃至社會一切領域的基礎。對於國家而言，資訊基礎設施的普及和資訊的廣泛使用與傳播，加快了經濟發展和社會進步的步伐，但同時給維護國家安全也帶來了一系列新問題。建置一個可以信賴的資訊使用環境，同時配合法律規定之修正將相關制度均融入現有的管理制度中，做為政府、民間共同建置可信賴資訊使用環境的準繩，以建立資訊安全的維護機制；同時，更期盼台灣地區能加重資訊安全技術領域的研究與發展，開展類似歐盟、新加坡政府等的密碼模組研發建置計畫，畢竟資訊安全技術的本土化及獨立自主是必須面對的問題[16]。

[16]管高岳（1995）現代經濟犯罪之界限及防制對策，國立台灣大學法學研究所博士論文。