電子化政府資通安全發展策略與展望

Information & Communication Security in E-Government

葉俊榮*（行政院研究發展考核委員會主任委員）
Jiunn-Rong Yeh,（Minister of Research, Development and Evaluation Commission, the Executive Yuan）

摘　要　Abstract

資訊科技的發展使得人類社會更加進步，不論是公私部門都廣泛受益。但是，伴隨而來的資訊與通訊安全問題，包括病毒攻擊、隱私保護及恐怖攻擊等議題，也逐漸成為國家安全、經濟發展及社會安定等各層面的隱憂。本文面對「電子化政府」大力推動之際，探討如何因應網路應用的潛在風險。

本文透過臺灣資安通報統計及TNS所做電子化政府民調等實證資料，探討臺灣實際面對資通安全問題的程度以及影響面；同時，參照美國及OECD以及APEC兩個國際組織對於資通安全相關規範，本文進而做出規範與實態的對應分析。

本文從現況的檢索中發現，隨著網路科技的擴展，資通安全所承受的風險也逐漸提升。政府雖然一直將資通安全列為重點工作，但是對於資訊的安全及風險管理概念仍有待加強。本文提出三項原則，首先強調資訊的利用與保護同等重要，以強化責任的認知；其次是全方位的觀念推動；第三則是重視顧客導向及宣傳。依循這些原則，N-SOC未來推動資通安全政策上，可以參照採行四項策略，分別是強化對於機敏性資料的保護、提高民眾對於資通安全警覺性的認知、檢討現行資通安全法規，並提升網路安全的偵防能力，最後加強資通安全技術研發與應用。本文認為唯有強化資通安全的重要性，建立讓民眾放心的資訊網路系統，才能有效的推動電子化政府。

The fast developing of the Information Technology (IT) has improved the efficiency of our society, regardless of the public or private sectors are both benefited much from it. Unfortunately, the problems followed by this technology, the information and communication security have become increasingly serious. This includes virus attacks, protection of privacy, and terrorist attacks. This issue might induce some potential problems which might lead to a major concern for our national security, economic development and social stability. In this article, it will discuss how to work against the potential risks when utilizing of the "Internet Technology", while developing and promoting a healthy "electronic government".

By utilizing the statistic data from the National Information and Communication Security Taskforce (NICST) and the Taylor Nelson Sofres (TNS) surveys about the topic of e-government development, this article is focusing on analysis the level of degree and the aspect of influences of the information and communication security in Taiwan. Meanwhile, by referencing the similar experiences of United States and other international organizations, such as OECD and APEC, this article will take a further comparative study from the normative researches and the empirical researches.

*
◇聯絡地址：台北市中正區濟南路1段2之2號7樓
◇聯絡電話：（02）23419066
◇e-mail：jryeh@rdec.gov.tw

This article finds that, under the current condition, the more the expansion of Internet Technology, the more the risk it increases. Even though the government has always takes the issue of information and communication security, as one of the major concerns, but the concept of information security and risk management must be further developed. This article suggests three main principles regarding to the information and communication security. First is the emphasis of the importance of the protection of data is equal to the use of information. All participants should understand their responsibility for the security of those information systems. Secondly, all dimensions of this concept must be widely promoted. Lastly, the most important of all, is that it must take a customer-orientated attitude, to strengthen and ensure the confidence about the security of users. Based on these principles, N-SOC should take four strategies in the future promotion of information and communication security which includes the following: to enhance the protection of the agile data, and to further lift up the recognition of the importance of the information and communication security to the general pubic; to review and discuss the current laws and regulations about information and communication security, and to boost the detection ability of the internet safety; to enhance the technology development and application of the information and communication security. This article concludes that only the further enhancement of information and communication security will establish an internet system that can let the public count on, and therefore it will be easy to promote a practical and user-friendly electronic government.

關鍵詞keywords：電子化政府、資通安全、網路安全、資訊安全、國家資通安全防護管理中心
Electronic Government, Information and Communication Security, Network Security, Information Security, National Security Operation Center

壹、前言

在當代科技發展中，網際網路與現代數位科技匯流的趨勢影響人類生活。Turner（2001）認為資訊革新將穿透國界，牽動國家政治、經濟與文化產生的變遷。面對這波資訊趨勢，先進國家紛紛採用各種政策因應，以美國為例，1993年美國聯邦政府便在「運用資訊科技再造政府」（Reengineering Government Through Information Technology）時，提出電子化政府的概念，透過資訊科技引導政府的革新（詹中原，1999）。而臺灣則是由行政院成立國家資訊通信基本建設專案推動小組，推動國家資訊通信基礎建設，展現主動進行資訊管理的企圖心，透過公開資訊來提升國家競爭力。此外，透過「電子化政府」及「政府便民服務電子窗口」等服務，不僅普及網際網路的使用率，也藉由資訊公開的程序促成政府效能提升。

儘管這波資訊革新的趨勢，擴展人類整體的視野，卻也潛藏著資訊與通訊安全（information and communication security，以下簡稱資通安全）的風險。所謂資通安全意謂著面對環境災害、人為疏忽及蓄意攻擊等的侵害，造成資訊系統的隱密性（confidentiality）、完整性（integrity）及可用性（availability）受到破壞而無法正常運作（吳瑞明，1994）。網路網路的普及使資通安全更為複雜化，諸如敵對國家間可能相互發動的資訊戰、恐佈份子透過網路發動攻擊、電腦駭客破壞網路系統與重要資料、商業間諜竊取商業機密、犯毒或洗錢集團利用密碼技術造成犯罪防制及調查上的困難等挑戰，都是資通安全下的課題。

由於資訊系統與網路科技已經成為政府與外界溝通的重要平台。若涉及網路犯罪、參與者隱私保護、智慧財產權保護等問題沒有妥善處理，將形成國家安全、經濟穩定及社會安定的隱憂，對於國民資訊隱私的保障也可能形成極大的損害（莊伯仲，2000）。面對政府推動數位台灣政策之際，本文從制度層面，希望強化政府對於資通安全管理的機制，建構具有高度安全性及值得信賴的網路環境，才能促進資訊科技之普及應用。

貳、電子化政府資通安全現況

由於網路科技的進步，使得網路逐漸從專業化擴展到生活化；而民眾接觸網路的機會大幅提升，也使得網路犯罪及資通安全問題日益嚴重（林宜隆、華讚松、楊麒麟，2001）。現今利用網路來犯罪的模式主要有兩種，首先是損害網路系統本身或周邊設備，或對輔助記憶體的資料或程式加以損害。其次是透過非法使用網路企圖獲利或妨害商業利益的目的，竄改或圖損等不法行為而使用電腦網路，或對網路輸入不實資料或程式，或不輸入應該輸入之資料（邱承迪，1999；蔡中翰，2003）。

而面對網路犯罪的擴大，網路參與者（participants）所承受的風險有五種的特徵，包括：一、犯罪時間縮短、二、犯罪區域擴增、三、犯罪方法新穎、四、資產型態改變以及五、犯案環境單純（林祝興、張真誠，2003）。若以網路犯罪的形式與程度來看，依據國家資通安全應變中心（以下簡稱資通應變中心）所公布的資料中（參見表1、2），從2001年起至2005年1月初，所通報516件資安事件中，以「非法入侵」居多，總共316件；而破壞程度以「網頁遭篡改」較嚴重，共有180件，造成影響則是以「業務短暫停頓」的情形較多，共有447件(註1)。

資通安全威脅主要來自於四個方面，分別是自然災害、機械故障、人為過失及故意破壞（王瑞之，1999：82）。就發生的時間點而言，當國內發生重大天然災變或者是兩岸政治局勢較為緊張時，往往連帶衝擊資通的

表1　政府資安事件通報統計（以事件分類及破壞程度區分）

事件分類破壞程度	非法入侵	感染病毒	阻斷服務	其他	合計
系統當機	4	19	5	4	32
資料庫毀損	1	3	0	1	5
網頁遭篡改	178	1	0	1	180
其他	133	88	17	61	299
合計	316	111	22	67	516

資料來源：（資通應變中心，203.69.37.223/infosec/notice/l_event1.asp）

表2　政府資安事件通報統計（以事件分類及影響等級區分）

事件分類影響等級	非法入侵	感染病毒	阻斷服務	其他	合計
A級)影響公共安全	0	0	1	1	2
B級)系統停頓	3	0	1	8	12
C級)業務中斷	15	23	7	10	55
D級)業務短暫停頓	298	88	13	48	447
合計	316	111	22	67	516

資料來源：資通應變中心，203.69.37.223/infosec/notice/l_event2.asp

安全性，諸如1999年8月時，兩岸因為「兩國論」的議題，引發兩岸關係緊張之際，便疑似大陸駭客計畫性地入侵政府網站，使得兩岸陷入爆發資訊戰的風險中。同年，發生921大地震時，受災地區政府資訊系統運作便受到嚴重衝擊，幾乎一度停擺。

2001年初中美海底電纜頻繁的斷纜，使得臺灣與中國、香港及新馬等地至北美的資訊通訊受到嚴重影響；該年9月納莉颱風來襲時，北市又因為捷運地下行控中心淹水，導致交通嚴重阻塞；到了10月底，則是台電工程人員施工時，不慎挖斷中華電信兩條光纖電纜，導致租用中華電信的桃園飛航總台區管中心無線電通訊中斷、飛航資料無法傳遞，造成全台航機延誤。而從2001年11月到2002年7月中間，對岸駭客進入中華電信網路服務備用電腦，植入木馬程式（Trojan horse），使得許多政府網站當機中斷服務，更藉機蒐集政府的機密資訊。2003年則發生在台北縣替代役男，利用職務以駭客程式入侵學術與政府將近1,000部電腦網路主機，從中牟取不法利益的情事。

從層出不窮的資安事件來看，顯示政府雖然持續推動資通安全，但是對於資通安全及風險管理的概念仍有待加強；同時內部缺乏良好的控管機制及作業程序；加上資通安全管理人力資源與專業技能均嫌不足，使得臺灣這幾年來頻頻出現資通安全的漏洞，儘管這些網路犯罪尚未影響到公共安全，但是也徒然地耗費許多政府與民間社會的成本，值得政府在擬定資通安全政策作為警訊。

參、民眾對電子化政府安全性的看法

模範市場研究民調公司（Taylor Nelson Sofres，以下簡稱TNS）在2004年9月公布關於電子化政府服務的民意調查中，對於全球32個國家3萬2千個民眾進行調查，結果顯示約有30%的受訪者曾使用過電子化政府所提供的服務。但是當問及「您認為使用網際網路提供個人資訊給政府，是不是覺得安全？」，僅有25%的受訪者認為電子化政府線上服務是安全的，認為不安全的比率卻高達58%。

從懸殊的比例來看，現今網路不僅實際上有各種風險存在，民眾對於應用網際網路也存在高度的不信任感。

若以TNS近幾年關於網路安全民調加以比較，可以看出民眾對於電子化政府的信任雖然慢慢提升，但是整體的比例仍是偏低(註2)，而臺灣受訪民眾認為不安全的比率又高居各國之冠。依據上述調查結果，各先進國家仍應該持續關心，並且採取有效對策來因應資通安全。

此外，電子化政府下資通安全也關係民眾隱私保護，特別是資訊隱私權的問題。其強調在沒有通知當事人並且獲得其同意的情況，資料持有者不可以將當事人為某特定目的所提供的資料用在另一個目的之上（李科逸，1999）。資訊隱私牽涉資通安全領域資訊濫用的問題，因為不當的蒐集、使用或公開資料所導致（黃慶堂，1999：40）。資訊隱私權的問題一直為立法機關、社會各界與人權團體所關心。舉例來說，1997年政府推動國民卡，其可能衍生的安全及隱私問題曾引起廣泛討論，這是資通安全首次成為焦點政策。儘管國民卡計畫在社會尚未建立共識，加以政府與廠商未能於期限完成議約而暫停實施。但是，國民卡所引發社會各界對現代資通科技的安全疑慮，並未停止或稍歇（行政院研考會，1998；紀佳伶，2000：289-322；蔡忠翰，2003）。隨著電子商務及電子化政府等數位台灣計畫的全面推動，會使資通安全及資訊隱私權會受到更多的重視，促使政府未來必須更為著重。而臺灣的資通安全政策究竟何去何從?本文認為參考其他國家或國際組織的規劃，或許有助於釐清臺灣本身的問題。

肆、國際間資通安全相關政策參考

面對前述所說的資通安全的風險，本文檢視其他國家與國際組織對於資通安全的規劃。本文首先以美國資訊基礎建設任務小組建立的安全信條為主；在國際組織方面，則是以經濟合作及發展組織（Organization for Economic Cooperation and Development，以下簡稱OECD）的相關資通安全所訂定的準則，還有亞太經濟合作組織（Asia Pacific Economic Cooperation，以下簡稱APEC）所制訂的資通安全策略為主。分析美國與兩個重要的國際組織對於資通安全的觀點，將有助於探討我國資通安全的政策。

一、美國資訊基礎建設任務小組建立的安全信條

美國政府在1993年為了推動資訊政策，提出國家資訊基礎建設計畫（The National Information Infrastructure，以下簡稱NII），同時成立資訊基礎建設任務小組（Information Infrastructure Task Force, 以下簡稱IITF）。在關於資訊安全的面向上，

IITF參酌各界意見後，提出資訊安全的五項基本信條，作為聯邦政府推動資訊安全工作的依據，其強調每個參與者有權利：（一）掌控誰能夠以及在何種條件下看到他們資訊（或是不能看到）的能力。（二）瞭解他們是跟誰在溝通的能力。（三）確定其儲存或傳送的資訊並未被更動的能力。（四）瞭解資訊及通信服務何時能使用（或不能使用的）的能力。（五）封鎖他們所不想要的資訊及組織惡意入侵的能力。

這些原則強調資通安全的重要性，也突顯資訊隱私權的意義。但是IITF也說明這些原則並非是絕對的，同時每個原則也都需要NII參與者更大的參與以及被賦予更多的責任。

二、OECD資訊系統與網路安全準則

2002年7月25日OECD理事會通過「資訊系統與網路安全準則」（the guidelines for the information systems and network，以下簡稱「安全準則」）修訂本，以發展安全文化（toward a culture of security）為方向，作為組織會員國推動資通安全相關政策、法令的參考依循，「安全準則」中所提出九項原則，分別為認知、責任、反應、道德規範、民主、風險評估、安全設計與執行、安全管理以及安全再評估，其含意如下（OECD, 2002）：

（一）認知（awareness）：此原則強調所有參與者都要認知資訊系統與網路安全的必要性，並意識到資通系統風險的存在及了解現有的安全保護措施，是保護資通安全的起點。資通系統可能會面臨來自內部及外部風險的威脅，相關的參與者應認知安全上的失誤會影響其控制的資訊系統與網路。同時，也應體認系統相互連通及相互依賴可能會產生的潛在風險。

（二）責任（responsibility）：此原則強調所有參與者對資訊系統與網路安全均負有責任。就資訊系統與網路安全而言，參與者應體認其負有與本身角色相對應的安全責任，OECD要求參與者應定期檢視本身政策、做法、措施和程序，是否與所處的環境合適。

（三）反應（response）：此原則強調參與者應以及時與合作的方式採取行動以預防、偵測及反應資訊系統及網路安全事件，同時要與其他參與者適當地分享有關危險的訊息。

（四）道德規範（ethics）：此原則強調參與者應尊重其他參與者的合法權利。同時意識到他們是否採取行動都可能對他人造成傷害。所以合乎網路道德規範的行為是相當重要的，參與者必須盡力維持，並且鼓勵符合安全的行為及尊重他人合法的權益。

（五）民主（democracy）：此原則強調資訊系統與網路安全必須符合民主社會的核心價值，包括思想及意見交換的自由、資訊流通的自由、秘密通信自由、適度保護個人資訊還有資訊公開及透明化。

（六）風險評估（risk assess-

ment）：參與者應進行風險評估，包括網際網路的威脅及脆弱性（vulnerabilities），而且應分別就內部與外部因素完整分析，以確認資訊的性質及重要性，並進而訂定風險標準及選定適當的風險管理措施。

（七）安全設計與執行（security design and implementation）：參與者應將安全視為關鍵因素納入資訊系統。並完整的設計、執行並協調系統與網絡。

（八）安全管理（security management）：參與者應對於安全管理進行整體評估。以此為基礎，安全管理應該積極涉及到參與者活動及業務相關的各個領域。安全管理包括對發生中的威脅進行預應及防止、偵測並反應突發事件、系統修復、日常維護、檢測與認證。資訊系統與網路安全的政策、作法、措施及程序應該整合為一致性的政策。

（九）安全再評估（reassessment）：參與者應檢討及再評估資訊系統及網路的安全性，並適度調整安全政策、作法、措施及程序。面對新興且變化中的威脅與脆弱性持續出現，參與者應該不斷地檢查、再評估、並調整與安全有關的各個面向，以應付這些變化中的風險。

OECD的這9項原則，對於資通安全提出較高的要求標準，諸如當中對於安全責任的釐清、對於安全措施與程序的認知、對於其他使用者的權利的尊重以及網路民主的精神等等都已經涵蓋，算是對於資通安全相當完整的規範。

三、APEC網路安全策略

APEC為防範網路犯罪及保護重要基礎建設，由電子安全專案小組（e-security task group）制訂APEC的「網路安全策略」（cybersecurity strategy），該項策略分別從6個面向建立網路安全策略（APEC, 2002）。

（一）法制發展面向（Legal Developments）

就法制面向來說，「網路安全策略」認為網路安全依賴各經濟體間的相互合作，因此各國必須採行三個步驟：1. 將網路上的攻擊行為透過實體法的訂定刑事化；2. 訂定程序法以確保法律的執行者擁有必要的權限來偵查或起訴；3. 促使各經濟體內的法律或政策得以促成國際合作來防止與電腦相關的犯罪。

在此3個步驟下，「網路安全策略」要求各成員經濟體在實體性、程序性、相互性的法律與政策上，各經濟體應該儘訂定，也責成APEC應督促各會員國努力發展。同時也要注意在此區域內其他國際組織的工作，特別是歐洲議會所訂定的「網路犯罪條約（Cybercrime convention）」(註3)。

（二）資訊分享與合作面向（Information Sharing & Cooperation）

「網路安全策略」認為打擊網路

犯罪與保護資訊公共建設，需要會員國間相互協力建立系統來偵測潛在的威脅與脆弱性，同時進行即時的警示與修復。透過這種模式來確保與分享資訊，使得相關的威脅在爆發之前便能受到控制，而會員國間的網路系統也能夠受到較好的保護。

實際上，許多APEC會員國都已經有相關的量能來因應（註4），除外，網路犯罪小組（cybercrime units）也需要發展與維持來強化法律與偵查議題（註5）。協助會員國加入國際網路犯罪聯防組織「24/7網路」（High-tech Crime 24/7 Point-of-Contact Network）。

（三）安全與技術綱領面向（Security and Technical Guidelines）

安全與技術綱領的作用在於支援政府與企業，使其能夠打擊網路犯罪以及保護重要公共建設。這些努力應該被鼓勵、予以公開化、獲得支持並進行合作。關於綱領的部分，可以分為3項行動計畫：1. 確認資訊科技安全標準及最佳的運作狀態。2. 檢測電子交易安全措施的法律與政策，如加密（encryption）、公共鑰匙基礎結構（Public Key Infrastructure，以下簡稱PKI）以及認證功能（Authentication）等。3. 建立企業資訊安全的模式，用來支持企業及網絡安全的努力，並且用來詮釋發展健全商業網絡安全運作的經濟因素。

（四）公眾認知面向（Public Awareness）

每個會員國的資訊系統都是息息相關的，任何一國資訊系統缺乏適當保護，都會造成他國資訊系統也會受到波及，網絡中的各種參與者必須清楚的認知到網絡中潛在的威脅及脆弱性，並且依照本身的角色與職能擔負起應有的安全責任。在關於數位安全與數位倫理，所有的會員國、企業與消費者都應該重視3個部分：1. 最好的保險與安全運作；2. 使用資訊網路的利益與責任所在，以及3. 對於網路誤用可能導致潛在的負在效果。

基於此，在公眾認知面向上，應該採取兩個行動：1. 藉由多邊組織檢視與推動區域對於網路安全的公眾認知，2. 持續推動教導參與者認知網路使用的權利與責任，建立相關推動計畫及網站。

（五）訓練與教育面向（Training and Education）

人類資源的發展與推動安全是否能夠成功兩者息息相關。為了達成網路安全，政府與企業必須就網路犯罪及網路公共建設保護，就複雜的技術與法律議題進行訓練。這些人員必須擁有嫻熟的技術且有能力回應突發事件與威脅。這些努力應該包含短期即時的訓練以及長期專業教育。

基於此，在訓練與教育面向上，應該採取3個行動：1. 提供與防範網路犯罪及保護重要基礎建設相關之技術及法規方面訓練。2. 建立資訊安全

專家驗證機制及推動訓練教材之交流。3. 建立相關網站公佈各經濟體訓練與教育最新訊息。

（六）無線安全面向（Wireless Security）

無線科技是網路應用的的新興方式，不僅使網路應用與服務更為迅速與便宜，也更具有經濟上的生產價值。的確，無限連接對於消費者與企業使用產生革命性的變化，然而其現今無限網路使用具有其脆弱性，同時無限的產品與應用（包括區域網絡）允許未經授權便能夠進入網路安全防火牆導致安全的漏洞。而對於無限網路產品與應用安全性質的疑慮，可能減緩對於該項有價值新科技的的發展。所以在無限安全面向上，「網路安全策略」強調必須對於無線網路的安全性進行持續檢視。

伍、臺灣電子化政府下資通安全的對策

臺灣為了強化國家資通安全建設，行政院於2001年1月核定「建立我國資通訊基礎建設安全機制計畫」，並依照計畫構想，成立行政院「國家資通安全會報」（以下簡稱「資安會報」），由行政院長與副院長分別擔任正、副召集人來宣示其重要性。會報下設標準規範、稽核服務、資訊蒐集、網路犯罪、技術服務、危機通報及國家資通安全應變中心等7個工作組，整合相關部會資源推動國家資通安全基礎建設工作，並建立國家層級的資通安全指揮機制，研析相關因應作為，有效保障臺灣本身的資通安全。

2004年8月「資安會報」進行組織調整，依據新的組織架構，會報下設「標準規範組」、「稽核服務組」、「法規偵防組」、「資訊蒐集分析組」、「通報應變組」及「綜合規劃組」（組織架構圖如圖1）。

從前述對於資通安全的分析，可知臺灣在資通安全政策上，必須建立事件緊急應變作業，透過各機關建立事前安全防護、事中預警應變以及事後復原鑑識等機制運作。同時依據組織風險評估，針對各種可能的風險，包括自然災害、機械故障、人為過失及故意破壞等，訂定有關危機通報緊急應變計畫暨處置復原作業程序。藉由事先擬定之相關災害預防、緊急應變對策、回復計畫等措施及定期演練，建立對於資通安全緊急應變量能。

在國家整體資通安全防設方面，「資安會報」正在規劃建置「國家資通安全防護管理中心」（National Security Operation Center, 以下簡稱N-SOC），一方面以N-SOC作為國家資通安全警訊分析與發佈中心，一方面對於重要政府資通安全設施進行必要的防護。隨著資通安全的防護及應變機制逐步建立，但是面對資通科技日新月異，加以電子化政府與電子商務的使用日益深化，仍有必要對資通安

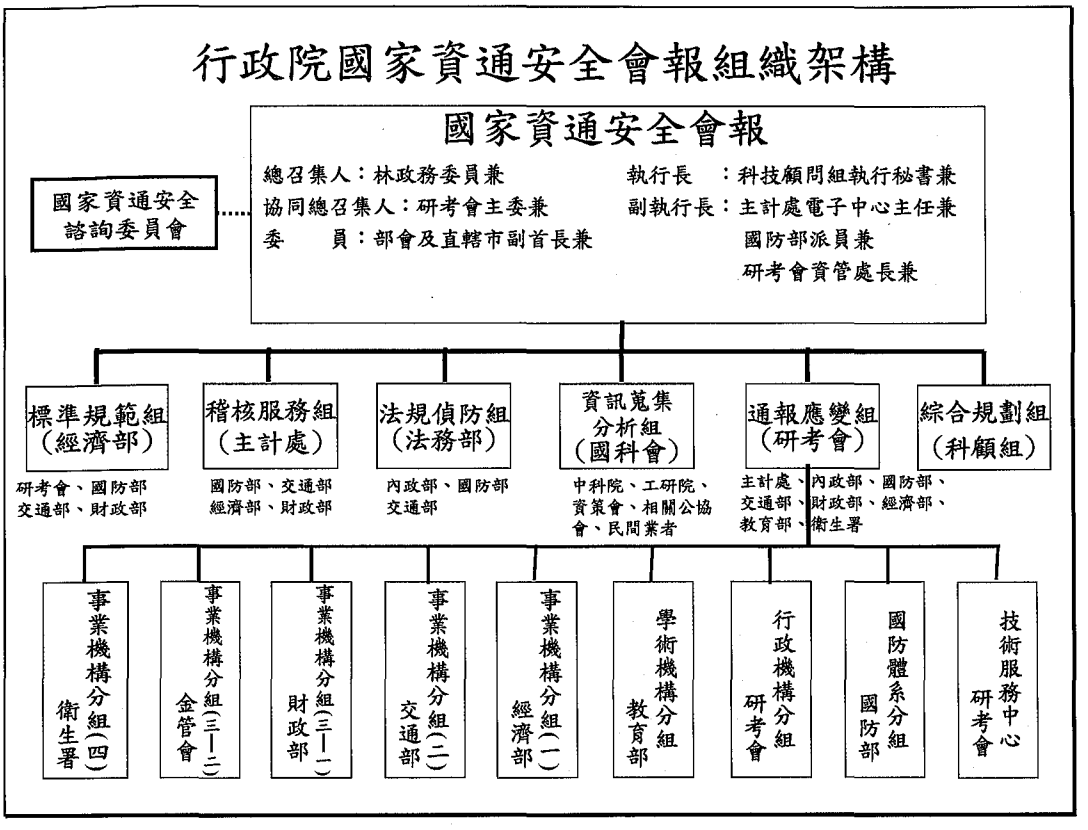

圖1　行政院國家資通安全會報組織架構圖

全相關工作進行評估，本文參照臺灣實際的資通安全狀況，以及國際間對於資通安全相關所擬定的政策，提出下數相關的原則以及實際的政策建議。

一、電子化政府資通安全原則

資通安全是推動電子化政府的重要關鍵，唯有安全可信賴及符合成本效益的資通安全管理制度及健全作業環境，才能使政府機關有效地提供民眾服務。資通安全的首務在於加強相關人員的資通安全教育訓練。同時資通安全也面臨兩難，若訂定較高的安全層級，雖然有助於確保網路安全性，但是也使得投入成本增加，並導致使用者的不便。如何建立適當、有效及相稱的資通安全管理制度將成為各機關推動資通安全管理工作的考量重點。參照OECD的「安全準則」及APEC的「網路安全策略」，本文就此提出建立政府機關對資通安全之幾項原則。

（一）利用資訊與保護資訊同等重要

「安全準則」中對於資通安全的

政策非常強調責任的重要性，其認為參與者對資訊系統與網路安全均負有責任。在對於資訊系統與網路安全的利用上，OECD要求參與者應體認其負有與本身角色相對應的安全責任，更應定期檢視本身政策、做法、措施和程序，是否足以因應資通安全的衝擊。APEC也呼籲其會員國、企業與消費者應該體認使用資訊網路的利益與責任所在。

依循這樣的精神，臺灣在電子化政府也必須意識到，既要充分利用資訊化及網路化所帶來的效益及便利，也要投入適當的資源維護及保護整體資通安全。從實際的政策措施來看，對於諸如電子公文、電子支付、電子採購等各項網路應用系統，加速政府運作的效率與效能，但是也都必須事前進行安全風險評估，進而採取適當及足夠的安全防護措施。

（二）資通安全宜以全方位的觀念永續推動

電子化政府之資通安全措施，除了要適度地採行各種技術安全措施外，也必需要認知到資通安全並非全然技術問題，而要以全方位的觀點檢視，不論是資訊系統的管理、相關法制配套、資通安全的教育訓練、組織與人力的適當安排，特別是現今全球化的時代，國際間安全合作及資訊分享等都是必須考量的層面。

再者由於臺灣面對特殊的國際情勢，整體的資通安全政策必須納入網路國防的思維，認知到資通安全是由社會所有成員，依據角色與職能共同承擔，而非僅僅是資訊單位的責任。特別是從近來臺灣頻繁的資通安全事件來看，許多是內部人員故意（例如替代役男利用職務入侵學術與政府網路的事件）或過失（例如2001年10月台電員工不慎挖斷中華電信電纜，造成機場無線通訊中斷）所造成，資通安全的工作除了防範外部的入侵者外，也必須加強內部人員的風險評估及教育訓練。

（三）資通安全也應強調顧客導向及宣導

從公共管理的角度來看，政府運作必須重視顧客導向（customer-orientation），重視民眾對於政策執行的感受。在資訊與通訊政策方面，為了提供民眾安全及可信賴的網路應用環境，政府應投入適當資源來保護電子化政府的安全。同時，資通安全措施也要符合國際組織訂定的安全標準及國家標準，並率先通過國內外認證機構的安全認證，讓政府資通安全的品質為社會各界所接受及認可，以增進民眾對於使用電子化政府各項網路申辦服務的信心，使得日後各項資訊與通訊相關政策推動也更容易獲得民眾的認同。

在OECD的「安全準則」中強調，其最終目標是要促進各會員國建立「安全的文化」。近來發生的資通安全事件顯示政府對於安全認知、風險管理、網路倫理規範的培育、尊重他

人隱私的道德建立及資訊專業人員職業道德的規範等，尚有待努力，在顧客導向的觀念下，唯有政府從基礎的資訊教育著手，培養及深植安全的文化，作為邁向數位台灣的核心價值，才能營建安全及可信賴的網路活動環境，強化網路公民對電子化政府的信心。

二、電子化政府資通安全策略

在前述資通安全的3項原則下，本文認為N-SOC在資通安全警訊分析，以及安全設施防護等兩項機制上，未來可以採取4項策略，使得整體臺灣資通安全更為完善。

（一）強化政府機敏性資料之保護與儲存

國家資通安全建構是以確保國家安全為核心，面對資安事件頻傳、電腦系統漏洞百出，以及對岸計畫性地對台灣發動網路攻擊，政府必須重視機敏性資料之保護與儲存問題，以防止重要資料外洩。建議政府各機關應全面檢討公部門資料之重要性及安全性，對於機敏性資料予以實體隔離，同時駐外單位必須全面檢討現有機敏性資料交換機制之安全性，以確實做好資料保密工作。

值得注意的是，目前政府資通安全工作以技術安全產品的建置應用為主，但是依循前述的資通安全原則，許多資安事件皆已經超越技術層次，而是相關人員內部控制、稽查及管理程序問題，建議除防止外部駭客、病毒的入侵外，更應重視人員及作業程序的安全管理問題。教育訓練則可以仿照APEC，採取提供相關之技術及法規訓練、建立資訊安全專家驗證機制以及建立相關網站公布體訓練與教育訊息等行動。

而整體的政府機關對於資訊的推動上，參考OECD的「安全準則」可以分為下述六個部分進行：1. 推動各機關遵循資通安全管理相關作業程序規定，建立快速反映處理資通安全事件的通報及復原制度。 2. 持續擴大辦理資通安全相關訓練，強化各機關資安管理能力。3. 強化資通安全資訊流通互享及預警制度，減少資通安全事件的危害。4. 推動重要系統及資料的備援作業。5. 檢討及強化各機關網路安全架構，減少網路遭入侵的風險。6. 配合行政院組織改造，檢討及強化各機關資通安全組織職掌及分工。

（二）提高民眾對資通安全的警覺性認知

從近來爆發的資通安全事件來看，許多都牽涉金融領域及民眾隱私被違法揭露的部分，嚴重降低民眾對於網路的信任感。未來國家資通安全推動，也必須加強對於資訊隱私權的重視，將民眾關心的身分安全（identification security）及隱私保護列為工作推動重點，除此之外，政府也必須教導民眾對於資通安全的警覺性認知。

如前述，在「安全準則」強調所有參與者對於資訊系統與網路安全所

必須要有所認知，包括風險性及相關保護措施等：而「網路安全策略」則提出參與者必須認知到網絡的威脅及脆弱性，並且擔負起應有的安全責任。政府可以參酌過去處理Y2K的經驗，加強推動全民資通安全的警覺性認知，建立人民資通安全的正確認知，提升民眾對電子化政府各項服務的使用信心。面對民眾對於資通安全的低認知性，政府可以結合私部門的力量，加強宣導資通安全的重要性及正確的網路安全行為準則，形成重視資通安全的網路文化。

（三）檢討資通安全法規，並提升網路安全之偵防能力

針對資通安全相關議題，參考國際立法趨勢，增修訂現有資通安全相關法規，以作為推動資通安全之依據。同時，加強培訓資通安全情報人才培訓，以充分掌握資安情資，並強化數位證據鑑識能力，提升執法單位之電腦犯罪偵防，加強國際交流合作，以有效打擊電腦犯罪，確保國家資通安全。落實N-SOC任務，提供政府、民眾及社會各界有關資通安全相關訊息及通報風險的管道。

（四）加強資通安全技術研發及應用，落實資安產品驗證及檢測

在OECD「安全信條」中關於安全再評估的原則，認為網路參與者應隨時檢討資訊系統的安全性，並適度調整安全政策、作法、措施及程序。面對新興且變化中的威脅與脆弱性持續出現，政府應該加強資通安全關鍵技術研發，以確保系統之安全性及可靠性，同時帶動我國資通安全產業發展，提升我國資通安全技術能力。

陸、結語

面對資訊與通訊科技的進步，政府得以建立電子化政府的虛擬組織（virtual organization），推動更有效能與效率的運作模式；而企業則以此帶動了電子商務的蓬勃發展，但是資通安全卻是這波趨勢快速發展背後的隱憂。本文認為政府除了建立N-SOC作為資安警訊分析與防護機制以外，更要積極與民間社會合作，建立相關的配套措施，諸如資訊系統的管理與監控、相關法制規範、資安教育訓練、組織與人力的適當安排等等，才能有效保護民眾資訊隱私權利、金融安全甚至於國家安全，並且更廣泛推動資訊科技的進步。

最後，本文認為由於網路科技的特殊性質，資通安全已經跨越國界形成全球性的議題，政府除了推動國內資通安全的防護機制外，也要認知本身對於全球性網路安全的責任，未來或許也能考量在資通安全議題上，就資訊分享、風險評估、安全設計與管理等面向上，與國際間積極展開合作行動，除了拓展臺灣的國際視野，更有助於臺灣與其他國家相互確保國家的資通安全。

附註：

註1：要說明的是，儘管這些數字都是經過正式通報的，但是考量到對於政府機關聲譽的維護、民眾的信心影響以及通報可能遭受連帶的責任追究等因素，本文認為實際發生的件數可能遠高於資通應變中心所公布的結果，這寫顯示當前政府資安事件的通報機制仍有加強的空間。

註2：這項調查結果重點摘陳如下：(一)在受訪的32個國家中，台灣(82%)、德國(81%)、捷克(74%)、法國(73%)及以色列(73%)是民眾認為電子化政府不安全比率最高的前五名；丹麥(48%)、新加坡(44%)、挪威(40%)、香港(40%)及芬蘭(36%)則是民眾認同電子化政府安全性比率最高的前五個國家。(二)如以性別區分，男人(29%認為安全)認為電子化政府是安全的比率較女性(22%認為安全)高。(三)如以年齡區分，34歲以下的使用者較認同電子化政府的安全性，45-64歲的使用者較不認為電子化政府是安全的。(四)如以電子化政府的使用者區分，58%的尚未使用電子化政府線上服務者(non-users)認為電子化政府不安全，是比率最高的族群。

註3：「網路犯罪條約」是在2001年11月由43個國家參與的歐洲議會(裡面成員又同時為APEC會員國)，這是第一個藉由國際多邊架構來遏阻網路犯罪的蔓延。面對越來越多的罪犯利用網路犯罪，此條約訂定最低的標準提供各國在訂定相關法律架構時的參考模式(APEC, 2002)。

註4：其中的成員可能來自於公部門、私部門或兩者兼有，例如許多會員國建立電腦緊急電腦系統緊急應變處理小組(Computer Emergency Response Team，以下簡稱CERT)來分享威脅性的資訊；或者成立企業間資訊分享聯盟的方式允許在某些特定部門內部的公司(例如通訊、能源業或銀行業)分享威脅性的資訊；其他則有透過政府機構來協助衡量其威脅性(APEC, 2002)。

註5：諸如打擊數位犯罪、資訊交換以及支援其他國家相關的網路犯罪小組等等。

參考資料

一、中文部分

1.國家資通安全應變中心(203.69.37.223/infosec/notice/l_stat.asp)

2.行政院研究發展考核委員會：國民卡專案相關應用之法源基礎與法律爭議說明，月旦法學雜誌，第43期，1998，頁28-38。

3.行政院研究發展考核委員會：政府機關公開金鑰基礎建設，台北：行政院研究發展考核委員會，2003。

4.林宜隆、華讚松、楊麒麟：網際網路與犯罪問題之研究，中央警察大學警學叢刊，31(6)，2001，頁197-220。

5.林祝興、張真誠：電子商務安全技術與應用，台北：旗標，2003。

6.邱承迪：網際網路上可疑不法資訊之自動化蒐集系統，國立中央警察大學資訊管理學研究所碩士論文，1999。

7.紀佳伶：資訊隱私權之探討—以國民卡引發的爭議為例，國立政治大學公共行政學報，第4期，2000，第289-322頁。

8.莊伯仲：網路隱私--電子化政府的一個迷思，網際先鋒，68，頁22。

9.黃慶堂：我國行政機關資訊安全管理之研究，國立政治大學公共行政研究所碩士論文，2003。

10.詹中原：新公共管理－政府再造的理論與實務，台北：五南，1999。

11.蔡中翰：政府部門資訊安全管理之研究，國立政治大學公共行政研究所碩士論文，2003。

12.謝美菱：從數位化、網路化、虛擬化的觀念論政府再造，元智大學資訊管理研究所碩士論文，2001。

二、英文部分

1.OECD, 2002. OECD Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security. http://www.oecd.org/document.

2.APEC, 2002. APEC Cybersecurity Strategy. http://www.apec.org/apec.html

3.Agranoff, Michael H. 1991. "Controlling the Threat to Personal Privacy: Corporate Policies Must Be Created", Information Systems Management 8(3): 48-52.
4.Bruce, Schneier 2000. Secrets and Lies: Digital Security in a Networked World, New York: John Wiley.
5.Kizza, Joseph Migga 2003. Ethical and Social Issues in the information Age, New York : Springer-Verlag.
6.Miller, Seumas 1998. " Privacy, Data Bases and Computers", Journal of Information Ethics, Spring: 42-48.