中研院推動資訊安全經驗分享

鄭哲聖[1]　徐讚昇[2]　王大爲[1,2]

[1]中研院 計算中心　[2]中研院 資訊科學研究所

【摘要】本院爲確保資訊資產安全，維繫研究及行政工作之正常運作，近年來陸續從制度、技術及人員訓練等三個層面強化院內資訊安全。本文闡述本院在推動各項資訊安全工作時所遭遇的問題與採取的解決方法，期望透過實務經驗的分享與交流，找出一套適用於學術研究機關（構）的資訊安全工作模式。

【關鍵詞】資訊安全管理系統、資訊安全事件通報機制、資訊安全事件管理平台

壹、前言

隨著電腦及網路的應用日趨普及與深入各個領域，病毒肆虐、駭客入侵、大量垃圾郵件、網路非法下載等資訊安全問題已成爲本院的重要課題之一。爲推動本院各單位加強資訊安全工作，本院李前院長於 2005 年第 687 次主管會報裁示，由總辦事處葉處長擔任本院資訊安全長，主管全院資訊安全事務。本院計算中心亦於 2006 年成立資通安全小組，負責規劃及推動本院資訊安全防護工作。

爲確保院內資料、系統、設備及網路之安全，以協助研究及行政工作之正常運作，本院從資通安全小組成立迄今持續推動各項資訊安全工作，包括：制定本院資訊安全規章、建構本院資訊安全管理系統框架、建立本院資訊安全事件通報機制、建置本院資訊安全事件管理平台、架設本院資訊安全服務網站、培訓本院資訊安全專業人才及種子教師、推廣本院資訊安全教育訓練等。本文將分別從制度、技術及人員訓練等三個層面說明本院資訊安全推動經驗，期望透過實務經驗

的分享與交流，找出一套適用於學術研究機關（構）的資訊安全工作模式。

貳、資訊安全制度

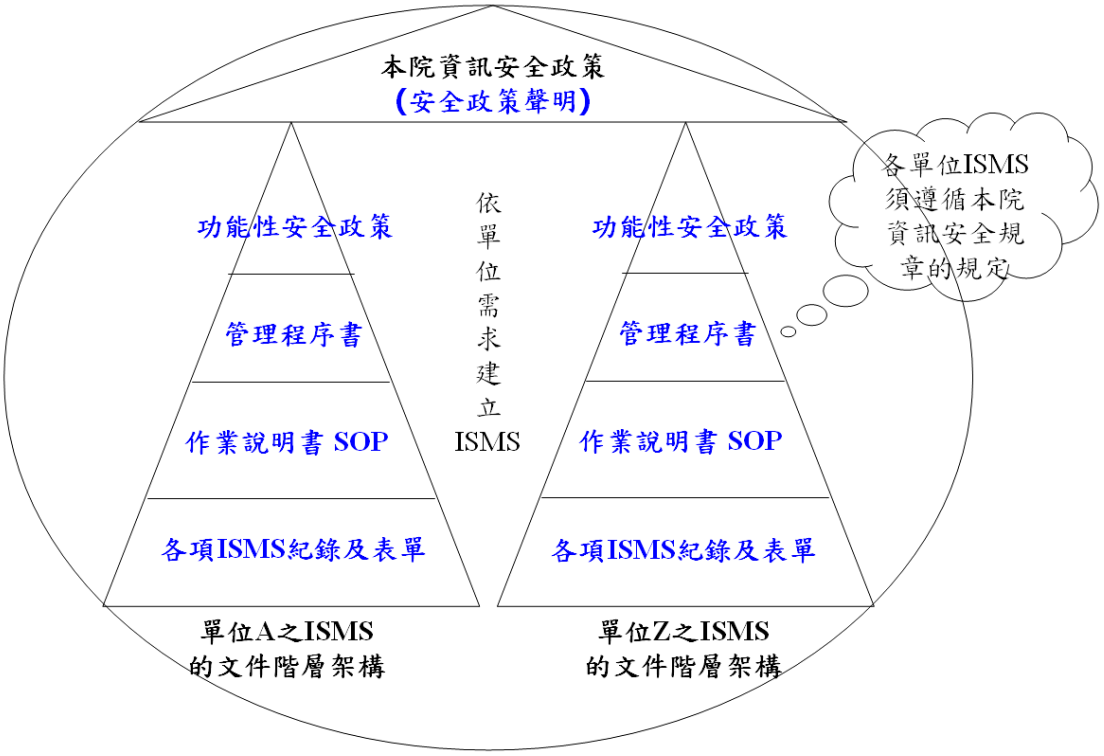
爲協助本院資訊安全工作走上制度化、標準化的軌道，本院計算中心從 2008 年開始在徐前主任讚昇的帶領下歷經近 30 次的內部會議討論，以及仰賴本院資訊安全委員會[1]各位委員付出許多時間及心力進行審議，於 2009 年完成本院資訊安全規章[2]的制定，工作歷程如表一所示。

表一、本院資訊安全規章的制定歷程說明

時間	工作事項
2008/12～2009/09	由中心各科組協力研擬、修訂12項資訊安全規章：（1）資訊安全政策、（2）資訊安全管理規範、（3）資訊安全委員會設置要點、（4）資訊安全訓練及管理實施要點、（5）電腦機房安全管理要點、（6）網路安全管理要點、（7）電腦系統安全管理要點、（8）應用系統存取控制管理要點、（9）應用系統發展及維護安全管理要點、（10）電子資料安全管理要點、（11）資訊安全事件通報及處理要點、（12）資訊安全內部稽核作業要點。
2009/04	推動成立本院「資訊安全委員會」。
2009/05～2009/09	本院「資訊安全委員會」審議、通過上述規章。
2009/06	召開「全院資訊室主管及管理者經驗交流座談會」，說明資訊安全規章的內容，並進行討論、溝通。
2009/09	陳請院長核定上述規章，正式實施。
2009/10	本院「資訊安全委員會」網站正式對外開放，公告上述規章。

在推動本院資訊安全規章的制定過程中，院內各單位曾表達不同的疑慮，主要可以歸納爲 2 個問題：（1）本院因組織較爲龐大，業務複雜，院內各單位對於資訊技術的需求程度不一，面臨的資訊安全問題也不同，本院資訊安全規章是否能適用於院內各個單位？（2）本院資訊安全規章規定應保存使用者之電腦系統使用紀錄以備資訊安全事件稽核之需，如何解除院內同仁對於侵犯個人隱私權之疑慮？

針對第 1 個問題，本院在研擬各項資訊安全規章之初，即以全院整體適用爲原則，將院內各單位的共同需求列入考量。以本院資訊安全政策[2]爲例，即屬於 ISO/IEC 27001 所稱之「安全政策聲明（Security Policy Statement）」，說明本院對於保全資訊資產方面所抱持的態度、信念以及要求，內容可適用於全院。而本院各單位可依據本院資訊安全政策，提出更具體符合所需的功能性安全政策（Functional Security Policy），並遵循本院資訊安全規章各項管理要點的規定，建立各單位的資訊安全管理系統（Information Security Management System；ISMS），圖一說明本院資訊安全管理系統框架。另外，考量院內大部分單位的資訊技術人員不多，無法抽調足夠的人力建立單位的 ISMS，本院將以計算中心爲示範點，從今（2010）年起到明年實作建立 ISMS，快速將風險管理的方法與觀念導入，並依本院文化修正，作爲後續擴充的基礎，以循序漸進將 ISMS 導入院內各單位。



圖一、本院資訊安全管理系統框架示意圖

針對第 2 個問題，本院特別首倡草擬電子資料安全管理要點[2]，對於院內各單位及個人的機敏性電子資料（包含個人隱私資料，如電腦系統使用紀錄等）訂定相關的保護及存取規定，有效紓解院內同仁對於侵犯個人隱私權之疑慮，使得本院資訊安全規章得以順利推動施行。

參、資訊安全技術

由於本院有許多單位使用 NAT（Network Address Tranlation）[3]機制讓多部電腦共用一個外部 IP 位址，加上本院的網路流量十分龐大，因此本院在資訊安全技術的使用上較少採用線上模式（inline mode）對異常網路行爲進行即時阻擋，而較著重於資訊安全事件之預防、預警及通報機制的建立，詳細說明請見表二。本院各單位可利用上述機制所提供的各項資訊，加強各單位的資訊安全防護措施，以達成全院的資訊安全。

表二、計算中心目前提供之預防、預警及通報等資訊安全機制說明

<table>
<tr><th colspan="3">機制類別</th><th>說明</th></tr>
<tr><td rowspan="3">預防機制</td><td rowspan="3">安全弱點評估工具</td><td>主機弱點掃描工具</td><td rowspan="3">系統化地檢測主機、網路設備、網站以及原始程式碼，找出各種潛藏的資訊安全漏洞，並提供修補建議。</td></tr>
<tr><td>網頁弱點掃描工具</td></tr>
<tr><td>原始碼弱點掃描工具</td></tr>
<tr><td>預警機制</td><td colspan="2">資訊安全事件管理系統</td><td>接收院內各單位之各種網路設備的日誌，分析異常的網路行爲，及早發掘潛在的資訊安全威脅。</td></tr>
<tr><td>通報機制</td><td colspan="2">資訊安全事件通報系統</td><td>記錄、追蹤資訊安全事件之處理狀況。</td></tr>
</table>

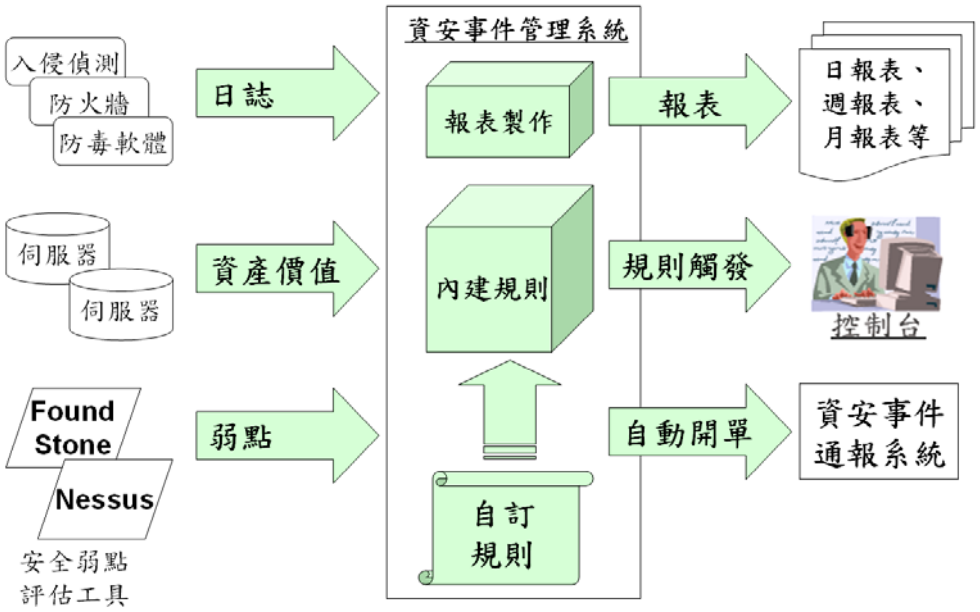
爲了進一步整合上述資訊安全機制，改善流程管理，本院將以資訊安全事件管理系統爲核心，整合安全弱點評估工具與資訊安全事件通報系統（如圖二），以達成下列目標：

（一）資訊安全事件監控：資訊安全專業人員透過控制台可即時掌握潛在的資訊安全威脅，並進行分析及研判，過濾出真正的異常事件。

（二）已知安全弱點之網路攻擊偵測：將重要之伺服器或設備的資產價值及其資訊安全漏洞的資訊一起匯入資訊安全事件管理平台，加強已知安全弱點之網路攻擊偵測。

（三）資訊安全事件通報：發現資訊安全事件後，在最短時間內通報相關單位進行處理。若該事件經研判爲緊急或重大事件，則啓動本院資訊安全事件處理小組進行危機處理與緊急應變措施，以避免危害的擴大。

（四）每天、每週及每月的定期報表：提供各單位定期性的資安事件統計、分析結果，以追蹤及掌握院內各單位的最新資安動態。



圖二、本院資訊安全機制整合示意圖

未來本院將基於圖二的整合方式，持續研析、導入最新的資訊安全技術，例如：日誌客製化工具、網頁應用程式防火牆、電子資料安全保護及稽核工具等，強化本院資訊安全機制。

肆、資訊安全宣導與人員訓練

本院對於資訊安全宣導與人員訓練的目標是確保本院同仁有能力履行被要求的資訊安全工作，並強化本院同仁之資訊安全共識與防護觀念。由於本院資訊安全人員較少，如何做好資訊安全宣導與人員訓練一直是本院相當大的挑戰。在有限人力的限制下，爲達成上述目標，本院目前在資訊安全宣導與人員訓練方面的作法如下：（1）建置資訊安全服務網站[4]，（2）培訓本院資訊安全專業人員及種子教師，以及（3）開設資訊安全推廣課程並錄製數位課程。

本院的資訊安全服務網站[4]成立迄今，已於網際網路上提供千餘則訊息，包括：資訊安全新聞、資訊安全通報、技術文件、軟體更新、教育訓練等訊息，及時提供院內同仁最新的資訊安全動態。

在培訓資訊安全專業人員部分，本院已派多名資通安全小組組員參加ISO/IEC 27001主導稽核員訓練課程，並取得證照。這些人員除了負責爲本院計

算中心建立ISMS外，亦負責培訓本院各單位資訊人員成爲單位的種子教師並讓其負責單位內的資訊安全宣導與教育訓練。

在開設資訊安全推廣課程部分，本院除經常邀請院外專家於「全院資訊室主管及管理者經驗交流座談會」分享資訊安全推廣經驗外，每年亦會針對總辦事處員工及院內各單位資訊人員舉辦教育訓練課程，這些課程也會逐步錄製成數位教材放置於院內網站供院內員工瀏覽。

藉由以上的作法，本院在有限的人力下，最大程度達成資訊安全宣導與人員訓練的工作目標。

伍、結語

資訊安全是長期而且必須持續進行的工作，該工作包括制度、技術、人員訓練等三個部份，三者環環相扣，缺一不可。本文闡述本院在推動各項資訊安全工作時所遭遇的問題與採取的解決方法，希望透過本院推動資訊安全實務經驗的分享與交流，爲本院及類似的學術研究機關（構），找到一套具有可行性、前瞻性的資訊安全工作模式。

參考文獻

[1] 中研院資訊安全委員會網站，網址：http://isc.sinica.edu.tw/

[2] 中研院各項資訊安全規章，網址：http://isc.sinica.edu.tw/data.htm

[3] Network Address Translation，網址：
http://en.wikipedia.org/wiki/Network_address_translation

[4] 中研院計算中心資訊安全服務網站，網址：
http://security.ascc.sinica.edu.tw/infosec-web/index.jsp

【作者簡介】

鄭哲聖　男

職　　稱：　中研院 計算中心 設計師

職　　務：　中研院 計算中心「資安小組」組長

研究領域：　計算機結構、資料檢索、資訊安全

聯絡電話：　886-2-27898846

聯絡郵箱：　chengcs@gate.sinica.edu.tw

徐讚昇　男

職　　稱：　中研院 資訊科學研究所 研究員

研究領域：　圖論基礎性質及相關應用的研究、演算法的設計、分析、實作與效率評估和資料密集運算

聯絡電話：　886-2-27883799 ext.1701

聯絡郵箱：　tshsu@iis.sinica.edu.tw

王大為　男

職　　稱：　中研院 資訊科學研究所 研究員

職　　務：　中研院 計算中心 主任

研究領域：　醫學資訊、隱私強化技術、圖學及演算法

聯絡電話：　886-2-27899254

聯絡郵箱：　wdw@iis.sinica.edu.tw