中央研究院
推動資訊安全經驗分享

鄭哲聖[1] 徐讚昇[2] 王大為[1,2]

[1]中研院 計算中心 [2]中研院資訊科學研究所

99.09.07

報告大綱

- 前言
- 資訊安全制度之規劃與制定
- 資訊安全技術之導入與發展
- 資訊安全宣導與人員訓練
- 結語

前言 (1/2)

- 為因應日趨嚴重的病毒肆虐、駭客入侵、大量垃圾郵件、網路非法下載等資訊安全問題，本院自2006年成立資安小組以來，持續推動：
  - 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與種子教師
  - 開設本院資訊安全教育訓練課程

➔ 確保本院資訊資產安全，維繫本院研究及行政工作之正常運作

前言 (2/2)

本院資安工作環圈圖

定期審查

本院資訊安全委員會

報告大綱

- 前言
- 資訊安全制度之規劃與制定
- 資訊安全技術之導入與發展
- 資訊安全宣導與人員訓練
- 結語

資訊安全制度之規劃與制定

- 目標
  - 協助本院資訊安全工作走上制度化、標準化的軌道
- 遭遇的問題
  - 本院組織龐大，業務複雜，院內各單位面臨的資訊安全問題也不同，如何制定全院適用的資訊安全制度？
  - 資訊安全工作須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？

本院資訊安全制度之規劃

政府資訊安全相關法規	中央研究院資訊安全規章	單位資訊安全管理系統
1.行政院及所屬機關資訊安全管理要點 2.行政院及所屬機關資訊安全管理規範 3.國家資通安全通報應變作業綱要 ⋮	1.中央研究院資訊安全政策 2.中央研究院資訊安全管理規範 3.中央研究院資訊安全委員會設置要點 ⋮	1.單位資訊安全政策 2.單位資訊安全推動委員會設置要點 3.單位適用性聲明書 4.單位資訊安全文件管理程序書 ⋮

以全院整體適用為原則，將院內各單位的共同需求列入考量

依院內各單位之需求，遵循本院資安規章及ISO/IEC 27001的規定建置單位資訊安全管理系統

本院資訊安全規章制定歷程

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。

計算中心資訊安全管理系統導入規劃

- 於今(2010)年至明年底先擇定計算中心之核心業務流程導入ISO/IEC 27001標準
- 作為後續擴大導入的基礎，以循序漸進將ISO/IEC 27001導入院內各單位
- 好處：
  - 降低組織適應新管理制度的成本
  - 快速將風險管理的方法與觀念導入，並依組織文化修正
  - 限制衝擊範圍

首倡研擬「電子資料安全管理要點」

- 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。
- 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。

報告大綱

- 前言
- 資訊安全制度之規劃與制定
- 資訊安全技術之導入與發展
- 資訊安全宣導與人員訓練
- 結語

資訊安全技術之導入與發展

- 目標
  - 利用各種妥適的技術與工具，例如：安全弱點評估工具、防火牆、入侵偵測系統、資安事件管理系統、資安事件通報系統等，有效落實本院資訊安全工作。
- 遭遇的問題
  - 本院的網路流量十分龐大，各單位內部的網路架構亦不相同，計算中心與各單位如何進行分工，做好資訊安全工作？

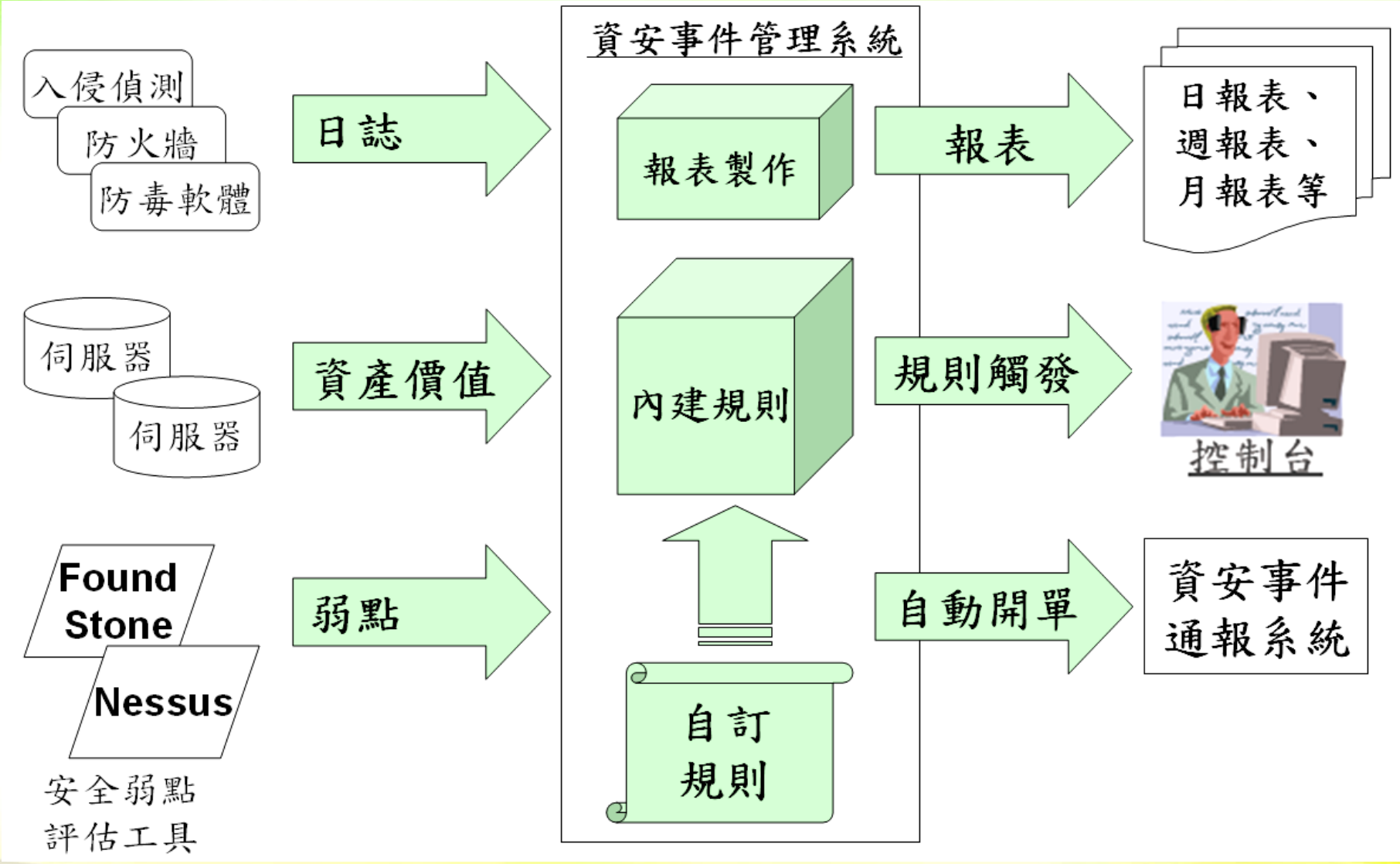
計算中心與各單位在資訊安全技術的分工

- 計算中心
  - 建立資訊安全事件之預防、預警及通報機制
- 各單位
  - 利用計算中心所提供的各項資訊，加強單位的資訊安全防護措施

計算中心提供之預防、預警及通報機制說明

機制類別			說明
預防機制	安全弱點評估工具	主機弱點掃描工具	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。
		網頁弱點掃描工具	
		原始碼弱點掃描工具	
預警機制	資訊安全事件管理系統		接收院內各單位之各種網路設備的日誌，分析異常的網路行為，及早發掘潛在的資訊安全威脅。
通報機制	資訊安全事件通報系統		記錄、追蹤資訊安全事件之處理狀況。

本院資訊安全機制整合示意圖



報告大綱

- 前言
- 資訊安全制度之規劃與制定
- 資訊安全技術之導入與發展
- 資訊安全宣導與人員訓練
- 結語

資訊安全宣導與人員訓練

- 目標
  - 確保被指定責任的人員，有能力履行被要求的資訊安全工作
  - 強化本院同仁之資訊安全共識與防護觀念
- 遭遇的問題
  - 各單位資訊安全人員大都是兼職，人力短缺的情形十分普遍

建置資訊安全服務網站

提供最新的資訊安全訊息

		8月新增	總數
• 資安新聞	Infosec News	28則	292則
• 資安通報	Infosec Announcement	10則	537則
• 技術文件	Technical Arcitle	2則	14則
• 軟體更新	Soft Updates	5則	240則
• 教育訓練	Latest Infosec Courses	8則	24則

培訓本院資訊安全專業人員及種子教師

- 派員取得或參加：
  - ISO/IEC 27001主導稽核員課程證照
  - 風險評鑑課程
  - CISSP(Certified Information Systems Security Professional)課程證照
- 取得證照的組員，充當種子教師，在院內開設資安相關推廣課程

開設資訊安全推廣課程並錄製數位課程

- 去(2009)年10月舉辦總辦事處個人資安宣導課程
  - 本課程已錄製成宣導影片
  - 短片網址：http://www.ascc.sinica.edu.tw/manual/Security/shortsubject.html
- 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
  - 去(2009)年6月邀請行政院主計處電子處理資料中心李茂基組長演講「政府推動資安之策略與省思」
  - 今(2010)年3月邀請英國標準協會(BSI)台灣分公司蒲樹盛副總經理演講「資訊時代的挑戰與機會」
- 下半年舉辦教育訓練課程
  - 個人資安概述
  - 本院資安規章與資安管理系統介紹
  - 弱點掃描與防火牆設定
  - Web應用程式攻防演練

前開課程亦將提供線上影片，便利院內同仁學習

報告大綱

- 前言
- 資訊安全制度之規劃與制定
- 資訊安全技術之導入與發展
- 資訊安全宣導與人員訓練
- 結語

結語

- 本文從制度、技術與人員等三個層面闡述本院資訊安全工作所遭遇的問題與採取的解決方法。
- 希望透過此次的分享與交流，為本院及類似的學術研究機關(構)，找到一套適用於學術研究機關(構)的資訊安全工作模式。

報告完畢
敬請指導