議題3. 建構資安產業發展環境

98年8月19日

簡報大綱

壹、前言

貳、全球資安趨勢

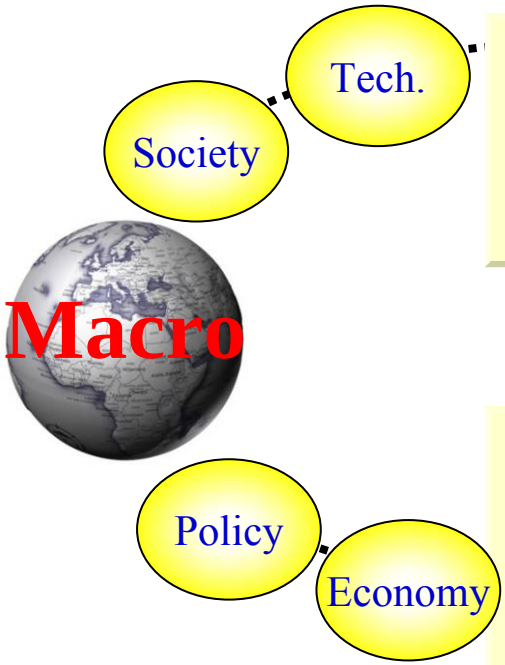
叁、台灣現況分析

肆、發展策略與行動方案

伍、討論題綱

壹、前言

資安攸關各層面 損害範圍逐年擴大



金融交易面

商業交易與相關活動日漸依賴資通訊技術，企業電子商務逐漸普及，民眾進行網路交易的頻率與金額日漸升高，也因此更遭受有心人事的覬覦。

科技與國防面

面對國際駭客對國家安全與政府機密的威脅，建構強力且完整的資安防護能力，方能確保國家安全，並且強化國家安全形象，並能配合科技發展。

商業經營面

不管是從生產流程、客戶資料、資訊或物品傳遞，政府與企業單位無不利用資通科技進行各類商業或機密和個人隱私管理，藉大量應用IT技術提升生產力與降低成本。

民眾防護面

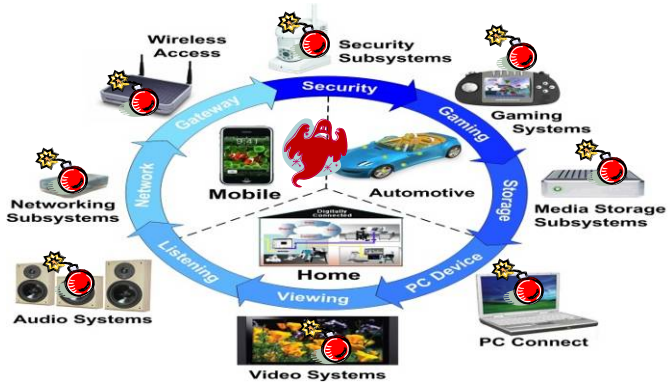
目前資安威脅與惡意攻擊大都為金錢或報復，攻擊型式已轉為複合型態。現成的攻擊軟體與操作方法已俯拾皆是，加上家用市場對資通安全概念不足，更顯資通訊安全防護能力不足。

- McAfee 研究指出2008年全球企業因資料外洩所造成的損失，達1兆美元以上
- 美國消費者統計報導，2006-2008年全美因電腦病毒/間諜軟體造成消費者達85億美元損失
- Gartner報告指出2007年全美因網路釣魚攻擊共造成32億美元損失
- 2007年5月愛沙尼亞爆發史上首場網路戰，全國電腦網路遭受可能來自俄羅斯的大量攻擊，網路癱瘓近一個月
- 根據台經院推估，台灣2007年約8%企業曾因資安事件而蒙受損失，損失金額達95.53億台幣

數位應用趨勢衍生新興資安挑戰

趨勢一、數位匯流及雲端服務架構 潛藏更多的資安疑慮

- 網路匯流— 惡意攻擊更易擴散
- 雲端服務— 易於駭客潛藏隱匿

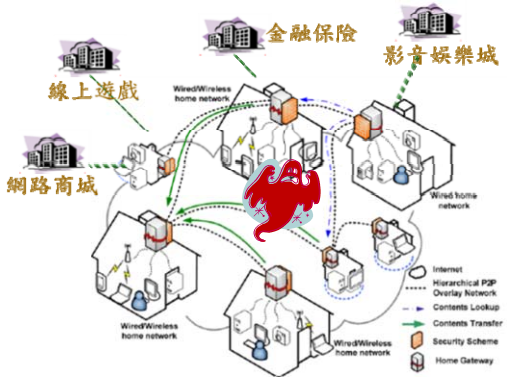


趨勢二、智慧行動應用崛起、引爆新興資安議題

- 終端平台多元整合— 資安脆弱性易於被利用
- 行動商務應用漸增— 成為駭客新一波目標

趨勢三、數位生活興起、資安威脅成隱憂

- 在家連網工作—居家網路安全需求升高
- 貼心生活應用—個資保護及隱私受重視



貳、全球資安趨勢

資安威脅與法規要求 驅動全球市場快速成長

全球資安產值 US$M

2009 Nokia 手機漏洞
影響簡訊功能

2008 花旗網路銀行個資遭竊,
DNS主要安全弱點揭露

2005 邏輯炸彈造成
Medco醫療產品斷貨

2003 SQL Slammer
造成核能電廠事故

2001 Code Red 蠕蟲，
攻擊全球各大網站, 金融系統停擺

2000 DDoS攻擊癱瘓Yahoo,
CNN, Amazon, e-Bay 網站

在法規與威脅的驅動下
全球資安產業蓬勃發展
預計2012年達到818億美金

資安威脅不斷翻新變化，
防禦需求緊追其後持續成長...

CAGR=14%

120000
80000
40000
0

1995 95/46/EC
1996 HIPPA法案
2002 SOX法案
2003 FISMA法案
2005 ISO 27001
2008 PCI DSS

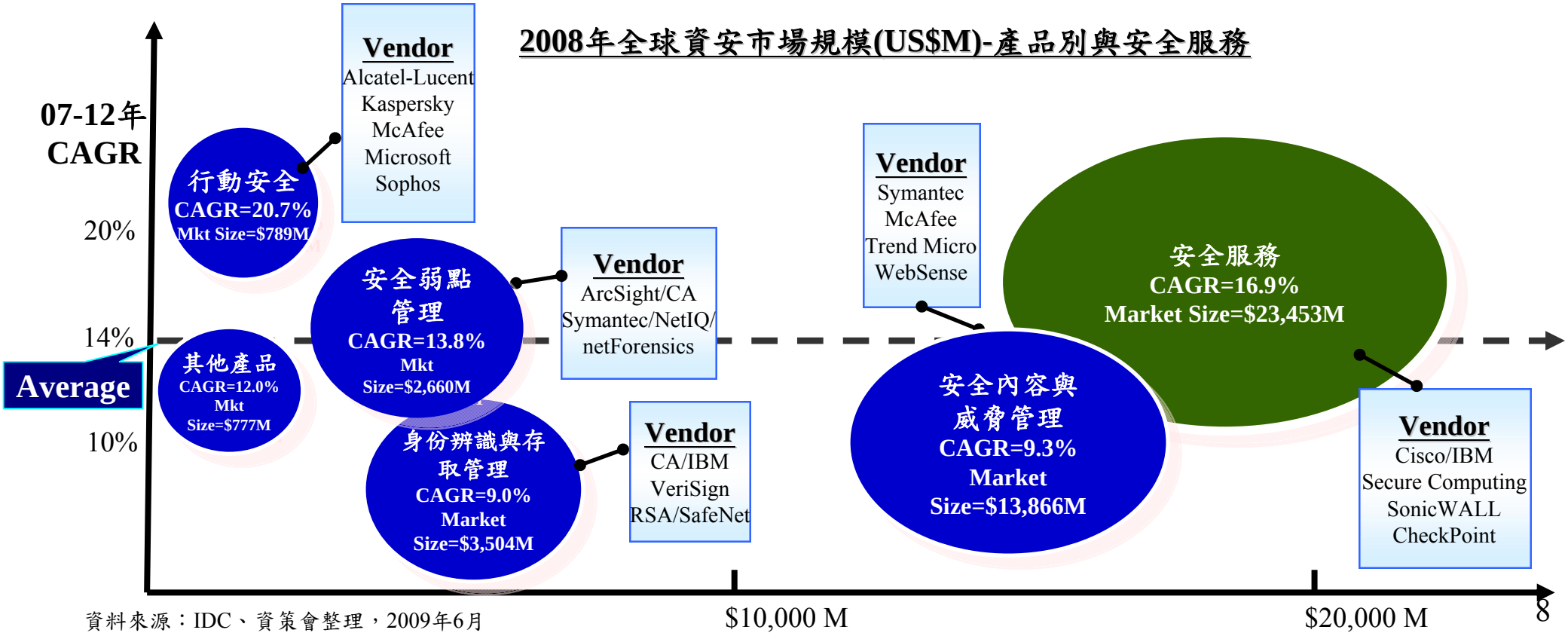
2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012

symantec.
McAfee
IBM
TREND MICRO
...

資料來源：IDC 資策會整理

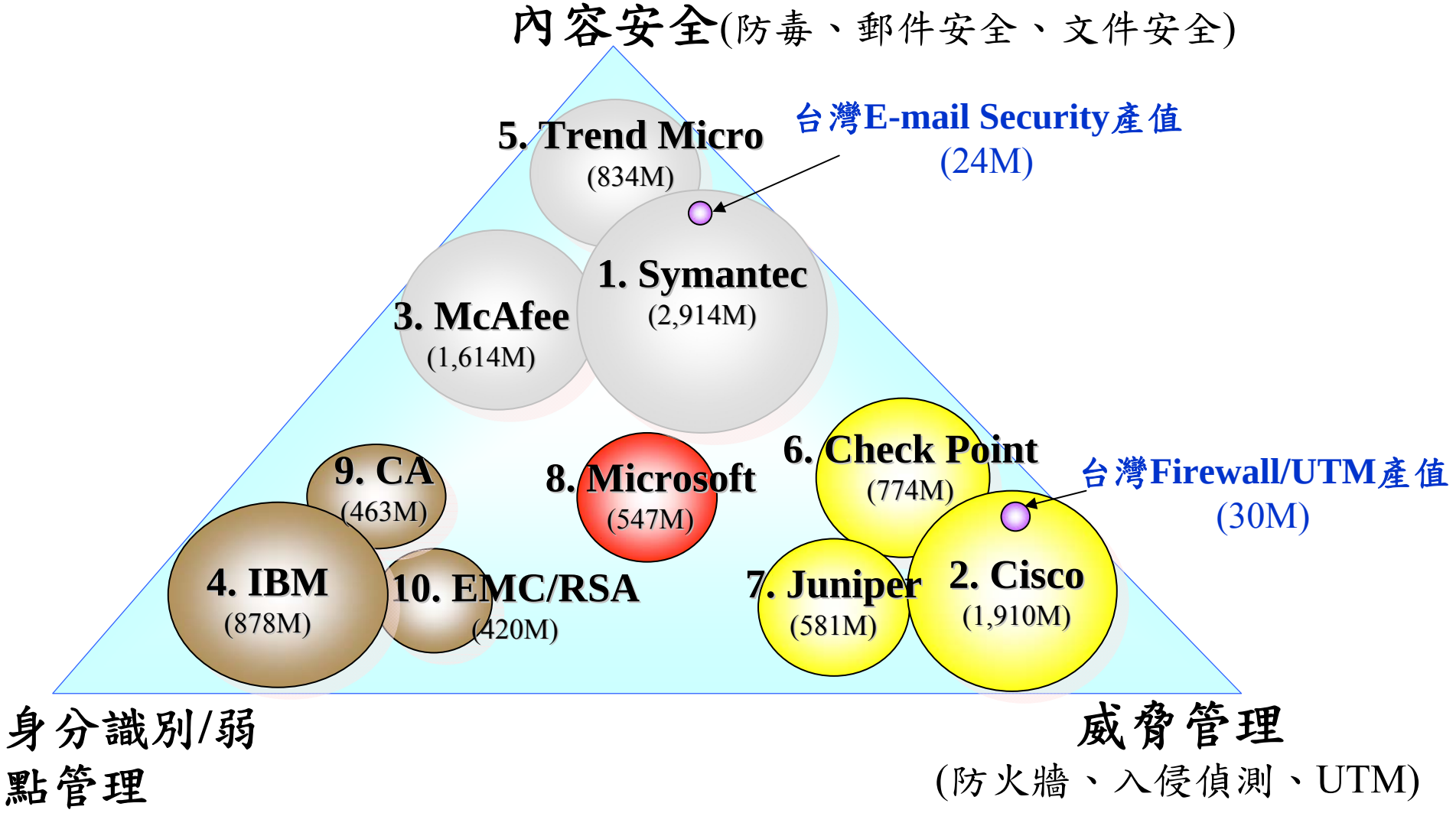
全球資安市場規模與成長預估

- 在資安產品中，以安全內容與威脅管理之市場規模最大，而行動安全成長率最高（CAGR=20.7%），安全弱點管理次之；這三個領域之市場機會均值得我國業界重視
- 資安服務市場規模龐大，業者仍需引用相關資安產品提供服務



資料來源：IDC、資策會整理，2009年6月

全球前10大資安廠商其主要產品類別



備註：圓圈大小表該廠商資安營收規模(百萬美元)相對大小，廠商前序號表該廠商於全球資安產值市佔率排名
資料來源：資策會MIC，2009年6月

資安應用需求趨勢

資訊應用

Internet 應用已進入Web Service 時代，並朝雲端與行動運算服務邁進，伴隨著更為嚴峻之資安挑戰…

Cloud & Ubiquitous Service Security

Cloud & Ubiquitous Service

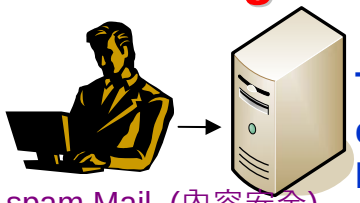
Virtual Resources
Cloud Client Mash-up
Cloud App (XML/RIA) FW (威脅管理)
Proactive Malware Detection (內容安全)
Mobile Security/Privacy (威脅管理/內容安全)

Web Service Security

Web Service

SOA, Blog,
Web-based Office..
Web App Firewall (威脅管理)
Web DB Security Monitor (威脅管理)
SIEM/Taint Analyzer (內容安全/ 弱點管理)

Inter-networking Security



Telnet/FTP/
e-Mail/
Browsing..

Internet service

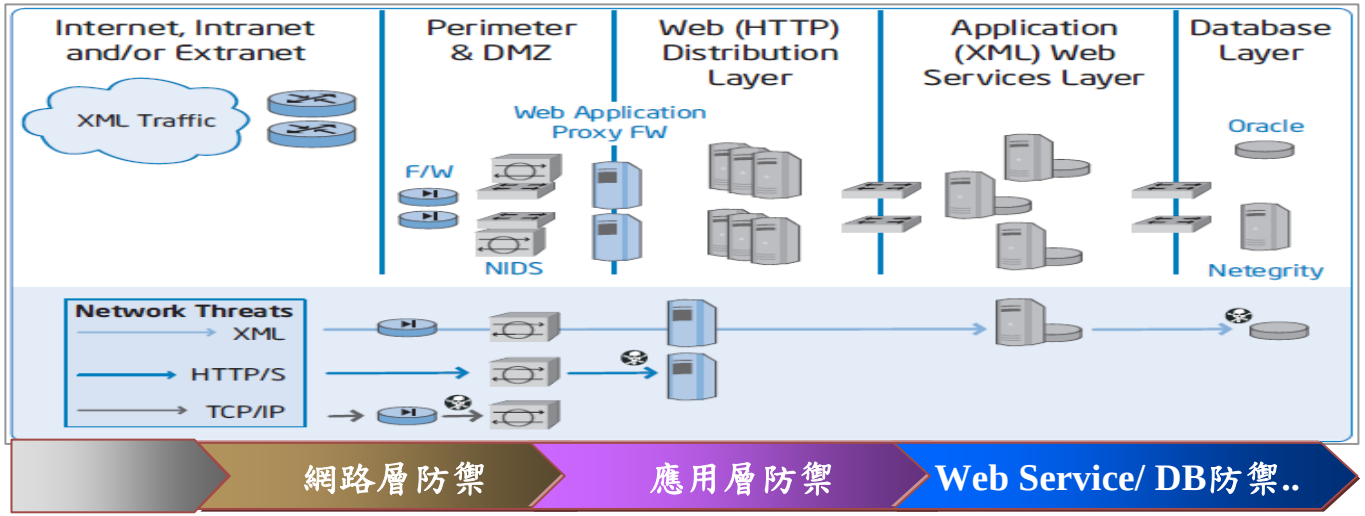
Anti-spam Mail, (內容安全)
VA, F/W, IDS, IPS (威脅管理)
PKI, VPN (身分辨識)

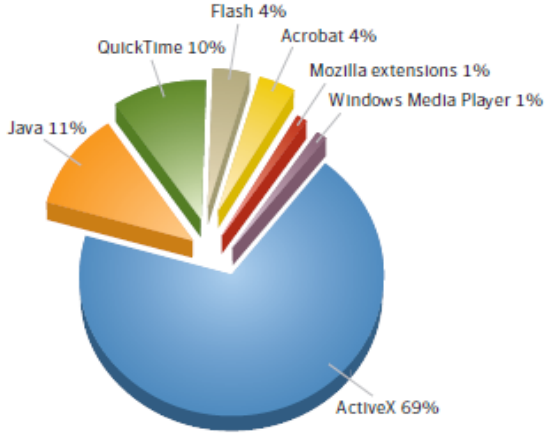
2005 **2010** **2015**

Web資安威脅翻新 防禦技術需不斷演進

超過70%之資安漏洞與Web應用相關，知名網站遭入侵後成為駭客中繼站(CNN, Business Week, McAfee…)。

- 目前Web應用層防禦技術多為網址(URL)過濾，然而攻擊趨勢已朝向XML、Web DB與 RIA (Rich Internet Application, 含：Active-X ,Acrobat, Flash...)等管道入侵。
- 因應不斷演進的Web安全挑戰，該領域資安市場持續成長(CAGR=13.7%)
- 資安防禦演進趨勢:





RIA 資安弱點比率
Source: Symantec

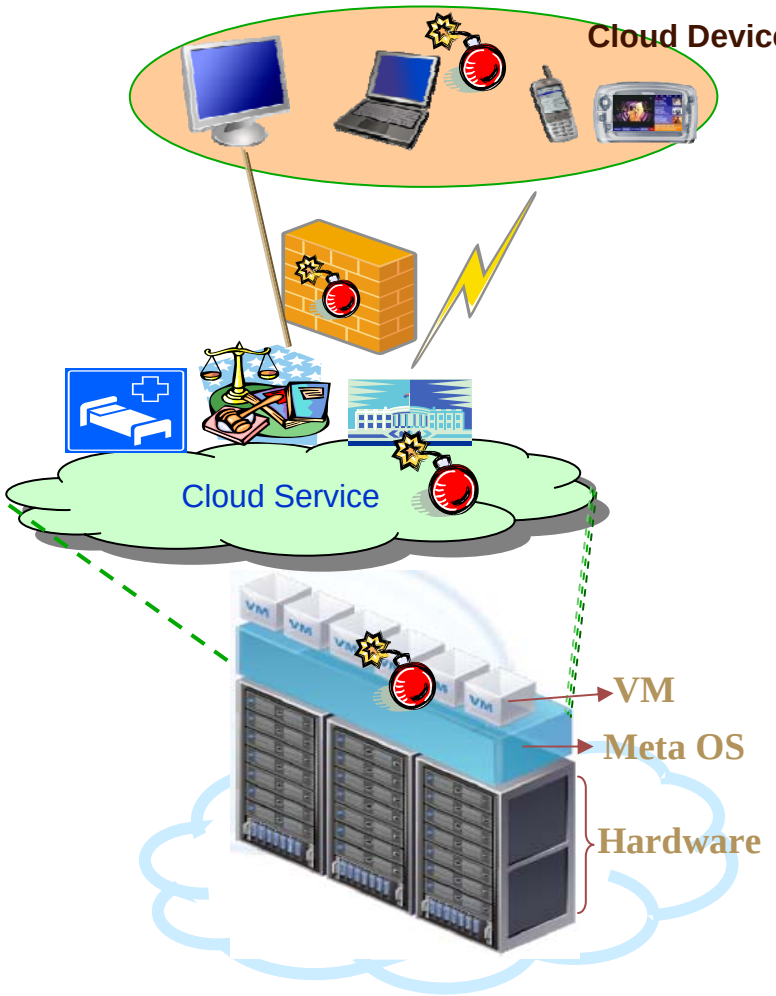
資安應用需求朝行動及雲端發展

雲端服務已經被視為繼Web 服務之後，下一波科技產業的重要應用趨勢，其多層次技術架構與動態融合應用，面臨更多資安威脅，主要涵蓋：服務終端裝置安全、Web入口威脅防禦、雲端內容存取安全與雲端系統弱點管控等新興關鍵技術。

雲端服務存取終端

雲端Web應用服務

雲端服務平台系統



服務終端裝置安全

Web 入口安全防禦

雲端內容存取安全

雲端系統弱點管控

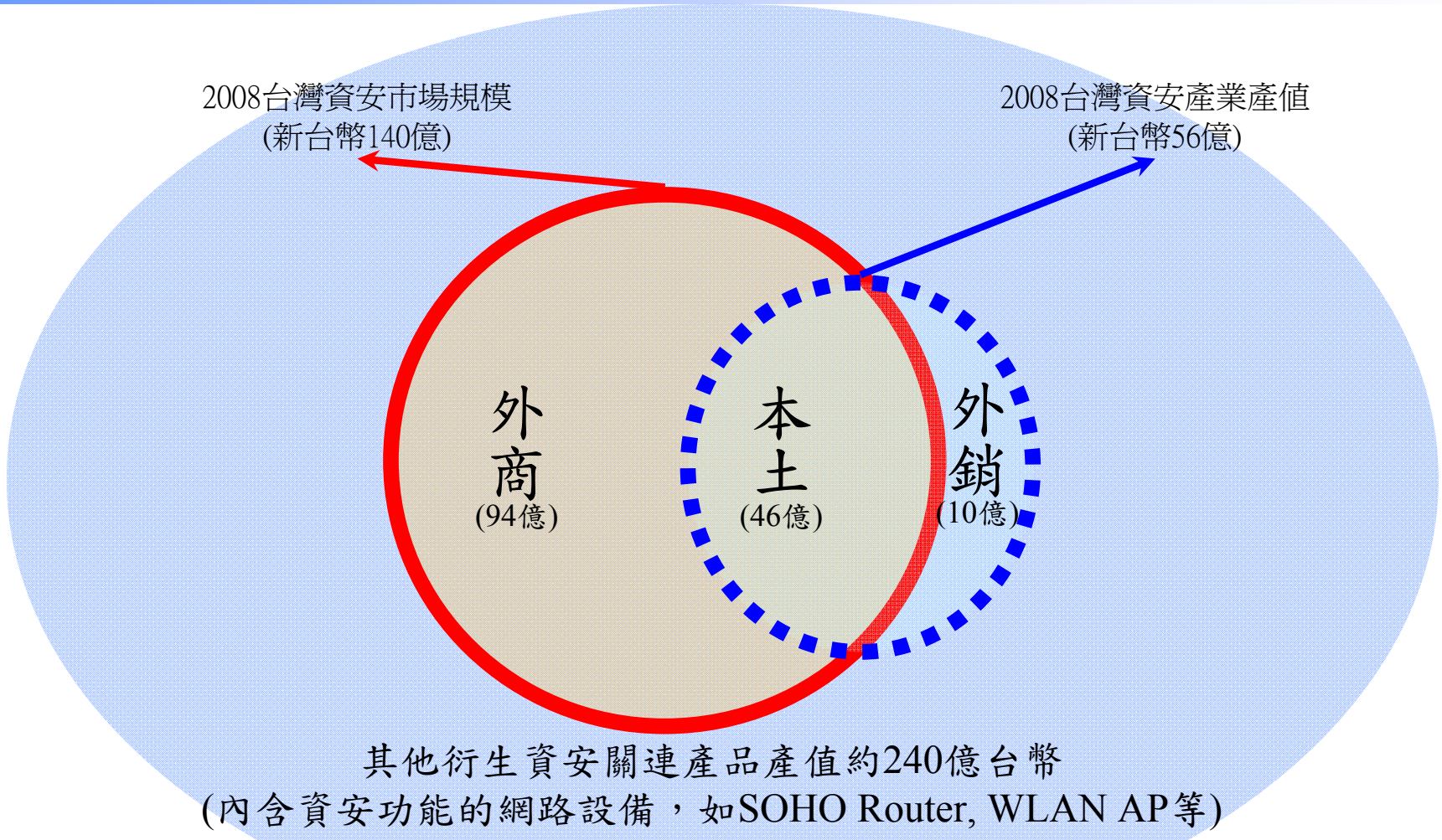
雲端資安議題

各國資安政策概況

- 美國總統歐巴馬2009年5/29宣布加強美國網路安全的新計畫，包括在白宮設立「網路安全總管」，職司協調相關作業，嚇阻、防禦針對美國政府和民間電腦網路的犯罪和間諜活動，以及駭客攻擊
- 2004年3月歐盟成立資安局（European Network and Information Security Agency,ENISA)，每年預算200~350億歐元
- 韓國2001年將資安研究組織提升，並命名為KISA (Korea Information Security Agency)，負責資訊安全技術與政策研究，以達到安全可信賴的資訊社會願景。
- 日本於情報處理推進機構(IPA)下設置ISEC作為專門負責推動資訊技術的發展，其中也包含IT Security之相關計畫，如電腦病毒、入侵、與密碼學技術等。
- 中國大陸於國家信息中心設網路安全部，負責信息安全發展規劃和戰略研究、大型安全工程建設與管理、資訊安全技術標準化、資訊安全仲介服務、資訊資源開發、及安全技術服務。

叁、台灣現況分析

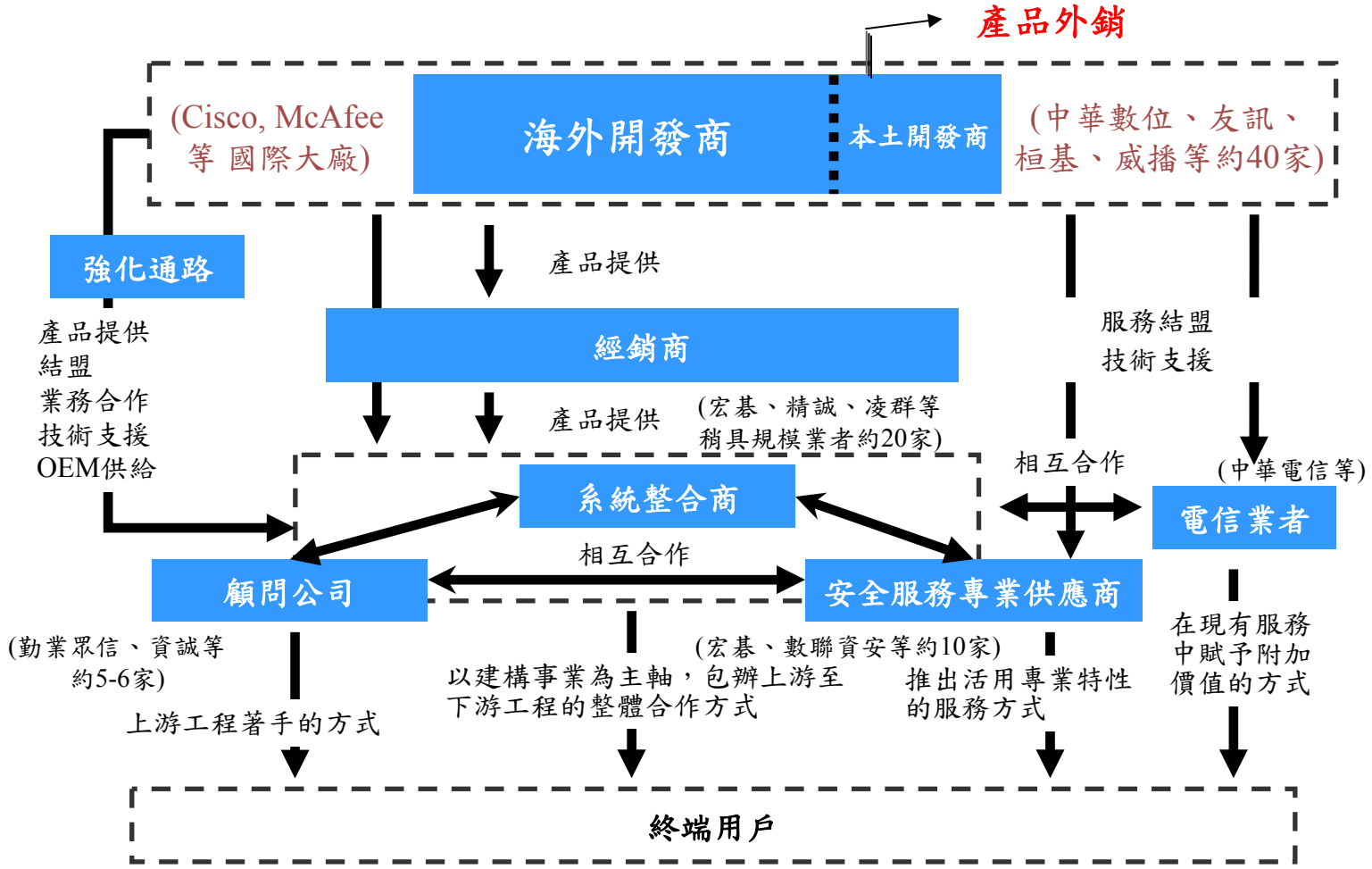
台灣資安服務與資安產品市場規模



- **台灣資安本土市場(含產品及服務)約140億台幣，本土廠商約佔1/3**
- **台灣本土資安廠商資安產品外銷金額約10億**
- **資安產品包含資安軟體、資安專屬硬體(Firewall/UTM)**

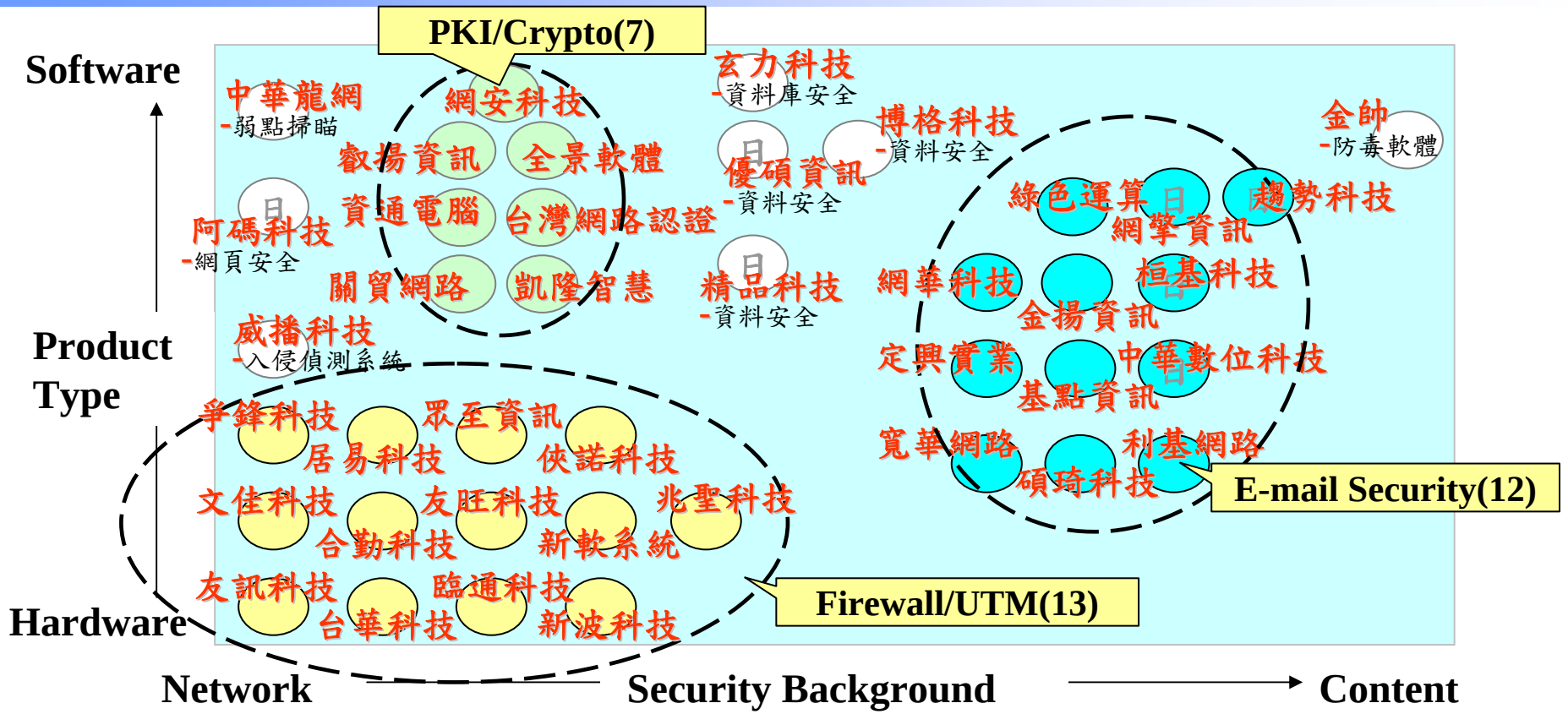
台灣資安市場生態

國內市場所需原生產品大都來自海外，本土約40家業者僅佔小部份，其規模普遍較小，研發及國際市場拓展能力不足。



資料來源：資策會MIC，2008年11月

資安產品本土開發商分析



- 台灣資安產業仍植基於台灣特有優勢，如結合網通設備硬體優勢的防火牆/UTM；雙位元語系的E-mail Security及學界研發成果的PKI/Crypto加解密等產品為主
- 可針對這些特色產品及趨勢發展， 並掌握對岸特有攻擊類型，研發台灣資安及進軍國際所需新興技術以提升產品價值及競爭力

備註1：本圖羅列41家台灣本土資安產品業者，不包含外商以及資安代理與服務業者
備註2：圈圈內的「日」代表產品有外銷至日本市場
資料來源：資策會MIC，2009年6月

台灣資安業者的內外銷困難與瓶頸

- **內銷方面**
  - 台灣本土市場有限，且完全開放，本土廠商須與外商知名品牌競爭
  - 本土廠商規模偏小，行銷資源不足，且SMB資安預算有限，故仍以大型企業為主
  - 大型企業重品牌信賴度，偏好外商資安產品，本土產品僅能爭得少數機會
- **外銷方面**
  - 國際行銷費用高昂，且須長期耕耘才能建立知名度
  - 資安產品須提供安裝設定及後續更新、維護服務，須建立在地化服務能量，本土廠商無力承擔
  - 資安產品相當須倚賴通路服務能量，廠商欠缺品牌，導致對通路議價能力低，難以獲利
  - 資安強調信賴安心，而非價格競爭，台廠規模偏小且品牌知名度低，無法取得客戶信賴，難與國際品牌競爭
- **總體問題**
  - 資安必須長期累積技術與快速演進，目前國內業者能量不易投資資安攻防研發與道德駭客養成
  - 我國廠商多單打獨鬥，難以自主發展資安整體解決方案，不易與國際知名廠商競爭

台灣資安環境現況

- 資安相關法規推動現況
  - 「電腦處理個人資料保護法修正草案」正在立法院審議當中
  - 「濫發商業電子郵件管理條例」立法院要求NCC與相關單位繼續協商後再重新提出
  - HIPAA、沙賓法案(SOX)目前尚沒有台灣版本的草擬
- 資安分級制度僅規範需建置哪類型資安防禦功能
  - 目前資安分級規範事項僅要求各機關建置各類型資安產品以確保防禦縱深，但未具體進一步規範所採用的資安產品應符合什麼樣的原則或標準，如資安產品原產地、 資安產品認證等
  - 大陸將資訊系統安全保護分為五級，並限定某些等級以上的機關必須採用中國大陸資安廠商的產品
- 資安國際認證規範龐雜，本土廠商規模偏小，難以全盤接受
  - 國際流通的共同準則(CC, Common Criteria)認證項目多且難，所需費用亦高，國內業者難以負擔，恐反造成國際品牌長驅直入

台灣資安技術研發現況

技術類別	主要學研投入	已建立重點技術
威脅管理 （FW,IDP/IPS,UTM..）	台科大、成大、清大、國防大學、中央、資策會	-入侵偵測平台 (IDEAs) -模擬驗測平台 (TWISC@Testbed) -IDS防禦力探析 (IDS Probing) -URL及網頁過濾 (WAF)
內容安全 (Botnet detect, Anti-Virus/Malware, Email Security..)	中山、成大、交大、台大、台科大、國防大學、大同、資策會	-異常IRC流量分析 -惡意軟體行為基本分析
弱點管理 (VA Scan, Pen Test, SIEM/SOC, Source Code Security..)	台大、中山、中研院、國防大學、資策會	- 源碼安全檢測 - 網路安全檢測系統(SAS) - 網路安全診測平台(CVS)
行動安全 (Mobile Protection/ Privacy, Wireless Security..)	交大、 中原、 中央、工研院	- 安全無線模擬驗測 (SWOON) - WiFi無線滲透
身份辨識與存取管理 (PKI, AAA)	成大、台科大、電信研究所	- 電子投票 (e-Vote) - 國家憑證中心

研發資源 (千元)	95	96	97	98
學界 (NSC Fund)	171,101	193,186	169,557	106,521
法人 (NSC&MOEA Fund)	74,333		72,529	72,480

台灣資安產業發展機會

- **雲端服務新興資安需求**：雲端服務多層次技術架構與動態融合應用，衍生更多資安威脅與需求，台灣業者可早期佈局，並藉此帶動上下游協力朝大型化發展
- **行動安全重要性提升**：行動應用安全威脅遽增，而我國行動應用及產品產業體系有良好基礎，可切入此一新興市場機會
- **網通業者雄厚基礎**：我國擁有資通訊硬體開發優勢，並已有防火牆/UTM等軟硬整合產品，未來可發展Web應用層防禦等高階功能，提高產品附加價值
- **特殊攻擊模式領先掌握**：
  - 我國處於敏感的政經情勢，較歐美業者更能掌握特殊資安攻擊模式，可發展利基之資安產品
  - 具雙位元語系優勢，搭配Email郵件過濾產品基礎，發展惡意軟體安全過濾產品，強化產業競爭力

肆、發展策略與行動方案

願景與目標

發展願景

1.配合iTaiwan計畫，滿足重點應用資安需求

2.發展創新資安技術，帶動產業成長與新契機

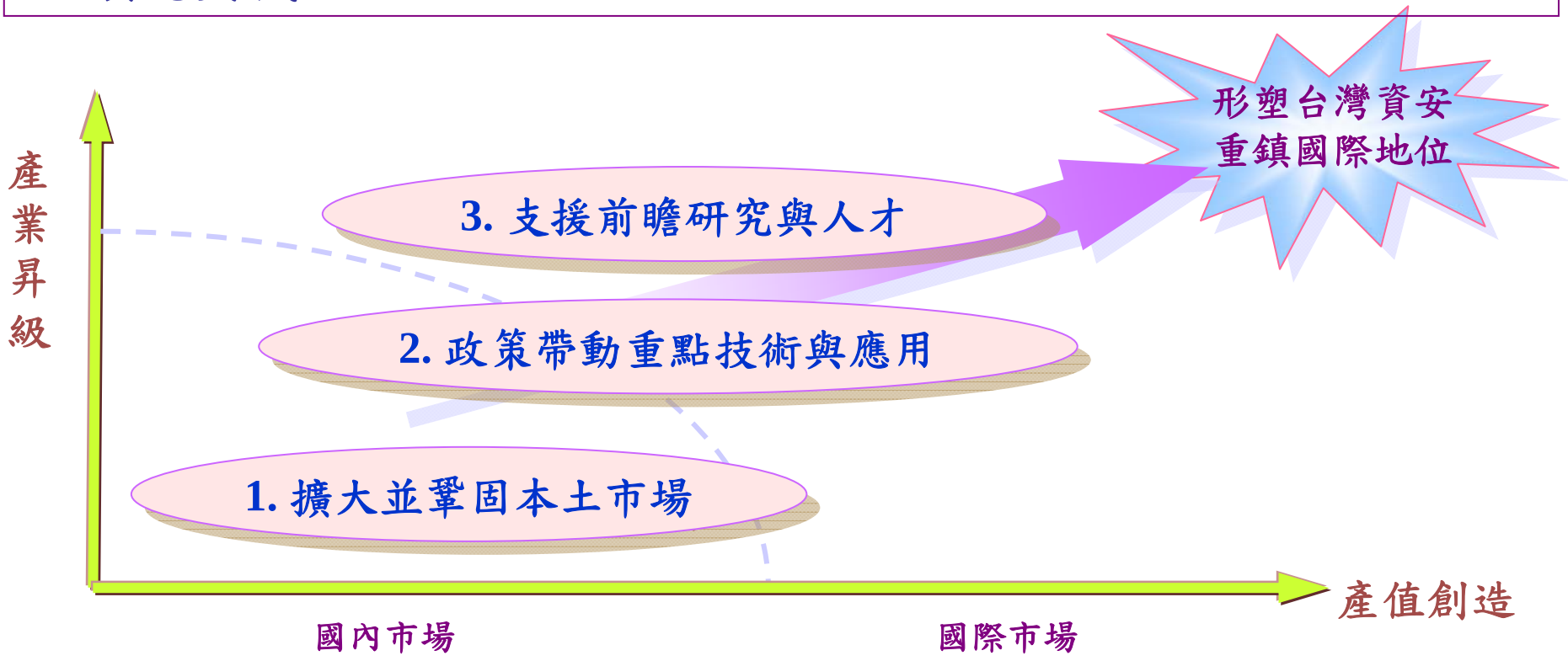
目標

- 促進五年內我國資安核心產值達300億台幣，衍生資安關聯產品產值達1,700億*
- 推動至少一項雲端服務為主的大型資安重點應用

*衍生資安關聯產品為內含資安功能的各種網路設備及終端產品等

發展資安產業之策略思維

- 擴大並鞏固本土市場，壯大我國資安產業及提升市場佔有率
- 政策帶動重點技術與應用，發展應用為導向之技術產品，強化我國資安水準及產業國際競爭力
- 支援前瞻研究與人才，早期佈局資安次世代研發，為產業創造領先契機



策略一、擴大並鞏固本土市場

- 建議措施：
  - 成立資安產業推動計畫，以利國內產業推動發展 (工業局)
  - 善用我國產業優勢(如工業電腦、網通、IC設計等)，以各種政策工具及獎勵補助措施，鼓勵廠商發展嵌入式資安產品 (工業局、技術處)
  - 在不違反GPA規定下，鼓勵公家機關優先採購本土資安解決方案，同時創造環境的使用經驗，為外銷創造參考案例 (工程會、工業局)
  - 結合智慧台灣計畫，鼓勵業者採用本土資安解決方案 (交通部、內政部、經濟部、研考會、文建會...)
  - 以產業輔導方式協助業者取得國際標準認驗證，促其與國際市場接軌 (工業局)

行動方案－輔導產業發展資安產品並進行應用導入

- **行動重點**
  - 結合安全產業推動計畫，進行資通訊安全產品開發與應用導入，建立應用輔導與補助機制
  - 因應智慧台灣資安需求，導入行動商務、數位內容等領域之資訊安全應用
  - 運用以軟扶硬、硬帶軟策略，協助廠商發展軟硬整合標竿產品並進軍國際市場
- **效益指標**
  - 完成至少十項資安產品開發或行動商務、數位內容等產業之資通訊安全加值應用輔導案例
  - 完成至少二項軟硬整合資通訊安全標竿產品開發，並促成一項標竿產品進軍國際市場
- **預計投入經費**

年度	99	100	101	102
額度(仟元)	96,000	96,000	96,000	96,000

策略二、政策帶動重點技術與應用

- 建議措施：
  - 投入資源以推動行動應用與雲端(Cloud Computing)服務為主軸之資安關鍵技術研發，支援新興應用需求 (技術處)
  - 藉由資安計畫以結合國內資服大廠，運用所研發之關鍵技術發展雲端服務資安平台 (技術處、工業局、國科會)
  - 吸引國外大廠來台，成立資安技術研究/測試中心(技術處)
  - 運用i236計畫之智慧小鎮(Smart Town)與智慧經貿園區(i-Park)應用環境，提供本土資安解決方案之焠煉發展場域 (技術處)
  - 以旗艦模式促成重點廠商結盟或整併，並切入國際市場 (技術處、工業局)

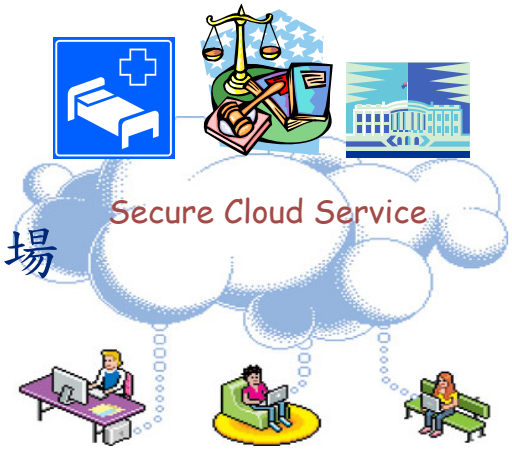
行動方案－發展雲端資安技術搶攻市場先機

- **行動重點**

1. 運用科專資源研發雲端服務資安關鍵技術
   - 雲端應用層安全防禦：針對雲端Web動態融合應用，發展應用層內容過濾與防禦技術
   - 雲端服務平台安全管理：以雲端服務平台系統安全為主軸，發展整合之監控管理解決方案
2. 運用所發展之技術導入大型資安重點應用，並以資安高需求之領域為優先

- **效益指標**

– 完成二個雲端服務所需之資安技術平台
– 達成至少一個大型重點資安應用導入
– 促成至少二項自主技術資安產品/服務進軍國際市場



- **預計投入經費**

年度	99	100	101	102
額度(仟元)	151,719	152,000	160,000	160,000

策略三、支援前瞻研究與人才

- 建議措施：
  - 鼓勵學術發展及營運先進資安虛擬攻防平台，以強化國內研發成果的可應用性及競爭優勢(國科會)
  - 鼓勵學術發展資安驗證/測試基礎技術，並提供驗測專業服務 (國科會)
  - 依據產業發展政策，導引學術進行前瞻資安技術研發，並培育資安技術人才(國科會)
  - 成立TWISC產學研聯盟，加強產學研合作，以加速研發成果之產業價值創造時程(國科會)
  - 強化TWISC學術社群的國際合作/價值創造/服務營運能量，並提高其自主營運能力(國科會)

行動方案－落實資安前瞻研究與人才長期佈局

- **行動重點**
  1. 藉資訊安全虛擬攻防，演練與研發新型攻擊/惡意程式產生攻擊與防禦之軟體技術，創造產業領先契機
  2. 導引學術研發資安驗證/測試技術，研發多層面與真實網路流量測試技術，並提供Web線上檢測服務，以保障資安產品品質與使用者之資訊與通訊安全
  3. 運用學術資源，佈局雲端/行動/普及計算先進資安技術研發，並培育資安產業高階技術人才
  4. 建立跨國合作交流平台，培植具國際水準技術團隊
  5. 成立TWISC產學研聯盟，落實學術研發成果，提昇產業競爭力
- **預計投入經費**

年度	99	100	101	102
額度(仟元)	200,000	210,000	220,000	230,000

伍、討論題綱

- 臺灣資安業者規模較小，如何協助及促成廠商朝大型化發展以利進軍國際市場?
  - 藉助政策工具輔導協助廠商持續發展資安解決方案
  - 透過新一代資安平台應用促成業者結盟及成長
  - 引進國際大廠來台技術合作成立業界研發/測試中心
- 為加強資安技術與專業人才培育，是否推動以社群為基礎的全球資安虛擬戰場?
  - 整合我國既有學術研發能量，依據產業需求培養專業人才
  - 建置資安攻防演練平台，測試與研發新型攻擊與防禦技術
- 為使資安業者及早因應國內市場需求，是否協助其掌握未來五年政府資安規畫方向?
  - 透過國家資通安全會報之資安諮詢小組溝通平台，讓產業界預先了解政府單位中長期資安規劃方向
- 為提升我國資安水準及市場需求，是否推動上櫃、市企業於公司治理範圍內納入資安要求?

附　錄

科顧組6/26業界研討會相關意見回應(1/2)

業界意見	部會	回應作法
仿效國外對資安產業的各項保護措施，適用促產條例投資抵減。而WTO針對國家安全、文化等需求是有例外的，建議工程會委託專家進行研究，例如，美國在國家安全方面的採購即有許多例外，可供參考。	經濟部、工程會	●經濟部現有之促產條例已適用於資安業者 ●針對國家特殊考量需求採用本土產品之情形，工程會主張在不違反GPA規定下由各機關自行認定以例外案例處理，鼓勵公家機關優先採購國產品。 (詳請參閱『策略1』)
整合國內資安軟硬體功能，發展自有產品及技術，共同拓展國際市場。而對於國內市場的擴充，應思考本土廠商的機會所在。	經濟部、國科會	●將擴大投入資源支持研發單位及業者自主開發資安技術產品，並藉助網通硬體優勢，以政策輔助工具鼓勵發展軟硬體整合利基產品，並促其運用既有通路切入國際市場(詳請參閱『策略1』之『行動方案 』) ●針對雲端服務及行動安全等新興資安需求，協助我國業界早期佈局相關技術研發及重點應用導入，以搶攻新一波市場機會。（詳請參閱『策略2』及其『行動方案』）
供需世界，沒有市場就沒有人才，資安產業在產品技術之外，另一項非常有價值的是專業人才的軟實力，目前安全領域台灣所培育出來的顧問專家依然領先，可在擴大內需（如建SOC）的同時，藉由經驗累積，建立專業團隊，並配合資訊科技服務行銷國際。	經濟部、國科會	●將擴大資安基礎及關鍵技術研發，培植專業技術人才，並藉由重點資安建設及應用，引導產學研合作並累積經驗，進一步建立具國際水準之專業團隊。（詳請參閱『策略3 』之『行動方案』）

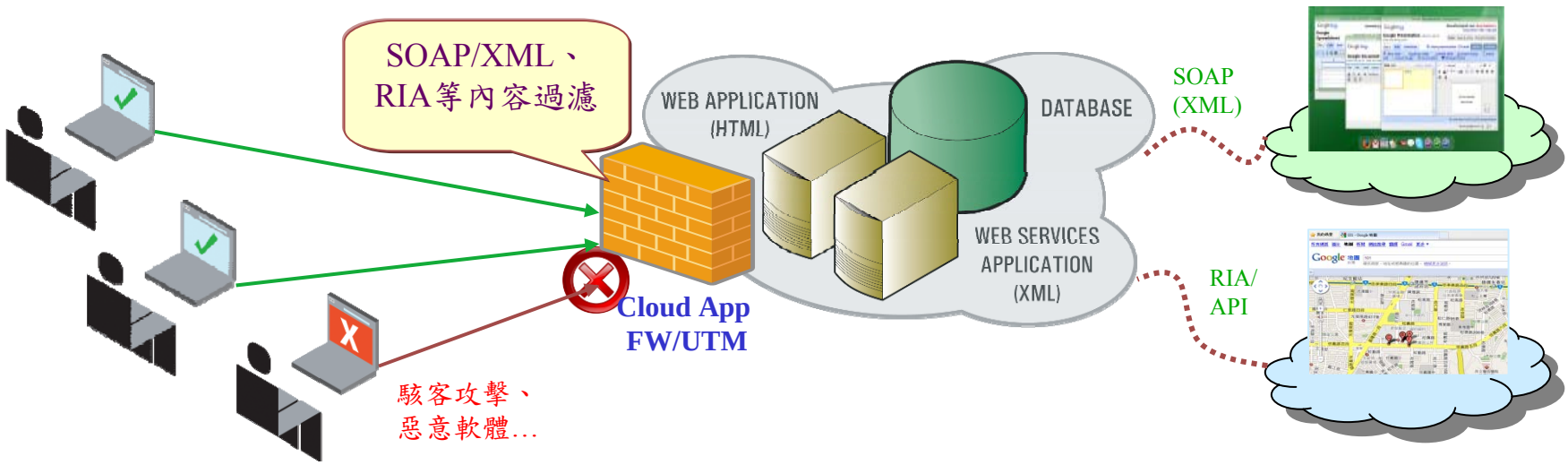
科顧組6/26業界研討會相關意見回應(2/2)

業界意見	部會	回應作法
扶持及輔導資安業者技術發展並提供相對之補助措施。	經濟部	●成立資安產業專責推動計畫，增列經費資源並運用政策輔助及專案措施，積極扶持及輔導資安業者。(詳請參閱『策略1』)
舉辦全國性資安技術交流/論壇及競賽，並搭配後續誘因（如獎金、就業機會等），以強化對於資安之重視。	國科會、研考會、經濟部	●藉由TWISC及其他相關資安交流平台，擴大辦理國內外技術交流，並吸引國際知名資安活動來台舉辦。。（詳請參閱『策略3』） ●藉助國內每年金盾獎等資安競賽活動，主動發掘優秀人才媒合就業機會。
建議本次SRB會後能設立專責單位主導產業輔導事宜。	經濟部	●將規劃成立資安產業推動之專責單位，以利SRB相關規劃之推動落實。（詳請參閱『策略1』）
DNS Security是目前發展趨勢之一，美國將會投入許多資源，此係Open Standard，估料將有龐大商機，建議業者可朝此方向努力。	NCC、國科會、經濟部	●DNS Security發展大都可藉助現有資安技術領域，然涉及Infrastructure運作及網域管理之改變，仍須進一步評估策定。 ●將鼓勵業者早期佈局DNS Security 所需之相容產品，以利未來可搶佔市場商機。

雲端應用層安全防禦技術發展構想

雲端應用層安全防禦：針對雲端Web動態融合應用，發展所需之應用層內容過濾與防禦技術

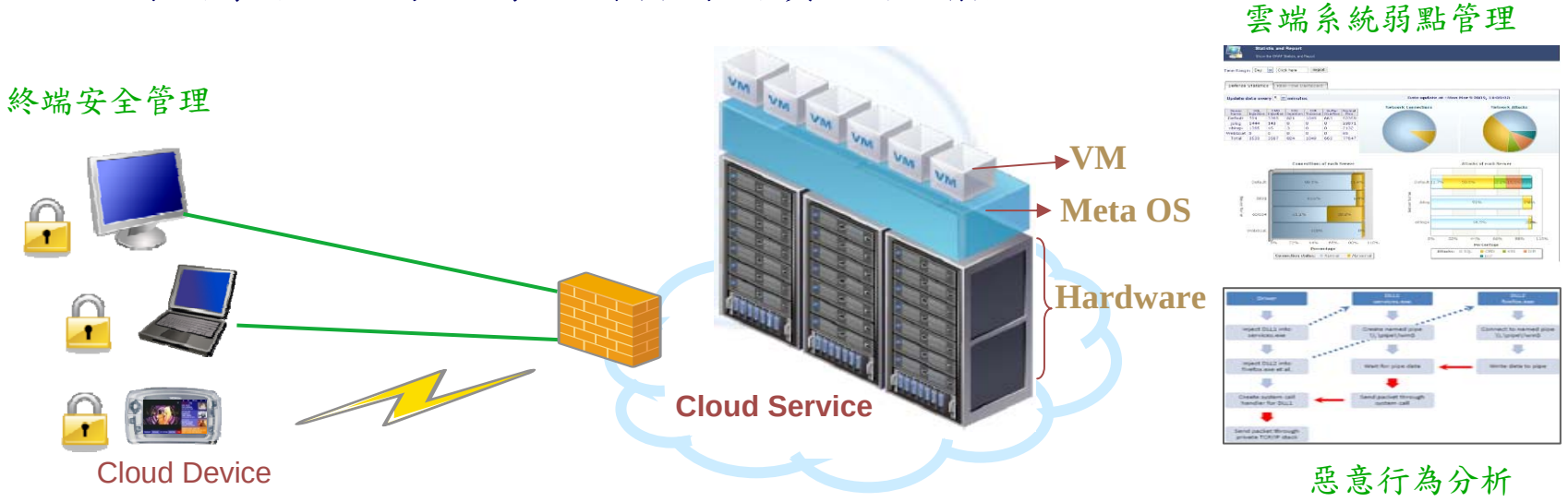
- **關鍵技術：**
  - 高效能Web App封包（XML, RIA）深層過濾，攔阻不當Web封包
  - Web DB存取行為監控，建構Web資安縱深防禦
  - Behavior Based惡意軟體閘道偵測，有效攔截各種新型惡意軟體
- **目標產品：**
  - 帶動網通廠商投入雲端應用防禦產品（如Cloud App Firewall/UTM等）開發
  - 協助郵件過濾業者，發展惡意軟體雲端閘道過濾產品，提升市場價值



雲端服務平台安全管理技術發展構想

雲端服務平台安全管理：以雲端服務平台系統安全為主軸，發展整合之監控管理解決方案

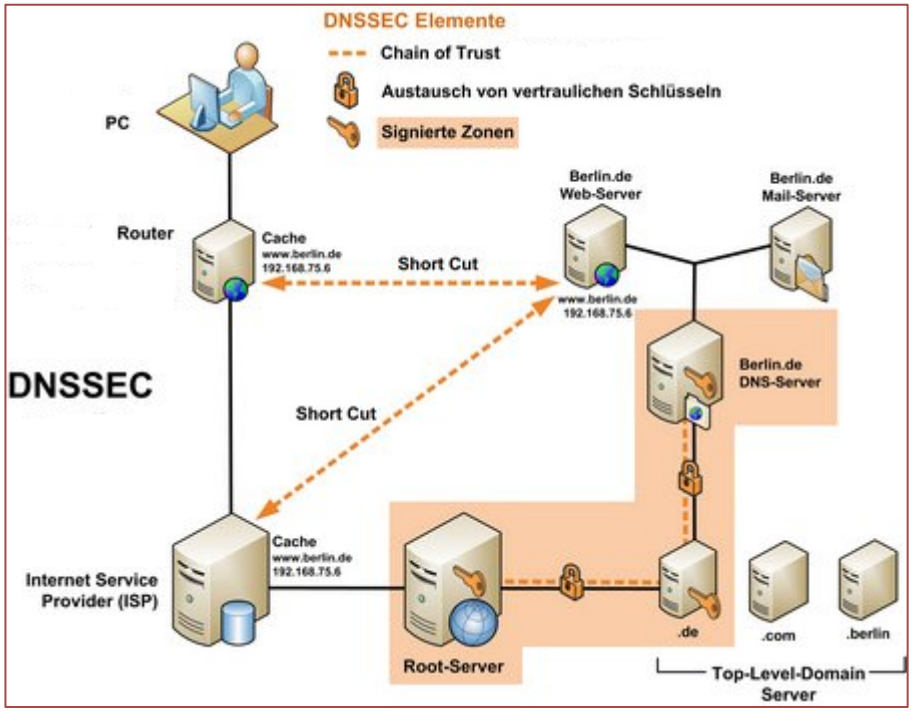
- **關鍵技術：**
  - 雲端系統弱點診測監控，提供資安健診以減少漏洞風險
  - 雲端服務平台資安事件分析，強化SOC資安事件分析與鑑識
  - 終端裝置安全管理，支援行動安全、隱私保護及終端防護
- **目標產品：**
  - 帶動業者建立監控分析技術，並發展Security as a Service相關產品/服務
  - 促進行動裝置/服務廠商，開發行動資安相關產品



網域名稱安全(DNSSEC)技術與現況

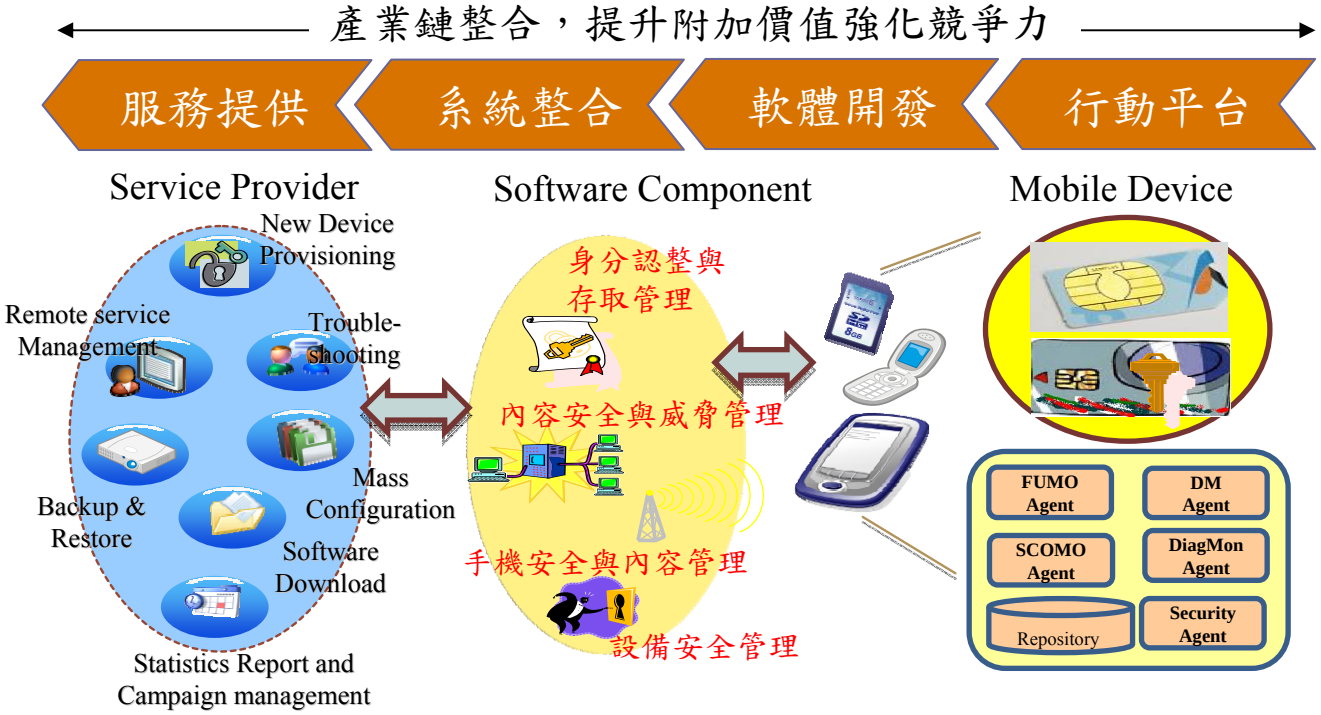
- 背景：DNSSEC（DNS Security Extension ）為確保DNS網名解析的真實與完整性 ，遏止因DNS伺服器被擾亂，致使用者被導引到惡意網站而蒙受損害。
- 技術概念：透過PKI簽章與驗證技術，確保網域伺服器從頂層網域到底層網域名整個解析過程紀錄是經過簽章的。
- 導入時程：美國政府已預定所有.gov網域必須在2009年12月之前全面部署DNSSec，而.org則是預定從2009年1月起分階段推展。

- 技術現況：相關技術已經成熟，Windows Server 2003/ 2008 R2均已經內建，且相關工具與套件可免費下載。(http://www.dnssec.net/software)
- 標準：DNSSEC Intro RFC (RFC 4033) 、DNSSEC Records RFC (RFC 4034) 、DNSSEC Protocol RFC (RFC 4035) 、DNSSEC NSEC3 RFC (RFC 5155) 、DNSSEC + EPP RFC (RFC 4310)
- 挑戰：技術均已成熟，在推廣上亟需建立DNSSec保護網名的註冊管理與認證核准機制。



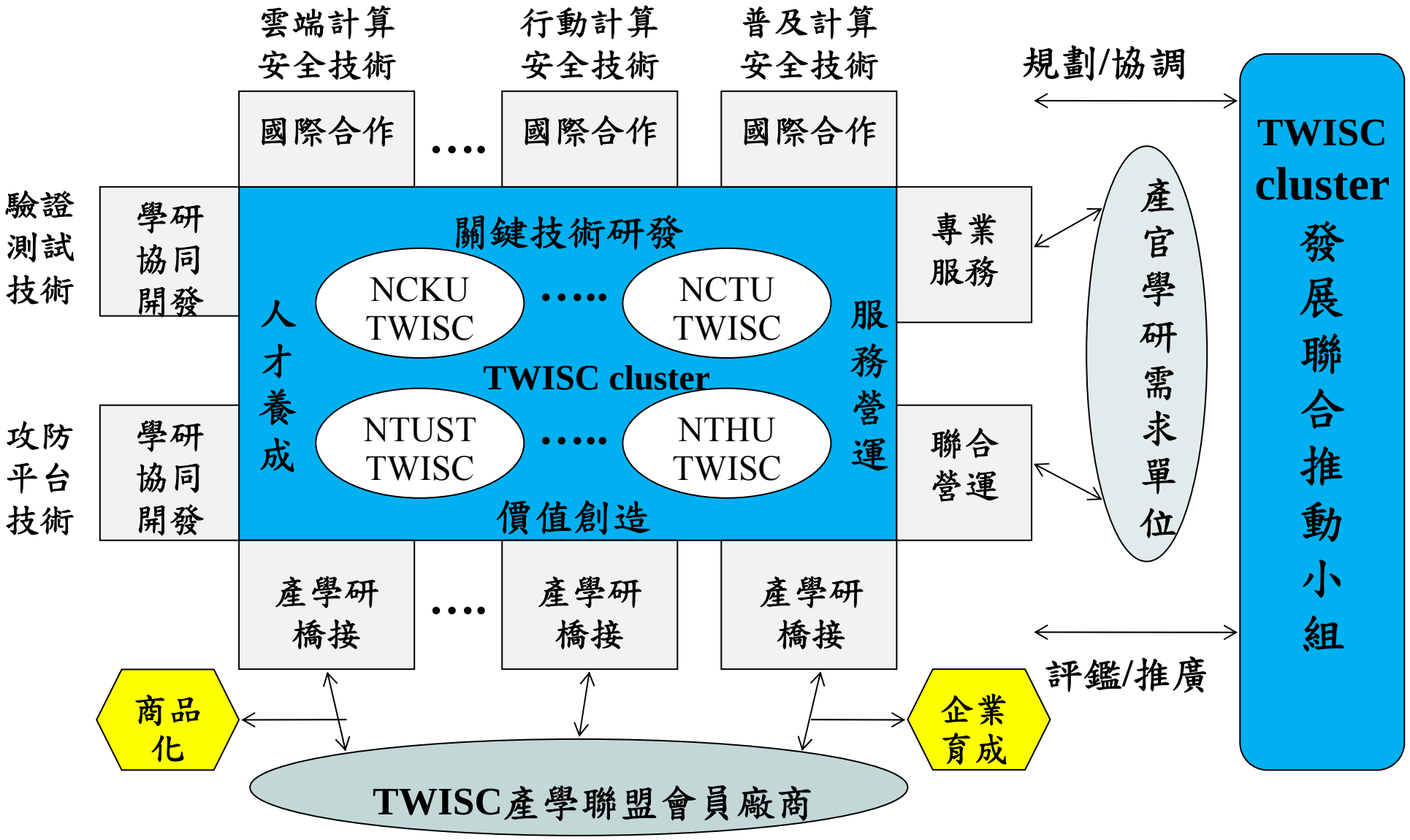
行動資安推動構想

- 優勢新興產業：國內在智慧型手機設計與製造上已具備優勢，2008年出貨逾5,000萬支，全球出貨近3分之1
- 發展機會：全球手機安全市場規模持續增長，展望至2011年，全球手機安全市場將以36.3%之CAGR大幅成長
- 策略作法：以新興行動終端、行動應用服務等之發展所需之資通訊安全技術為出發，藉由優勢之行動終端設計與製造產業，整合行動終端業者、資安系統整合廠商，建立整體解決方案，國內試煉並進行國際行銷



落實資安前瞻研究與人才長期佈局(1/6)

前瞻資安科技研究推動架構



落實資安前瞻研究與人才長期佈局(2/6)

- 規劃暨推動學術社群在雲端/行動/普及計算先進資安技術研發路程，並培育資安高階技術人才
- 協助TWISC社群推動前瞻資安技術國際合作計畫
- 成立TWISC產學研聯盟，強化橋接、產學研合作機制，加速落實學術研發成果之產業價值
- 建構TWISC社群自主營運，爭取多元資源的能力

落實資安前瞻研究與人才長期佈局(3/6)

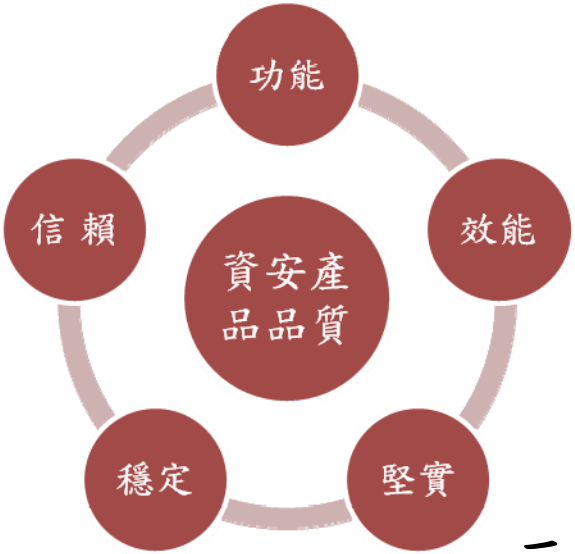
建立驗證/測試技術服務能量

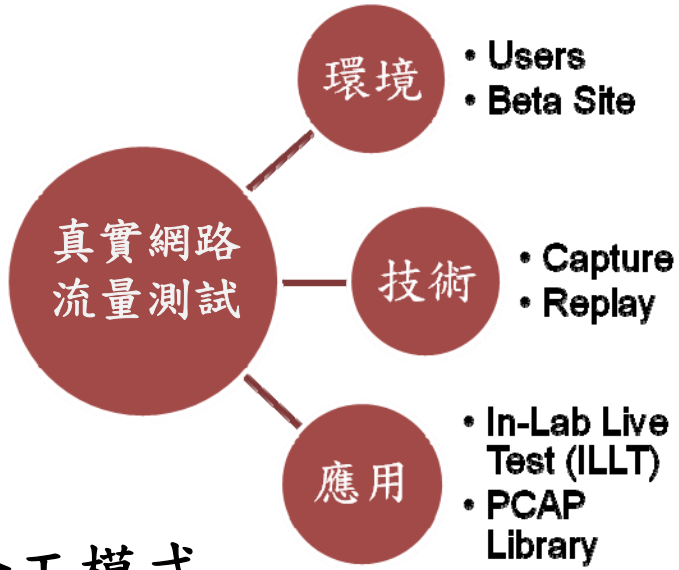
- 行動方針：
  - 運用學術資源研發進行資安產品驗證/測試服務
  - 多層面測試以保障資安產品品質與使用者之資訊與通訊安全
  - 研發真實網路流量測試技術以及開發客製化測試工具
- 效益指標：
  - 輔導學術界成立國內之資安驗證/測試實驗室，提供測試服務以提升國內整體研發能量與技術水準
  - 發展真實環境測試及除錯系統，減少產品的問題發生，進而降低成本與商譽的損失，以協助國內廠商進軍高階市場
  - 開發客製化測試工具，降低廠商投資硬體設備之開發的成本並提高產品開發時程

落實資安前瞻研究與人才長期佈局(4/6)

建立驗證/測試技術服務能量

多層面資安產品測試





真實網路流量測試

三陣線分工模式

屬性	工作任務	產出
測試服務 (第一線)	1. 產品測試 2. 測試計畫之完整報告	測試報告書、認證標章
測試工具 (第二線)	1. 開發測試工具 2. 測試工具除了給第一線使用外，亦授權給廠商或與廠商共同合作開發	測試工具與使用說明文件
測試研究 (第三線)	1.測試環境上研發測試方法、技術與分析測試結果 2.研發另類產品驗證/測試機制	論文、專利

落實資安前瞻研究與人才長期佈局(5/6)

資訊安全虛擬攻防環境

- 行動方針：
  - 整合學術與研究界之資源研，發資安虛擬攻防前瞻關鍵技術
  - 藉由資安虛擬攻防演練研發反制各類駭客、惡意程式行為之機制
- 效益指標：
  - 在TWAREN與GigaPOPs建置智慧型資安攻防演練平台，提供學研界攻防演練之環境
  - 藉由攻防演練擴大收集各類駭客、惡意程式行為樣本，提出防制之機制
  - 同步與產業界進行技術交流，強化產品功能性與市場競爭力
  - 積極參與國際資訊安全相關研究與進行交流，以收集並掌握先進研究資訊

落實資安前瞻研究與人才長期佈局(6/6)

資訊安全虛擬攻防環境演練架構