網路智慧新臺灣政策白皮書

基礎環境構面_子題三：網路資安隱私

行政院資通安全辦公室彙整

中華民國104年3月2日

大綱

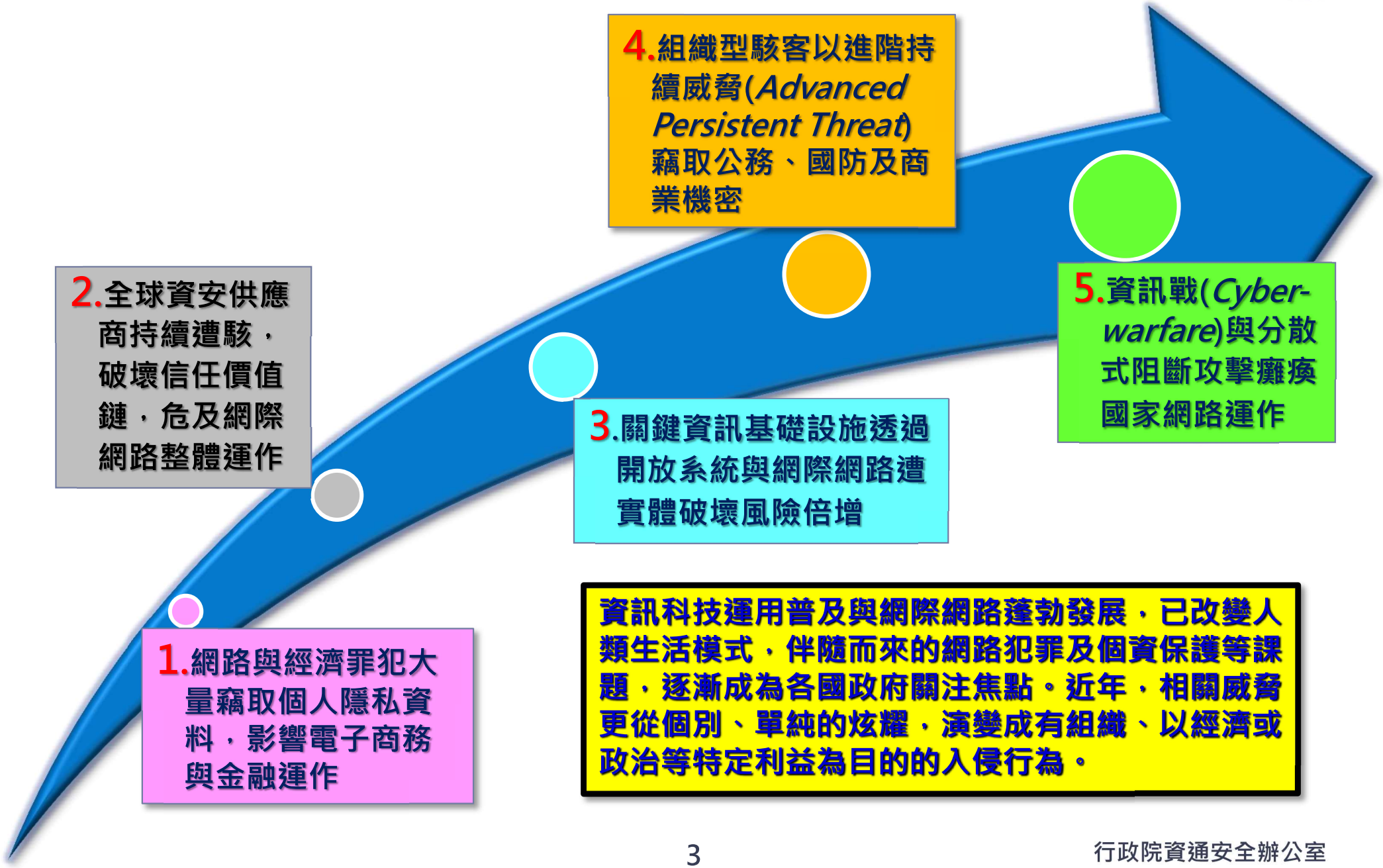
一、背景說明

二、國際發展趨勢

三、國內現況與檢討

四、政府作為

背景說明 - 網路五大資安威脅



資訊科技運用普及與網際網路蓬勃發展，已改變人類生活模式，伴隨而來的網路犯罪及個資保護等課題，逐漸成為各國政府關注焦點。近年，相關威脅更從個別、單純的炫耀，演變成有組織、以經濟或政治等特定利益為目的的入侵行為。

背景說明 - 網路資安隱私相關議題

本土資安業者在技術上的掌握度與國際大廠相比尚具競爭力，惟行銷能力、國際化能力、通路與售後服務等方面較不及國際大廠。

新版個資法於2010年5月26日公布、2012年10月1日實施，企業為避免因資料外洩而遭求償或刑罰，已提高對資安防護的重視。

資安人員必須隨時充實專業知識以因應新的威脅情勢。政府正思考從「課程」、「平臺」、「競賽」、「實習」及「產學合作」等主軸擴大資安科研人才培育。

隨著網路科技進步，歹徒犯罪手法與管道亦不斷翻新，而網路犯罪常涉及跨部會合作，共同研商網路犯罪偵防相關政策與重要業務之推動。

國際發展趨勢 - OECD資安策略面向

- **經濟合作與開發組織(OECD)) ：**
  - 1992年即針對資訊系統發布安全指引，隨著網際網路的興起，2002年該指引加入了網路安全，成為全球各經濟體提出國家資安政策之依據。
  - 2012年參考10個OECD會員國(包括澳洲、加拿大、芬蘭、法國、德國、日本、荷蘭、西班牙、英國及美國)的國家層級資安策略，針對新一代策略基本原理(Rationale) 、範圍(scope)、主要概念、管理結構及行動方案(Action Plans)進行研究與改版。
  - 根據其研究結果，世界各國在制定國家層級的資安策略都朝向整合且全面性的方向思考，涵蓋經濟、社會、教育、法律、執法、技術、外交、軍事及情報等相關的面向。
  - 此外主權(Sovereignty)的概念也越來越重要。各國的資安策略多圍繞著四大概念，分別是：
    - 政府溝通協調(Government co-ordination)
    - 公私合作協同關係(Public-Private Partnerships)
    - 國際合作(International co-operation)
    - 強調尊重基本價值，例如隱私、言論自由及資訊自由流通。

OECD
BETTER POLICIES FOR BETTER LIVES

國際發展趨勢 - APEC資安政策

- 亞太經濟合作組織(APEC)：
  - APEC為一極富彈性的經貿論壇，其決策過程係以「共識決」（Consensus）及「自願性」（Voluntary）為原則，經由各成員間相互尊重及開放性政策對話達成尋求區域內共享經濟繁榮之目標。
  - APEC的策略主要環繞三大支柱（Pillars）：貿易與投資自由化、貿易與投資便捷化、以及經濟與技術合作（ECOTECH）。除自由化、開放之外，透過便捷化的工作，可以減少貿易投資成本，間接促成自由化；透過經濟與技術合作，可以幫助開發中經濟體建構能力，從而提高參與自由化的能力，因此，三支柱彼此相輔相成。
  - 2012年APEC與OECD合作，透過共同檢視OECD在2002年發布的資訊系統與網路安全指引與APEC在2005年發布的確保信任、安全及持續的線上環境策略，來重新思考在網路經濟下各經濟體如何有效制定政策來管理資安風險並面對新興的網路威脅與挑戰。

Asia-Pacific Economic Cooperation

國際發展趨勢 - 歐盟資安策略實務指引

•歐盟(EU)：

– 歐盟的歐洲網路及資訊安全局(European Network and Information Security Agency，以下簡稱ENISA)有感於國際上對如何制定國家層級的資安策略尚缺乏普遍的共識，在2012年透過問卷的方式了解歐盟與非歐盟國家制定與執行國家層級資安策略的方式。

– 經過分析比較後，將OECD與ENISA提出的國家安全策略，綜整了1份發展與執行國家資安策略的實務指引。

– 該文件除了建議資安策略應有的項目外，也針對這些項目如何實施與設定關鍵效能指標(Key Performance Indictor)提出了建議。

– 參照歐盟實務指引有關我國待補強之部分

  ➢ 建構國家層級風險評估

  ➢ 建立國家層級的網路與通訊應變計畫

  ➢ 供應鍊安全相關議題

  ➢ 發展網路國防軍事能量

國際發展趨勢 - 美國資安研發與推動策略

- 美國(US)：
  - 美國國家網際安全倡議：
    - 2008年1月依據布希總統的第54號總統指令(NSPD-54)與第23號國土安全總統指令(HSPD-23)所制定。此倡議擘劃了美國整體的網際安全發展目標，並影響了國土安全部與國家安全局等機關的發展方向，因此可說是美國最重要的資安上位策略。
    - 2008年布希總統簽署此倡議時本倡議是列為機密文件，但在2010年3月歐巴馬總統將部分文件解密。
  - 資安研發與推動策略：
    - 美國訂有網路與資訊技術研發計畫(The Networking and Information Technology and Development Program, NITRD Program)。該計畫授權聯邦政府可以針對網路與資訊技術研發設定目標、投資優先順序及跨部會協調。
    - 網路與資訊技術研發計畫目前年度預算高達40億美金，其中約有8億美金為資安基礎與應用研究經費，特別是安全軟體方面的研究。

國際發展趨勢 - 各國加強資安人才培育

國家	專業人才培育
	• 英國「政府通訊總部」（GCHQ）授權六所大學提供網路安全碩士學位，訓練新一代的網路間諜和網路安全專家 • GCHQ授權「道德駭客」課程，學習防禦網攻
	• 韓國政府推展 BoB（Best of the Best）菁英計畫，延攬世界頂尖駭客指導韓國的資安菁英 • 首爾大學設有資安系，400餘學校有資安社團
	• 日本行政法人「資訊處理推進機構」（IPA）2004年起舉辦「駭客菁英教育」培育活動，選拔大學生及高中生，培育能夠對抗網站駭客的人才

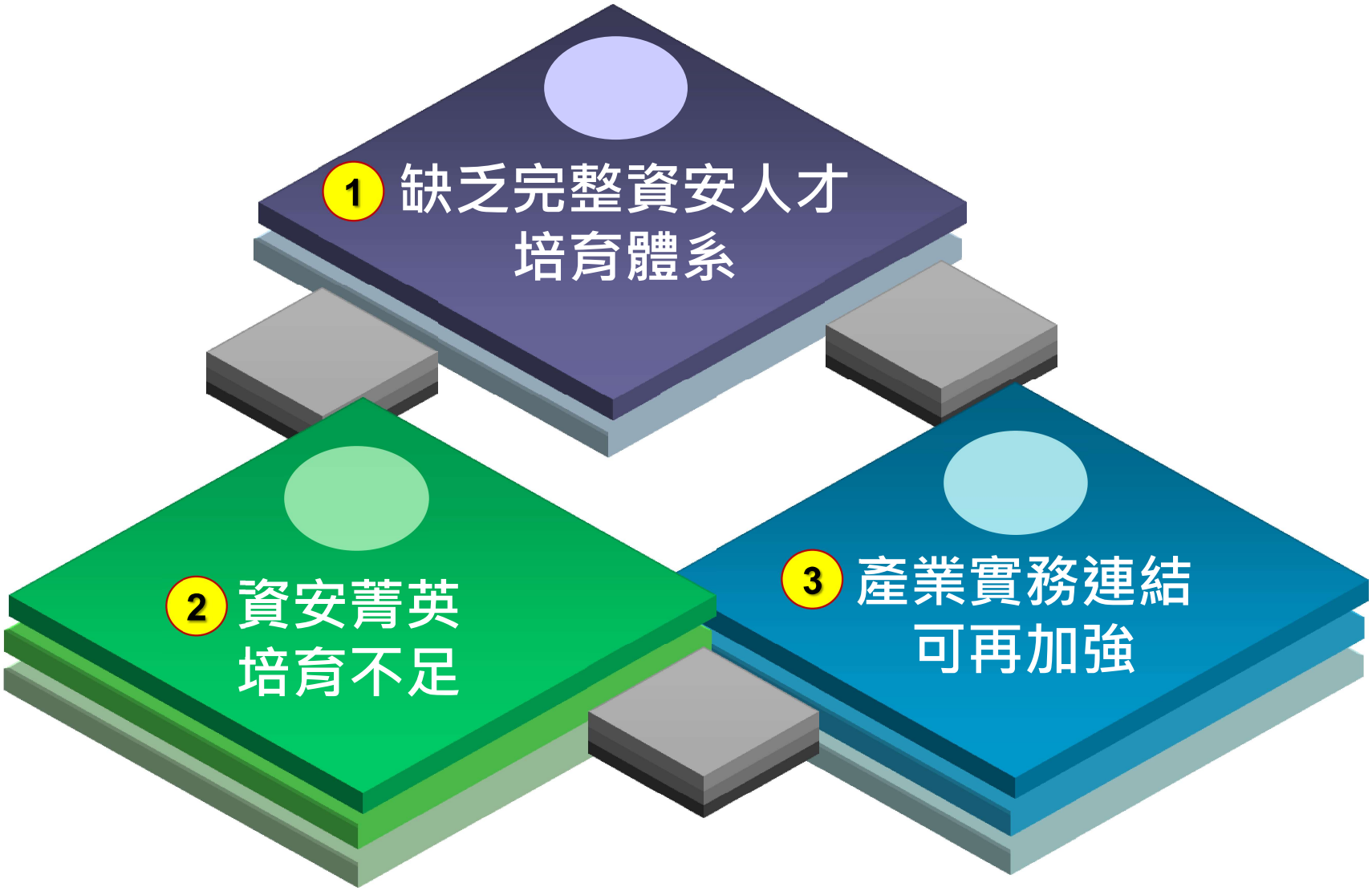
國際發展趨勢 - 跨國網路犯罪問題

- 目前世界各國在打擊網路犯罪上都面臨相當大的挑戰，犯罪者常利用境外網站或跨國網路業者提供之服務進行犯罪，因重要線索留存異地，若無邦交關係或簽訂司法互助協議(定)，常無法透過跨境取得犯罪者行蹤。
- 各國執法機關因有各自的法律規定，加上世界潮流之人權觀念對於個人資料保護愈趨嚴謹，常無法進行聯合或即時犯罪調查等網路犯罪偵防互動，造成案件懸宕。

國內現況與檢討-資安產業發展

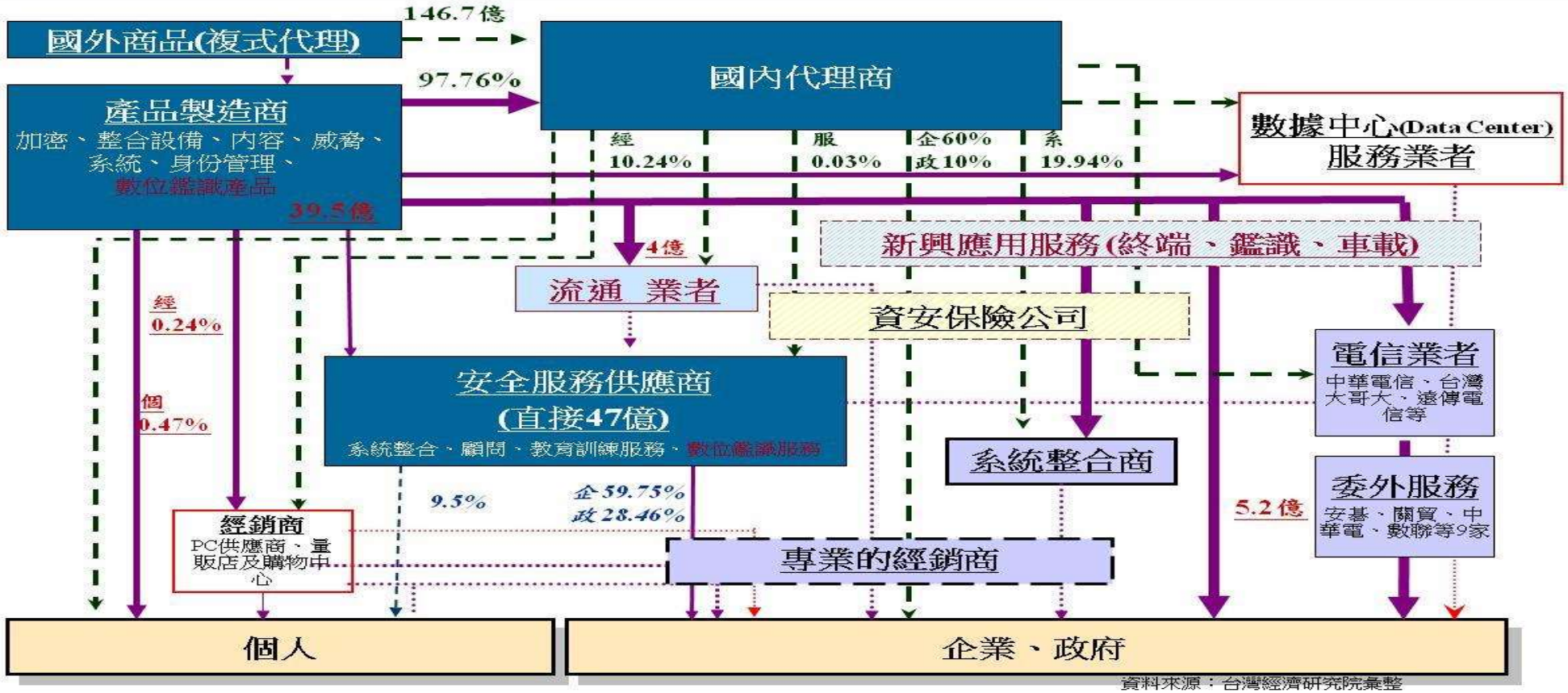
優勢（Strengths; S）	劣勢（Weaknesses; W）
1. 資通訊產業發達，具完整產業鏈及研發環境。 2. 擁有高素質人力，具創新性且對新科技接受度高。 3. 積極投入智慧行動、Big Data及雲端應用領域。	1. 應用程式存在許多漏洞，資安事件頻傳，駭客手法防不勝防。 2. 資安關鍵技術為先進國家所掌握，不易突破。 3. 缺乏系統化資安人才培育規劃。
機會（Opportunities; O）	**威脅（Threats; T）**
1. 在資安事件蔓延、法令規範效應下國內外資安產業市場顯著成長。 2. 隱私權與智慧財產權保護議題漸受重視，且個資法業已施行。 3. 公私部門持續強化資安協同合作。	1. 駭客手法日益精進，且已轉為組織型犯罪，資安威脅大增。 2. 先進國家積極投入資安科技研發及人才培育。 3. 資安資訊分析分享機制未盡完善。

國內現況與檢討 - 資安人才培育



國內現況與檢討 - 資安產品應用

- 在國內產品製造商方面： 2013年國內自行研發產值約39.5億元，近98%委由國內代理商經營，絕大部分透過資安服務業及流通業作加值服務；顯見國內自行研發資安產品銷售管道由多元轉為集中代理制度，系統整合商擔任供需橋樑的角色逐漸被取代。
- 在複式代理方面：國外進口代理規模約147.6億元，銷售管道主要為直接銷售至企業與政府部門，大企業和政府部門對於國外產品的使用比率高於國內產品。

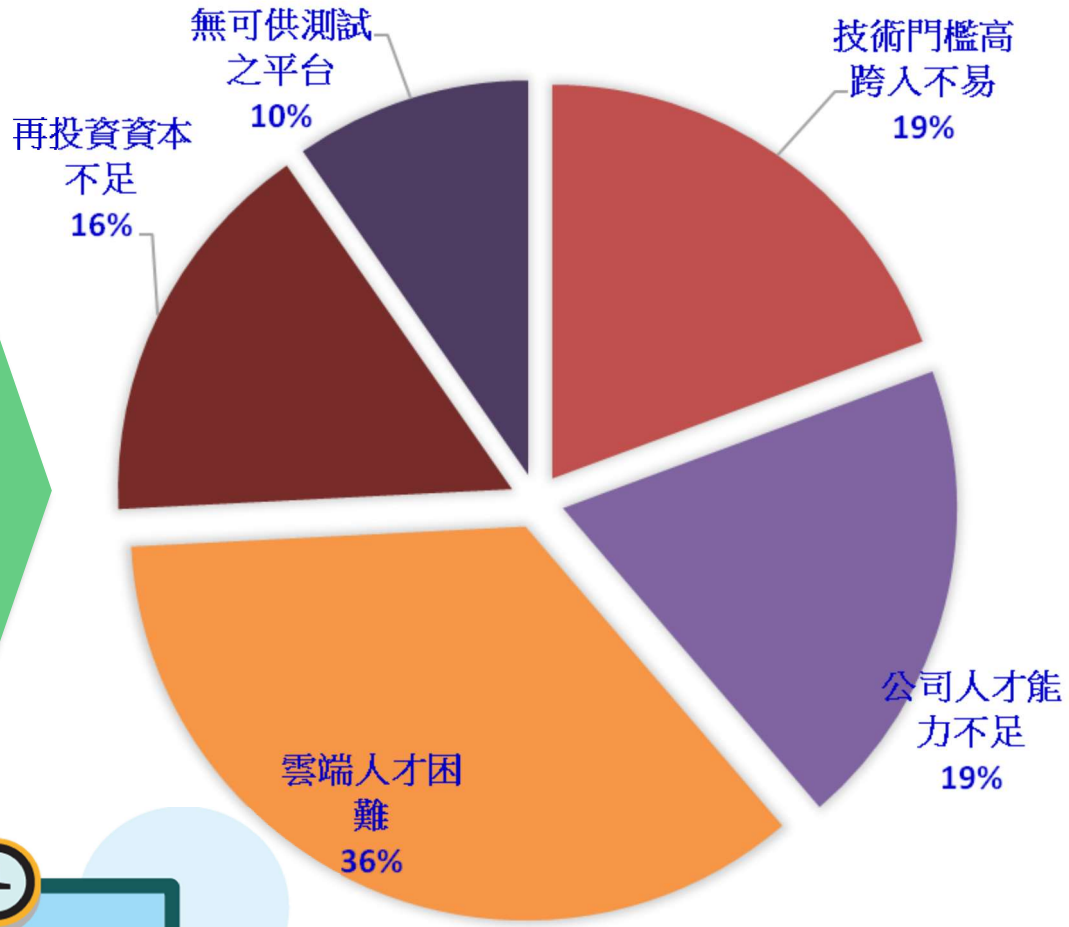


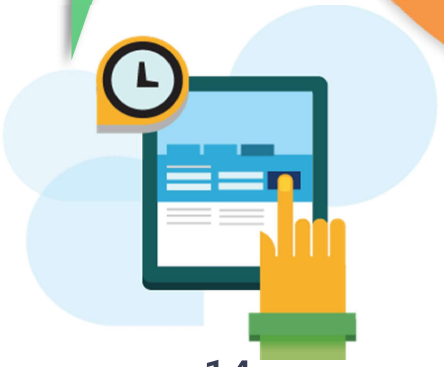
資料來源：台灣經濟研究院彙整

國內現況與檢討 - 產業發展困難原因

- 目前企業對於資安產業發展困難之主要原因為招募人才不易
- 其次為資安產業再投資資本不足

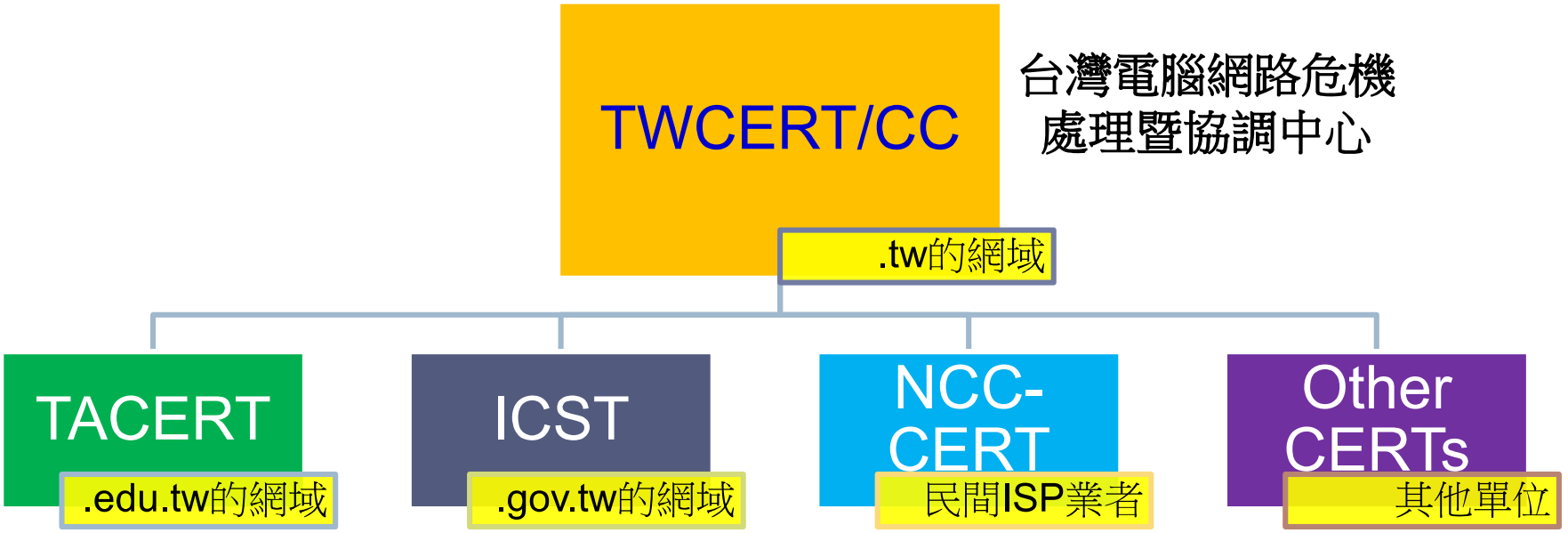
主要發展困難





資料來源：台經院103年調查報告

國內現況與檢討 - 我國CERT分工



目前臺灣CERTs的分工是以ISP(Internet Service Provider)來做責任範圍的劃分。

- TACERT負責臺灣學術網路(TANet)
- TWNCERT負責政府單位(GSN)
- NCC-CERT負責民間ISP業者
- 其他特殊機構，例如：國防、金融機構、關鍵基礎設施維運等單位則由專責單位負責。

國內現況與檢討 - 網路犯罪防治(1/2)

跨境犯罪問題 來源追查困難	• 警方追查IP多為VPN（虛擬私有網路）、跳板或境外IP，常造成偵查人員無法繼續追查相關涉嫌人。
網路業者資安 防護機制薄弱	• 業者對於網路帳號密碼控管及個人資料防護薄弱，民眾個人資料遭竊取後即易遭利用或成為被害案件。
巨量網路資料 不易解譯分析	• 各種調查犯罪資料來源廣泛，仍須透過資料探勘技術與分析軟體輔助，強化案件追查能力，以找出破案關鍵。

國內現況與檢討 - 網路犯罪防治(2/2)

•成立跨部會協商平臺會議

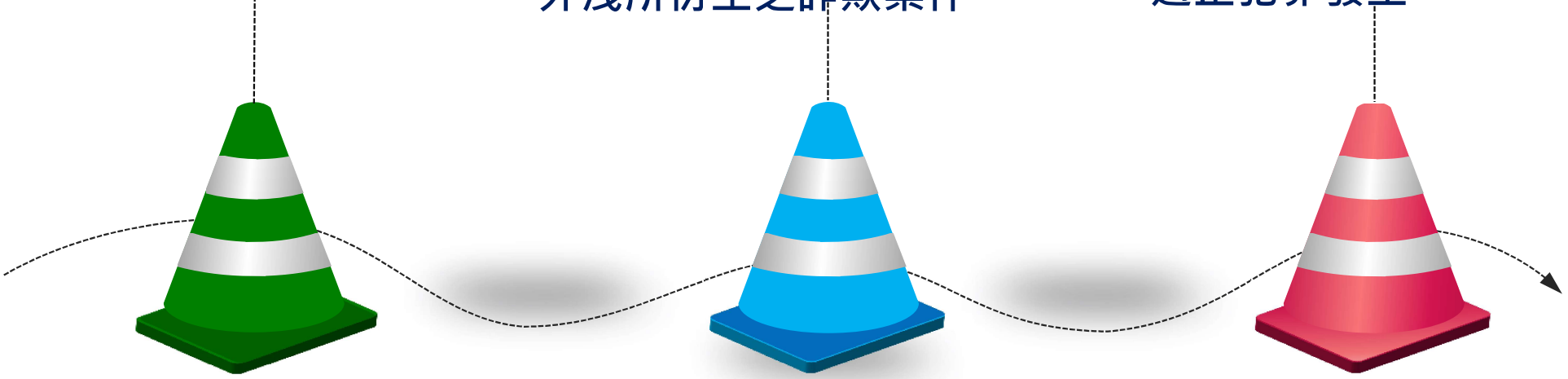
由內政部召集，每3個月定期邀集法務部、通傳會、經濟部、金管會及科技部等相關部會，共同研商網路犯罪偵防相關政策與重要業務之推動。

•要求國內網路平臺業者協助防治網路犯罪

內政部警政署（刑事警察局）自98年10月起，特與相關網路業者成立「防制網路詐欺工作小組」，促請網路業者加強網站安全控管及使用者個人資料保護，以有效降低個人資料外洩所衍生之詐欺案件。

•持續推動跨境合作查緝網路犯罪

近年來內政部警政署與大陸及東南亞等國，透過共同合作打擊跨境犯罪機制，持續打擊電信網路詐欺等犯罪案件，未來將持續深化兩岸暨香港、澳門共同打擊跨境犯罪合作平臺，遏止犯罪發生。



政府作為 -
推廣網路隱私保護，加強資安人才培育

政府作為 -
發展資安自主技術，提升產業競爭力

• 法制環境

法律未全面實施

1995年「電腦處理個人資料保護法」施行時，規範對象並未包括電子商務業

↓

法律部分實施

2010年法務部與經濟部完成協商，**指定「無店面零售業」適用電腦處理個人資料保護法**

↓

個人資料保護法施行

2010年4月立法院三讀通過新版個人資料保護法，新法並自2012年10月起正式施行

↓

個人資料保護法及產業配套子法深化

2013年**各目的事業主管機關制定產業別個人資料檔案安全維護計畫標準辦法**

電子商務隱私安全受到重視

2009年6月行政院產業策略會議(SRB)主軸設定為資訊安全，商業司針對電子商務安全進行報告

↓

2009年12月行政院正式核定「塑造資安文化、推升資安產值」推動方案，電子商務隱私安全為子計畫之一

↓

2010年10月經濟部推動「電子商務個人資料管理制度建置計畫」，建置**臺灣個人資料保護與管理制度（TPIPAS）**。

↓

2012年起，經濟部持續**推動「電子商務個人資料管理制度推動計畫」**，辦理制度驗證、標章授證及個資管理專業人員培訓。

政府作為 -
發展資安自主技術，提升產業競爭力

104.2.4日經總統公布「電子支付機構管理條例」，提供經營第三方支付之法源依據 ，訂定相關子法時將參考電子商務經驗，適度規範業者資安配套措施

網路購物、網路拍賣興起

↓

消費者與網路商家間缺乏信任

↓

個人及小商家無法收受特定支付工具(如信用卡)

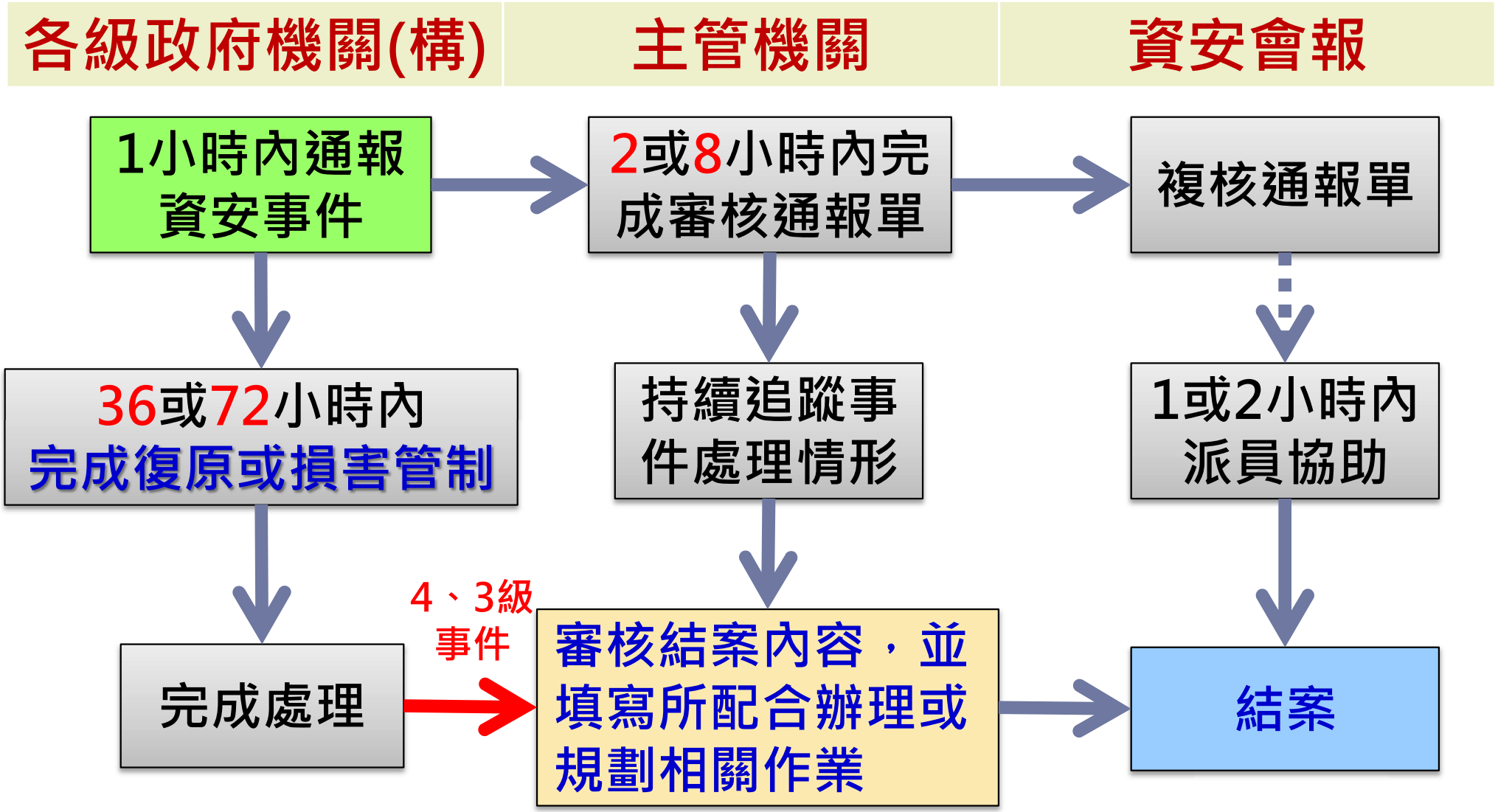
政府作為 -
發展資安自主技術，提升產業競爭力

從行動與巨量資料應用帶動產業升級

發展「ABC」策略解決行動應用安全、巨量資料隱私與雲端資安認證普及等問題，並可達到產值提升等目的

面臨問題	解決方案
研議推廣App資安認證 App Security Certification 研議發展巨量資料隱私保護機制 Big Data Privacy-Preserving 研議擴展雲端資安認證 Cloud Security Certification	•研議建構完善行動App資安環境，期能引領產業投入App安全檢測、行動個資與終端安全管理解決方案研發，進而帶動產業升級 •研議推動企業行動安全應用，進而媒合國產產品提高資安產值 •研議以龐大學術網路行為資訊為基礎，逐年透過資料安全規範與privacy-serving為基礎之資料交換機制的應用帶動產業資料間資料流通 •研議推動產業資料流通以帶動國內產業加值應用 •研議邀請產官學研參予制定符合市場之認證標準，期能擴大檢測對象，進而強化認證效益等 •研議媒合台灣雲端資安廠商進軍國際市場

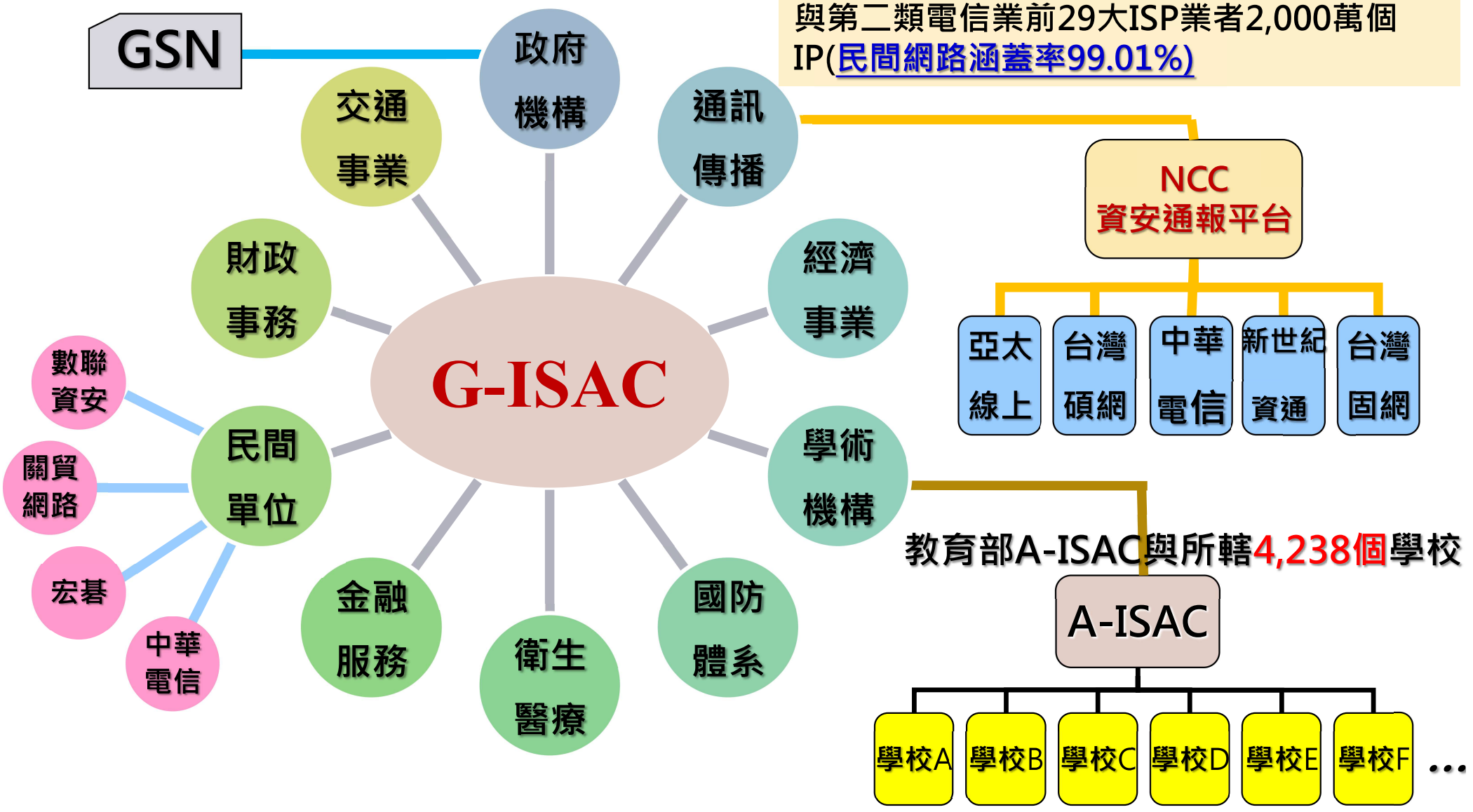
政府作為 -
強化公私協同合作，健全資安通報機制



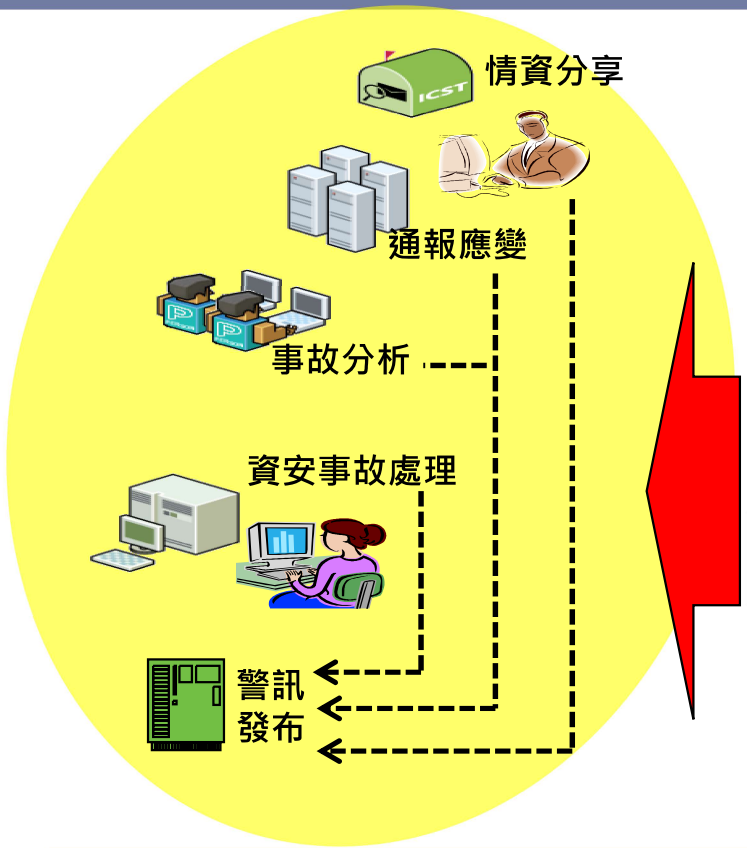
我國資安通報作業

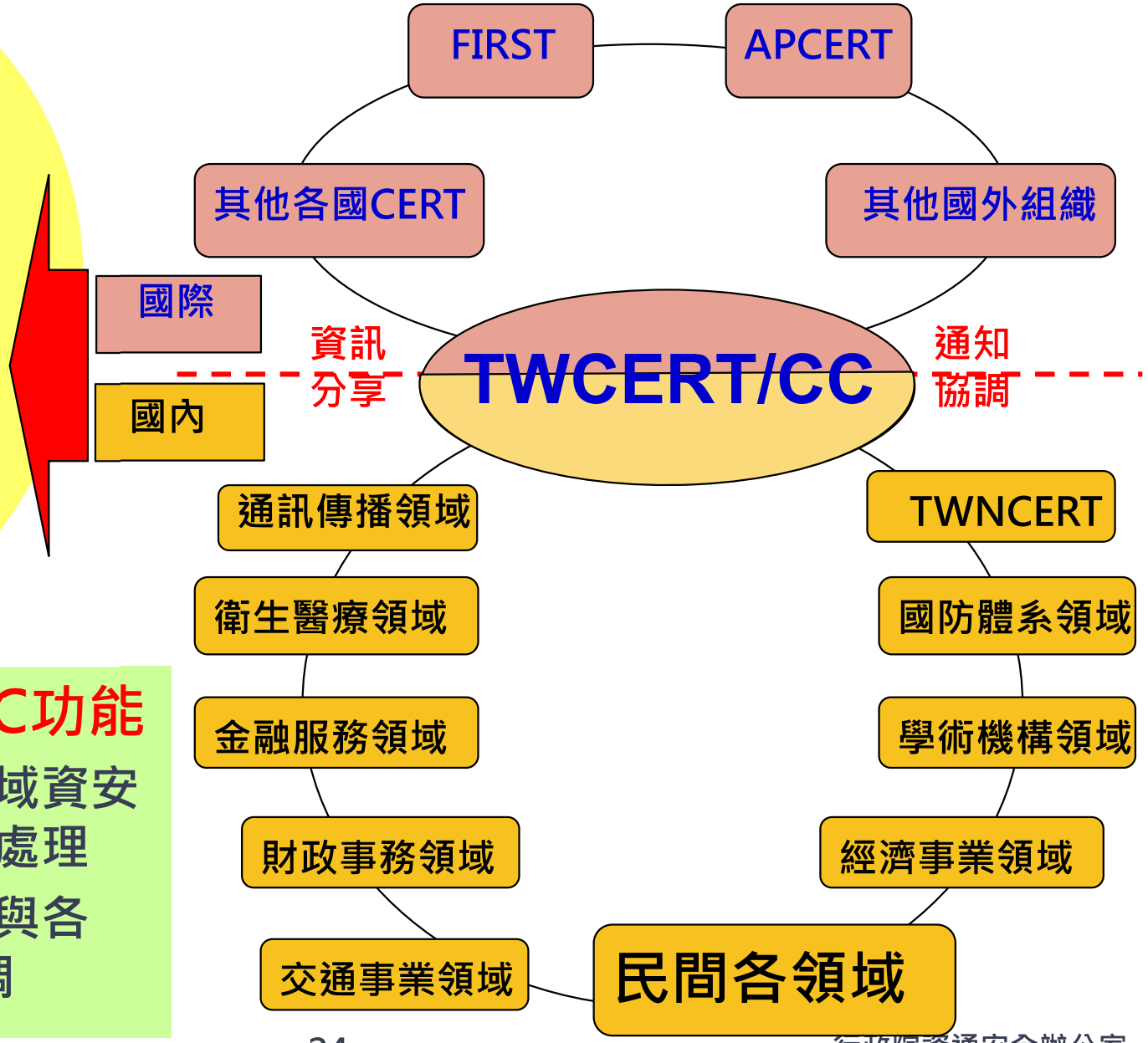
政府作為 -
強化公私協同合作，健全資安通報機制

G-ISAC範圍由GSN擴及教育體系600萬個IP與第二類電信業前29大ISP業者2,000萬個IP(民間網路涵蓋率99.01%)



政府作為 -
強化公私協同合作，健全資安通報機制





- 強化TWCERT/CC功能
  - 接收來自民間各領域資安事件通報、諮詢及處理
  - 加強國內外各領域與各CERT之溝通與協調

討論題綱

一、如何推廣網路隱私保護，加強資安人才培育?

二、如何發展資安自主技術，提升產業競爭力?

三、如何強化公私協同合作，健全資安通報機制?

報告完畢　恭請指導