我國政府資通安全現況及策進作為

行政院國家資通安全會報第27次委員會議會後記者會

行政院國家資通安全會報

104年1月22日

大綱

壹、國際資安威脅趨勢

貳、國內資安情勢及監控機制

參、政府重要施政說明

肆、後續工作重點

壹、國際資安威脅趨勢

國際資安威脅主要樣態

資訊與資安供應商持續遭駭，破壞信任價值鏈，危及網際網路整體運作

組織型駭客以進階持續威脅(Advanced Persistent Threat)竊取公務、國防及商業機密

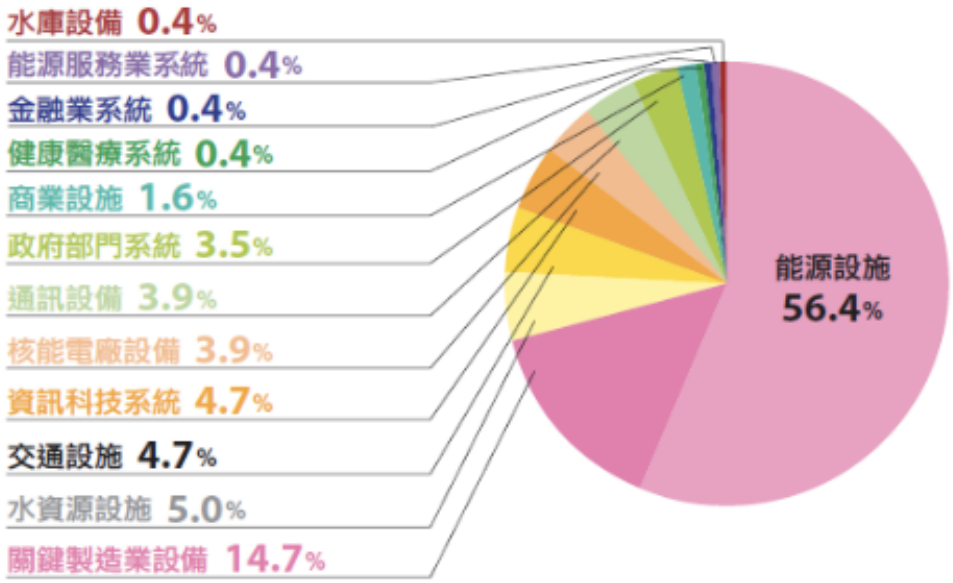
關鍵基礎設施透過開放系統與網際網路遭實體破壞風險倍增

網路與經濟罪犯大量竊取個人隱私資料，影響電子商務與金融運作

資訊戰(Cyber-warfare)與分散式阻斷攻擊癱瘓國家網路運作

關鍵基礎設施面臨威脅日增

- 2010年首次在網路上發現**專門攻擊工業控制系統的電腦蠕蟲(Stuxnet)**，感染伊朗國內 60% 個人電腦，癱瘓接近 1/5鈾濃縮工廠，估計**延緩伊朗的核武發展至少 18 到 24 個月。**
- 2013年3月20日，南韓多家電視台、銀行與保險機構遭駭客攻擊， 多達 **48,000 台**伺服器與電腦受害。
- 美國國土安全部(DHS)所屬的工業控制系統緊急應變小組(ICS-CERT)針對2013年，美國油、水、電和核能電廠等關鍵基礎建設統計：
  - 2013年遭到外部駭客攻擊的次數就高達257次
  - 其中就有一半的攻擊事件是鎖定能源設備
  - 攻擊核電廠設備的攻擊事件，一年甚至有10起之多



資料來源：美國ICS-CERT，2014年6月

國家網路運作遭癱瘓

- 於2014年 6 月中起，香港大學民意網遭大規模阻斷服務攻擊癱瘓：
  - 攻擊流量最大時，DNS反射攻擊流量每秒超過100Gbps，而NTP(Network Time Protocol)反射攻擊流量甚至更高達每秒300Gbps
- 2014上半年全球發生超過100起規模超過100Gbps的分散式阻斷攻擊。
- 2015年1月，「伊斯蘭國」(IS)支持者向法國1.9萬個網站發動攻擊，包括商業機構、宗教團體、大學等在內的19,000個法國網站，遭到伊斯蘭國支持者攻擊，主頁變成黑色伊斯蘭國旗幟，國防部網站一度無法登入。

中國網軍入侵美國防供應商

❖美參議院軍事委員會2014年9月發布調查指出：

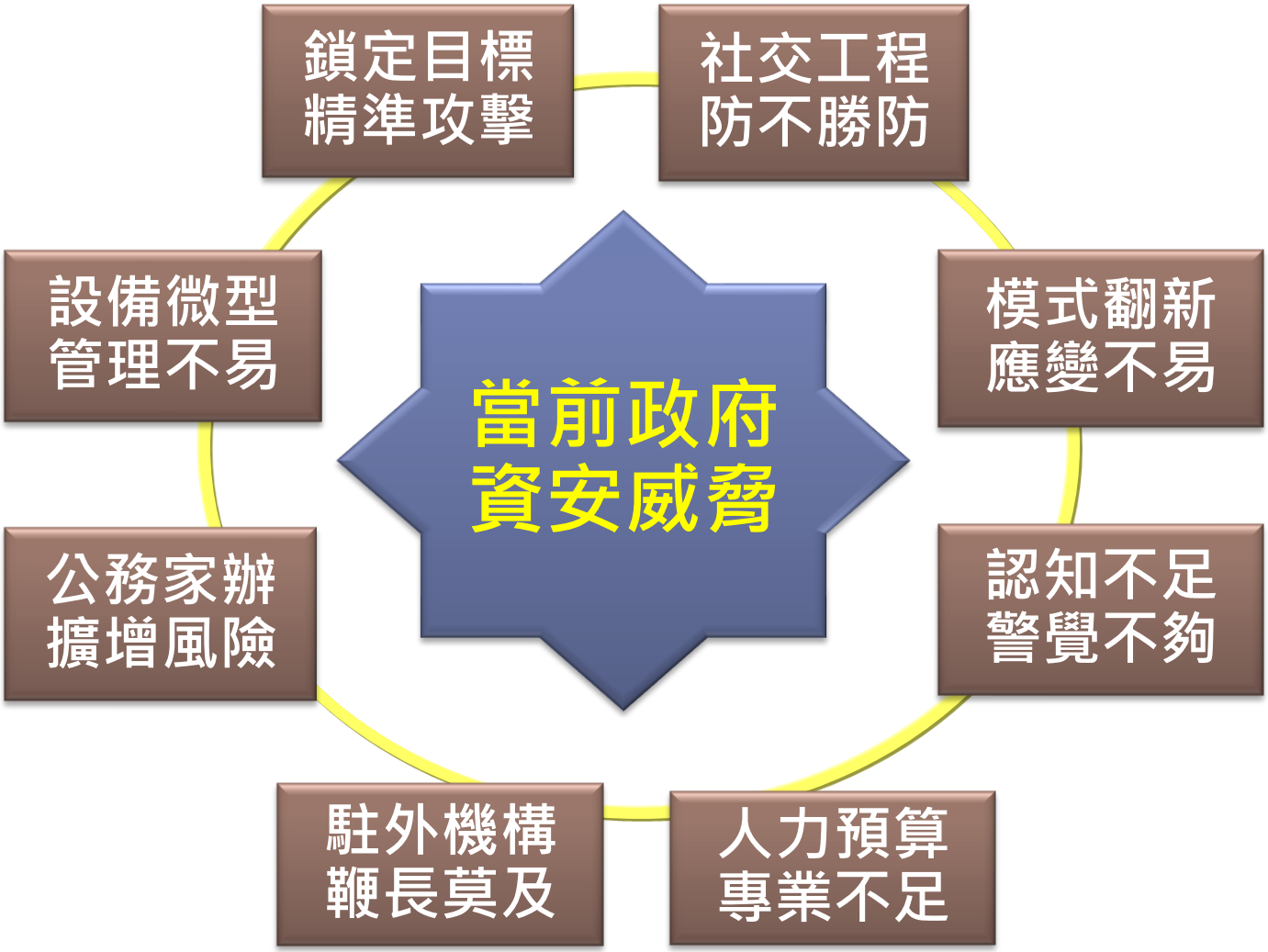
- 從2012年6月起一年的期間，在運輸司令部承包商電腦網路發生的50起資安事件中，其中20起是中國網軍的APT攻擊，運輸司令部只知悉其中2起
- 此調查顯示政府部門之間缺乏資訊分享，承包商對於通報資安事件認知不一，使得運輸司令部對於用來部署及動員軍力的電腦被駭事件在多數時候毫不知情
- 運輸司令部估計，超過90%的國防運輸部署交易在民網上執行，顯示美國軍方用來部署軍隊與設備的系統漏洞有曝露國防機密的危機

資安廠商與企業持續遭駭

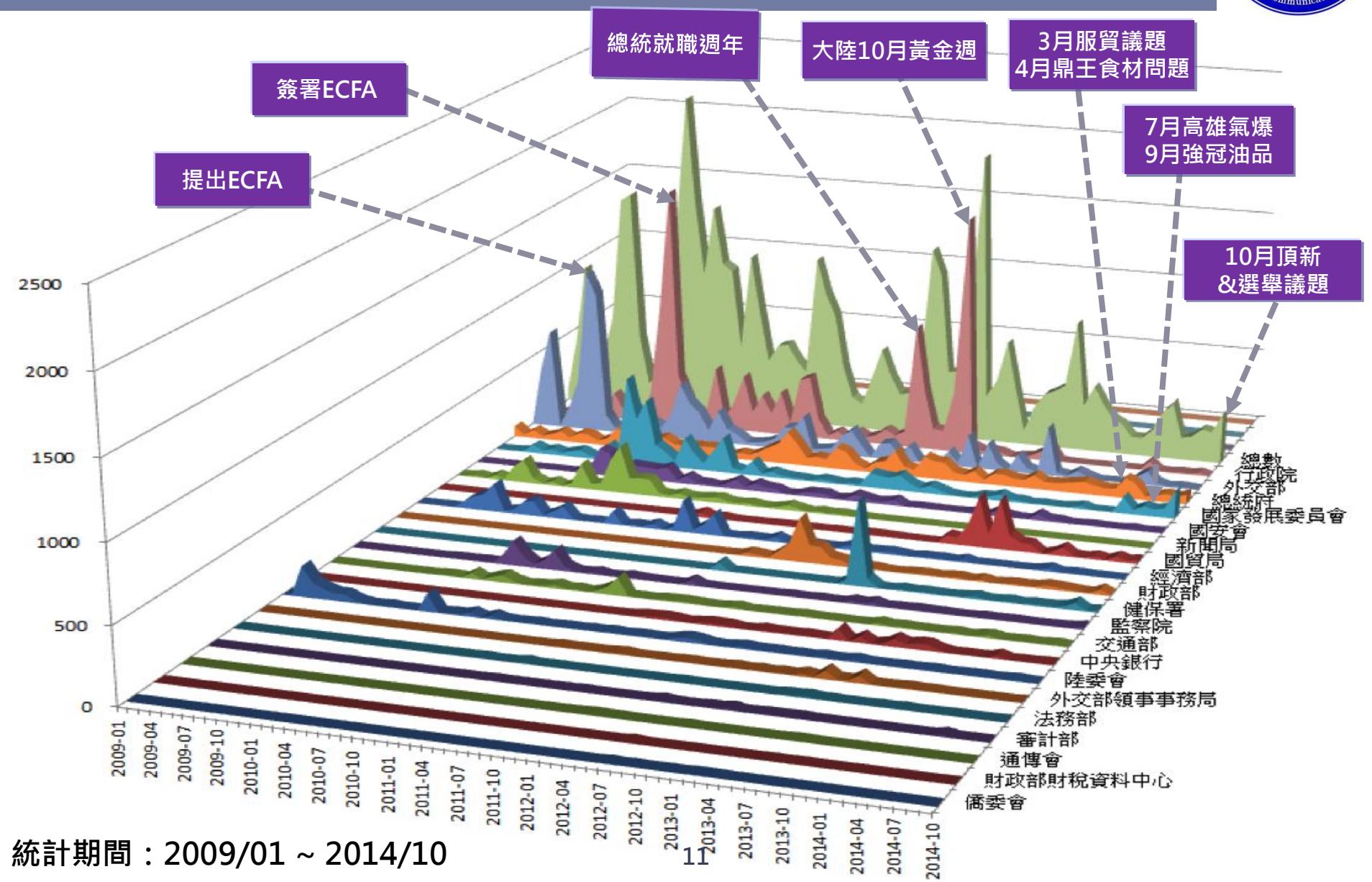
- RSA遭駭被竊：
  - 2011年3月17日資安公司RSA發生資安產品SecurID技術資料遭竊，包括該公司OTP(一次性密碼)Token產品SecurID的雙因素認證技術資料遭到外洩，影響2億名用戶
- 美國第二大連鎖零售商店：
  - 2013年12月駭客入侵Target的供應商電腦後，進而於Target的1,900家門市POS系統中植入惡意程式，竊取1.1億筆消費者資料(含4,000萬筆信用卡)
  - 其他六家POS廠商已經證實終端機感染Backoff惡意程式，擴散影響之企業已超過千家

貳、國內資安情勢及監控機制

政府資通安全威脅趨勢

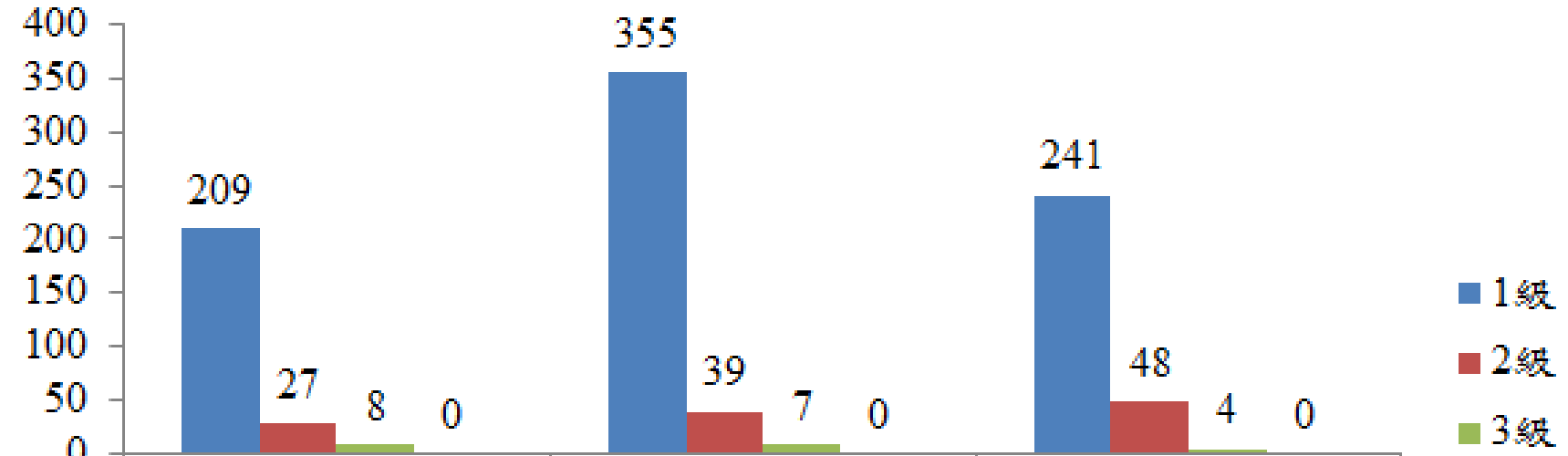

當前政府
資安威脅
鎖定目標
精準攻擊
社交工程
防不勝防
模式翻新
應變不易
認知不足
警覺不夠
人力預算
專業不足
駐外機構
鞭長莫及
公務家辦
擴增風險
設備微型
管理不易

進階持續威脅(APT)攻擊長期趨勢



統計期間：2009/01 ~ 2014/10

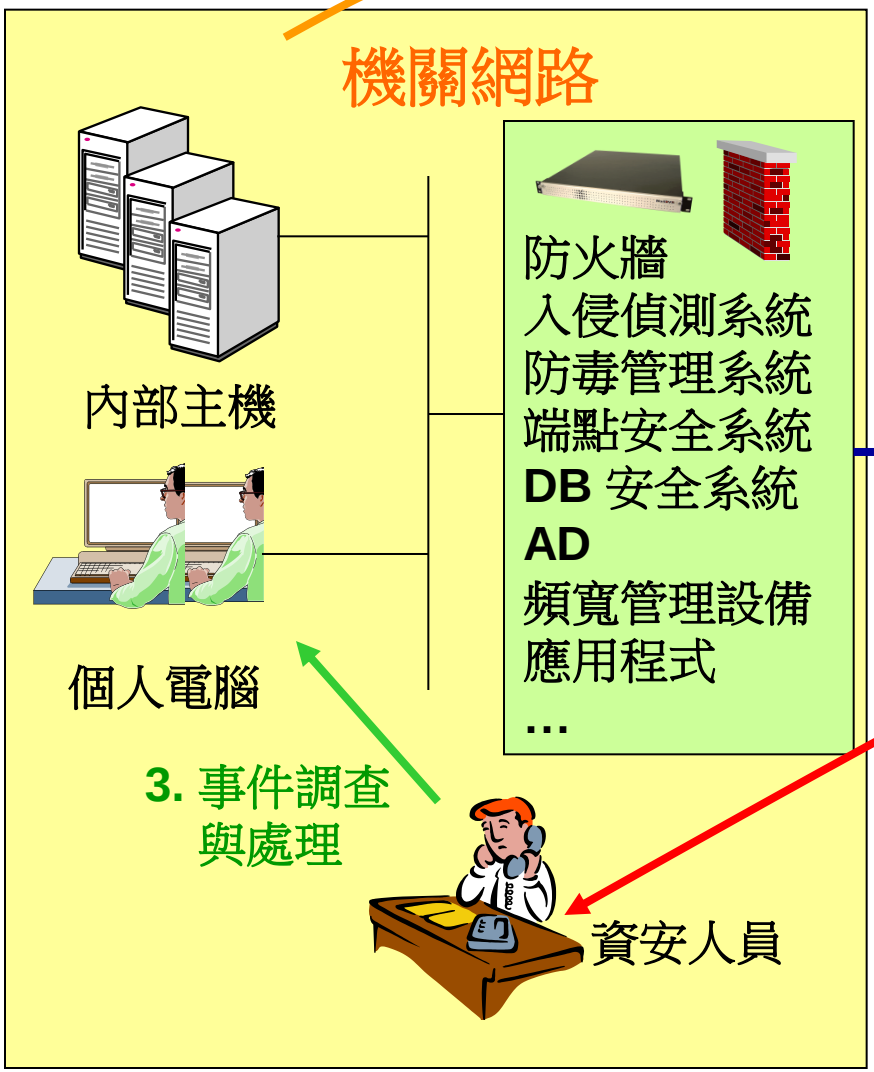
政府機關近3年通報資安事件數



	101年	102年	103年
1級	209	355	241
2級	27	39	48
3級	8	7	4
4級	0	0	0

資安事件係指業務系統遭影響或竄改；抑或業務資料遭洩漏或竄改，以機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)3個面向評估其影響等級，由重至輕分別為「4級」、「3級」、「2級」及「1級」。

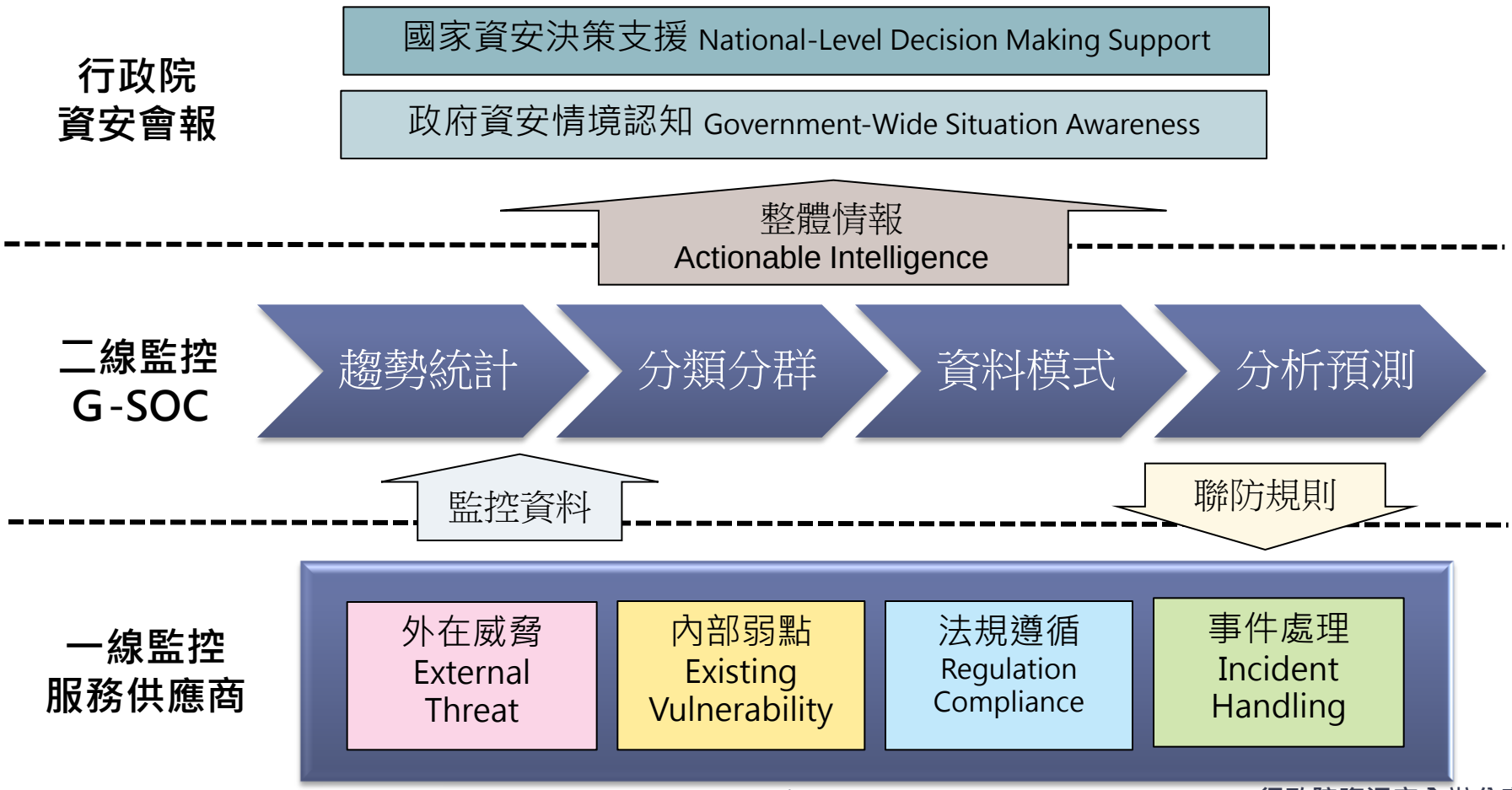
機關資安監控機制



Security Operation Center 無時不刻監看政府網路的異常行為，發出警訊通報即時處理

國家資安二線監控機制

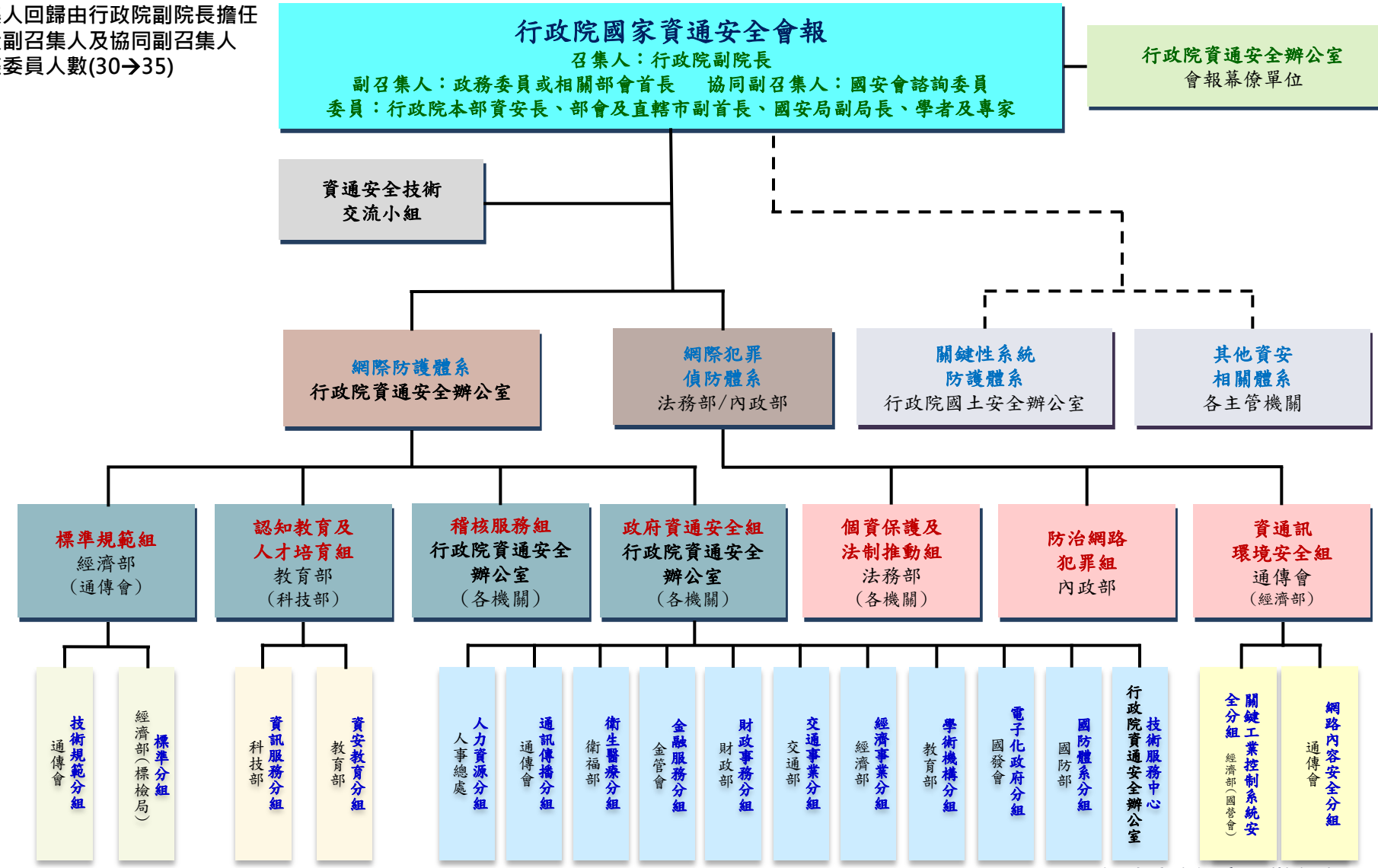
- 建立政府資安情境認知(Situation Awareness)
- 支援政府資安決策(Decision Making)與推動公私資安協同合作



參、政府重要施政說明

行政院國家資通安全會報組織架構

- 召集人回歸由行政院副院長擔任
- 增設副召集人及協同副召集人
- 調整委員人數(30→35)

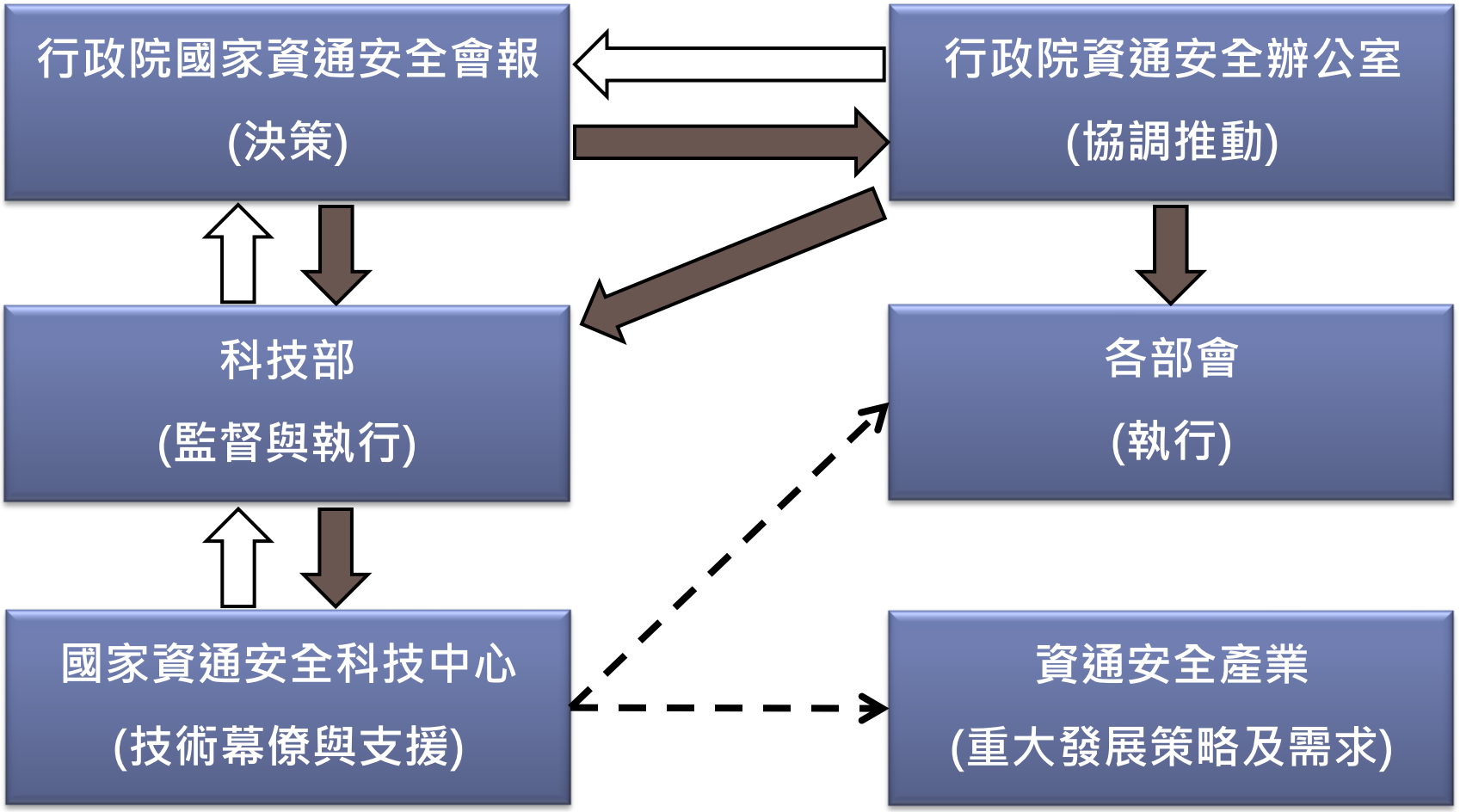


技服中心行政法人化(1/2)

- 行政院於90年3月規劃成立技服中心，協助資安會報逐步建置政府機關分級管理、國家資安防護管理平台(G-SOC)及資安專案管理(SPMO)等重要機制，並提供政府機關事前安全防護、事中預警應變、事後復原鑑識等資安技術服務。
- 因應資安情勢，積極推動技服中心轉型為行政法人，賦予執行特定資安「公共事務」之權責，並引進企業經營精神，培養成為守護我國資通安全的精實專業團隊。
- 行政院已指定科技部為資安主管機關，並為技服中心行政法人化後之監督機關。「國家資通安全科技中心」成立後，我國即形成資安三級制，符合國際趨勢，有利整體資安防護及相關業務之健全發展。

行政院國家資通安全會報技術服務中心
ICST Information & Communication Security Technology Center

技服中心行政法人化(2/2)



資通安全稽核(1/2)

【依據標準】
-依「國家資通安全發展方案(102年至105年)」
-ISO 27001:2013、資訊安全管理要點及規範、個資法

【事前準備】
-以負責財政與經濟機關(構)為主要受稽對象
-受稽機關自行辦理資安健診作業及稽核自評作業

【資安稽核】
-技服中心進行技術檢測
-赴機關進行策略、管理及技術3面向實地稽核
-責成機關研議因應作為及時程進度

【檢討強化】
-共同發現事項及建議提供各機關參考運用
-獎勵稽核結果績優及表現良好之機關(構)
-相關強化措施及建議提供各權責機關參酌

1.策略面
✓導入資訊安全管理系統範圍適切性
✓機關首長對資安業務支持度
✓資源投入資安業務狀況
✓業務運作規劃與落實

2.管理面
✓個人資料保護與管理
✓風險評鑑、資訊資產清查與管理
✓人力資源管理

3.技術面(含技術檢測)
✓通訊與作業管理適切性與落實執行狀況
✓資安事件通報與管理
✓應用系統開發及維護安全管理

資通安全稽核(2/2) - 強化行政管理措施

- 行政院資安辦：
  - 持續推動資安長制度
  - 強化**機關(構)資安責任等級分級**及資訊系統分級機制
  - **推廣**「行動裝置安全參考指引」、「政府資訊作業委外安全參考指引」等，持續辦理基礎資安環境實務教育訓練
- NICI小組：研議**整體政府機關資訊(安)人力不足之因應對策。**
- 工程會：研修「資訊服務採購契約範本」，**增列資安相關條文。**
- 工業局：研議「**建立資訊服務廠商分級制度**」之可行性
- 法務部：加強教育訓練及實務演練，提升各機關**個資管理能力。**

網路攻防演練

網路攻防演練

【情境演練】
以桌上模擬方式，演練機關遭受嚴重網路攻擊，以瞭解機關處理標準程序、通報應變程序及聯防機制的熟悉度

【實兵演練】
由攻擊手實際入侵攻擊各機關網站系統，以測試資訊系統防護能量、通報應變能力及資訊環境組態設置正確性

【電子郵件社交工程演練】
隨機寄發引人注目之電子郵件給各機關人員，並記錄其開啟及點閱的次數，藉以測試機關人員資安意識及警覺性

102年

行政院所屬二級機關 (33個機關)

482個系統發現108項網站系統弱點

郵件開啟率4.5%；附件點閱率3.3%

103年

總統府、五院、直轄市政府、各縣(市)政府 (28個機關)
【情境：交控系統及DNS系統】

1,267個系統發現217項網站系統弱點

郵件開啟率8.23%；附件點閱率4.18%

肆、後續工作重點

104年工作重點

提升資安組織效能	• 持續推動資安組織三級制 • 落實「政府機關(構)資安責任等級分級作業施行規定」
改善資安基礎環境	• 持續推動各機關導入政府組態基準設定(GCB) • 研議建構資安警示燈號 • 檢討修訂資訊系統分級相關規定，要求機關落實資安防護基準
強化資安防禦縱深	• 推動G-SOC資安二線監控機制 • 研議強化GSN防護機制 • 持續落實資通安全稽核作業
擴大公私協同合作	• 維運「政府資安資訊分享與分析平臺(G-ISAC)」 • 召開「資通安全技術交流小組」委員會議 • 強化資安服務專案辦公室(SPMO)功能
提升機關應變速度	• 督導機關落實資安相關演練 • 逐步強化網路攻防演練 • 持續推動資安服務納入共同供應契約

報告完畢