議題1. 打造安全信賴的資通訊環境

1.1 建立資通訊基礎建設安全信賴機制

報告單位：國家通訊傳播委員會

中華民國 98 年 8 月18日

報告大綱

- 壹、施政願景
- 貳、現況分析
- 叁、發展趨勢
- 肆、具體策略
- 伍、行動方案
- 陸、討論題綱

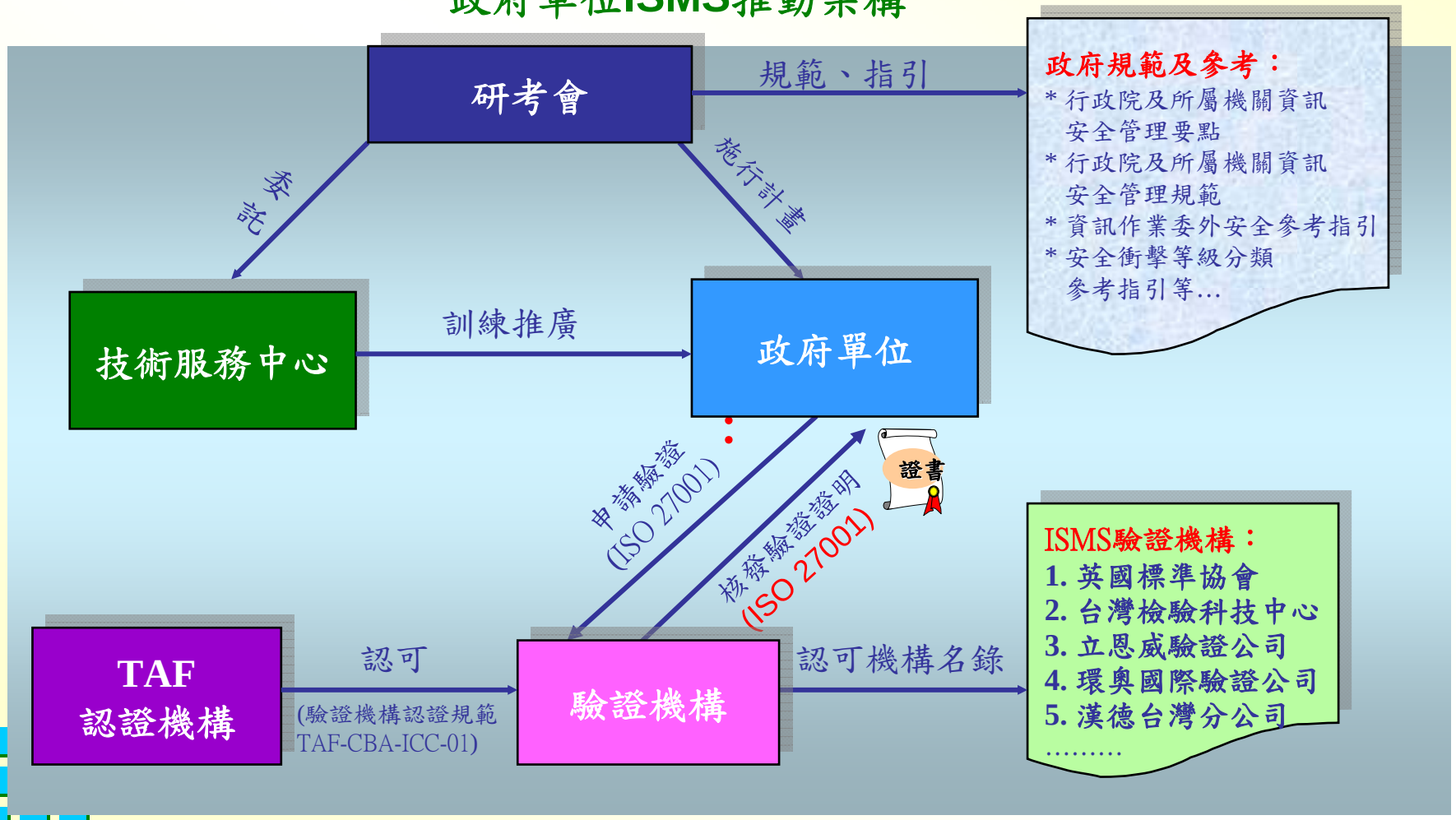
壹、施政願景


資通訊基礎建設安全信賴機制
資安管理
防護機制
設備驗證
資通訊基礎建設
相關法規
寬頻建設
標準規範
◎資安管理
◎防護機制
◎設備驗證
網路偵測
資安通報
資安應變
資訊分享
架構安全無慮的環境下,使用資通網路資源

貳、現況分析(1/12)

一、資訊安全系統管理-1

政府單位ISMS推動架構



ISMS：Information Security Management System

貳、現況分析(2/12)

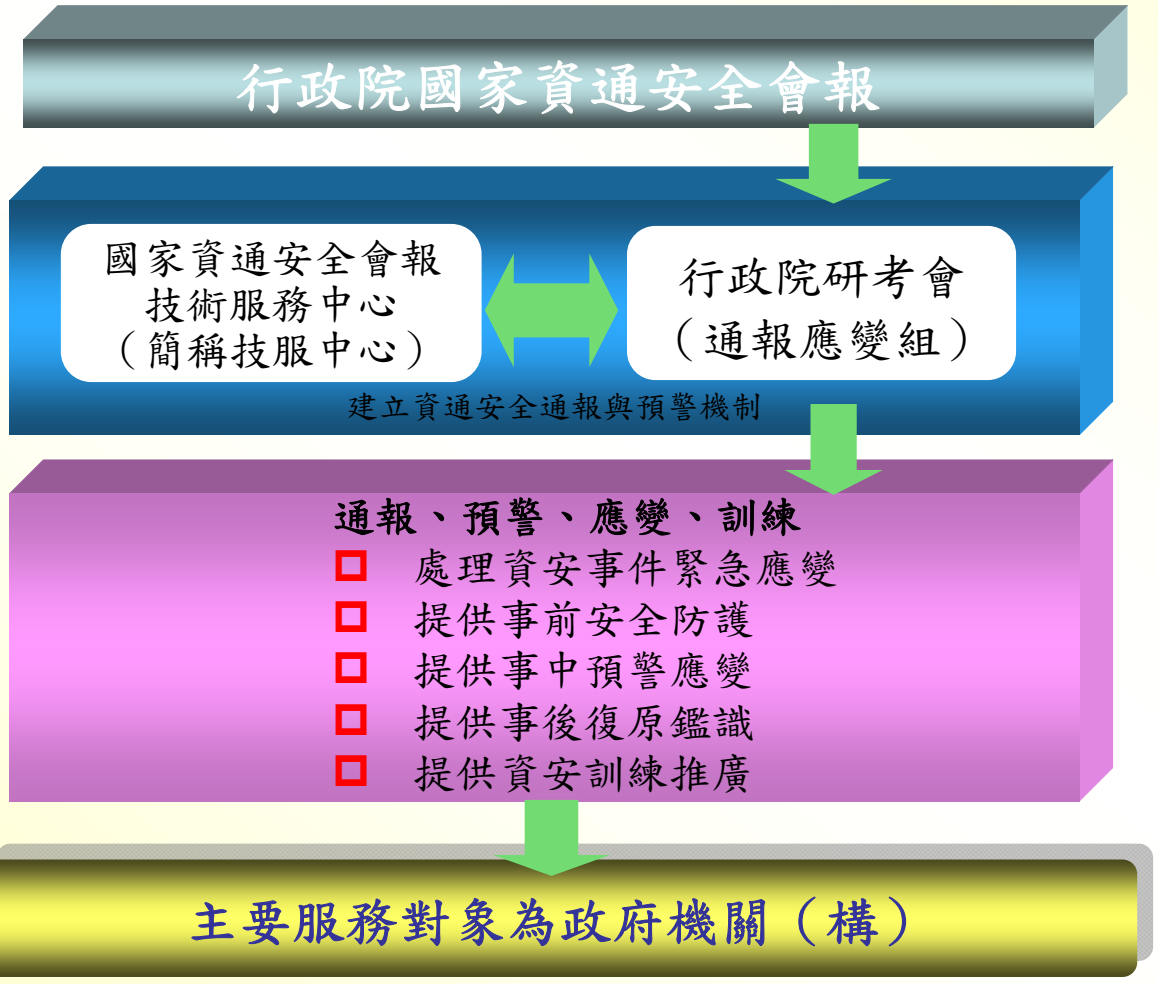
一、資訊安全系統管理-2

目前面臨的問題：

- ISMS已落實於我國政府機關，但目前尚未導入電信事業ISMS 。
- 缺乏電信事業導入ISMS之法源，尚須配合增訂電信相關法規。

貳、現況分析(3/12)

二、基礎設施資通安全防護-1



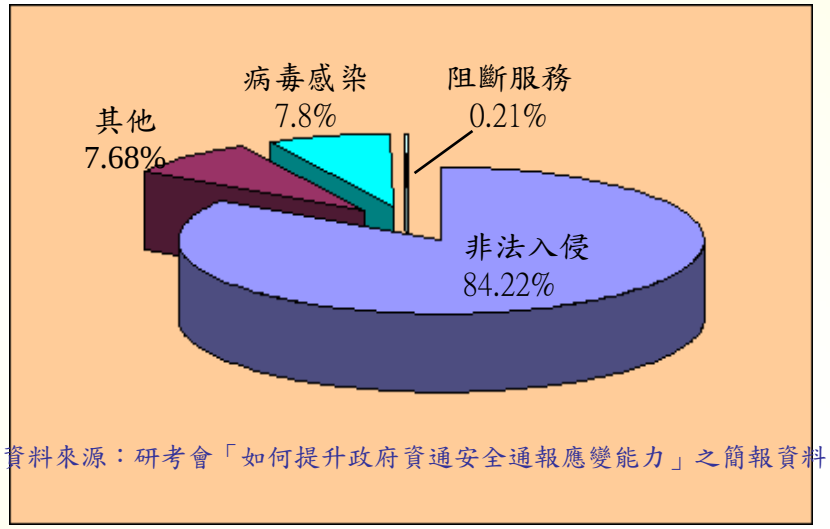
資料來源：研考會「如何提升政府資通安全通報應變能力」之簡報資料

貳、現況分析(4/12)

二、基礎設施資通安全防護-2

政府機關通報資安事件情形

- 國家資通安全通報應變網站，已建立約7,000個政府機關、15,000資安聯絡人資料。
- 97年共接獲963件資安事件通報，其中368為機關接獲技服中心資安警訊後進行通報。
- 接獲通報之資安事件等級由高至低共計：
  - 4級事件：0件
  - 3級事件：2件
  - 2級事件：87件
  - 1級事件：874件



資料來源：研考會「如何提升政府資通安全通報應變能力」之簡報資料

貳、現況分析(5/12)

二、基礎設施資通安全防護-3

國內民營企業資訊安全事件損失情形

- 有形的損失為時間與金錢，無形的損失為商譽。
- 資訊安全事件危害與復原時間： 2008年遭遇資安事件損失至復原平均所需時間為12.52個小時，較2007年有升高之趨勢。
- 資訊安全事件損失金額 ：2007年民營企業大多能將因資安事件所損失的金額控制在5萬元以下(70.2%)，平均為每件事件24.32萬，相較2006年53.55萬損失較為縮小。
- 資安事件商譽損失：絕大多數之民營企業認為資安事件並不會對其商譽或名譽造成損失，2008年僅有6.5%企業認為資安事件會產生商譽損失，相較2007年調查7.4%較為縮小。

（資料來源：財團法人台灣經濟研究院委託調查）

貳、現況分析(6/12)

二、基礎設施資通安全防護-4

國內主要IASP業者現行資安防護情形：

- 目前有提供最新版本的防毒軟體，部分係免費提供。
- 提供付費之防毒或偵測服務，針對特定病毒、系統漏洞或影響用戶之駭客手法都會立即發布在專屬的通告網站上。
- 有入侵防護系統(IPS)及入侵偵測系統(IDS)之服務。
- 針對國內外知名機構通告之釣魚網站、中繼站與受害主機，皆會告知消費者。
- 如發現釣魚網站，業者會立刻協助處理。但botnet與用戶木馬問題相當複雜，尚無 法全面性深層處理。部分確實造成危害的動作中惡意中繼站，會協助用戶處理。

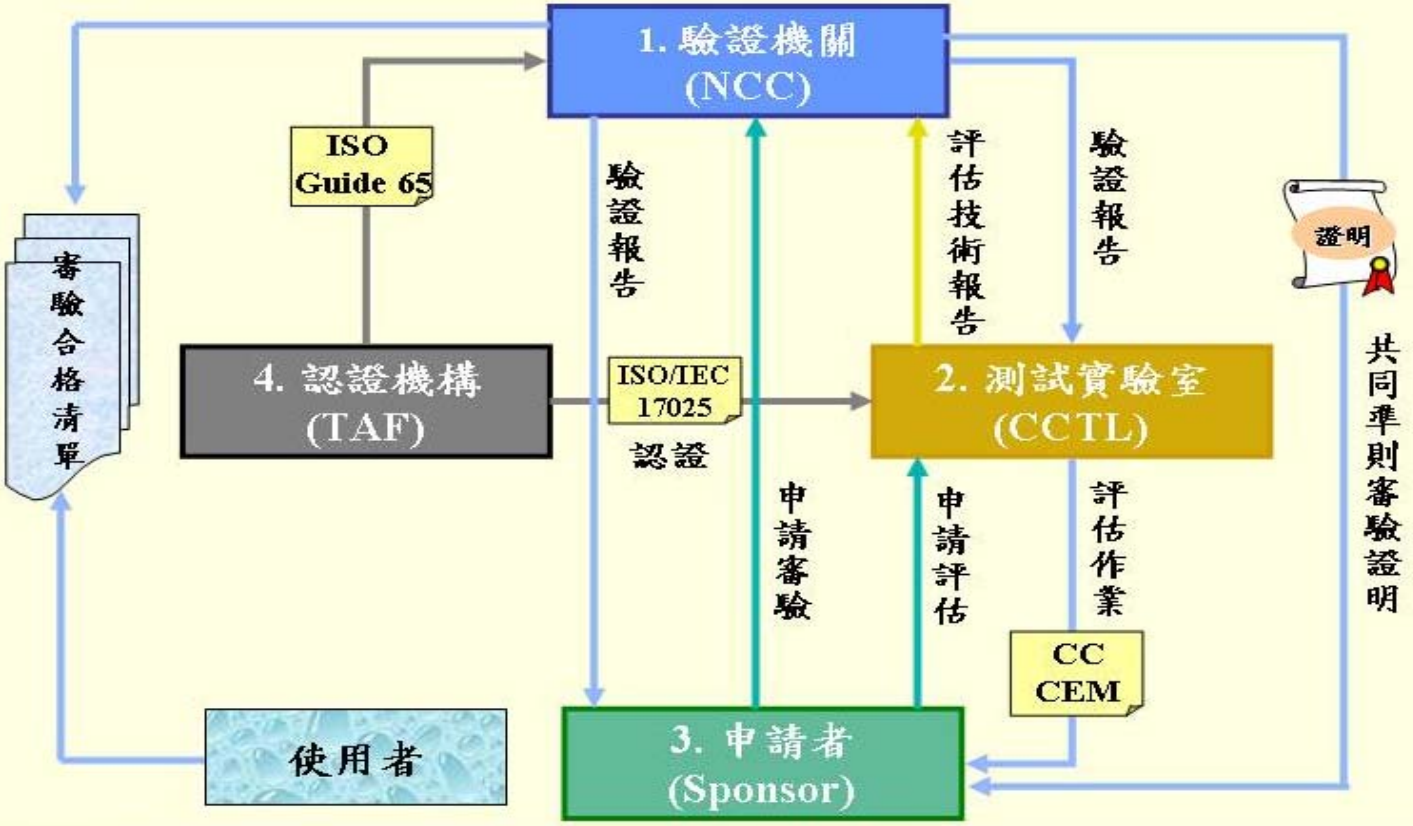
目前面臨的問題：

- **目前尚未建構整合IASP資安之預警、通報、應變及資訊交換**

貳、現況分析(7/12)

三、資通設備安全驗證-1

CC：Common Criteria
CEM：Common Evaluation Methodology



參與單位

1. 驗證機關 (Certification Body) ：國家通訊傳播委員會(NCC)
2. 測試實驗室 (Common Criteria Testing Laboratory)
3. 申請者(Sponsor/Developer)：設備供應商、開發者或政府機關（構）
4. 認證機構 (Accreditation Body) ：財團法人全國認證基金會(TAF)

貳、現況分析(8/12)

三、資通設備安全驗證-2

電信技術中心(Telecom Technology Center, TTC)實驗室評估能量

- 現有14位具有CC能力之評估員
- 實驗室檢測時程預估

等級 / 時程	EAL 1	EAL 2	EAL 3	ELA 4
實驗室評估時程	1-2 個月	2-3 個月	3-5 個月	4-6 個月
廠商修改文件時程	2-4 個月	4-6 個月	6-7 個月	8-12 個月
總評估時程	3-6 個月	6-9 個月	9-12 個月	12-18 個月
主管機關審核	1 個月內	1 個月內	1-2個月內	1-2個月內

- 總評估時程為累計(含實驗室評估時程及廠商修改文件時程)所得
- 申請廠商如已具備送檢經驗，總評估時程可視狀況再縮減
- 送評估產品以EAL 2-3為大宗

貳、現況分析(9/12)

三、資通設備安全驗證-3

TTC與國際實驗室收費標準比較

單位：新台幣

安全等級	TTC資安實驗室收費標準		歐洲實驗室收費標準		北美實驗室收費標準	
	檢測	顧問	檢測	顧問	檢測	顧問
Protection Profile	90萬	180萬	400萬	600萬	180萬	360萬
EAL 1	90萬	180萬	400萬	600萬	180萬	360萬
EAL 2	150萬	300萬	650萬	1,000萬	300萬	600萬
EAL 3	240萬	480萬	1,000萬	1,500萬	480萬	960萬
EAL 4	450萬	900萬	1,500萬	2,250萬	900萬	1,800萬

TTC收費雖遠低於歐美，對小廠及低單價產品，仍造成其成本負擔。

貳、現況分析(10/12)

三、資通設備安全驗證-4

NCC資通設備審驗業務辦理情形

- 完成制訂行政規則及相關技術規範
  - 資通安全產品及保護剖繪審驗作業要點
  - 資通安全設備及保護剖繪測試實驗室管理作業要點
  - 資訊技術安全評估共同準則(CC)技術規範(第2.2版、第2.3版及第3.1版)
- 完成共同準則審驗案件
  - 資通安全保護剖繪審驗1件
  - 資通安全產品審驗2件

貳、現況分析(11/12)

三、資通設備安全驗證-5 產業界認同的標準

測試實驗室	美國ICSA	法國NSS	台灣NBL(Network Benchmarking Lab)
主要測試層面	功能面	效能面	穩定面
主要測試產品	Anti-Spam, Anti-Spyware, Anti-Virus, Firewalls, IPSec	IPS, Anti-Malware, Next Generation Firewall, UTM, WAF, VA	Firewall, Anti-Virus, IPS, UTM, Anti-Malware
廠商送測	國際領導廠商，如: IBM, Symantec, Kaspersky Lab, Fortinet, McAfee, Microsoft, CA, F-Secure, Avira,	國際領導廠商，如: IBM, McAfee, Fortinet, Juniper, Symantec, 3Com, CA, Cisco	國內廠商為主，如: 趨勢、友訊、合勤、明泰、威播、新軟、文佳、利基、盛達電業、友旺、居易、兆聖、鴻璟、碩琦
其它	成立已20年。	成立已18年。	成立7年，目前已服務超過100家國內外廠商、總計測過的產品超過500個

貳、現況分析(12/12)

三、資通設備安全驗證-6

目前面臨的問題

- CC檢測費用偏高，驗證時程過長，不易推行。

  國內資通安全設備廠商規模小，難與國際廠商抗衡。
- 國內缺乏如美國ICSA、法國NSS等等受國際業界認同測試實驗室來整合各界之資安技術能量、制訂測試標準、執行測試。
- 是否需要自訂適合國內資安設備驗證標準？
- 是否宜限制政府機關(構)採購國產資安設備？
- 缺少鼓勵國內廠商投入資安設備研發之獎勵措施。

叁、發展趨勢(1/6)

一、資訊安全系統管理-1

國際

ISO/IEC 27001
（Information Security Management System (ISMS) requirements standard ）

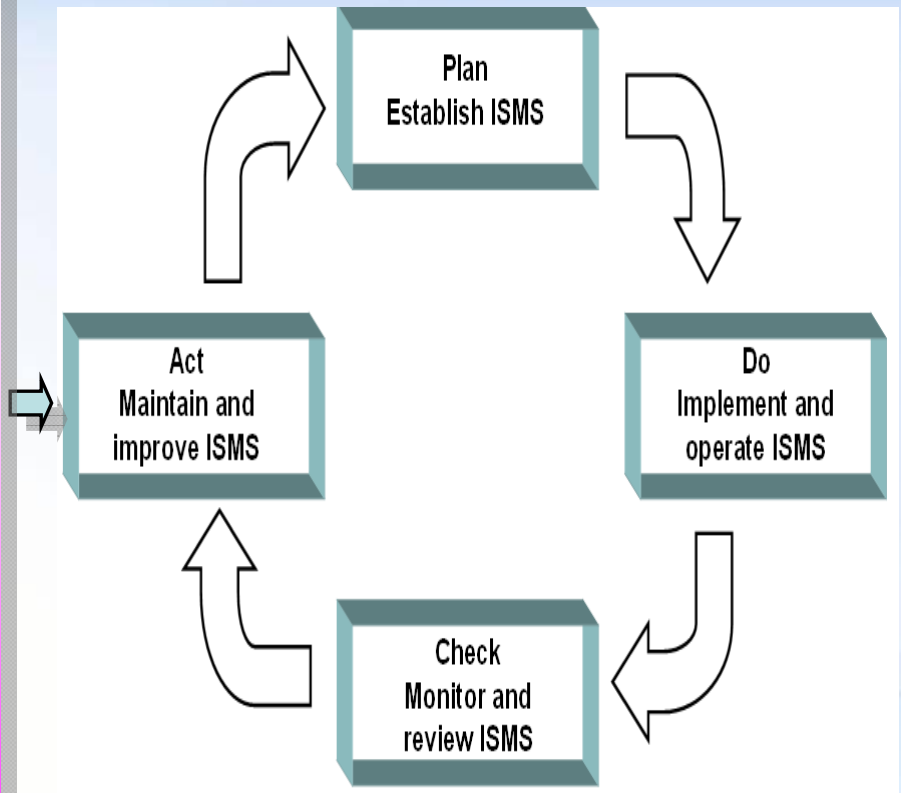
ISO/IEC 27002
（code of practice for information security management ）

ISO/IEC 27003
(ISMS implementation guide)

ISO/IEC 27004
(standard for information security management measurements)

ISO/IEC 27005
(designed to assist the satisfactory implementation of information Security based on a risk management approach)

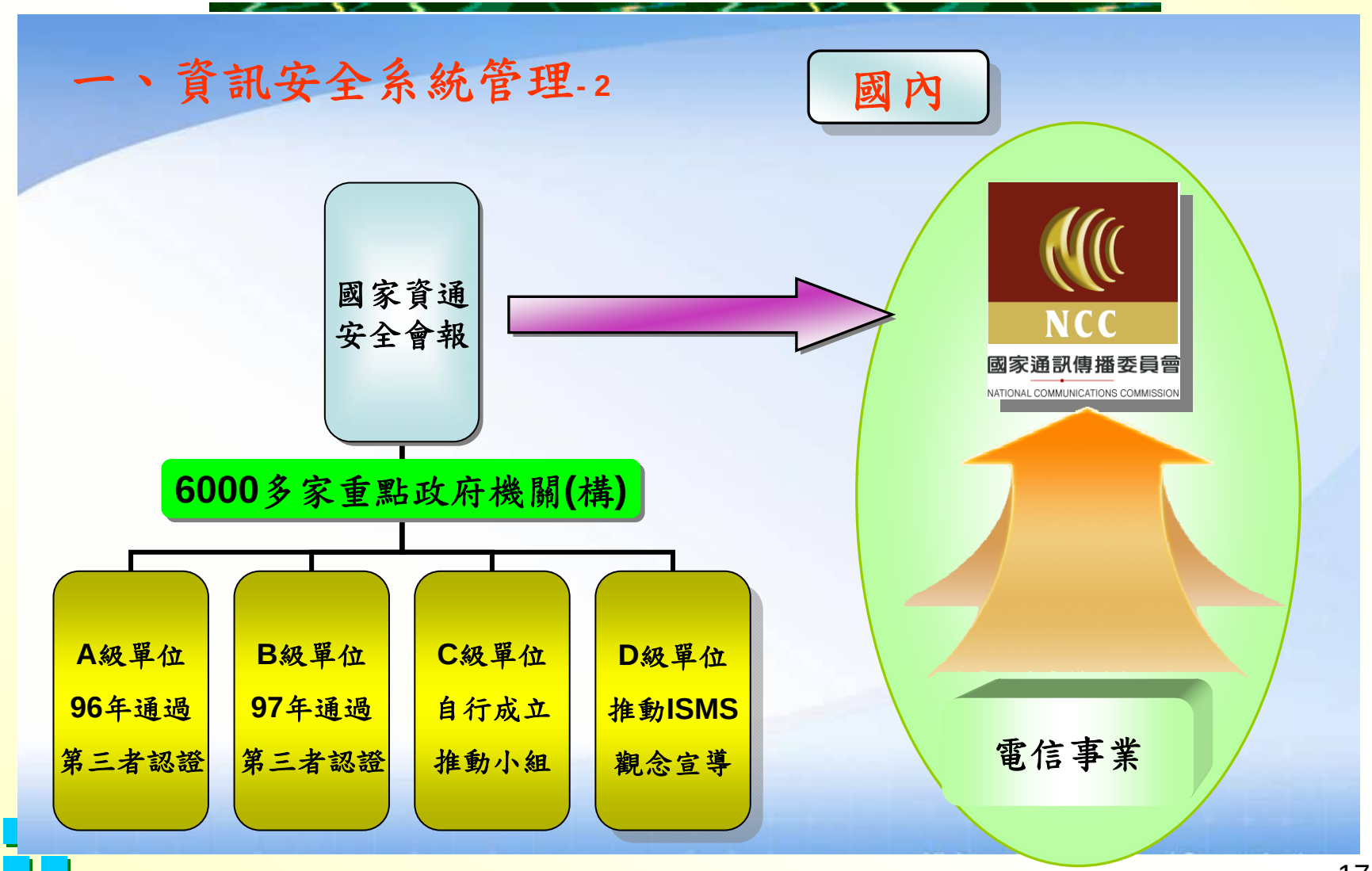
ISO/IEC 27011
（information security Management guideline for telecommunications organizations ）



政府單位和企業組織最佳參考規範

國際資訊安全管理的準則及規範

叁、發展趨勢(2/6)


一、資訊安全系統管理-2
國內
國家資通
安全會報
NCC
國家通訊傳播委員會
NATIONAL COMMUNICATIONS COMMISSION
6000多家重點政府機關(構)
A級單位
96年通過
第三者認證
B級單位
97年通過
第三者認證
C級單位
自行成立
推動小組
D級單位
推動ISMS
觀念宣導
電信事業

參、 發展趨勢(3/6)

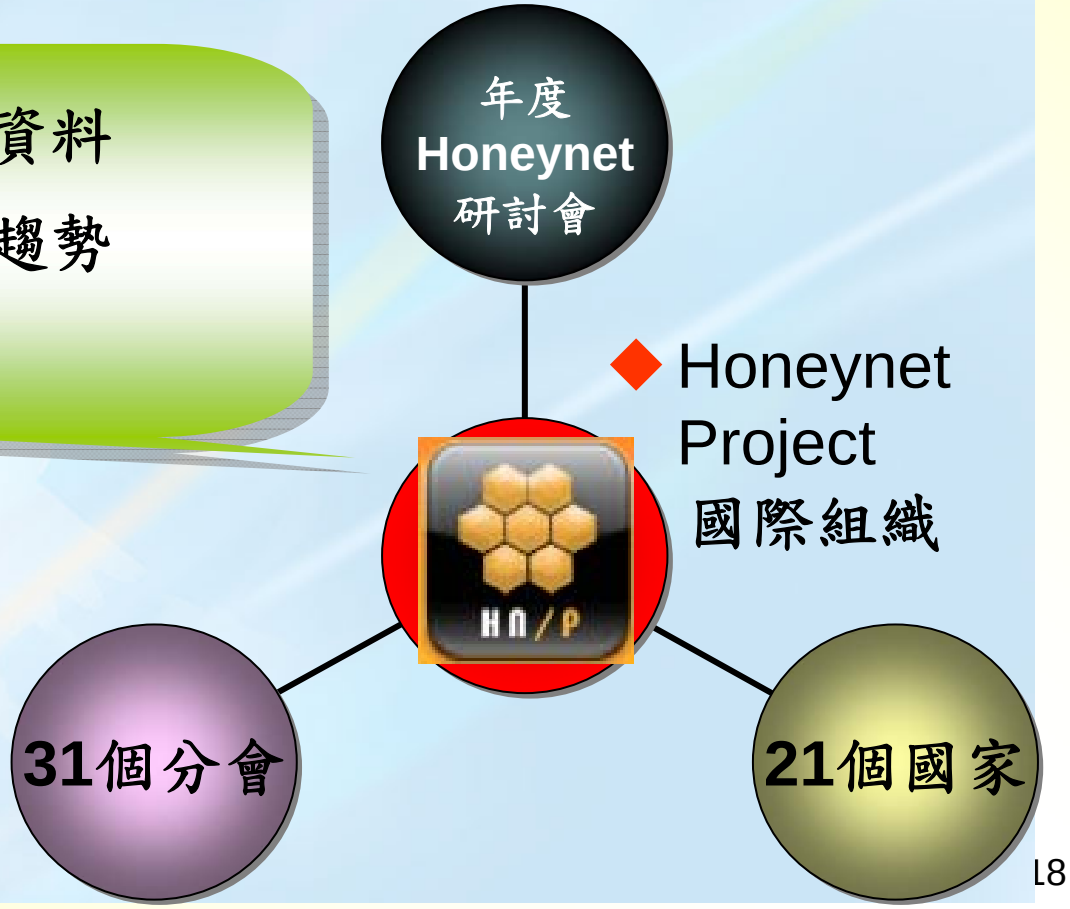
二、基礎設施資通安全防護-1

國際

☆分享各國攻擊活動資料

☆解析各國攻擊威脅趨勢

☆了解各國資安現況



叁、發展趨勢(4/6)

二、基礎設施資通安全防護-2

國內

系統安全保證及反駭客控制技術研究計畫
(行政院科技顧問組)

網際網路反駭客偵測及資安通報系統建置計畫
(國家通訊傳播委員會)

收集分析網際網路駭客攻擊行為

資安事件之通報、處理及回報

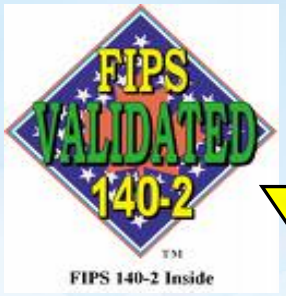
避免資安事件危害擴大
降低網際網路使用者被攻擊及威脅
提升整體基礎設施資通安全防護能力

叁、 發展趨勢(5/6)

三、資通設備安全驗證-1

國際

FIPS 140



CC part 1
CC part 2
CC part 3

International Organization for Standardization

ISO/IEC 19790

ISO/IEC 15408-1
ISO/IEC 15408-2
ISO/IEC 15408-3

叁、發展趨勢(6/6)

三、資通設備安全驗證-2

國際

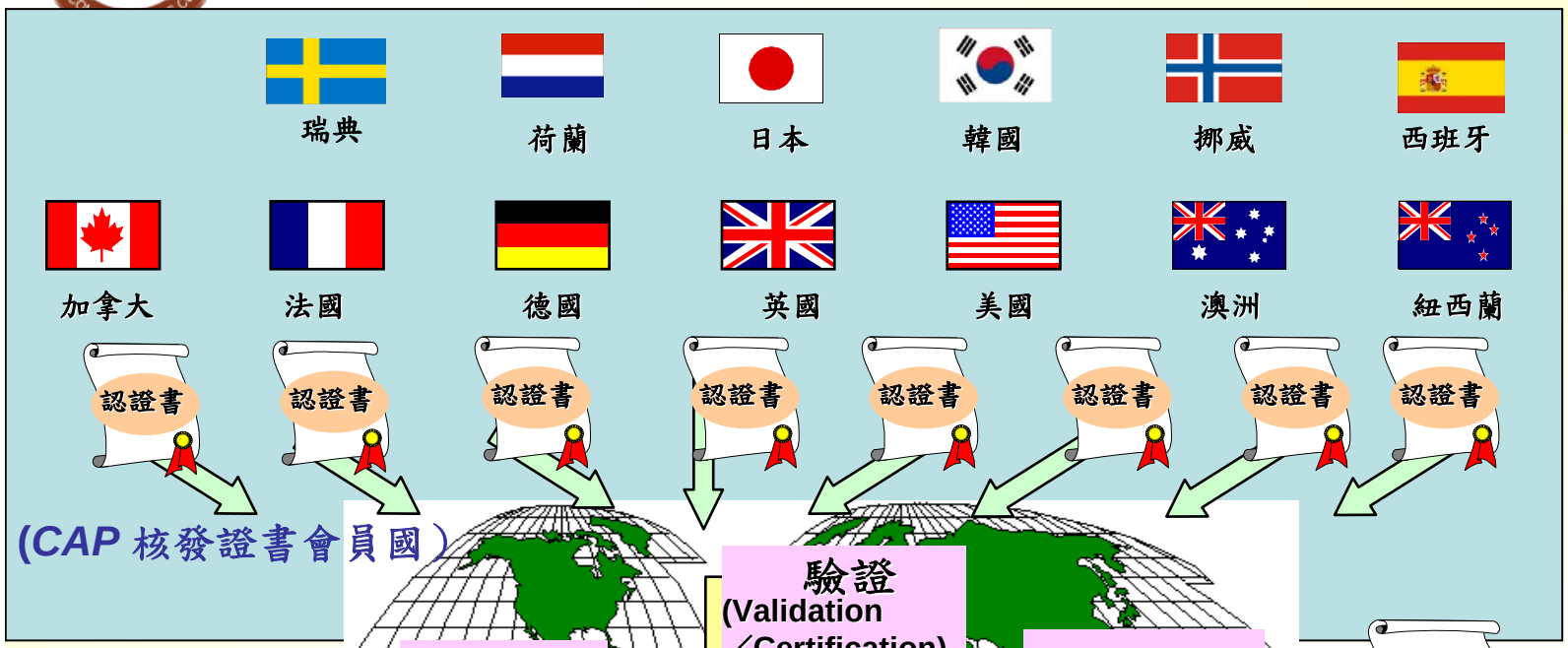
- CCRA國際組織：

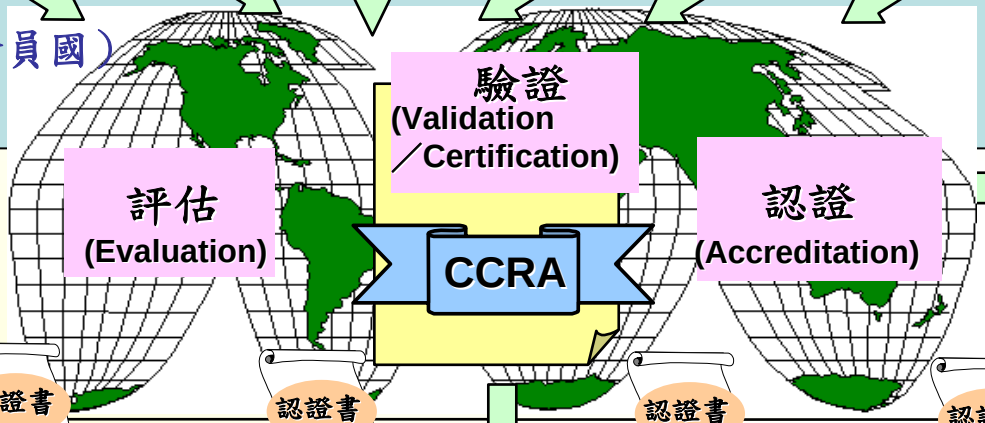
負責推動資訊技術安全共同準則之相關標準制定，確保資通設備確實達到安全品質管控，降低資通安全的潛在威脅。目前共有26個會員國。

CCRA: Arrangement on the Recognition of Common Criteria Certificates in the filed of Information Technology Security

- 資通設備安全驗證屬自願性。
- 大部分國家之資通安全主管機關要求政府機關採購資通安全設備時，應自主管機關所發佈之「資通安全設備合格清單」中選購。

CCRA參與會員國





芬蘭
希臘
義大利
以色列
奧地利
匈牙利
土耳其
捷克
新加坡
印度
丹麥
馬來西亞
巴基斯坦

CAP核發證書會員國(13) + CCP接受證書會員國(13) = 共26國

(CCP 接受證書會員國)

CCRA核發驗證證書統計表

	USA	UK	Canada	France	German	Australia	Japan	Netherland	Norway	Korea	Spain	小計
1997	0	0	1	0	0	0	0					1
1998	1	6	0	0	1	0	0					8
1999	1	5	2	4	1	0	0					13
2000	2	7	2	11	0	1	0					23
2001	4	4	2	16	1	1	0					28
2002	26	7	2	12	8	2	2					59
2003	18	13	7	5	13	5	5					66
2004	31	6	6	22	49	3	17		1			135
2005	62	6	7	23	46	2	23		1			170
2006	39	4	4	21	44	1	43	1	0	53	4	214
2007	45	10	18	22	32	5	43	0	1	13	4	193
2008	43	7	15	29	56	4	71	0	0	2	9	236
2009	10	1	5	0	12	1	3	0	1	0	0	33
合計	282	76	71	165	263	25	207	1	4	68	17	1,179

統計至03/23/2009

- 各國第一年推行驗證所核發之證書為**1-6**件，件數逐年成長
- 美國、德國、日本為核發證書件數前三名之國家
  - 1st 美國282件(共12年期間)→平均每年23件
  - 2nd德國263件(共12年期間) →平均每年21件
  - 3rd日本207件(共8年期間) →平均每年25件

肆、 具體策略(1/5)

一、導入資訊安全管理系統機制

- 電信事業導入資訊安全管理系統(ISMS)，確保其資料、系統、設備及網路安全，保障使用者權益。
- 電信事業透過管理及稽核方式維持及改善其安全性。
- 電信事業應先完成內部稽核制度。
- 電信事業委由公正第三者通過驗證。

肆、 具體策略(2/5)

二、健全電信事業資通安全防護能力

- 佈建誘捕網路於電信事業端，偵測及蒐集網路攻擊活動與傳播的惡意程式。
- 建置網際網路反駭客偵測與資安通報系統，進行通報、處理及回報等應變措施。

肆、 具體策略(3/5)

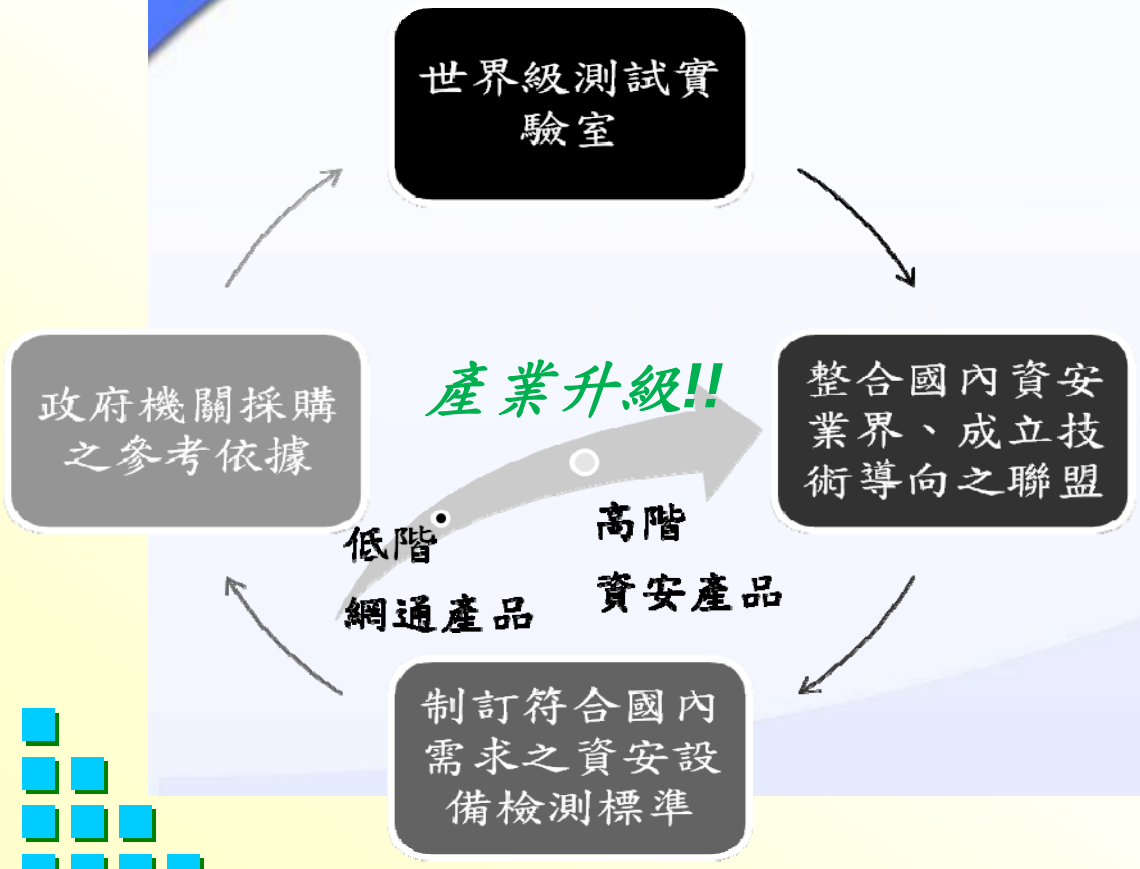
三、推動資通設備驗證機制 -1

- **持續提供國際共同準則(CC)驗證服務**
  - 國內資通設備廠商，如有意願申請國際CC驗證，仍可充分利用已建立之國內CC驗證服務能力，以協助我國生產的資通安全設備能夠推廣到國際舞台。
- **強化符合產業界需求之資通安全測試實驗室**
- **自訂國內資安設備驗證標準**
  - 以簡化驗證項目、降低測試評估費用及縮短驗證時程，可儘速導入政府採購資通設備適用驗證標準。
- 不違反WTO之政府採購協定(Agreement on Government Procurement, GPA)規定下，**鼓勵政府機關採購經驗證之資安產品。**
- **研擬獎勵國內廠商投入資安設備研發之配套措施。**

肆、 具體策略(4/5)

三、推動資通設備驗證機制 -2

促進產業升級之配套策略



- 政府輔導培養世界級測試實驗室，再由測試實驗室整合業界提升資安技術水準
- 網通產品如SOHO Router，台灣廠商產值已達世界第一，占全球市場50%以上
- 資安產品產值有很大的進步空間，台灣廠商占國內市場約1%、占全球市場約3%

肆、 具體策略(5/5)

四、宣導資通安全認知及公佈資安設備驗證資訊

◆ 建立資安宣導網站

- 提供最新資通訊基礎建設安全之相關資通安全訊息及知識，提高使用者的警覺性，防範潛在的資通安全威脅。
- 公佈經驗證合格資通設備清單資訊，提供政府機關參考。

伍、行動方案(1/5)

一、建立電信事業資訊安全系統管理

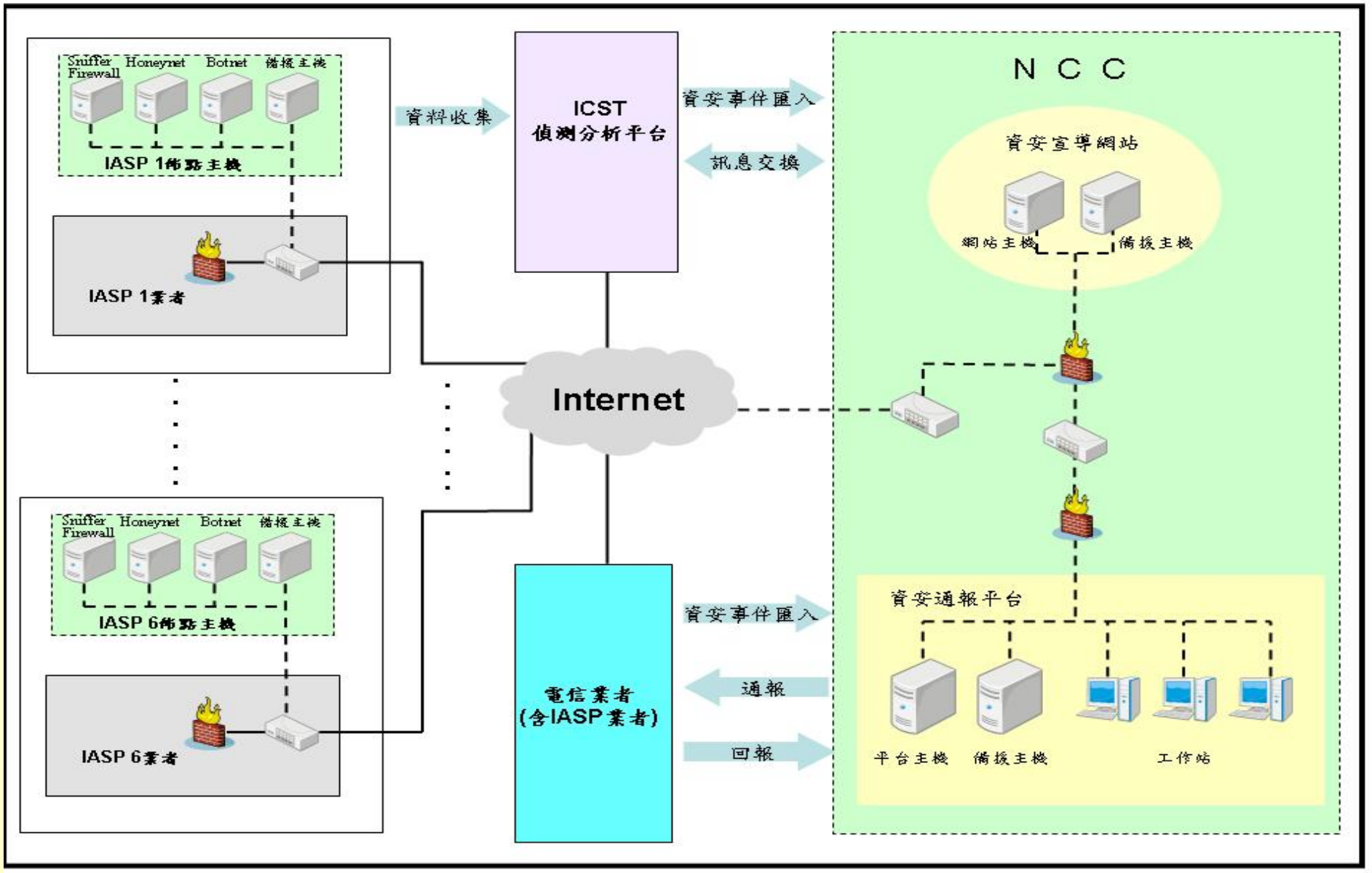
- 國家資通訊安全發展方案第16項行動方案：「依法規授權，促進事業機構運用第三方評鑑」
- 執行要點
  - 推動各目的事業單位建立資安內部稽核制度並落實執行。
  - 推動資通安全成為企業內稽內控循環之一。
  - 指導各目的事業單位委由公正第三者進行資通安全外部稽核。
  - 本會將建立電信事業資訊安全系統管理機制。
- 將於電信法增訂相關條文，要求電信業者應落實資通安全管理，辦理資安內部稽核，並委由公正第三者進行資安外部稽核，落實各項安全防護措施，以期及時發現資安事件，及時通報及應變處理。

伍、行動方案(2/5)

二、建置網際網路反駭客偵測與資安通報系統

- 國家資通訊安全發展方案第14項行動方案：「發展關鍵資訊基礎建設保護策略」
- 執行要點
  - 建立各關鍵基礎建設領域資安預防與早期預警、偵測、反應、危機管理能力。
  - 規劃與設計網際網路接取服務提供業者(IASP)聯盟與通報處理作業機制。
  - 建置電信網路「資訊安全通報處理平台」，包括通報資訊共享平台、資訊分享介面及入口網站。
- 本會將於99年完成建置網際網路反駭客偵測與資安通報系統，可偵測及分析網際網路駭客攻擊行為，有效處理、通報及回報資安事件，具有CERT、SOC、ISAC多功能平台。

網際網路反駭客偵測與資安通報系統架構圖



伍、行動方案(3/5)

三、推動政府機關(構)採購經驗證之資通設備-1

- 國家資通訊安全發展方案第9項行動方案：「推動政府機關（構）採購符合安全驗證之資通訊設備」
- 執行要點：
  - 建立資通安全之機敏裝備項目。
  - 辦理資通安全驗證作業訓練。
- 推動政府機關(構)採購經驗證之資通設備，先行研訂國內產業標準，再推動試辦。

伍、行動方案(4/5)

三、推動政府機關(構)採購經驗證之資通設備-2

實施期程	實施方法	實施範圍
規劃99年完成制訂國內產業標準、採購指引及獎勵措施，再推動試辦三年。 (評估規劃中)	◆ 規劃成立專案工作小組，並於本年6月及7月間邀集產、官、學、研代表研商可行方案。 ◆ 提出適合我國資通設備驗證之方案，並可與國際共同準則制度並行之機制。	網路安全相關資通設備

配套措施

◆提供Pre-Test讓業界可以逐步適應
◆提供技術輔導讓業界可以加速產品品質改良
◆提供經費補助讓“有技術能力”、”積極改良”的廠商取得補助

伍、行動方案(5/5)

四、建置資安宣導網站

- 資安宣導網站設置於網際網路反駭客偵測與資安通報系統，99年建置完成。
  - 提供相關資安訊息，達到資訊分享及教育宣導功能。
  - 公布「資通安全設備合格清單」，使資通設備廠商及政府機關相關單位得以了解最新取得驗證之資通安全設備資訊。

陸、討論題綱

一、如何導入適合國內電信事業之資通安全管理機制？

二、如何健全網際網路之資通安全防護能力？

三、如何培養資安業界認同之世界級測試實驗室？

四、如何推動適合國內環境之資通產品安全驗證機制？

建立資通訊基礎建設安全信賴機制

敬請 指導