資安現況與未來趨勢

howard@ey.gov.tw
行政院資通安全處
111年4月

2020 資安事件(1/2)

- 英國倫敦外匯交易公司Travelex遭勒索軟體Sodinokibi攻擊
- Magnallium駭客組織入侵美國電廠、煉油及天然氣公司網路

1月

- 以色列選舉系統因委外廠商設計疏失產生漏洞導致選民資料外洩
- 網路攻擊者以武漢肺炎名義散發電子郵件，企圖發動惡意攻擊

2月

- 歐洲電能組織辦公室IT系統遭惡意攻擊
- 捷克新冠肺炎篩檢中心遭勒索軟體攻擊

3月

- BGP劫持事件導致全球約200家CDN供應商流量導向俄羅斯
- 舊金山國際機場網站遭駭客掛碼竊取使用者帳密

4月

- 供應鏈攻擊鎖定GitHub開源軟體專案駭侵
- 泰國最大電信業者AIS數千萬用戶即時網路瀏覽資料外洩
- NAS廠商產品QNAP傳多項漏洞

5月

- 印度資安業者BellTroX涉非法監控數萬個電子郵件
- UPnP協定存在CallStranger漏洞
- 全美逾200所警局與情資整合中心之機敏資料外洩

6月

2020 資安事件(2/2)

- 駭客利用區塊鏈技術隱匿行蹤，鎖定Docker環境建置殭屍網路
- 推特大批名人帳號被駭，用來發送比特幣詐騙訊息

- 阿根廷移民署遭植入Netwalker勒索軟體
- 微軟Elasticsearch伺服器遭駭客攻擊刪除6.5TB用戶資料

- 西班牙網路軟體開發商Prestige Software雲端伺服器配置錯誤，造成至少10萬用戶機敏資料外洩
- 駭侵組織Cicada對日本組織發動大規模駭侵，掌握內網AD控制權

7月

8月

9月

10月

11月

12月

- 駭客透由Tor網路惡意節點，攔截置換傳輸資訊以竊取比特幣
- 紐西蘭證券交易所遭DDoS攻擊
- 逾20萬中國傳音所生產手機預載廣告詐騙程式

- 韓國多家銀行遭受UDP Flood DDoS分散式阻斷服務攻擊
- 網路券商Robinhood用戶帳號遭駭，部分用戶資產遭盜賣

- 駭侵組織利用Zerologon漏洞攻擊日本企業全球據點
- APT駭侵團體以最新macOS後門惡意軟體發動攻擊
- SolarWinds產品Orion遭駭，影響33000個公私營部門

凡事皆有價

SEPTEMBER 2019

THE ARMOR 2019 BLACK MARKET REPORT

A LOOK INSIDE THE DARK WEB

Extracts from one hacker's price list:

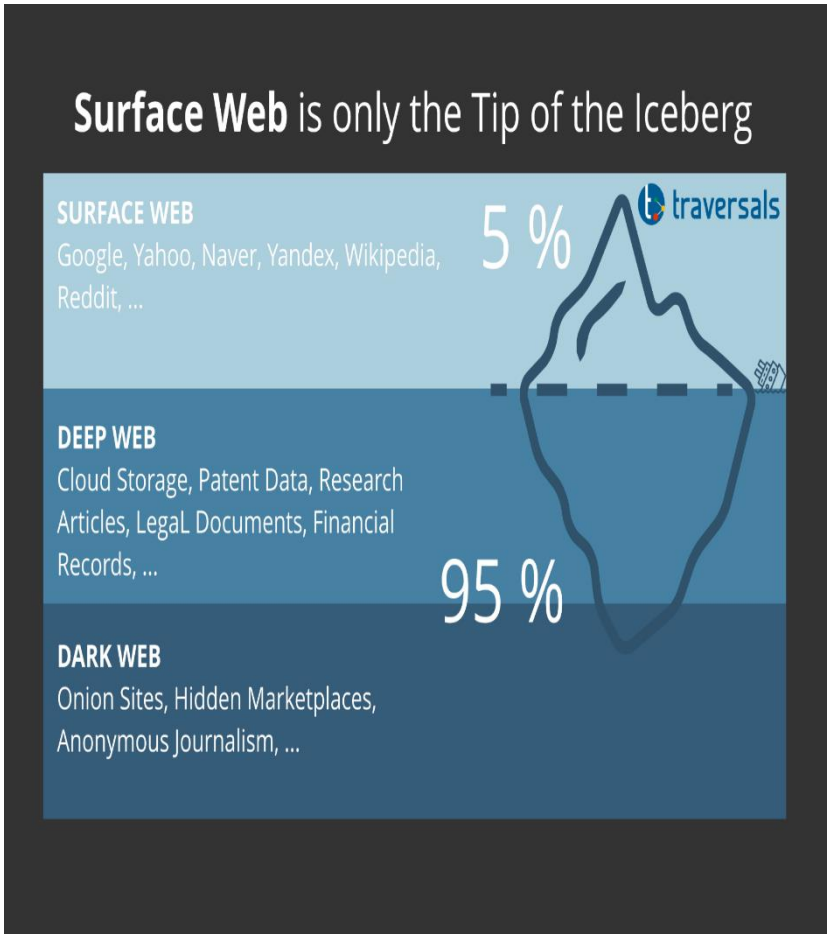
Black Market Service and Goods	Cost
U.S. Visa/Mastercard data (U.S. prices)	$15-$20 dollars (rising to $25-$30 for BIN number and DOB)
US Fullz data (Full ID package)	$30-$40
Generic Ransomware	$225 – $660
Ranion (Ransomware-as-a-service)	$120 per month
MegaCortex	$1000 or 1000 Euros and 10% of ransom
Unhacked Remote Desk Protocol Servers in multiple countries	$20 per RDP server
Amazon gift card with $1000 balance	$100
ATM skimmers	£500 to $1500
DDoS attack	$60 per hour
Money Transfer Services (PayPal, Bank Transfer, Western Union and Skrill)	Average of $800 for a balance of $10,000
Changes to credit history	From $130

暗網


1076C6206C6974746C6
DE3100A16C20Data Breach
2202E6F6163686573204C69
Cyber Attack696EA1
106564207368
C6E207468652

Darknet介紹(1/2)

一般使用者所熟悉存取之網站與資料相對整體網際網路而言，如同冰山一角，約只占5%



Surface Web

透過搜尋引擎對網站頁面進行索引，使用者可透過瀏覽器搜尋並進行存取

Deep Web

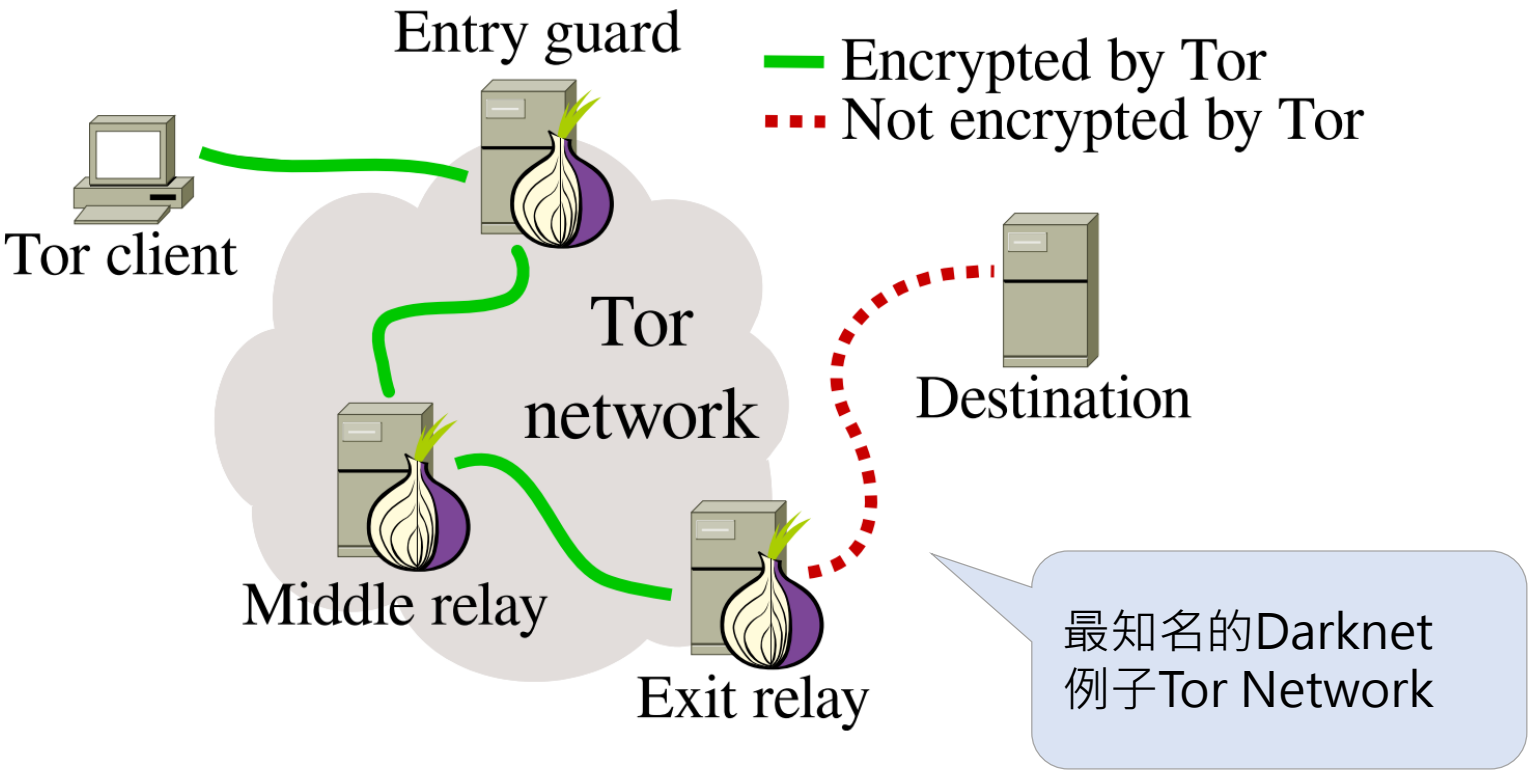
網路中不被搜尋引擎索引之網路頁面，必須登錄或透過特定方式連結才能訪問之服務與資料

Dark Web

僅能夠通過特定軟體，透過一定之設置與非標準通訊協定，在取得授權後，才能訪問之網站

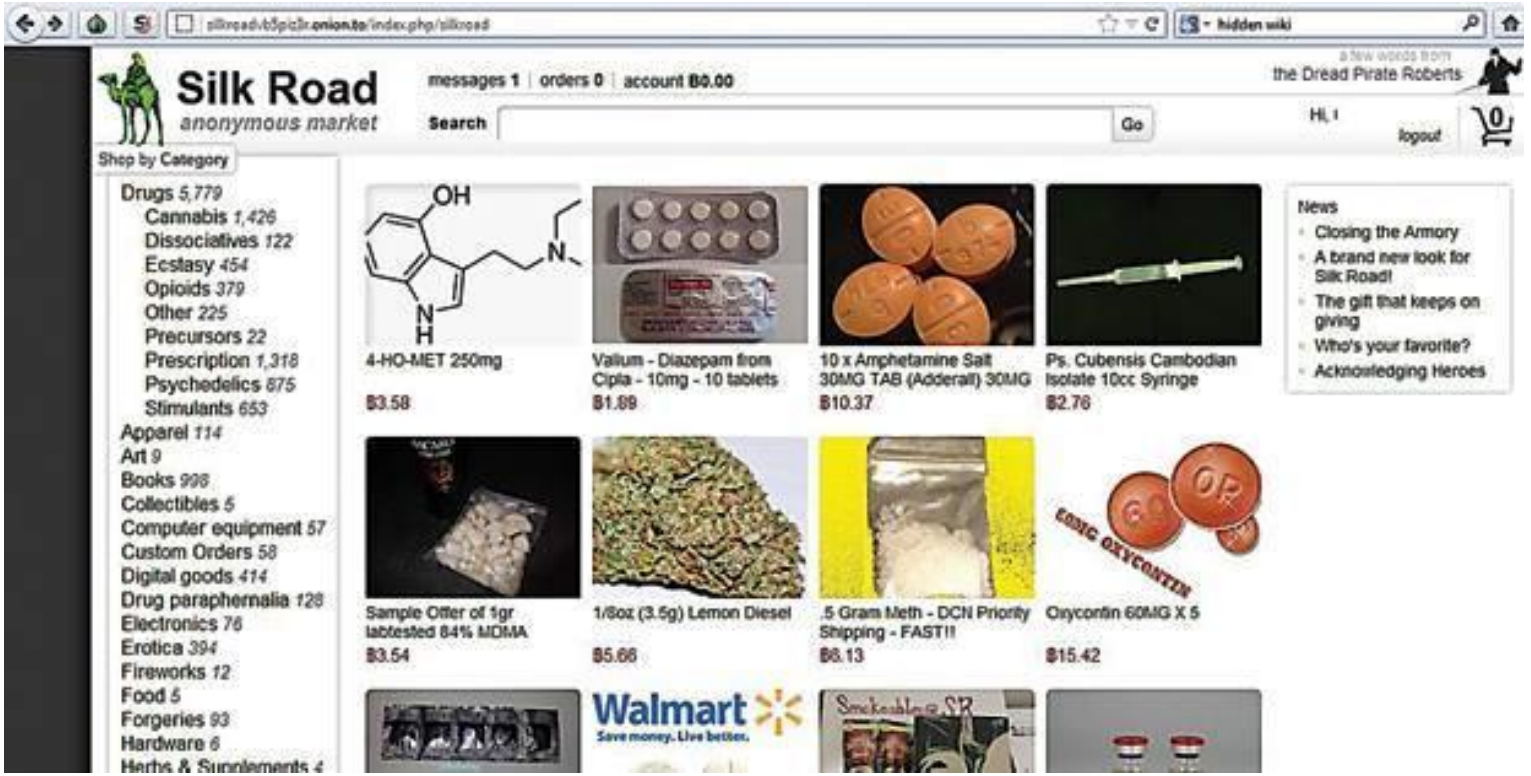
Darknet介紹(2/2)

- 通稱只能用特殊軟體、特殊授權、或對電腦做特殊設定才能連上的網路。通常採用匿名、匿蹤的技術
- 2015年匿名者以DDoS攻擊我國政機關網站，即透過此類網路確保攻擊IP的匿名性



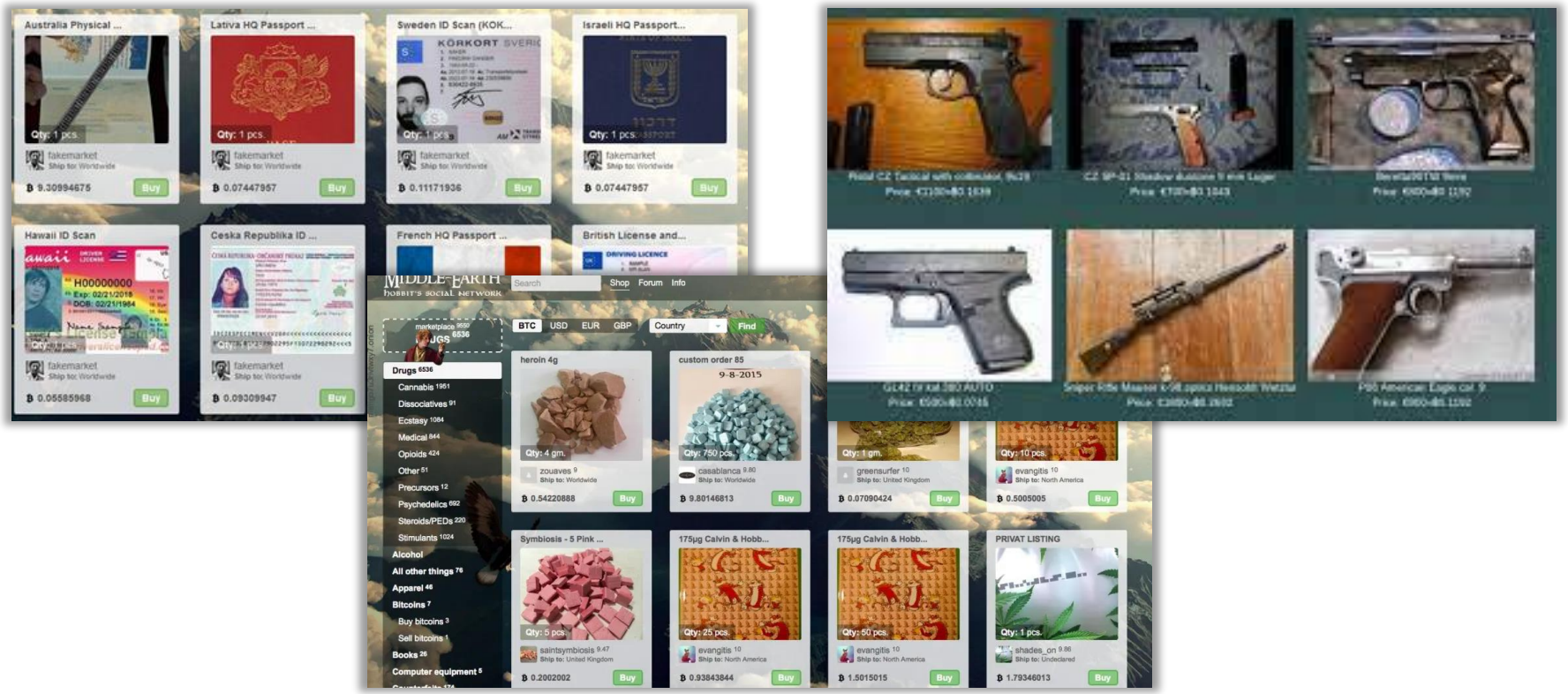
DarkWeb範例(1/4)

- 網路黑市–絲綢之路(Silk Road)
  - http://reloadedudjtjvxr.onion/
  - 簡單保密的交易媒合網站
  - 在2011年2月開辦，在2013年初被破獲



DarkWeb範例(2/4)

暗網本身雖不違法，惟其技術具備完整匿名特性，被犯罪分子廣為利用於槍枝、毒品、個資等非法交易之上



DarkWeb範例(3/4)

槍械店 – The Armory

- 供了多種重型槍械，滅聲槍、AK、散彈槍系列等，而且可以運輸至多達23個國家。

DarkWeb範例(4/4)

假鈔店 –

- http://factory6wldetihw.onion/

Tor 網站的分類比例

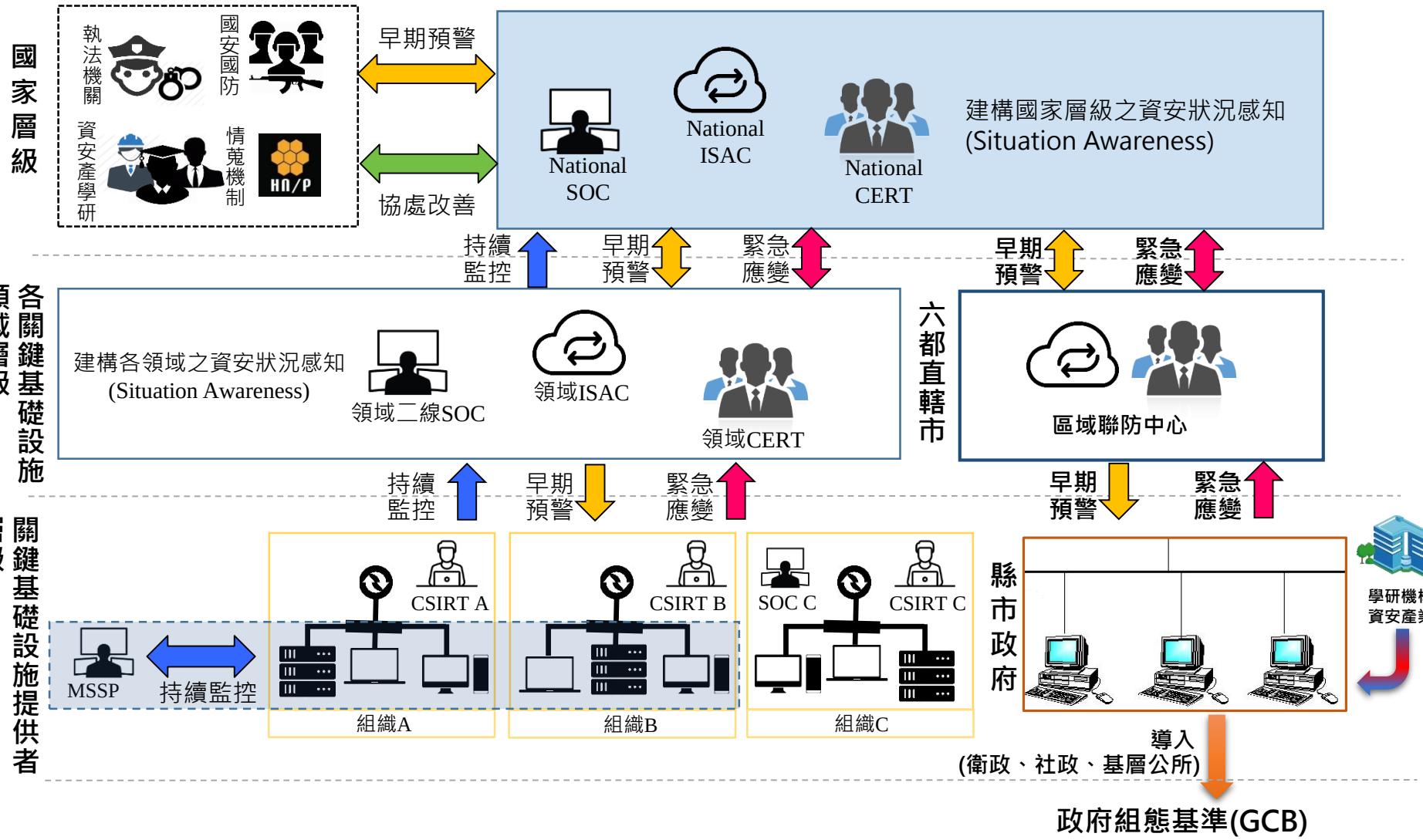
- 暴力資訊 0.3%
- 武器 0.8%
- 社會資訊 1.2%
- 黑客資訊 1.8%
- 非法色情 2.3%
- 社交網絡 2.3%
- 極端主義資訊 2.7%
- 未知的資訊 3.0%
- 其他非法資訊 3.8%
- 金融資訊 6.3%
- 毒品資訊 8.1%
- 其他資訊 19.6%
- 無意義數據 47.7%

政府領域資安防護現況


1076C6206C6974746C6
DE3100A16C20Data Breach
2202E6F6163686573204C69
BA701Cyber Attack696EA1
023 106564207368
C6E207468652

4層式政府資安防護縱深

資安聯防整體架構


國家層級
執法機關
國安國防
資安產學研
情蒐機制
早期預警
協處改善
National SOC
National ISAC
National CERT
建構國家層級之資安狀況感知
(Situation Awareness)
持續監控
早期預警
緊急應變
早期預警
緊急應變
領域層級
各關鍵基礎設施
建構各領域之資安狀況感知
(Situation Awareness)
領域二線SOC
領域ISAC
領域CERT
六都直轄市
區域聯防中心
持續監控
早期預警
緊急應變
早期預警
緊急應變
層級
關鍵基礎設施提供者
MSSP
持續監控
CSIRT A
CSIRT B
SOC C
CSIRT C
組織A
組織B
組織C
縣市政府
學研機構
資安產業
導入
(衛政、社政、基層公所)
政府組態基準(GCB)

機關資安責任等級核定情形

- 資通安全管理法自108年1月1日開始實施
- 核定之納管對象：7,709個(111年1月13日止)

公務機關

- 中央與地方機關(構)
- 公法人

(不包括軍事機關及情報機關)

特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

機關類型	A級	B級	C級	D級	E級	總數
中央機關	44	113	463	227	111	958
地方政府	0	103	578	4,938	708	6,327
特定非公務機關	46	123	149	85	21	424
全部類型	**90**	**339**	**1,190**	**5,250**	**840**	**7,709**

政府機關威脅情勢綜合評估

- APT惡意電郵為組織型駭客主要攻擊手法，各機關須持續加強人員資安意識，防範社交工程電子郵件攻擊
- 行動裝置或物聯網設備遭利用擴散惡意程式或殭屍網路，建議使用行動裝置應遵守相關資安規範，同時妥善管理物聯網設備
- 重大資安事件仍以個資外洩造成之衝擊為主，多肇因於網站或權限設計不當，建議機敏資料非必要不得置於公開網站
- 部分資安事件起因「廠商維護環境或管理疏失」，顯示委外廠商資安管理之重要性，應落實委外管理機制
- 資安事件缺乏相關紀錄，以致無法有效針對根因進行改善，顯示對於日誌紀錄保存仍有改善空間

關鍵基礎設施(CI)提供者

資通安全管理法第3條第7款：
關鍵基礎設施(CI)

定期檢視並
公告領域

資通安全管理法第3條第8款：

維運或提供關鍵基礎設施全部或一部

資通安全管理法第16條：
關鍵基礎設施(CI)提供者核定程序

中央目的事業主管機關指定

行政院核定

書面通知本法納管之CI提供者

建構國家資安聯防體系-地方政府

共同成果

1.建置區域ISAC並成為N-ISAC會員。
2.建置區域CERT
3.強化聯防資安監控，監控件數達50,000筆以上。

桃園市政府
1. 新竹縣
2. 新竹市
3. 苗栗縣

新北市政府
1. 宜蘭縣
2. 基隆縣

臺北市政府
1. 金門縣
2. 連江縣
3. 花蓮縣

臺中市政府
1. 彰化縣
2. 南投縣

臺南市政府
1. 嘉義縣
2. 嘉義市
3. 雲林縣

高雄市政府
1. 屏東縣
2. 臺東縣
3. 澎湖縣

桃園市區域聯防建構情資分享平台，並辦理通報演練就多種入侵手法與情境下進行實地攻擊。

臺中市區域聯防建構區域聯防APT動態威脅偵測系統，對可疑惡意程式進行沙箱分析，並將產出之特徵碼，同步派送至聯防縣市，另結合產官學合作促進技術交流及辦理鑑識營隊。

臺南市區域聯防提供實證場域予成功大學，對市府資訊系統進行滲透測試活動，找出相關弱點並修復，建立官學合作。

臺北市區域聯防建構端點防禦機制，109年發現1,101個新種惡意程式、235個風險IP。

新北市區域聯防建構區域聯防平台涵蓋聯防縣市共318 個機關(單位)，另推動公私協同合作，提供實證場域予國內業者建置Honey Pot。

高雄市區域聯防建置自動化弱點掃描系統，已收納聯防縣市892個主機共578個系統，並可排程掃描、弱點追蹤並自動複驗等，有效節省人力成本。

統計至109年12月31日止

加強資安整備(1/2)

- 強化漏洞修補
  - 隨時注意重大漏洞訊息，即時修補防護
  - 導入VANS系統，掌握即時訊息
  - 執行滲透測試與紅隊演練，主動發掘資安防護漏洞
- 完善備援機制
  - 做好系統備援，確保服務不中斷
  - 除熱備援與異地備援，宜同時考量資料離線備份，以防勒索軟體攻擊

- 落實系統紀錄保存
  - 妥善規劃保存系統紀錄，以利資安事件鑑識分析
  - 系統紀錄應包含應用程式與資料庫等紀錄訊息，以利分析事件根因，改善資安管理

加強資安整備(2/2)

機敏資料採取加密、遮罩、混淆等保護機制

使用高安全性之加密簽章憑證
使用加密傳輸協定傳遞資料，採行更安全加密演算法

定期分析資料庫稽核紀錄，發現潛在異常行為

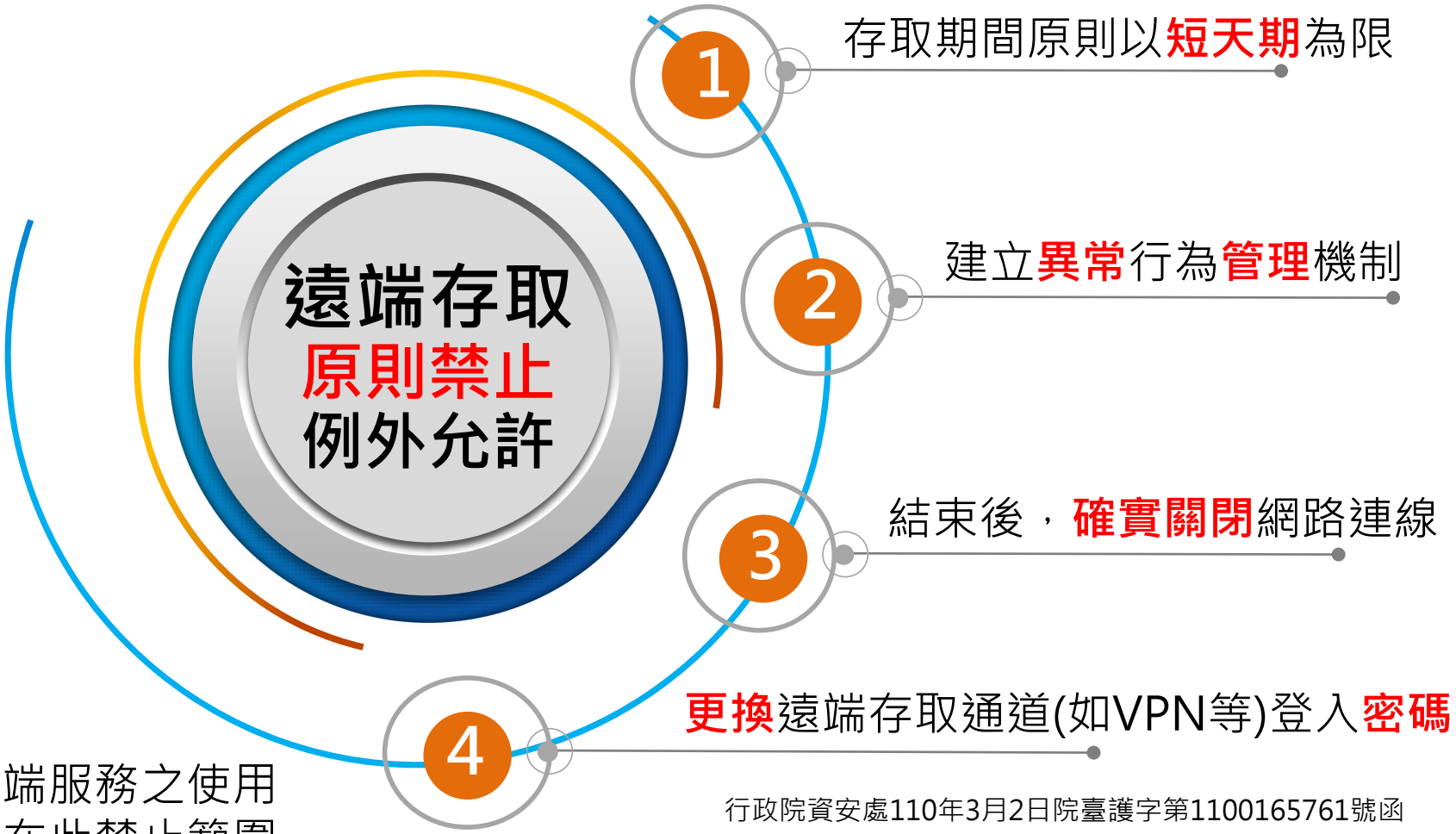
啟用帳號與密碼原則設定，強化帳號密碼安全性

精進縱深防禦(1/2)

- 落實黑名單部署
  - 於防火牆等資安防護設備定期更新黑名單，以技服中心提供黑名單為基礎，增列機關自有防護規則，確保資安防護即時有效
- 精進資安監控防護
  - 妥善規劃資安監控範圍，監控內外異常活動，即時告警
  - 加強關聯分析能量，提升資安監控防護有效性
- 落實權限控管
  - 人員帳號密碼採用最小權限原則，同時配合異常紀錄檢視，監控可疑活動
  - 資通系統權限設定，應納入上線前之檢驗項目
  - 加強供應商管理與來源管制，遠端連線原則禁止例外開放

精進縱深防禦(2/2)

- 針對供應商連線至機關內部環境應加強來源管制，遠端連線原則禁止例外開放



※雲端服務之使用不在此禁止範圍

行政院資安處110年3月2日院臺護字第1100165761號函

及時應變處理

- **阻斷APT竊密**
  - ●公務人員使用公開之雲端服務，應遵循機關之管理規範，並隨時通報異常事件，以利分析防護資安事件
  - ●機關之資安防護設備如 IPS/IDS 等，可部署APT攻擊偵測規則，及時阻斷駭客攻擊
- **完善系統紀錄收集保存**
  - ●妥善規劃保存系統紀錄，以利資安事件鑑識分析
  - ●系統紀錄應涵括應用程式與資料庫等紀錄訊息，以利分析事件根因，改善資安管理

公務機關資通訊產品使用原則

- 109年12月18日院臺護長字第1090201804A號行政院秘書長函諒達
- 公務用之資通訊產品**不得使用大陸廠牌**，且**不得安裝非公務用軟體**
- 個人資通訊設備不得處理公務事務，亦不得與公務環境介接
- 各機關應就已使用或採購之大陸廠牌資通訊產品**列冊管理**，且**不得與公務環境介接**，並儘速汰換
  - 大陸廠牌認定方式由機關「**從嚴認定**」

資通安全管理法架構


1076C6206C6974746C6
DE3100A16C20Data Breach
2202E6F6163686573204C69
Cyber Attack696EA1
106564207368
C6E20746865

資安法施行後之變革


適用範圍面
納管對象擴大
特定非公務
機關
資安管理
規定位階提
升為法令
維護計畫、
專職(責)人力
資安法
明定資通
安全推動事項
及情資分享
明定應辦
事項及控制
措施
規範面
管理面
政策及整合面
技術面

資通安全管理法之法案結構

- §1：立法目的
- §2：主管機關為行政院
- §3：名詞定義

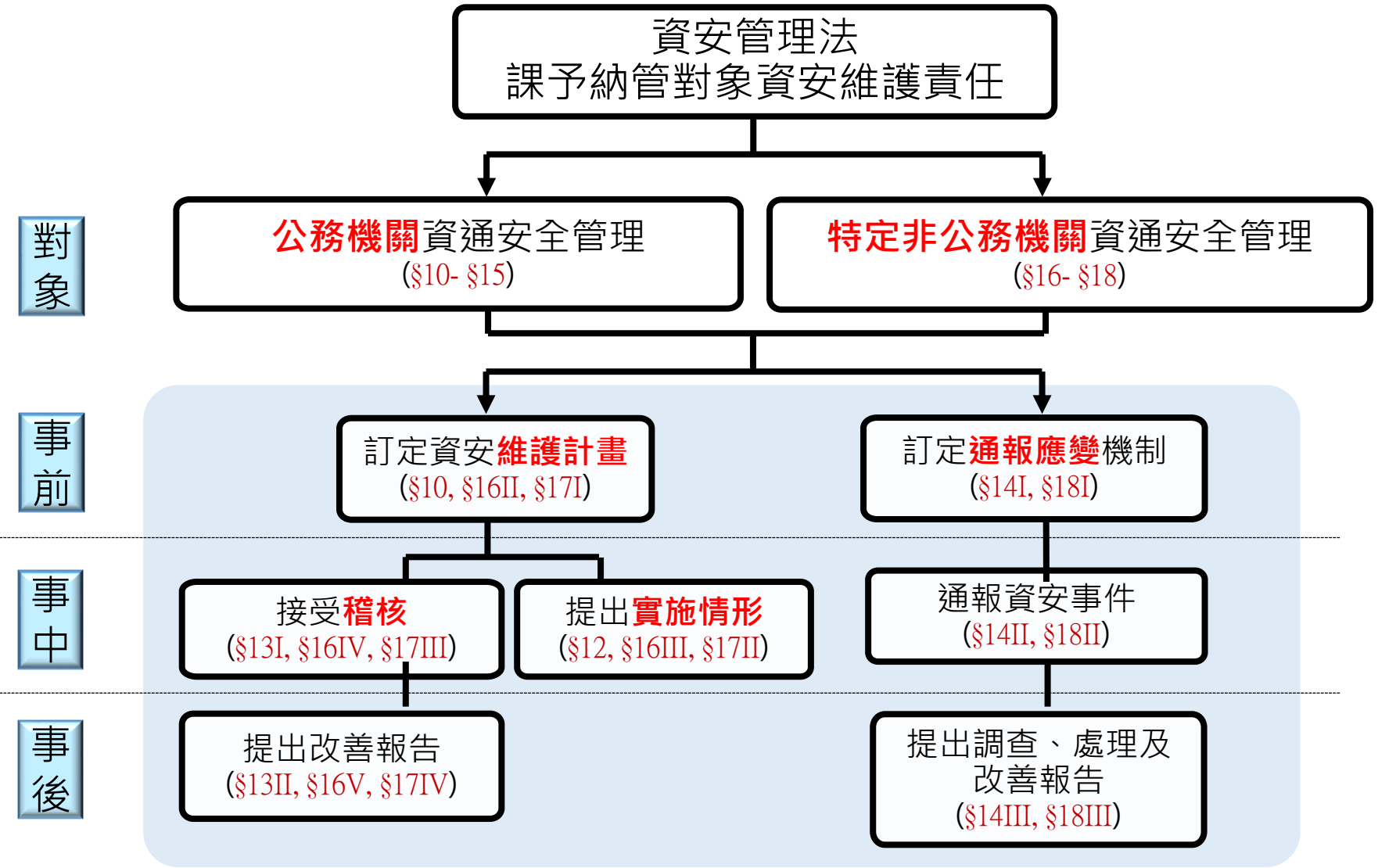
- §4：政府應整合民間力量推動資通安全相關事項
- §5：主管機關應規劃推動資安事務，並應提出相關報告
- §6：主管機關得委任委託公務機關、法人或團體辦理資安事務
- §7：主管機關應訂定責任等級分級辦法，並得稽核特定非公務機關
- §8：主管機關應建立情資分享機制

- §9：委外應注意事項
- §10：資安維護計畫之制定實施
- §11：應置資通安全長
- §12：資安維護計畫實施情形提出
- §13：上級機關應稽核所屬資通安全維護計畫實施情形
- §14： 應制定資安事通報及應變機制
- §15：所屬人員對於機關資通安全維護優良者，應給予獎勵

- §16：關鍵基礎設施(CI)提供者之資通安全管理(指定核定程序、維護計畫制定、實施情形提出、稽核)
- §17：CI提供者以外特定非公務機關之資通安全管理 (維護計畫制定、實施情形提出、稽核)
- §18：應制定資安事件通報應變機制

- §19：公務機關所屬人員之懲戒或懲處
- §20、21：特定非公務機關之罰則

資安管理法之規範架構


資安管理法
課予納管對象資安維護責任
對象
公務機關資通安全管理
(§10- §15)
特定非公務機關資通安全管理
(§16- §18)
事前
訂定資安維護計畫
(§10, §16II, §17I)
訂定通報應變機制
(§14I, §18I)
事中
接受稽核
(§13I, §16IV, §17III)
提出實施情形
(§12, §16III, §17II)
通報資安事件
(§14II, §18II)
事後
提出改善報告
(§13II, §16V, §17IV)
提出調查、處理及
改善報告
(§14III, §18III)

立法目的及規範對象

□立法目的

為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。

□規範對象

以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象。

公務機關

- 中央與地方機關(構)
- 公法人

特定非公務機關

- 關鍵基礎設施提供者
- 公營事業
- 政府捐助之財團法人

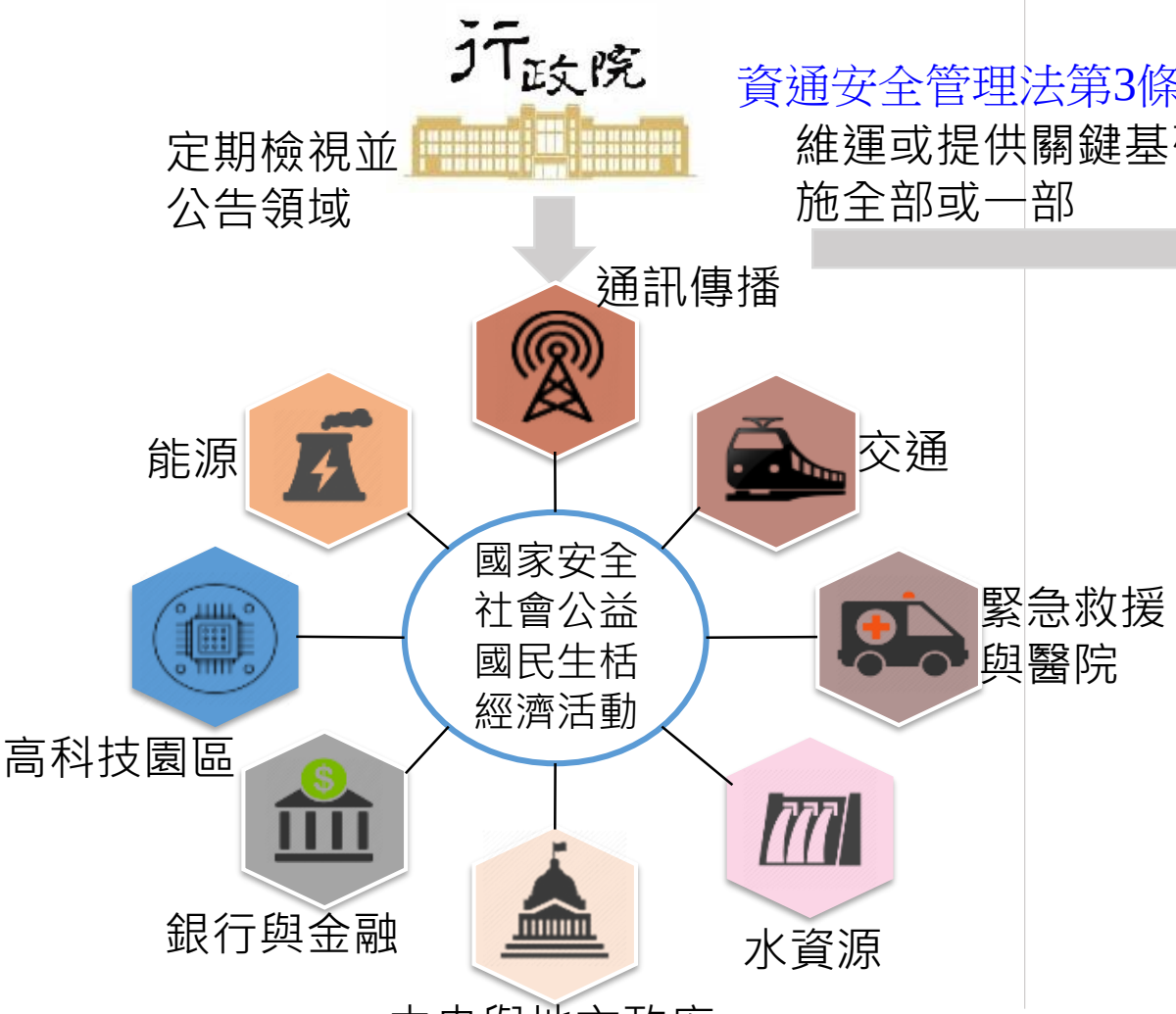
*資安管理法第三條第五款
公務機關：指依法行使公權力之中央、地方機關(構)或公法人。但不包括軍事機關及情報機關。

*資安管理法施行細則第二條
所稱軍事機關，指國防部及其所屬機關(構)、部隊、學校；所稱情報機關，指國家情報工作法第三條第一項第一款規定之機關。

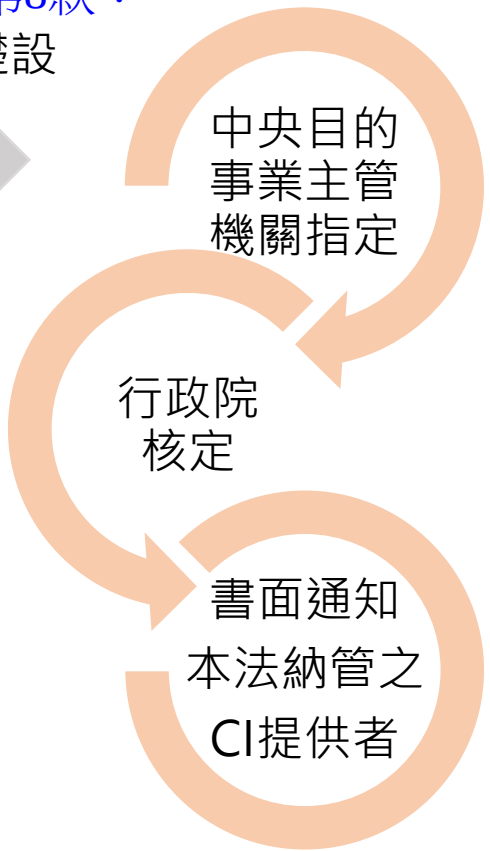
關鍵基礎設施(CI)提供者

資通安全管理法第3條第7款：
關鍵基礎設施(CI)

資通安全管理法第16條：
關鍵基礎設施(CI)提供者核定程序

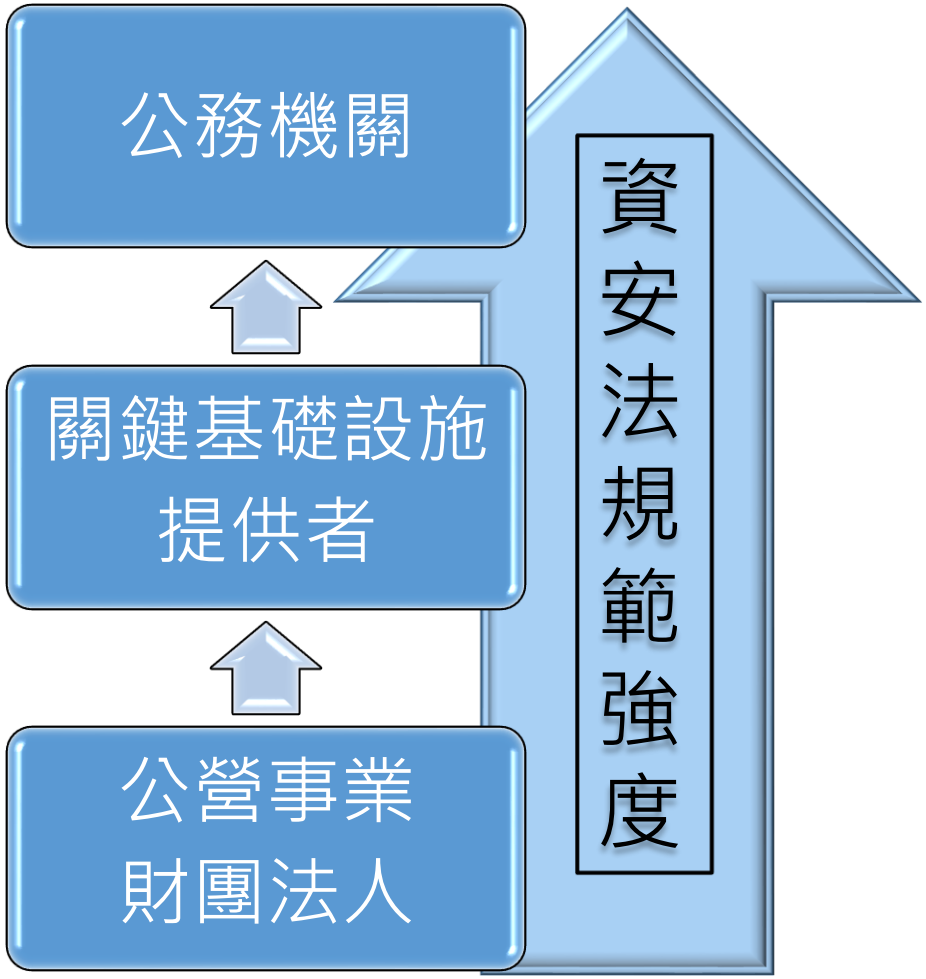


資通安全管理法第3條第8款：
維運或提供關鍵基礎設施全部或一部

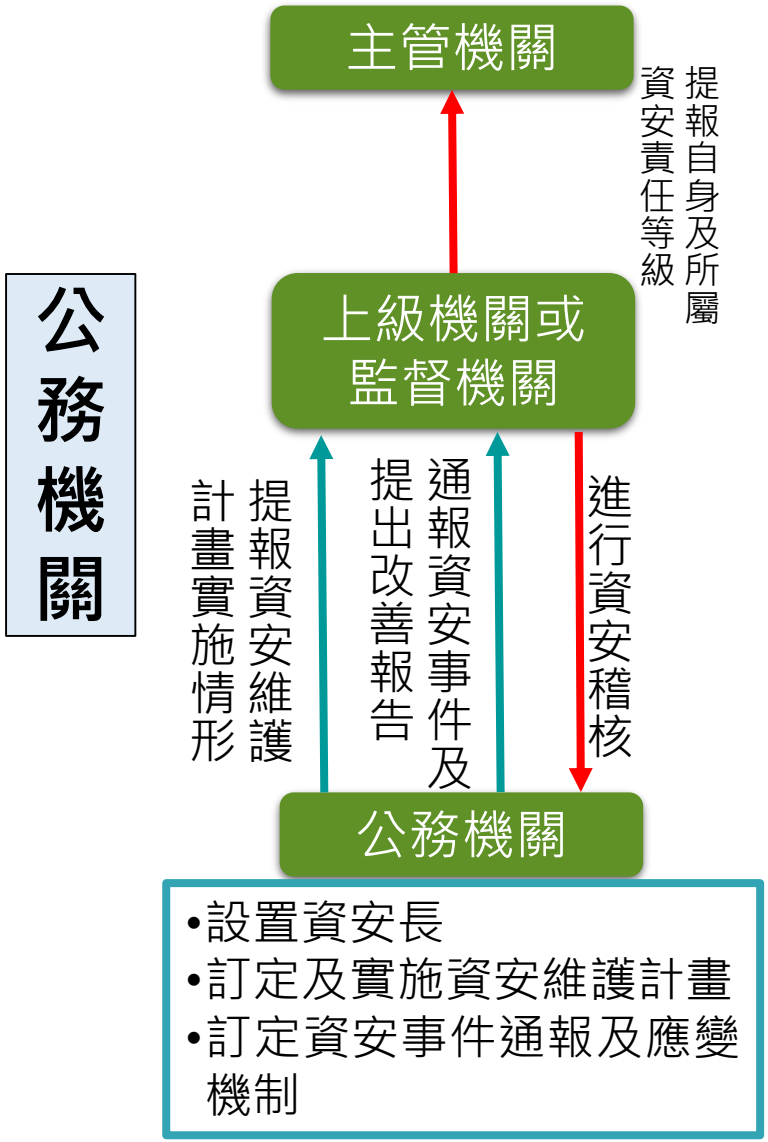


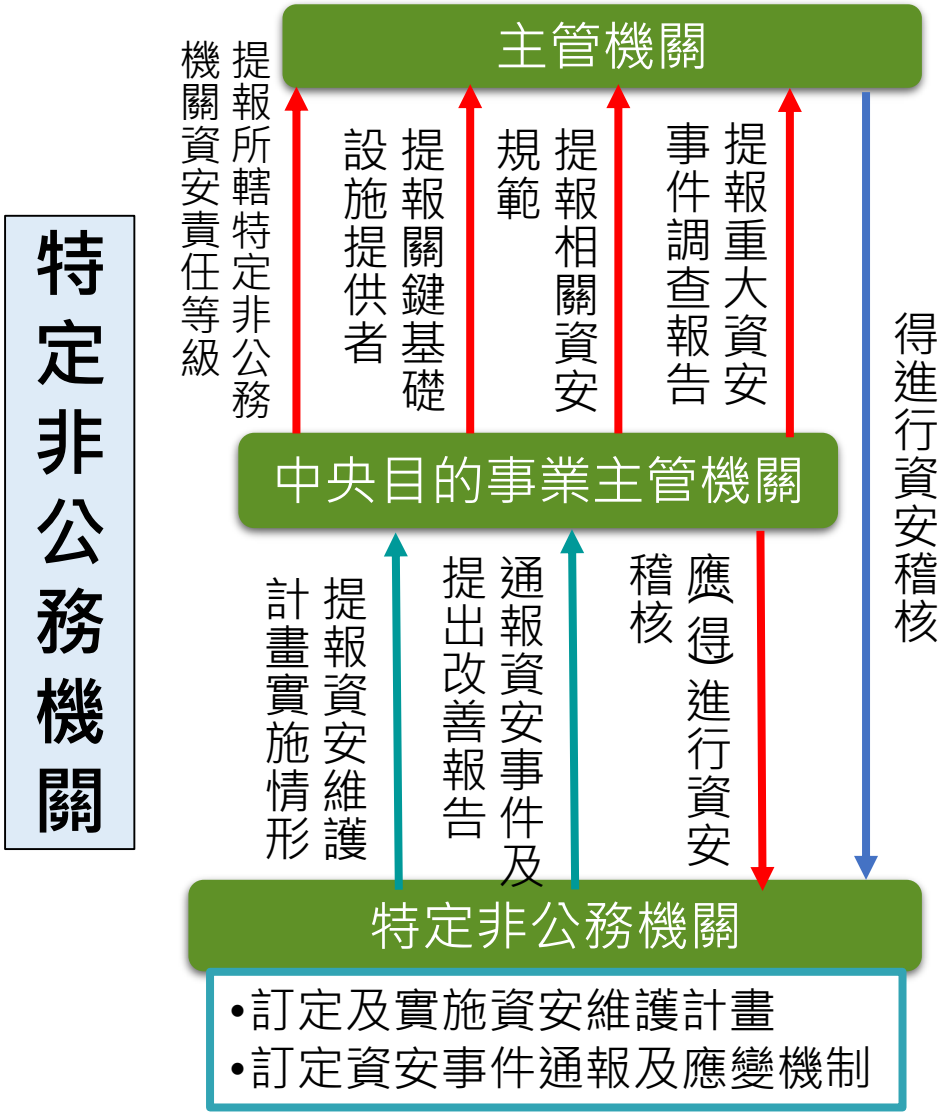
本法規範適用先後

- 兼具公營事業/財團法人及CI提供者
  - 優先適用CI提供者之規定
  - 如：台電、中油



角色與權責


公務機關
主管機關
提報自身及所屬資安責任等級
上級機關或監督機關
提報資安維護計畫實施情形
通報資安事件及提出改善報告
進行資安稽核
公務機關
•設置資安長
•訂定及實施資安維護計畫
•訂定資安事件通報及應變機制


特定非公務機關
主管機關
提報所轄特定非公務機關資安責任等級
提報關鍵基礎設施提供者
提報相關資安規範
提報重大資安事件調查報告
得進行資安稽核
中央目的事業主管機關
提報資安維護計畫實施情形
通報資安事件及提出改善報告
應(得)進行資安稽核
特定非公務機關
•訂定及實施資安維護計畫
•訂定資安事件通報及應變機制

公務機關之資通安全管理

✓ 應訂定、修正及實施資通安全維護計畫§10
✓ 應訂定通報及應變機制§14 I

行政院

- 擘劃並推動國家資通安全政策
- 資通安全科技發展
- 國際交流合作及資通安全整體防護
- 定期公布國家資安情勢報告及資通安全發展方案

訂定

- 應提出年度資通安全維護計畫之實施情形§12
- 應提出改善報告§13 II
- 應通報資通安全事件§14 II
- 應提出資通安全事件之調查、處理及改善報告§14 III

上級或監督機關 ⇄ 下級或受監督機關

- 應稽核資通安全維護計畫實施情形§13 I

總統府、立法院、司法院、考試院、監察院、直轄市政府、直轄市議會、縣（市）政府及縣（市）議會

設置資通安全長§11

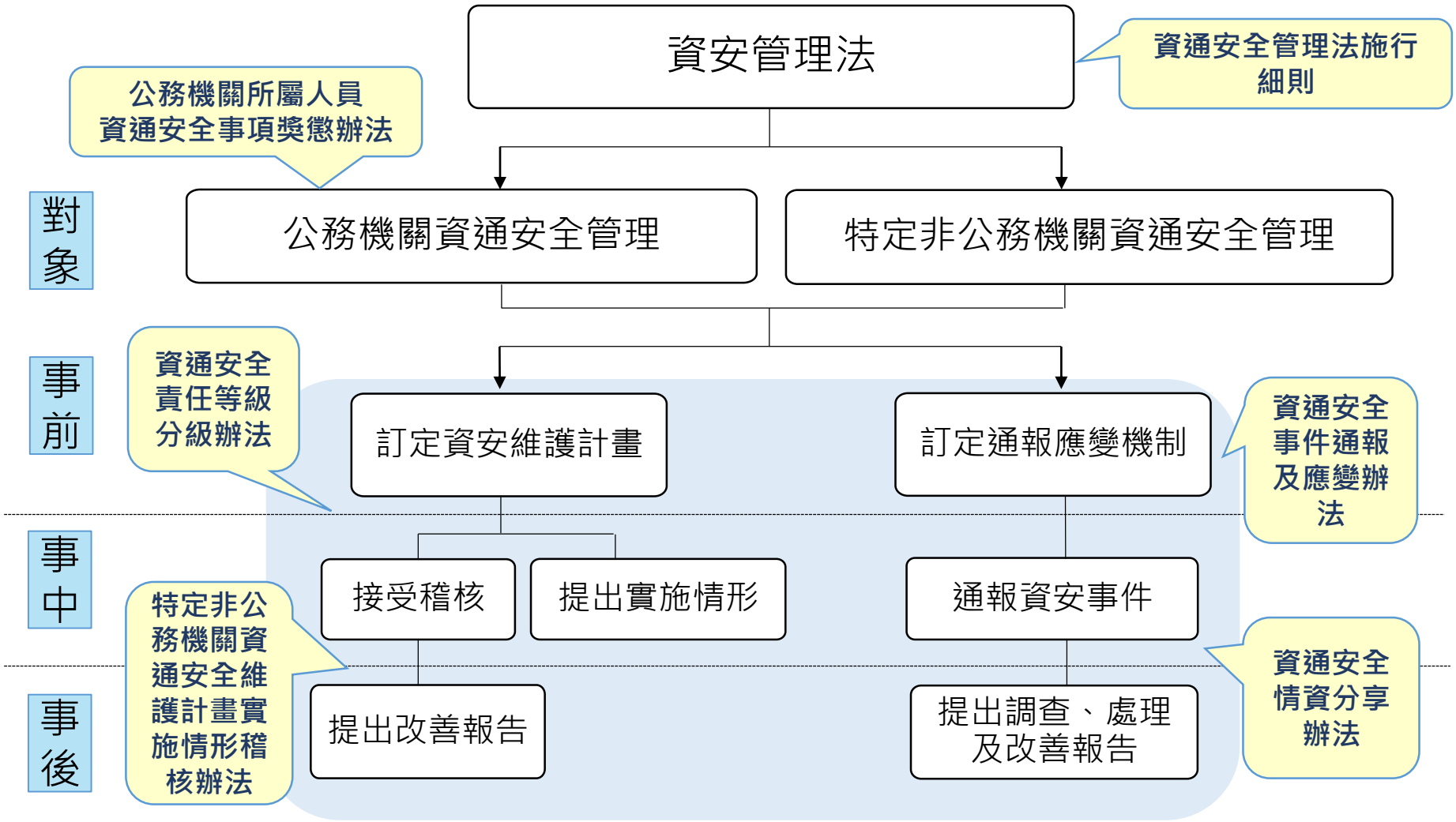
- ✓資安管理法施行細則§22
- ✓資安責任等級分級辦法§7
- ✓資安事件通報及應變辦法§14、18
- ✓維護計畫實施情形稽核辦法§7、13
- ✓資安情資分享辦法§8
- ✓公務人員獎懲標準§15、§19

特定非公務機關之資通安全管理

	關鍵基礎設施提供者	公營事業、政府捐助之財團法人
資通安全維護計畫	①應訂定、修正及實施資通安全維護計畫§16 ②應提出資通安全維護計畫之實施情形§16 ③應提出資通安全維護計畫之改善報告§16	①應訂定、修正及實施資通安全維護計畫§17 ②得提出資通安全維護計畫之實施情形§17 ③應提出資通安全維護計畫之改善報告§17
通報應變	④應訂定通報及應變機制§18 ⑤應通報資安事件，並提出調查、處理及改善報告§18	

罰則 §20~§21

資安管理法各子法授權來源



資通安全管理法施行細則

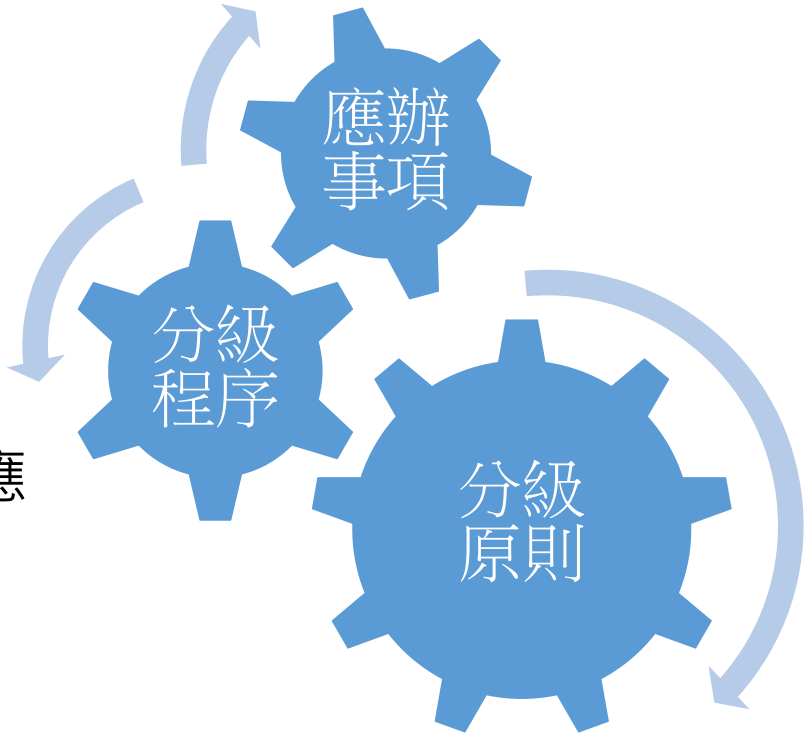
法令遵循義務重點

- 資通安全維護計畫實施情形稽核有缺失或待改善者，應提出改善報告之內容、方式及時間(§3)
- 委外辦理資通系統之建置、維運或資通服務之提供，於選任及監督受託者時應注意事項(§4)
- 資通安全維護計畫及其實施情形之內容應載明事項(§6)
- 核心業務及核心資通系統定義(§7)
- 資通安全事件調查、處理及改善報告應載明之事項(§8)

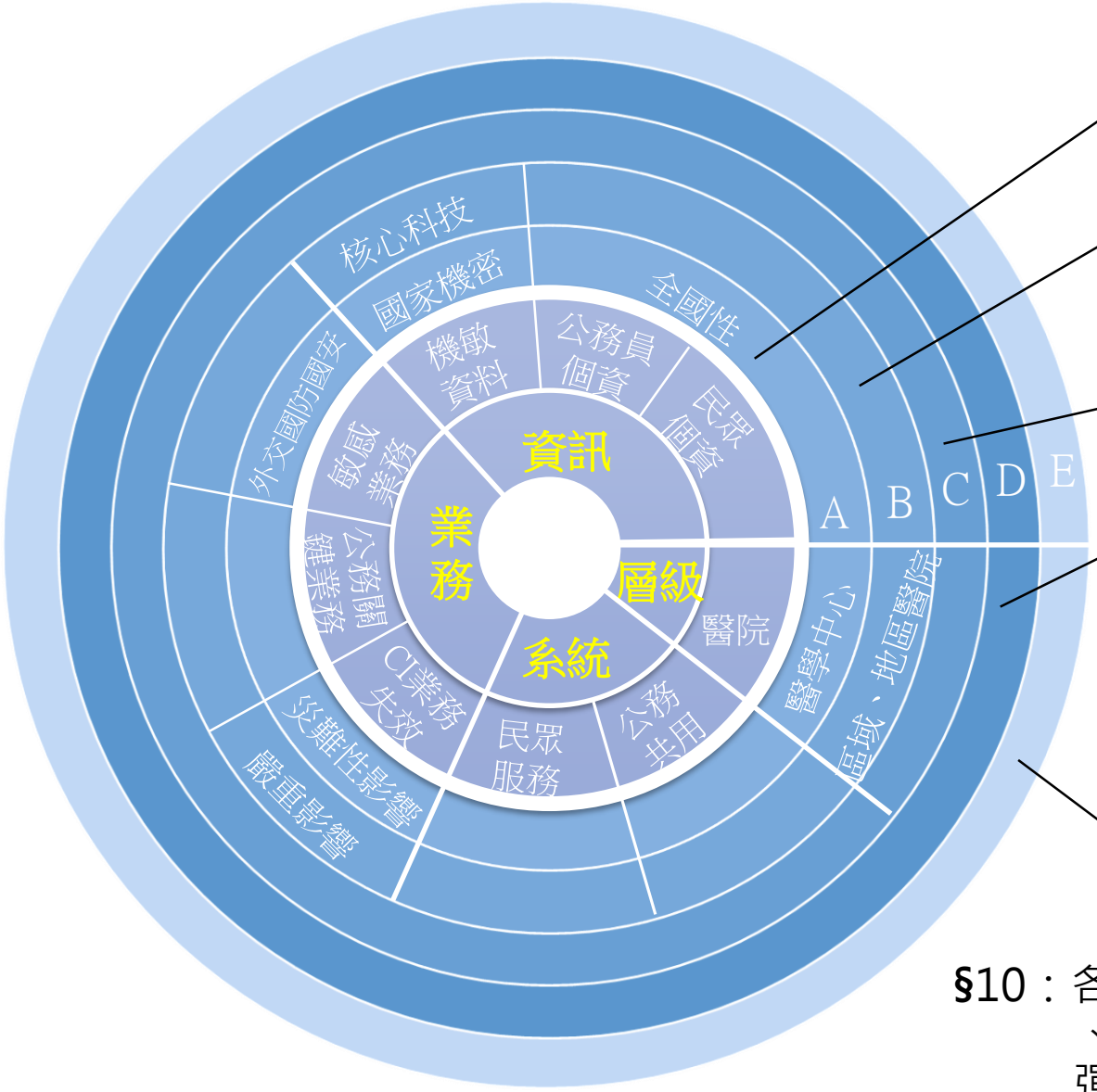
資通安全責任等級分級辦法

法令遵循義務重點

- 各機關應提報或核定責任等級(§3)
- 各機關應依附表規定辦理其資通安全責任等級應辦事項(§11)
  - 附表1至附表8：各等級機關應辦事項
  - 附表9：資通系統防護需求分級原則
  - 附表10：資通系統防護基準



資通安全責任等級分級原則



A級：**全國**性

B級：**區域**或地區性

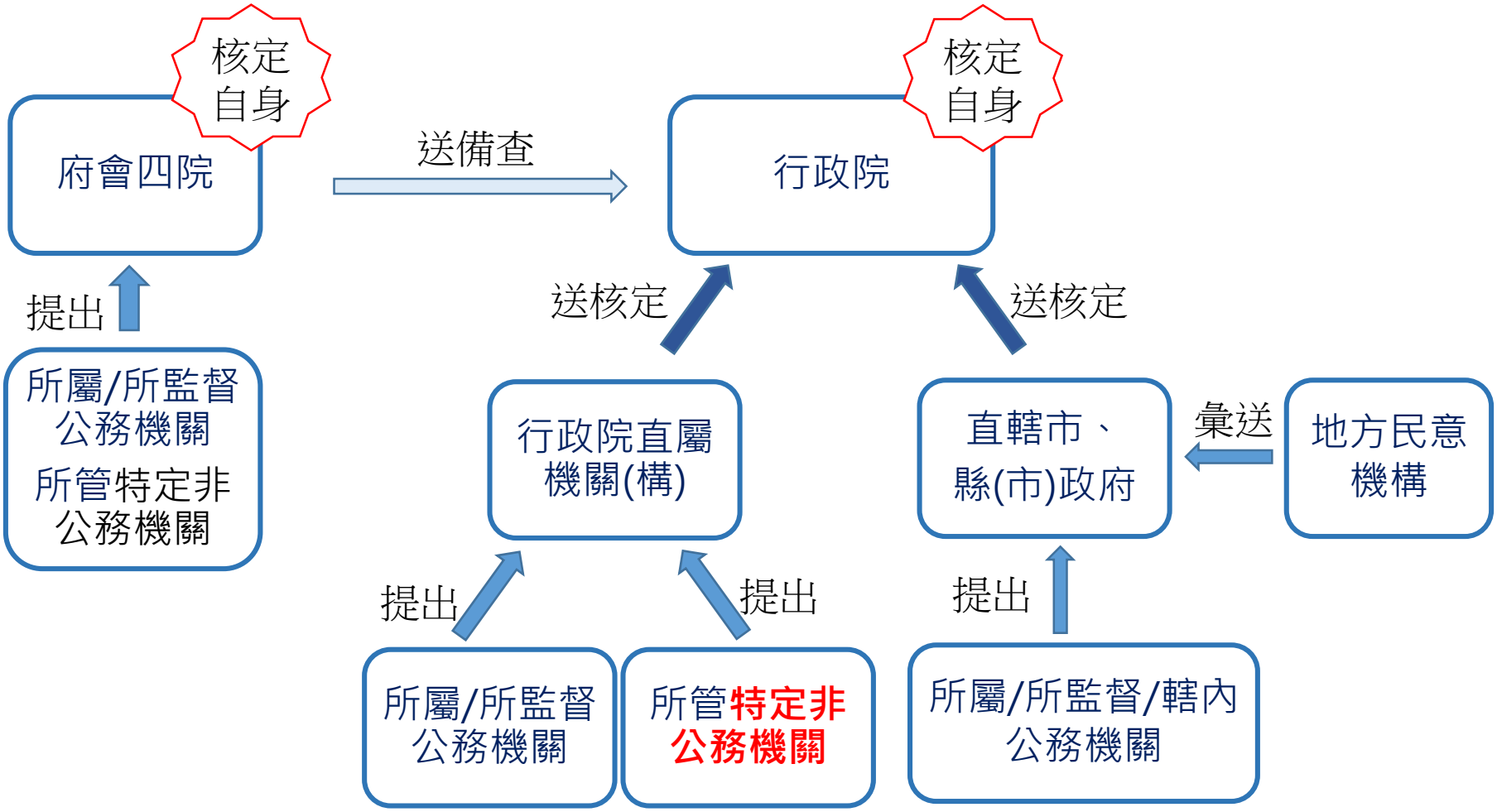
C級：維運自行或委外設置、開發之**資通系統**者

D級：自行辦理**資通業務**，未自行或委外開發資通系統者

E級：無資通系統且未提供資通服務、全部資通業務由上級、監督或中央目的事業主管機關兼辦或代理。

§10：各機關得考慮其對國家安全、社會公益或人民之影響，彈性調整其等級

資通安全責任等級分級程序

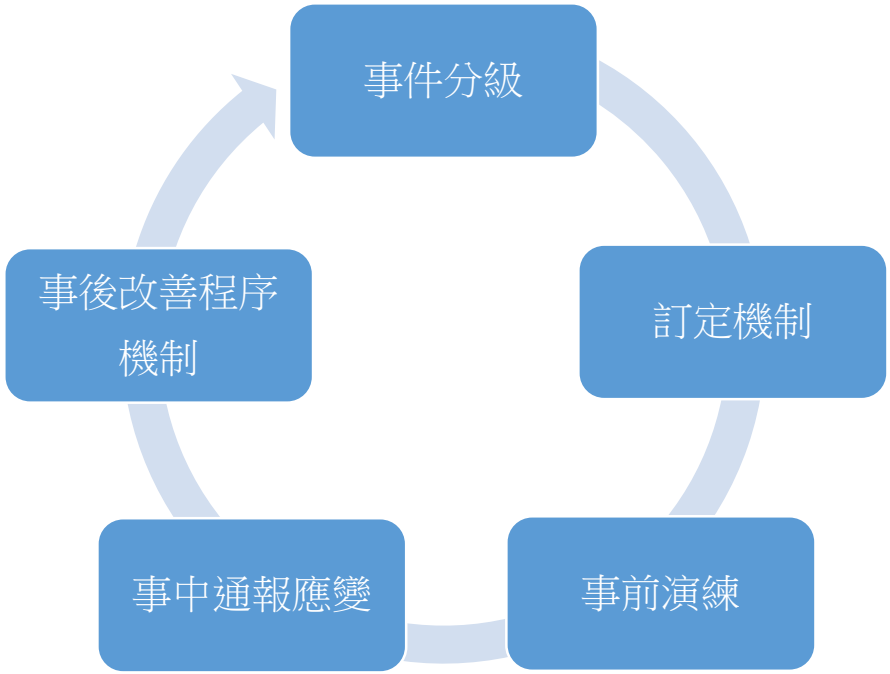


一般機關：每2年核定一次
新設或職務調整機關：1個月內辦理等級辦更

資通安全事件通報及應變辦法

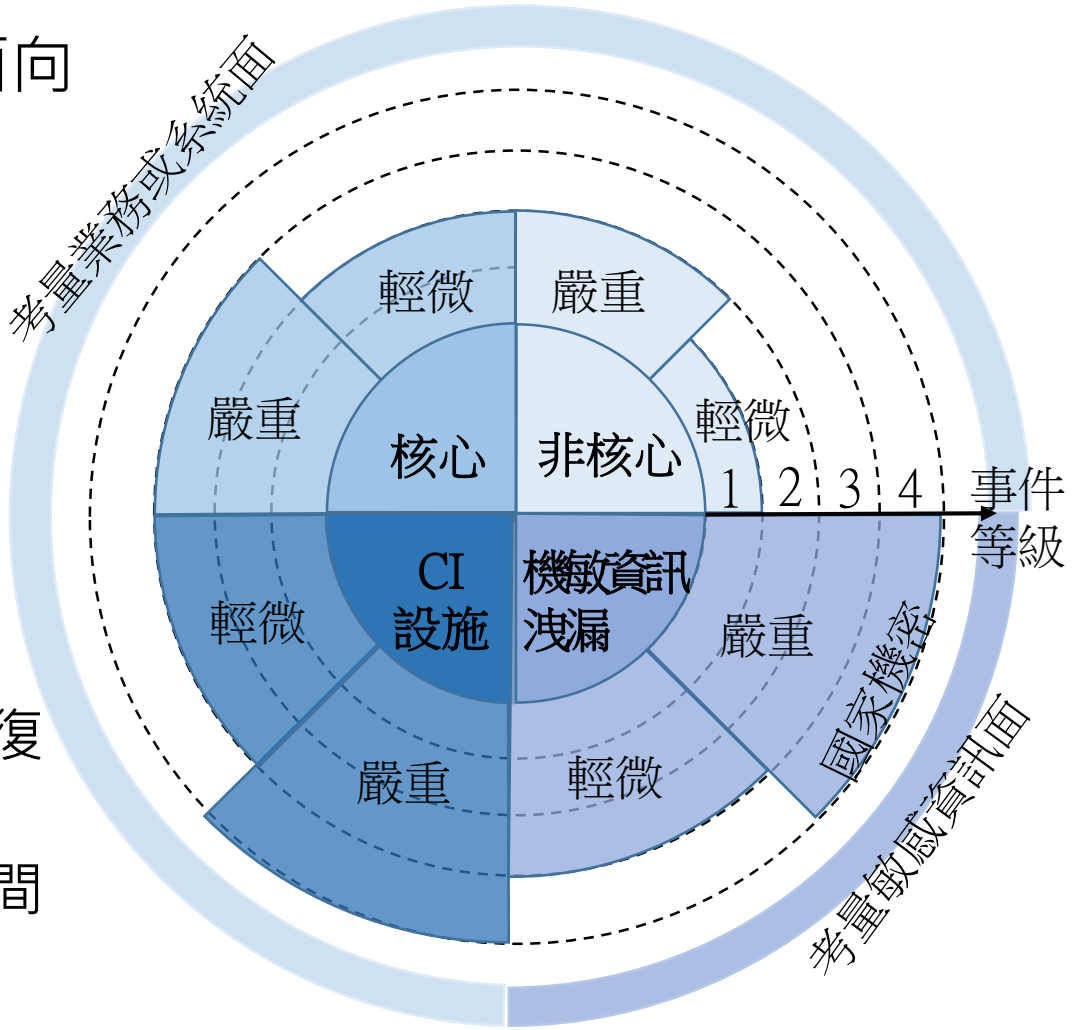
法令遵循義務重點

- 資通安全事件之通報方式、時限及程序(§4、§11)
- 資通安全事件等級之審核、時限及程序(§5、§12)
- 資通安全事件之應變方式、時限及程序(§6、§13)
- 機關應就資通安全事件之**通報與應變**訂定作業**規範**及其應包括事項(§9、§10、§18、§19)
- 公務機關資通安全**演練作業**之**規劃**、辦理及其內容(§8)



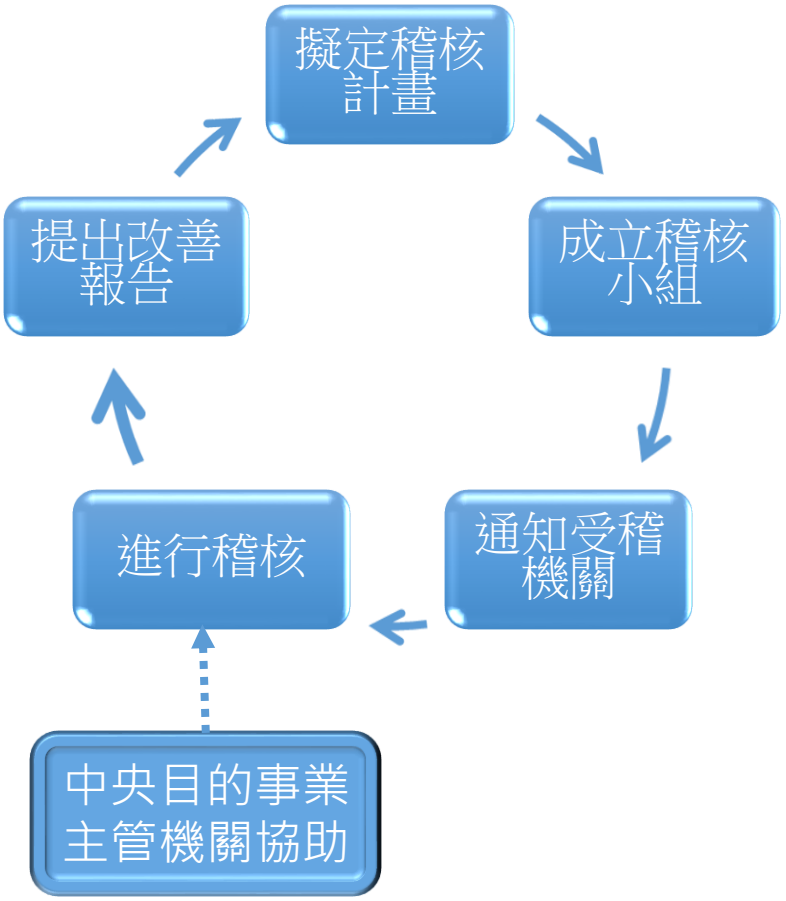
資通安全事件分級

- 確認資安**事件標的**
- **影響程度**：C、I、A三面向
  - **機密性(C)**
    - 業務資訊遭**洩漏**
  - **完整性(I)**
    - 業務資訊遭**竄改**
    - 資通系統遭竄改
  - **可用性(A)**
    - 業務受影響或**停頓**，是否於可接受時間內回復
    - 核心資訊系統受影響或停頓，是否於可接受時間內回復



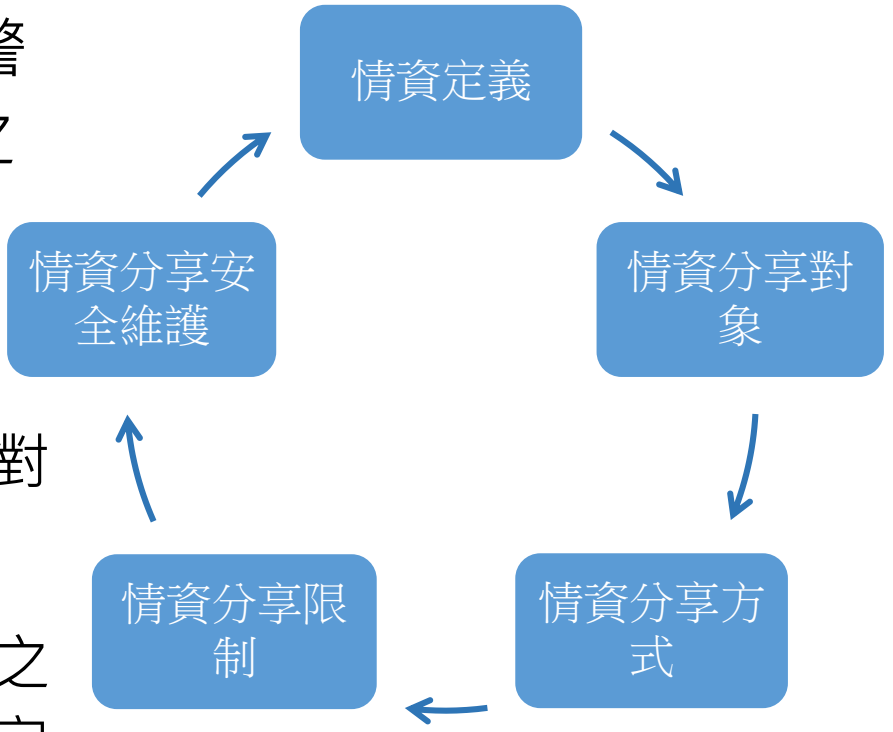
特定非公務機關資通安全維護計畫稽核辦法

- **主管機關**對特定非公務機關進行稽核之辦法。
- 敦促實施資安維護計畫，協助其發現該計畫內容或實施之不足。
- **法令遵循義務重點**
  - 受稽核機關就主管機關之稽核應配合之事項(§5)
  - 受稽核機關改善報告與執行情形之提出方式及時程(§8)
  - 主管機關得要求受稽核機關之中央目的事業主管機關協助辦理稽核(§9)



資通安全情資分享辦法

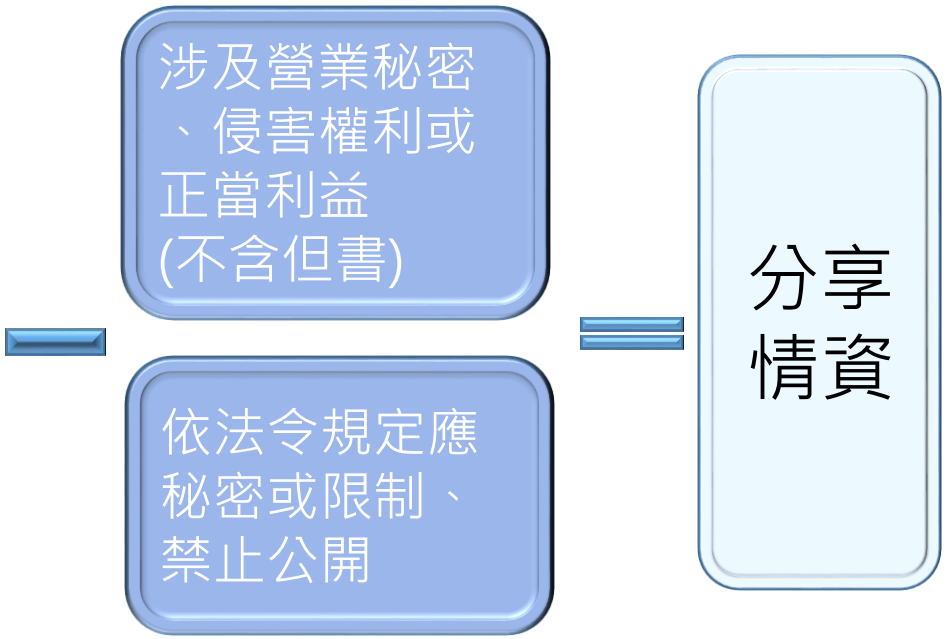
- 提升各機關對於資安之預警能力，強化資安相關資訊之交流。
- **法令遵循義務重點**
  - 進行資通安全情資分享之對象及義務(§3)
  - 分享及接收資通安全情資之注意事項及安全維護之規定(§5、§8)
  - 資通安全情資分析及整合之規定(§6、§7)



情資分享之內容

情資定義(§2)

情資分享例外(§4)



公務機關所屬人員資通安全事項獎懲辦法

□法令遵循義務重點

- 公務機關就其所屬人員辦理業務涉及資通安全事項之獎懲，**得**依本辦法之規定**自**行**訂**定**獎懲基準**(§2)
- 公務機關所屬人員辦理業務涉及資通安全事項，應予獎勵及懲處之情形(§3、§4)
- 公務機關辦理所屬人員之平時考核，應審酌本辦法所定獎勵 、懲處情形及事實發生之原因等因素為之(§5)
- 公務機關對所屬人員作成懲處前，應給予當事人**申辯**之機會；必要時得就所涉資通安全專業事項，徵詢相關專家學者之意見(§6)

國家資通安全發展方案


1076C6206C6974746C6
DE3100A16C20Data Breach
2202E6F6163686573204C69
BA701Cyber Attack696EA1
023 106564207368
C6E207468652A

一步一腳印，逐步擴大

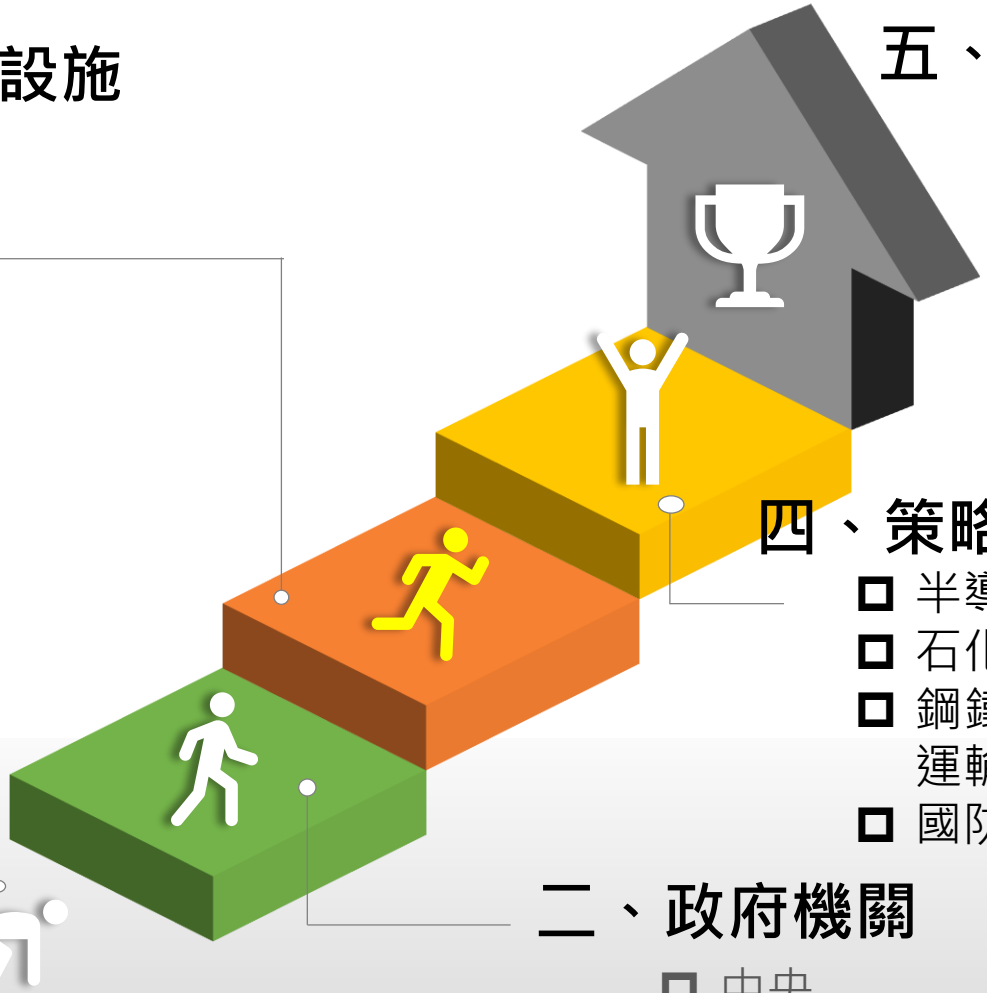
三、關鍵基礎設施

- 水
- 能源
- 通訊傳播
- 交通運輸
- 緊急醫療
- 金融
- 科學園區

五、帶動資安產業發展

四、策略性產業

- 半導體、資通訊
- 石化、食品醫藥
- 鋼鐵、工具機、運輸工具
- 國防、航太



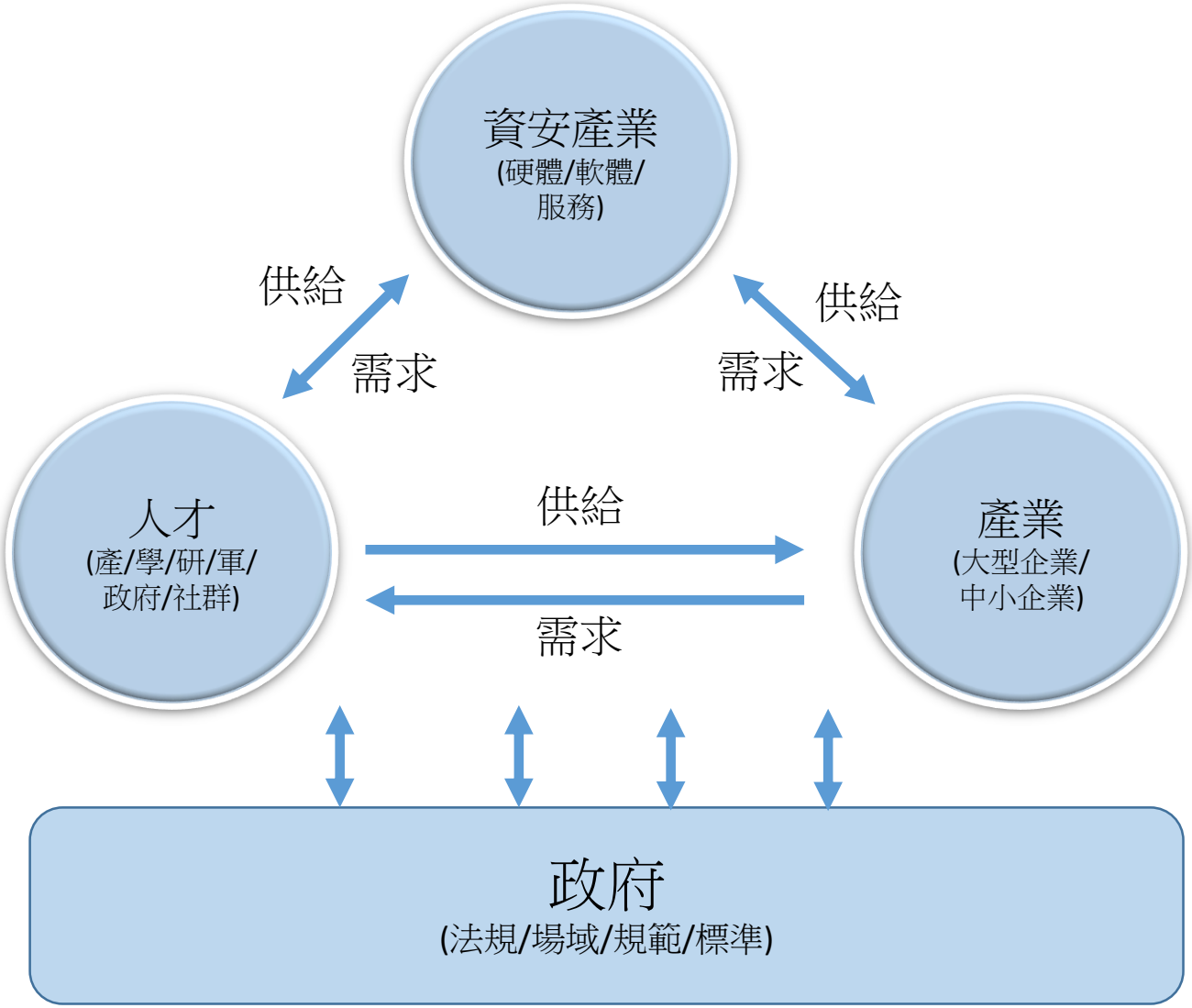
一、資通安全管理法

- 107 年6月6日公布
- 108 年1月1日實施

二、政府機關

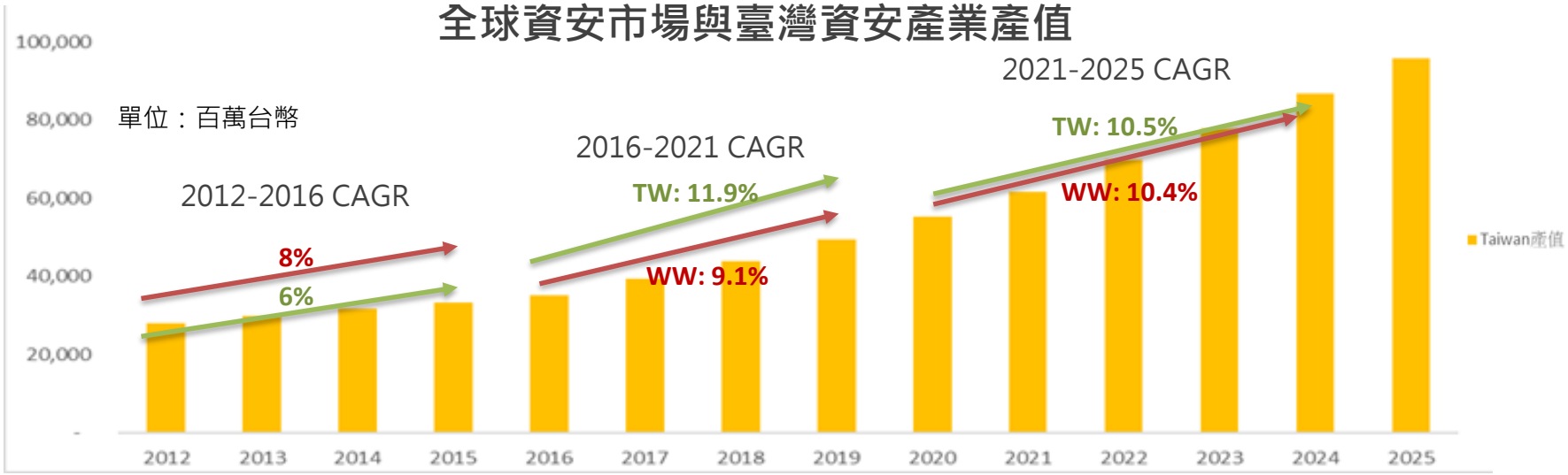
- 中央
- 地方
- 國營事業
- 財團法人

建構資安生態系


資安產業
(硬體/軟體/
服務)
供給
需求
供給
需求
人才
(產/學/研/軍/
政府/社群)
供給
需求
產業
(大型企業/
中小企業)
政府
(法規/場域/規範/標準)

2025年臺灣資安產業產值推估

- 2025年臺灣自主產品與服務產值可達900億
  - 2016-2021年在資安即國安政策推動下，國內產業複合成長率達**11.9%**超過全球的9.1%，2021-2025年預期將可同步全球達**10.5%**。
- 台灣資安產業多屬中小企業，受限於資源及人力，創新自主性不足，國際拓展不易，若能由政策面著手，強化新興領域資安解決方案的淬煉，擴增國內資安需求，將可促成資安產業之**自主化**、**規模化**及**國際化**。



資料來源：工研院產科國際所

國內資安產業現況

資安產業總產值
2017年：393.5億元
2018年：439.4億元
2019年：493.4億元
2020年：552.0億元
2020年共324家廠商

網路與閘道安全

2017年產值：新臺幣115.9億元
2018年產值：新臺幣124.5億元
2019年產值：新臺幣139.5億元
參與廠商：53家
↑12.0%

防火牆, IDS/IPS,UTM, APT防護,...

物聯網安全

2017年產值：新臺幣16.5億元
2018年產值：新臺幣18.1億元
2019年產值：新臺幣20.0億元
參與廠商：13家
↑10.5%

IOT加密模組、ICS Gateway、IC PUF...

終端與行動裝置防護

2017年產值：新臺幣84.8億元
2018年產值：新臺幣95.9億元
2019年產值：新臺幣108.3億元
參與廠商：31家
↑12.9%

身份驗證、存取控制、防毒/惡意程式防護...

資安支援服務

2017年產值：新臺幣2.6億元
2018年產值：新臺幣2.8億元
2019年產值：新臺幣3.3億元
參與廠商：12家
↑17.9%

資安教育訓練、資安保險服務...

資安營運管理服務

2017年產值：新臺幣41.3億元
2018年產值：新臺幣45.0億元
2019年產值：新臺幣50.3億元
參與廠商：13家
↑11.8%

SOC監控服務、ISAC服務、雲端資產管理...

資料與雲端應用安全

2017年產值：新臺幣23.6億元
2018年產值：新臺幣24.6億元
2019年產值：新臺幣26.5億元
參與廠商：24家
↑7.7%

Email安全、WAF設備、內容過濾軟體、資料庫安全...

資安檢測/顧問服務

2017年產值：新臺幣50.3億元
2018年產值：新臺幣55.0億元
2019年產值：新臺幣61.7億元
參與廠商：46家
↑12.2%

資安顧問、資安驗證、稽核鑑識、資安檢測...

資安系統整合建置

2017年產值：新臺幣58.5億元
2018年產值：新臺幣73.5億元
2019年產值：新臺幣83.8億元
參與廠商：132家
↑14.0%

資安系統整合、經銷服務...

資料來源：
工研院 產科國際所

建構整體防護網

外部情蒐

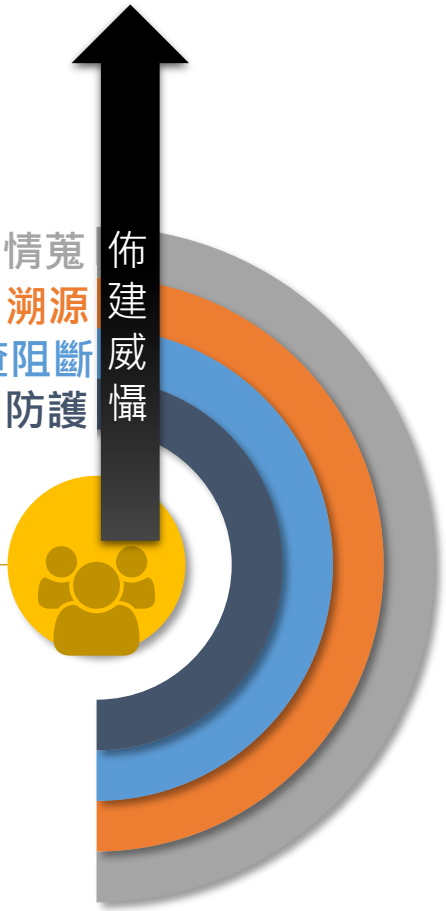
威脅溯源

事件追查阻斷

防護支援

各部會及政府機關

人才培育/資安產業協同合作



提升主動防禦能量

網路攻擊狙殺鏈(Cyber Kill Chain)

偵查
(Reconnaissance)
研究、識別及選擇目標，可以在網際網路上搜尋相關資訊，或是利用工具掃描或探測目標環境。

武裝
(Weaponization)
針對特定的安全漏洞，設計遠端存取木馬程式，包裹在可遞送的資料中，多數以自動化工具產生，且利用常見資料檔案進行偽裝。

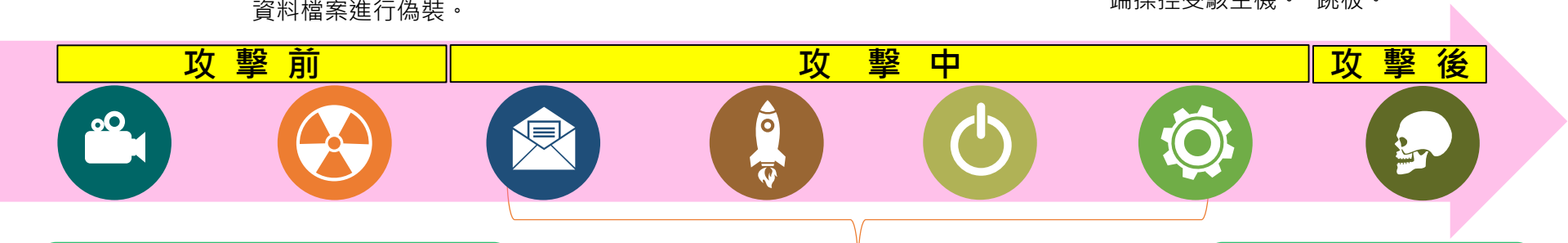
遞送
(Delivery)
設法將惡意程式傳送到目標環境，如電子郵件附件、網站及可移動的USB媒體等遞送管道。

攻擊
(Exploitation)
惡意程式遞送到目標主機後，將觸發內部的程式碼，以應用程式或作業系統的安全弱點為目標，開始進行攻擊。

安裝
(Installation)
於受駭主機安裝遠端存取的木馬或後門程式，而攻擊者可繼續隱藏於受駭環境中。

發令與控制
(Command and Control)
受駭主機須向外連結網際網路上的控制伺服器，以建立控制通道，攻擊者便可利用此通道遠端操控受駭主機。

採取行動
(Actions on Objectives)
攻擊者開始採取行動，如竊取資料、破壞資料的完整性與可用性、或是做為入侵其他系統的跳板。



加強資安整備

- 強化漏洞修補
- 完善備援機制
- 加強資料庫防護

精進縱深防禦

- 完善黑名單防護部署
- 精進資安監控防護
- 落實權限控管

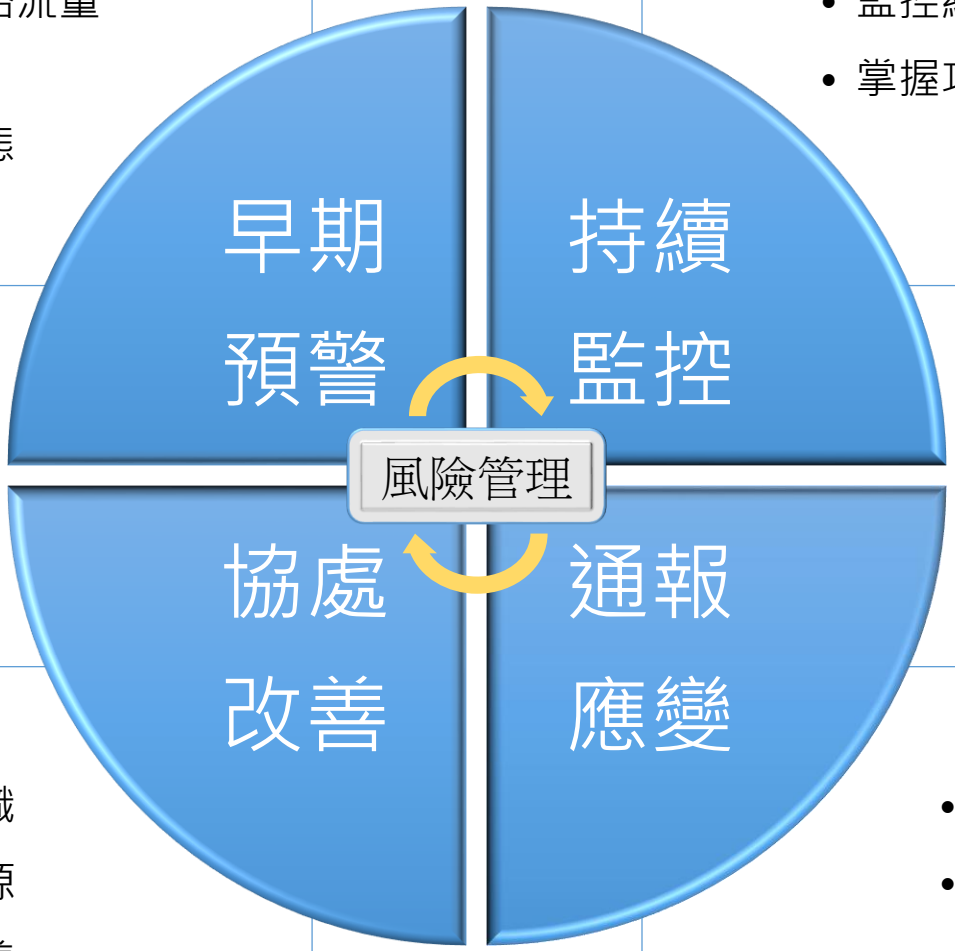
及時應變處理

- 阻斷APT竊密
- 完善系統紀錄

以風險管理為核心的資安防護

- 蒐集網路流量資訊
- 分析樣態

- 監控網路流量
- 掌握攻擊潛勢



- 數位鑑識
- 追查來源
- 落實改善

- 即時通報
- 應變聯防
- 損害控制

資通安全實施架構

核心理念

實施步驟

具體措施

風險管理

事前

- 界定範圍
- 訂定資安維護計畫
- 採取防護措施
- 資料蒐集分析

事中

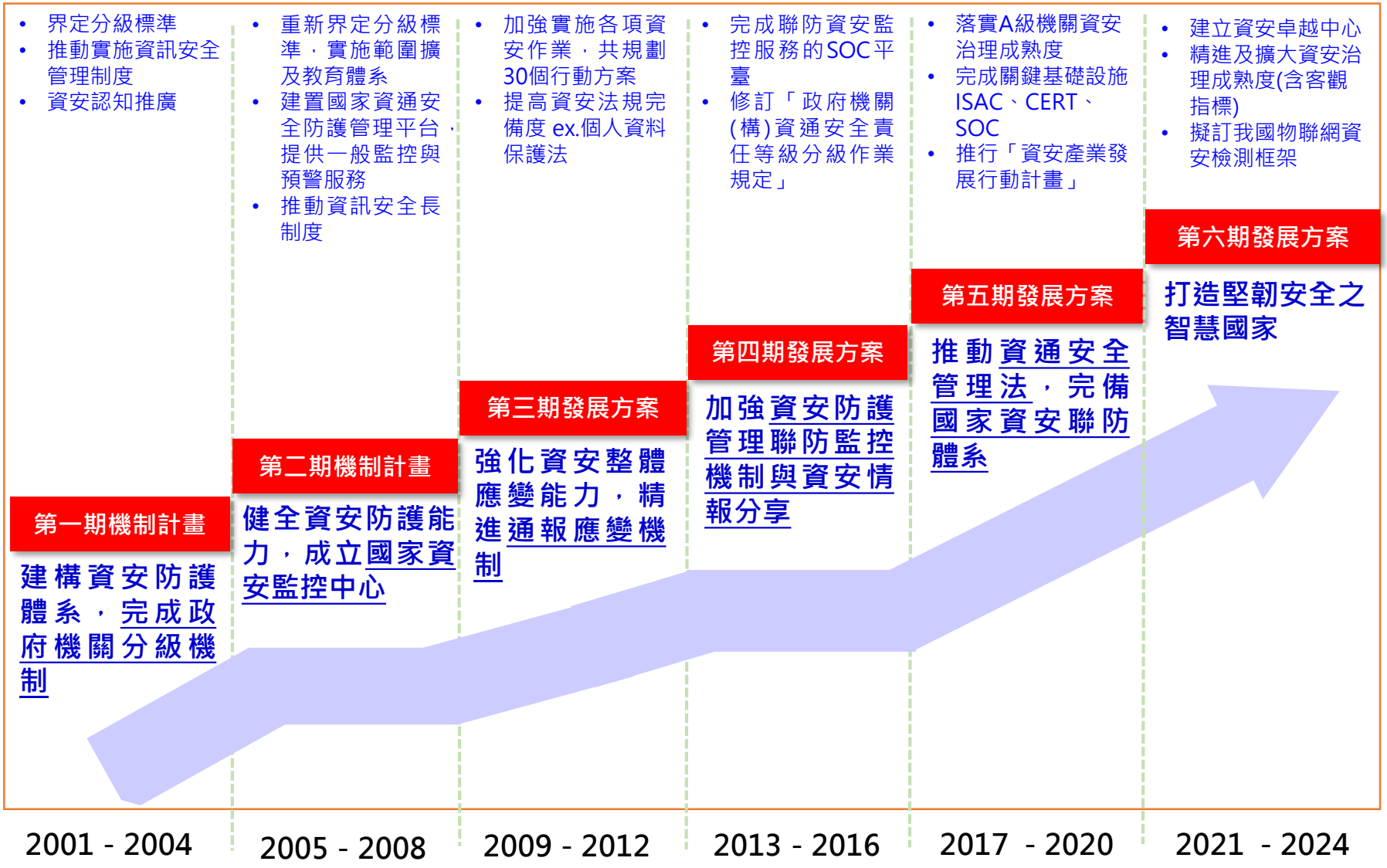
- 事件偵測
- 事件通報應變
- 外部稽核及演練

事後

- 復原
- 改善計畫
- 專案查核

國家資通安全發展方案

我國資安推動進程


界定分級標準
推動實施資訊安全管理制度
資安認知推廣
第一期機制計畫
建構資安防護體系，完成政府機關分級機制
2001 - 2004
重新界定分級標準，實施範圍擴及教育體系
建置國家資通安全防護管理平台，提供一般監控與預警服務
推動資訊安全長制度
第二期機制計畫
健全資安防護能力，成立國家資安監控中心
2005 - 2008
加強實施各項資安作業，共規劃30個行動方案
提高資安法規完備度 ex.個人資料保護法
第三期發展方案
強化資安整體應變能力，精進通報應變機制
2009 - 2012
完成聯防資安監控服務的SOC平臺
修訂「政府機關(構)資通安全責任等級分級作業規定」
第四期發展方案
加強資安防護管理聯防監控機制與資安情報分享
2013 - 2016
落實A級機關資安治理成熟度
完成關鍵基礎設施ISAC、CERT、SOC
推行「資安產業發展行動計畫」
第五期發展方案
推動資通安全管理法，完備國家資安聯防體系
2017 - 2020
建立資安卓越中心
精進及擴大資安治理成熟度(含客觀指標)
擬訂我國物聯網資安檢測框架
第六期發展方案
打造堅韌安全之智慧國家
2021 - 2024

我國現有資安推動政策架構

推動組織	主要推動政策	主要推動計畫	相關部會

行政院國家資通安全會報

國家資通安全發展方案
(106年至109年，行政院資安處)

重點推動項目：

包含基礎環境(如法規、標準)、聯防體系(如協防機制)、產業發展(如產業標準、技術)、人才培育

資安產業發展行動計畫
(107年至114年，行政院資安處)

重點推動項目：

包含人才培育(如設置研訓機構)、技術研發(聚焦利基市場)、場域試煉、國際拓銷

六大核心戰略產業

資安旗艦計畫
(106年至109年，33.3億元)
行政院資安處

前瞻基礎建設資安相關計畫
前瞻1.0(39億元)

- 強化政府基層機關資安防護及區域聯防計畫(34.5億元)
- 強化國家資安基礎建設計畫(4.5億元)

資安卓越產業發展方案
(110年至113年) (66.6億元)

方案計畫包含：

- 前瞻2.0預算35億元，如臺灣資安卓越深耕-資安卓越中心計畫(資安處)及5G及物聯網資安防護-健全電信資安防護設備建置計畫(通傳會)等5項計畫
- 科技預算31.6億元，如資安產業推動暨關鍵基礎設施資安強化旗艦計畫(經濟部)等8項計畫

科會辦
資安處
國發會
經濟部
科技部
衛福部
內政部
通傳會
教育部
交通部
農委會
國防部

國家資通安全發展方案(110年至113年)

願景

打造堅韌安全之智慧國家

目標

- 成為亞太資安研訓樞紐
- 建構主動防禦基礎網路
- 公私協力共創網安環境

推動策略

吸納全球高階人才 培植自主創研能量	推動公私協同治理 提升關鍵設施韌性	善用智慧前瞻科技 主動抵禦潛在威脅	建構安全智慧聯網 提升民間防護能量

具體措施

1. 擴增高教資安師資員額與教學資源 2. 挹注資源投入高等資安科研 3. 培育頂尖資安實戰及跨域人才	1. 建立各領域公私協同治理運作機制 2. 增強人員資安意識與能力建構 3. 公私合作深化平時情資交流與應變演練	1. 賡續推動政府資訊(安)集中共享 2. 擴大國際參與及深化跨國情資分享 3. 制敵機先阻絕攻擊於邊境 4. 提升科技偵查能量防制新型網路犯罪	1. 輔導企業強化數位轉型之資安防護能量 2. 強化供應鏈安全管理 3. 建構安全智慧聯網

資安產業將在5+2產業創新的既有基礎上，配合六大核心戰略產業之「資安卓越產業」規劃持續推動

策略一：吸納全球高階人才培植自主創研能量

成為亞太高階資安人才及技術創新基地

- 擴增高教資安教學資源
  - 擴增資安師資員額
  - 大學區網中心場域
  - 政府開放場域
- 設立資安卓越中心
  - 關鍵核心前瞻研究
  - 深耕學術資安研究
  - 跨國交流合作研究
- 培育資安實戰跨域人才
  - 培育在學資安人才
  - 培訓在職資安人才
  - 研訓頂尖實戰人才

策略二：推動公私協同治理提升關鍵設施韌性

行政院資通安全處

1. 賡續推動資通安全管理法
2. 建立模擬場域，作為實證應處能力及進行教學訓練
3. 建構工控領域資安治理成熟度
4. 推動國家層級資安風險評估

辦理關鍵基礎設施跨領域(或跨國)攻防演練

中央目的事業主管機關

1. 定期稽核所屬關鍵基礎設施提供者
2. 精進關鍵基礎設施資安聯防機制(情資分享、通報應變、資安監控)

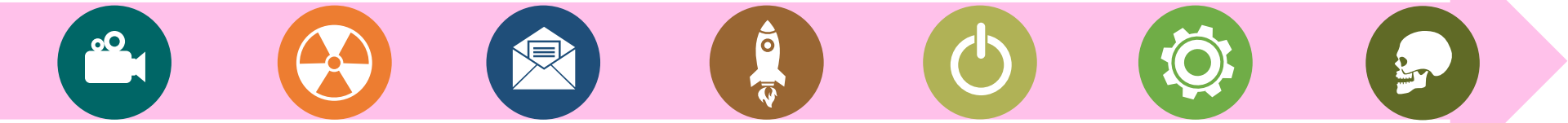
定期於場域進行公私聯合攻防演練

關鍵基礎設施提供者

1. 設置資安長並強化人員資安專業能力
2. 落實資安防護基準

策略三：善用智慧前瞻科技主動抵禦潛在威脅

藉由網路攻擊狙殺鏈(Cyber Kill Chain)，制定各個階段之主動防禦作為



- 推動政府大內網及資安防護向上集中
- 整合國內外情資來源，並深化國際合作
- 建立資訊系統弱點之主動發掘、通報及修補機制
- 應用新興技術淬鍊有效情報，發展主動式防禦前瞻研究及技術應用
- 完善政府網際服務網防禦深廣度
- **提升科技偵查能量防制新型網路犯罪**
  - 強化新型網路犯罪偵查能量
  - 提升資安事件溯源追蹤能力
  - 加強跨境網路犯罪偵查機制

策略四：建構安全智慧聯網提升民間防護能量

政府機關

- 提升委外供應鏈風險管理
- 強化資通訊晶片產品安全性

- 協助企業提升資安防護能量
- 健全通訊網路安全
- 推動物聯網合規驗證

- 提升民眾資安意識

民間企業

提供安全網路及物聯網設備

社群個人

資安為基底推動產業發展以邁向智慧國家

資安是持續精進的風險管理