
108年
打造高效能及安全
雲端資料中心

高效安全的資料中心
規劃與建置實務

勤業眾信



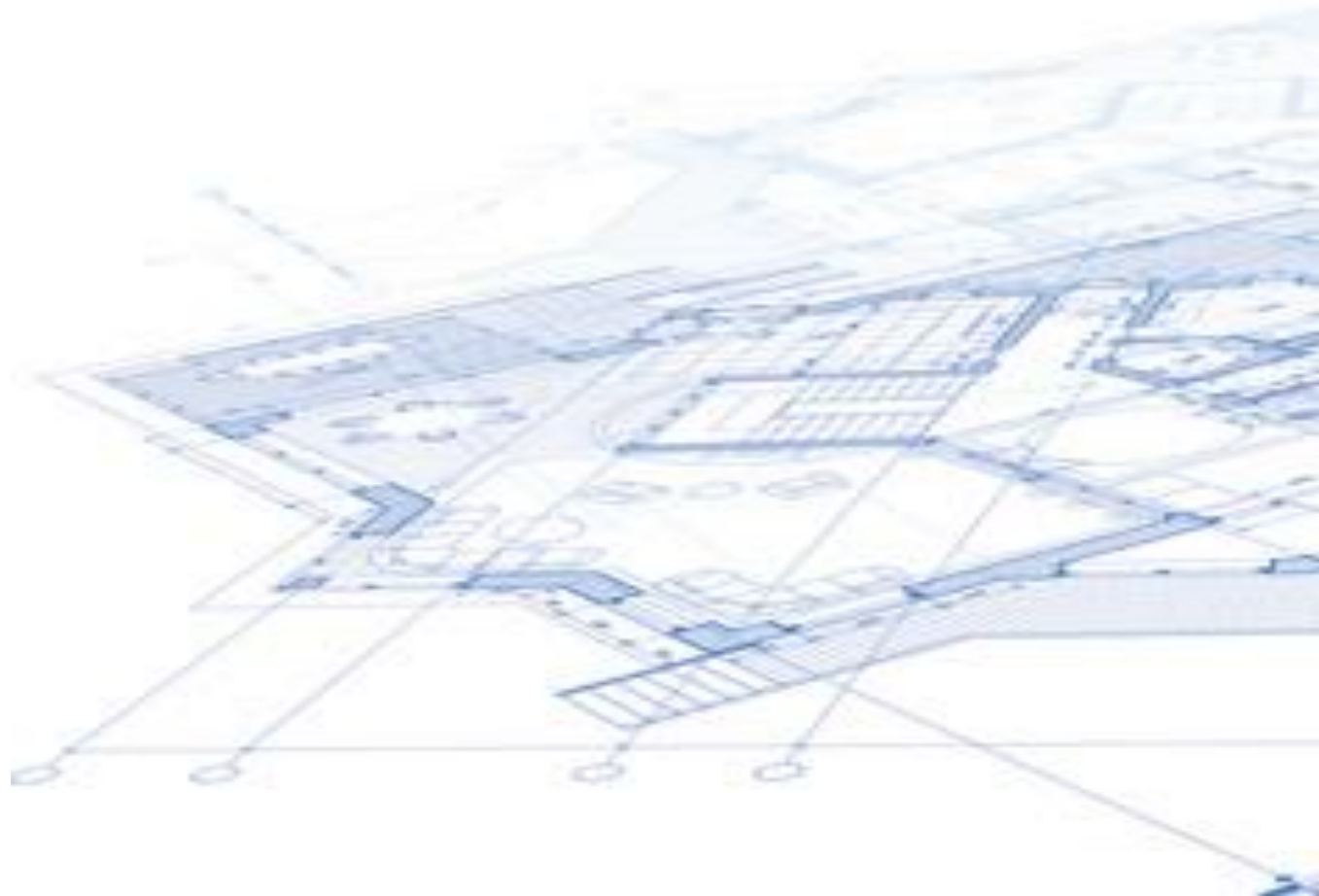


高效安全的資料中心規劃與建置實務

勤業眾信風險管理諮詢股份有限公司
唐從文 副總經理 / 2019.05

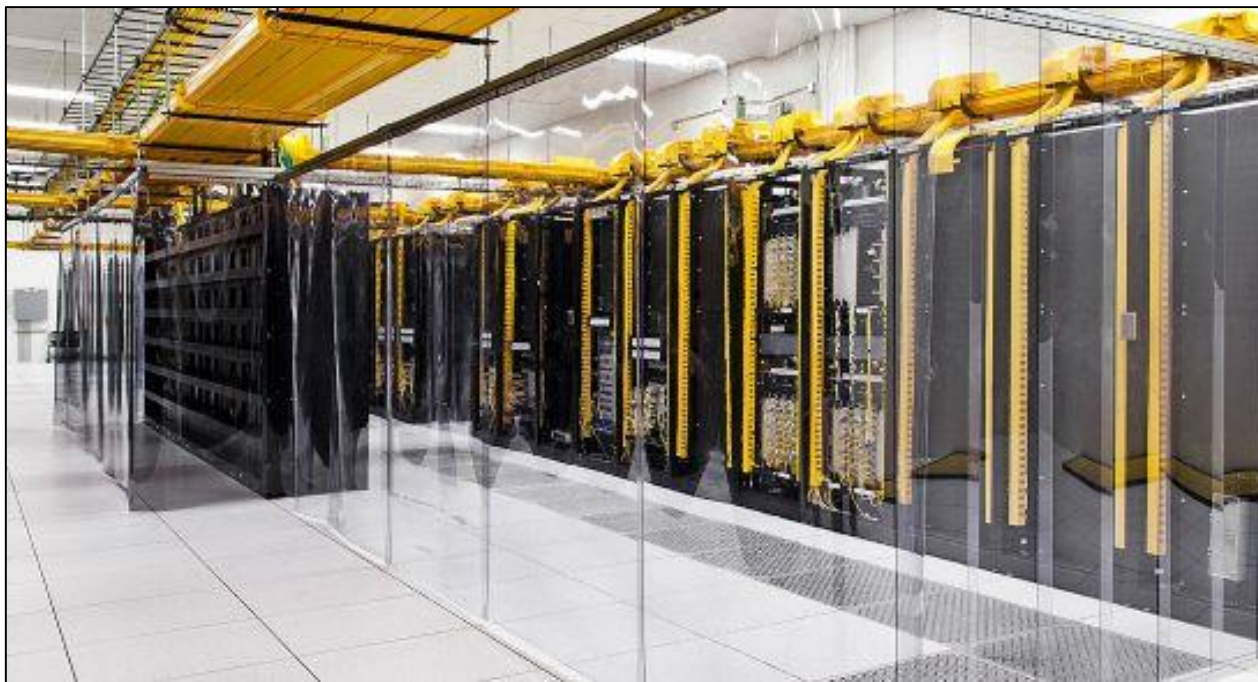
簡報大綱

- 資料中心節能規劃與趨勢
- 資訊安全與網路頻寬議題
- 機房管理實務
- 意見交流

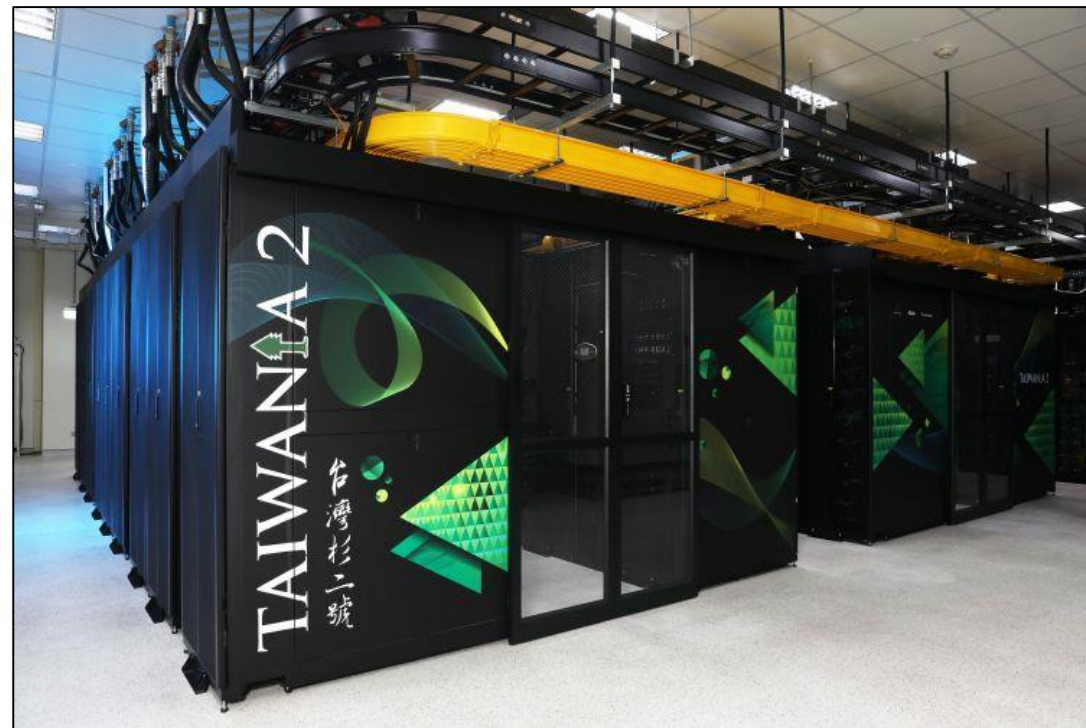


資料中心節能規劃與趨勢

資料中心節能設計



Google資料中心利用塑膠簾將電信設備機櫃區與機房走道區隔(照片來源：DIGITIMES)



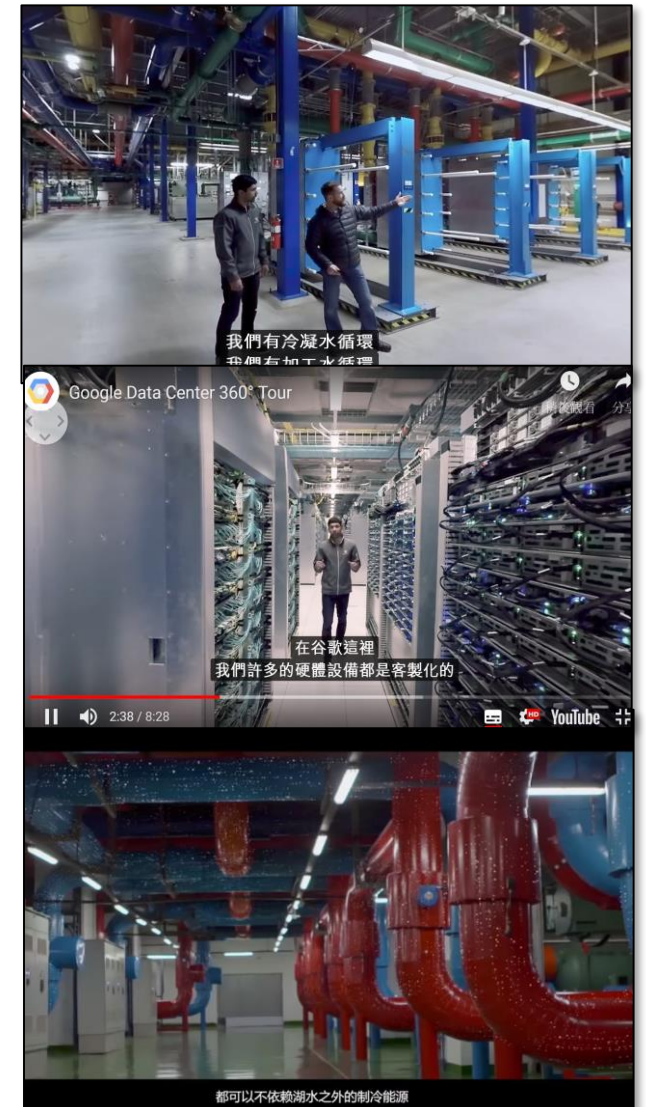
國家高速網路中心AI雲端資料中心冷熱通道式(照片來源：DIGITIMES)

資料中心節能建置案例

- 國內：中華電信板橋機房、台灣大哥大內科IDC機房、台達電等...
- **Google**奧勒崗州戴爾斯資料中心(水力發電廠、**100%綠電**)
- 阿里巴巴張北數據中心(自然冷風)、千島湖數據中心(湖水)

節能策略與作法

- 設備：採用高效率產品、模組化設計，提高設備使用率
- 電力：減少電力轉換次數、變頻系統導入，
- 空調：溫度設定、氣流管理(冷熱通道設計)，縮減空調循環路徑、提高空調系統效率
- 空間：機櫃設備擺設密度規劃
- 整體：降低冰水系統能源消耗、進出管制、智慧環控系統協助
- 使用綠電



智慧雲端資料中心

策略規劃 / 服務發展

- 未來願景
- 發展策略
- 資訊服務轉型需求

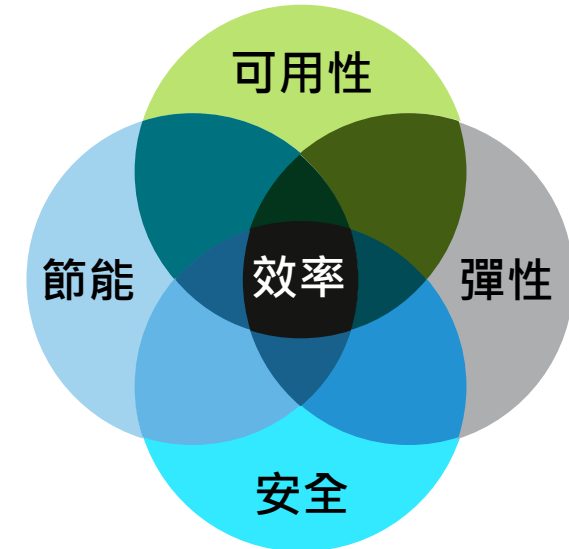


智慧雲端
資料中心



維運重點 / 效率安全

- 研發趨勢
- 風險管理
- 委外管理
- 營運模式



整體營運基礎

- 地點選址/空間設計
- 環控/防災系統建置
- 資訊治理/資安架構規劃
- 能源效率量測/分析
- 國際標準規範導入
- 組織配置/人力資源發展

資料中心基礎設施設計及改造建置指引(草案)



運用RPA提升資料中心維運管理效能

透過安裝從事規則規則性(決定性)任務的軟體，實現機器人流程自動化(RPA)，而這並非指稱在生產線上，有實際的機器人存在

RPA 是...

- ✓ 電腦編碼的軟體
- ✓ 運行反覆、規則基礎任務的程式
- ✓ 多功能且多應用類型的巨集(macros)

RPA 不是...

- ✗ 可行走、談話的機器人
- ✗ 處理紙上作業、實體存在的機器
- ✗ 人工智慧、或語音辨識與回應軟體

Manual Process

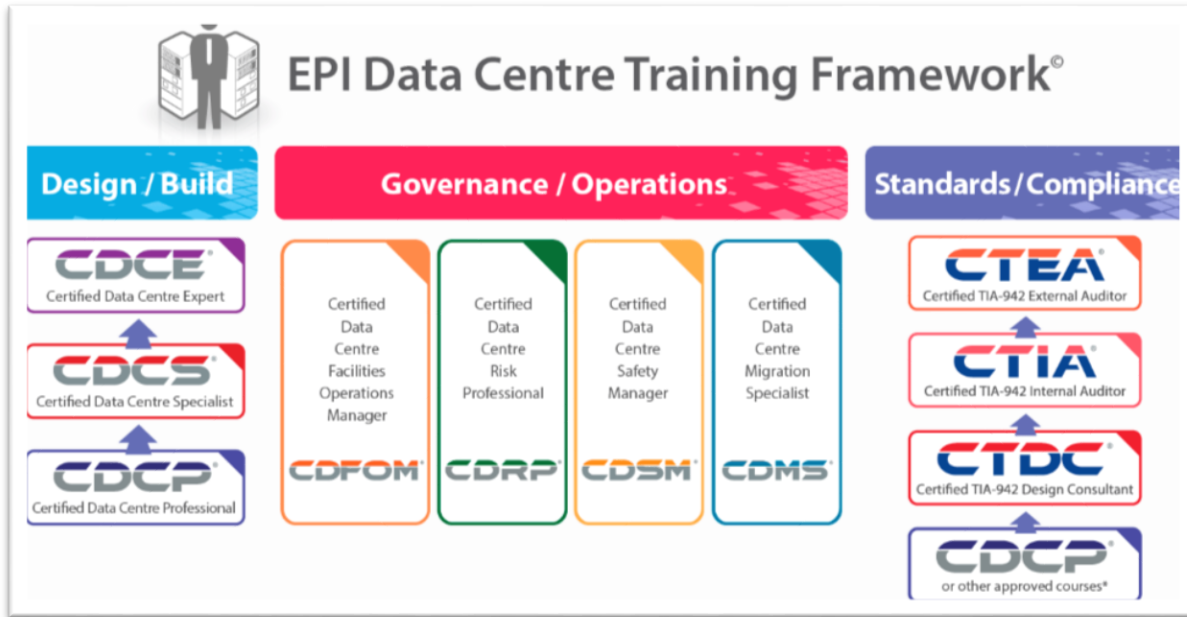
- 登入網路/ 公司應用
- 系統對系統的資料登錄
- 開啟e-mail與附件
- 移動資料與資料夾
- 複製貼上
- 執行流程
- 填寫表格
- 閱讀與編寫資料庫



Judgment Process

- 從網路上移除資料
- 從系統上抹除資料
- 執行計算
- 遵循“if/then”的決策或規則
- 協調資訊
- 搜尋、上傳與核對資訊
- 依據e-mail內容啟動流程
- 從文件中(例如PDF)選取結構性資料
- 收集社群媒體統計資料

其他有關議題



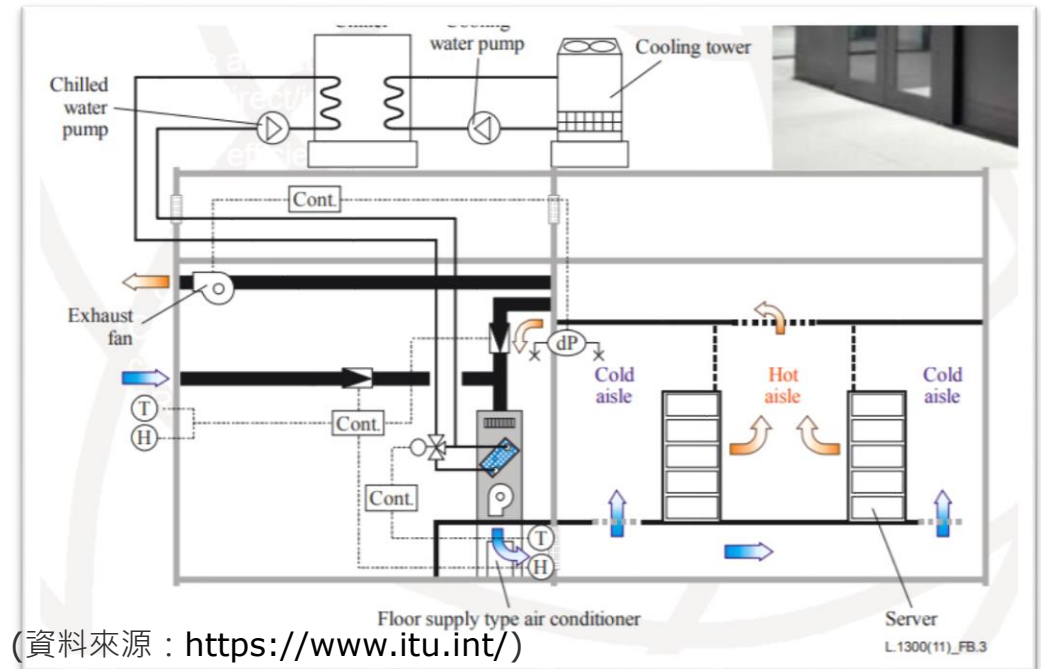
(資料來源：<https://www.epi-ap.com/>)



(資料來源：<https://new.usgbc.org/>)

能源與環境先導設計(LEED)

(Leadership in Energy and Environmental Design)



(資料來源：<https://www.itu.int/>)

資訊安全與網路頻寬議題

資安本質—網路的攻防(1/2)

Unclassified




Assessing Actions Along the Spectrum of Cyberspace Operations

Presented by USCYBERCOM/JA

This presentation does not necessarily reflect the position of the US Government.


Unclassified

Unclassified



Spectrum of Cyber Operations

With that background, we will discuss several real world and exercise examples of cyber operations to determine where they fall on the spectrum of cyber operations



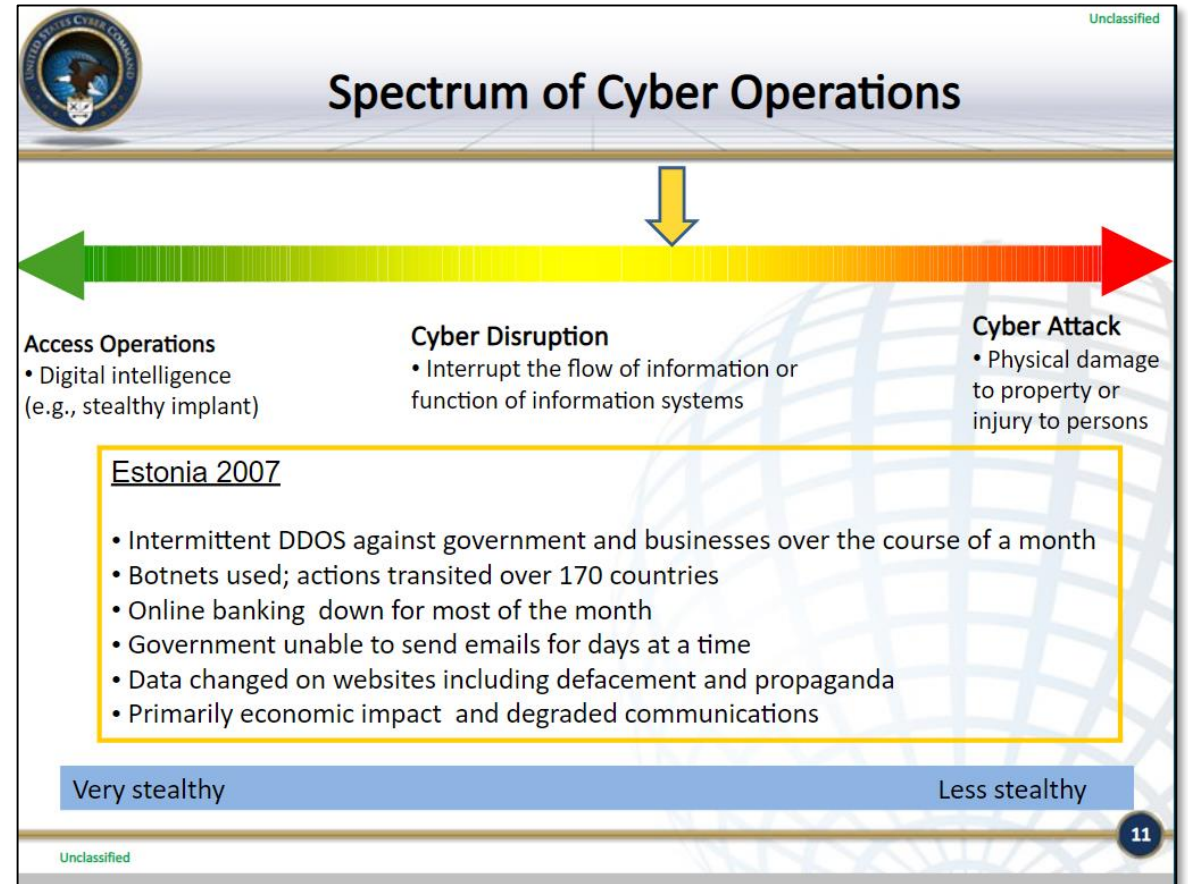
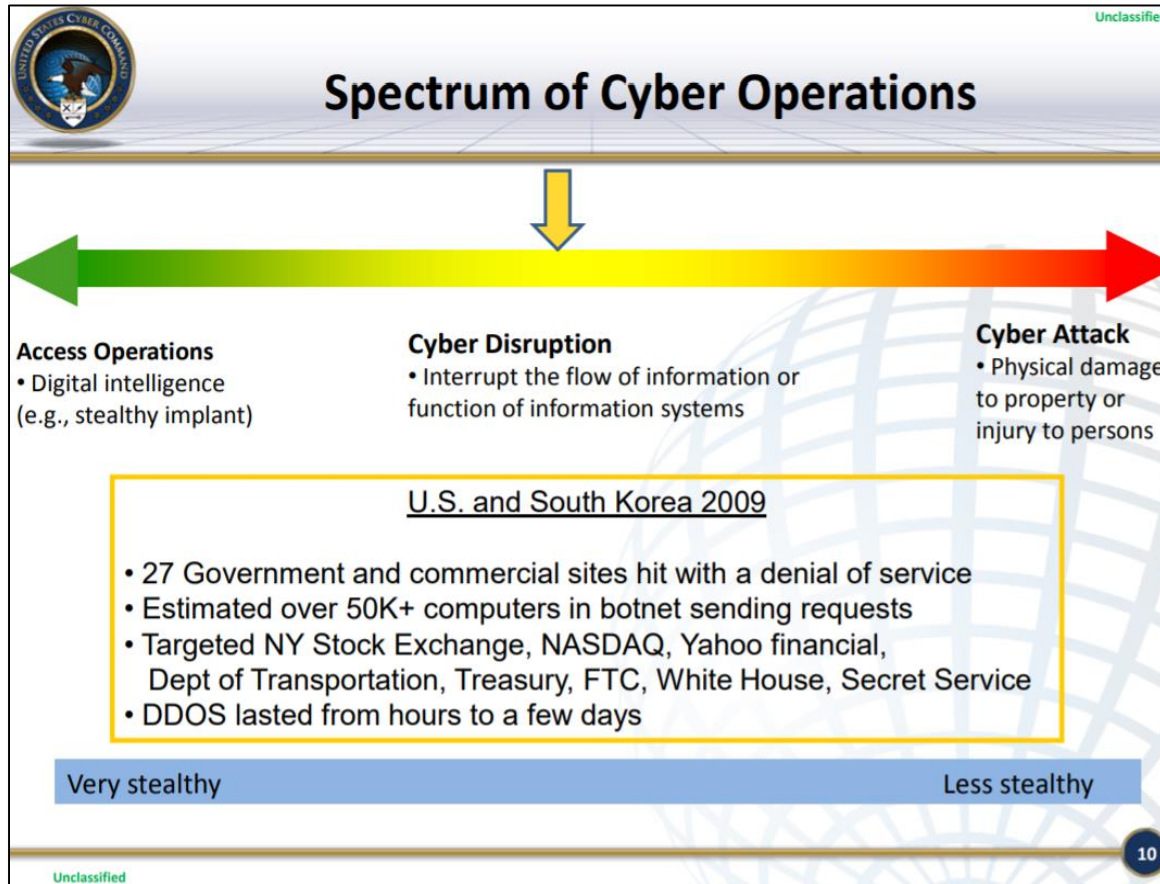
| | | |
|--|--|--|
| Access Operations <ul style="list-style-type: none">• Digital intelligence (e.g., stealthy implant) | Cyber Disruption <ul style="list-style-type: none">• Interrupt the flow of information or function of information systems without physical damage or injury | Cyber Attack <ul style="list-style-type: none">• Use of force• Physical damage or destruction• Physical injury or death |
|--|--|--|

Very stealthy Less stealthy

Unclassified 3

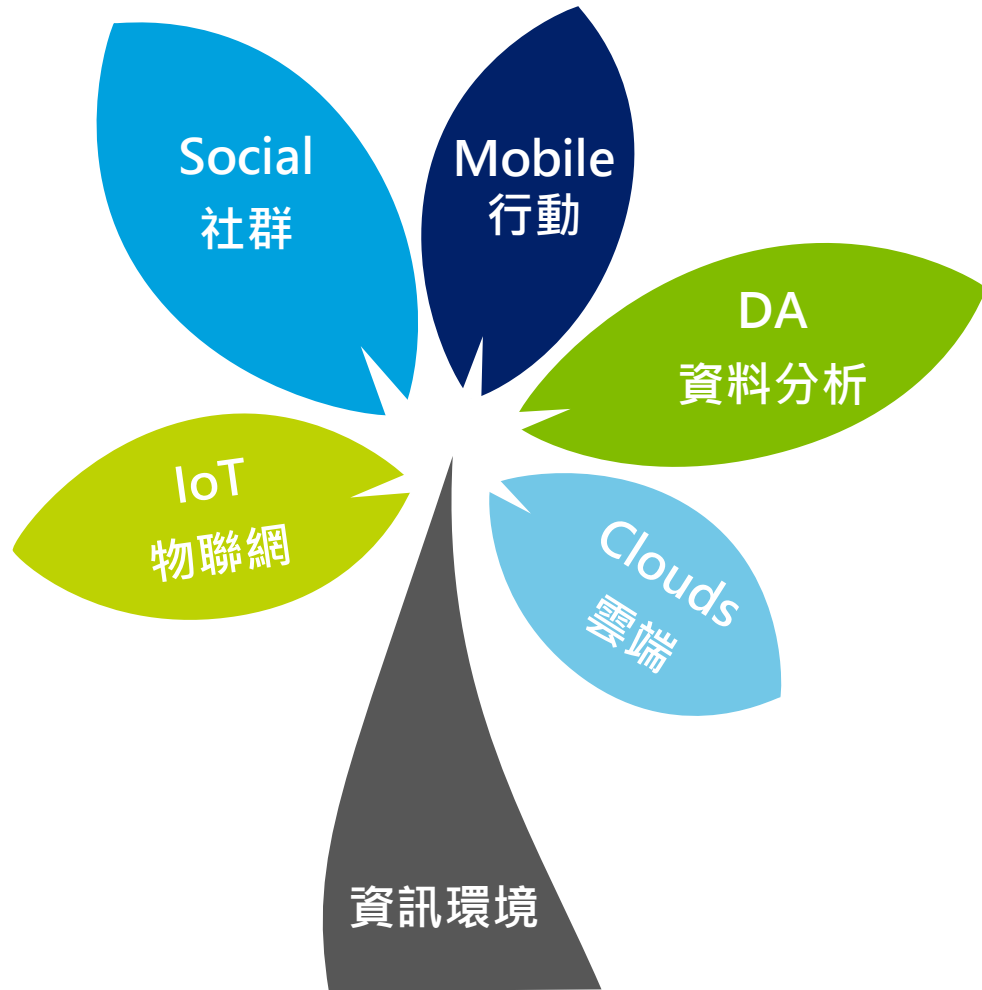
(資料來源：USCYBERCOM)

資安本質—網路的攻防(2/2)



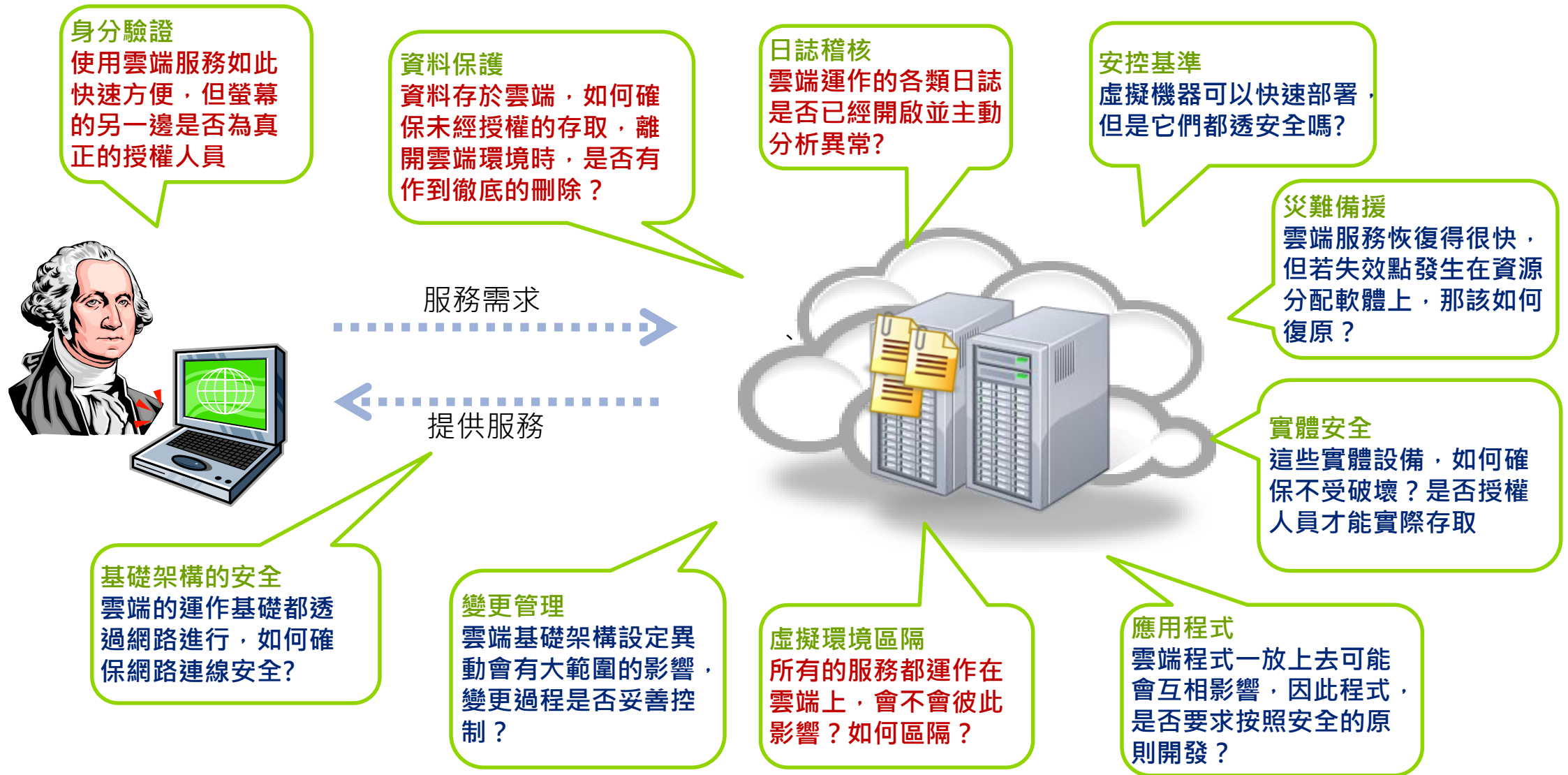
(資料來源：USCYBERCOM)

資訊安全發展趨勢



- Internet of Things 物聯網**
2020年將有100億個以上的連網物體，潛藏商機超過1兆美元。
- Social 社群**
全球25億人使用網路，其中18億人有使用社群網站。
- Mobile 行動**
全球使用手機約有70億人，智慧型手機/平板使用者於2016年將突破20億人。
- Data Analytics 資料分析**
全球有6兆GB的資料量，90%是在過去兩年內產生。
- Clouds 雲端**
2020年全球資料量將達40兆GB，超過1/3的數據儲存在雲端。

雲端安全的可能風險



雲端安全控管提升策略

透過自動化工具的輔助強化資安控管之有效性，如日誌管理、程式安全碼檢查、弱點掃描、多因子認證、行動裝置MDM/MAM ...

強化ISO27001(ISMS)資訊安全管理，並持續改善，如：系統管理、應用程式安全性、供應商管理



再透過CSA STAR / Euro Cloud ECSA雲端標準，深化控管的有效性。

雲端安全標準驗證



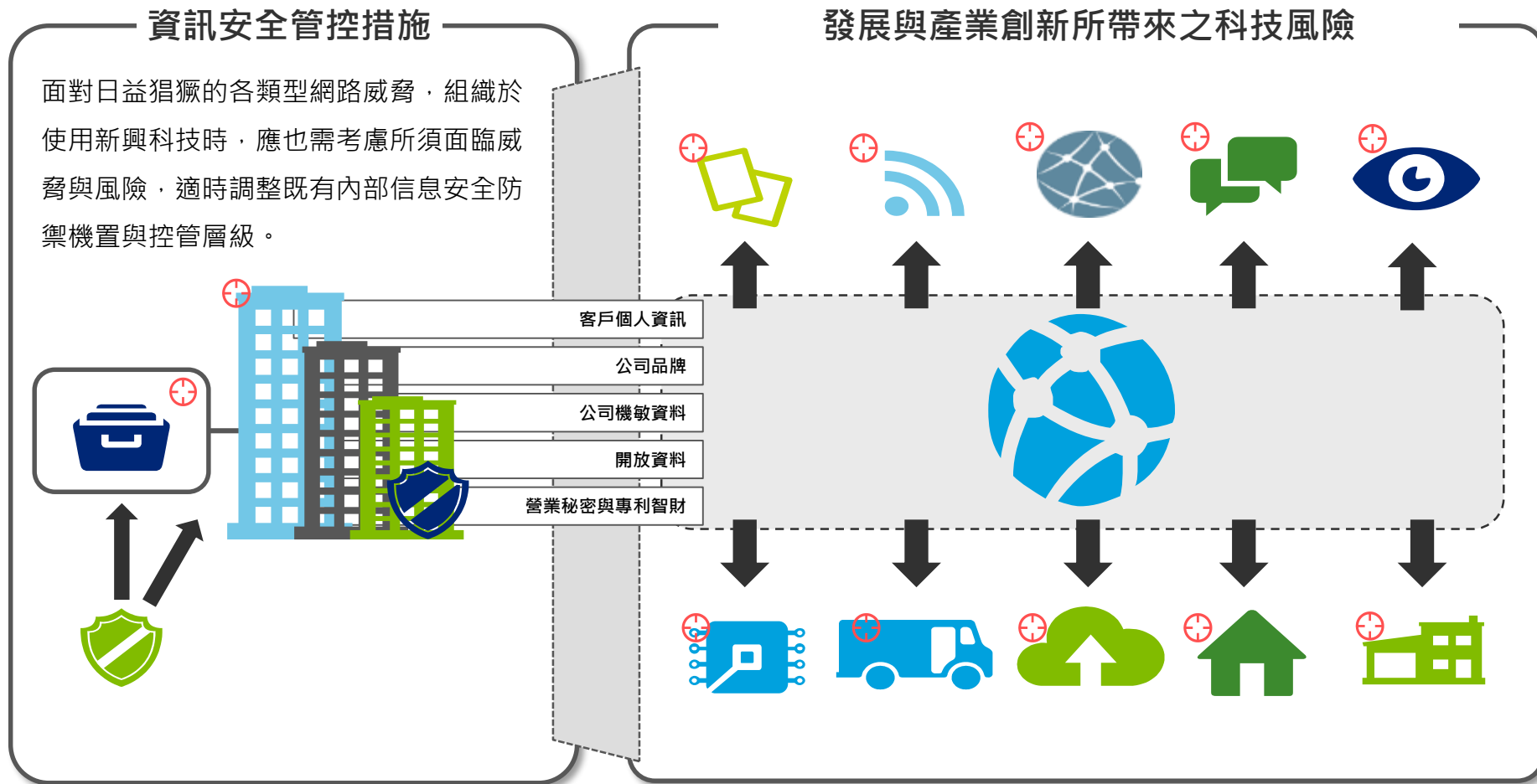
自動化工具輔助



強化ISMS管理



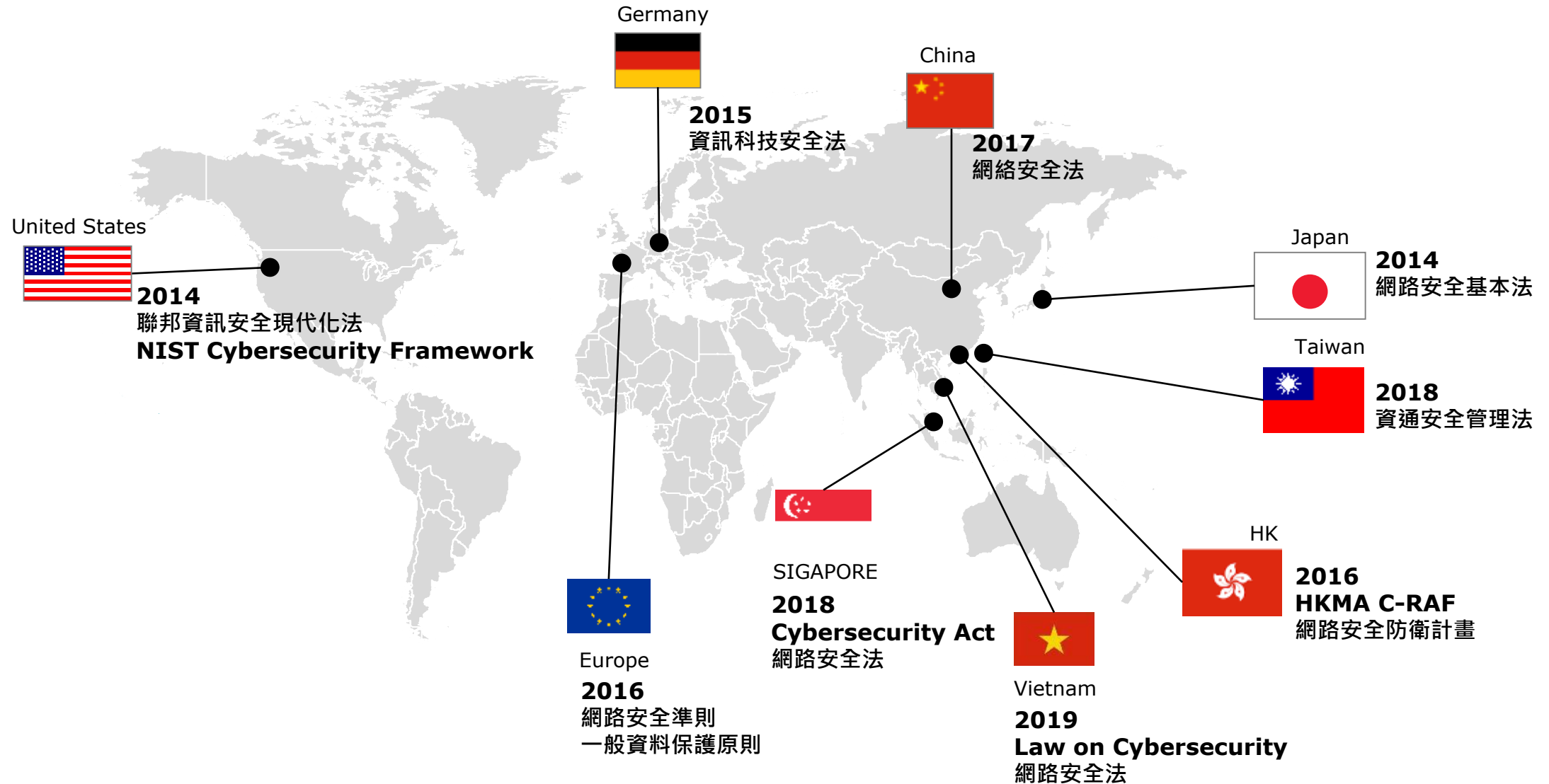
科技發展與產業創新面臨全新的挑戰與威脅



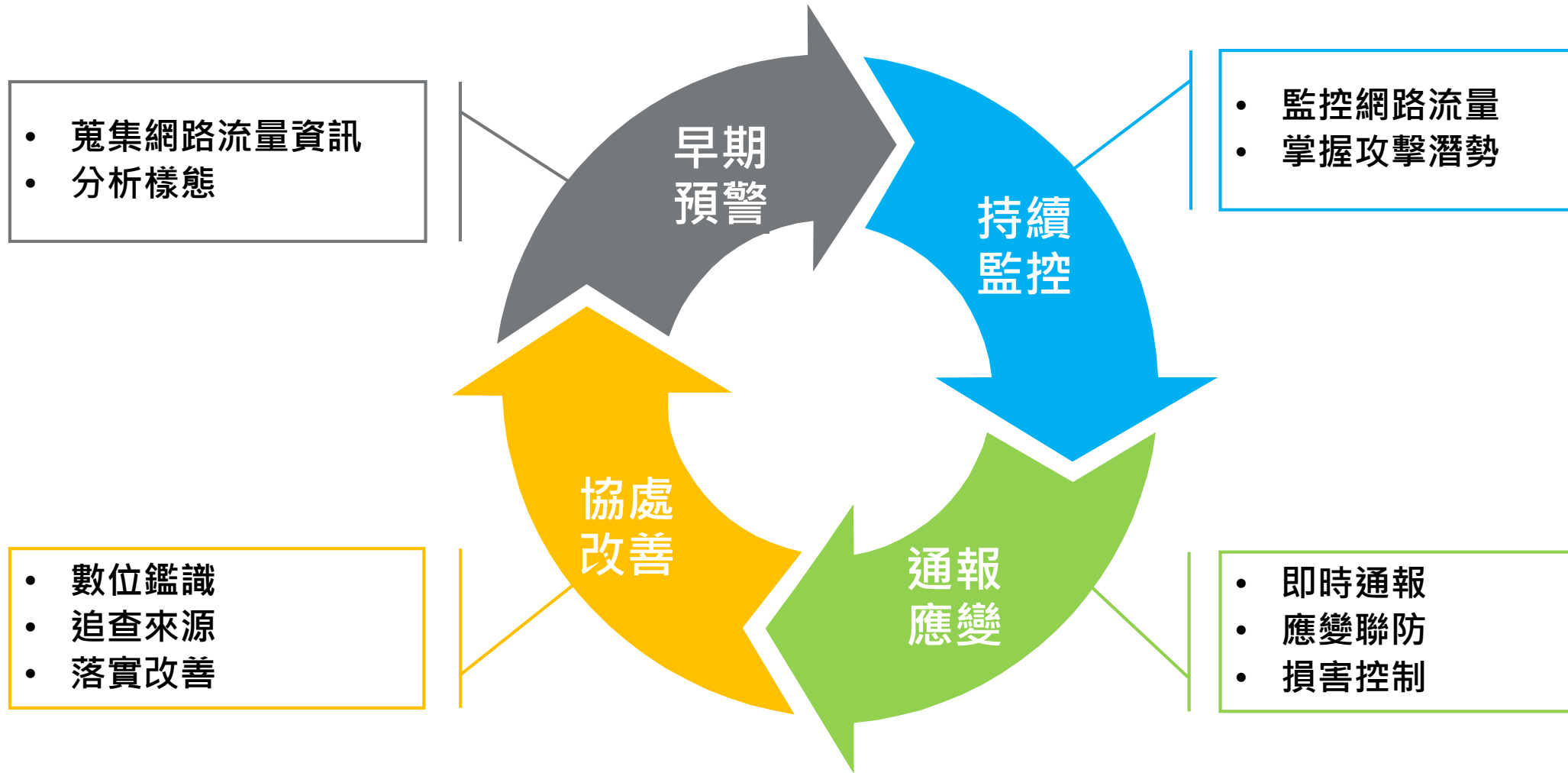
需與組織**未來發展策略緊密結合**，確保及時應對面臨的**挑戰與威脅**！

- 新興科技應用須遵循法律法規
- 虛擬世界法規調適
- 隱私資料保護相關法及產業配套子法
- 資訊安全管理法、

全球主要國家相關法規不斷推陳出新



資通安全管理法與發展



連線費用議題

- 跟哪些單位連線?
 - 要傳些資料?
 - 什麼型態的資料?
 - 多少資料要傳?
 - 傳送資料的頻率多少?
 - 資料可不可以簡併?
- 以上各項問題再一次自我確認

服務項目

- 關於GSN
- GSN上網服務
- GSN VPN服務**
- 機房租用服務
- 視訊連網服務
- 網域名稱註冊
- GSN客戶服務系統
- GSN IPv6服務
- 網路安全服務
- iTaiwan服務專區
- 客服專區

服務施工公告

- 2019/05/25 東七機房發電機啟動演練 [詳細內容](#)
- 2019/05/11 國光機房發電機啟動演練 [詳細內容](#)
- 2019/05/09 中華電信澎湖地區網路設備維護作業 [詳細內容](#)

費率表

GSN VPN光纖網路(多機型)費率表
單位：新臺幣元

GSN VPN FTTB (多機型)(108.4.1)

| FTTB速率 | 月租費 | | | | | | 裝置費 | | |
|----------------|---------------|-----------|----------------|------------|--------------|-----------------|--------------|---------------|-----|
| | 每月應繳 電路月租費 | 8折 優惠價 | GSN VPN 寬頻費 | 每月應繳 費用 | VPNv6 寬頻費 | VPNv6 每月應繳費用 | 接線費 (不綁約) | 接線費 (綁約2年) | 設定費 |
| 6M/2M (下架) | 280 | 224 | 53 | 277 | 不提供 | 不提供 | 1,500 | 500 | 200 |
| 12M/3M (下架) | 306 | 245 | 120 | 365 | 不提供 | 不提供 | 1,500 | 500 | 200 |
| 20M/5M (下架) | 365 | 292 | 135 | 427 | 不提供 | 不提供 | 1,500 | 500 | 200 |
| 16M/3M | 307 | 246 | 130 | 376 | 230 | 476 | 1,500 | 500 | 200 |
| 35M/6M | 383 | 306 | 170 | 476 | 270 | 576 | 1,500 | 500 | 200 |
| 60M/20M | 407 | 326 | 180 | 506 | 280 | 606 | 1,500 | 500 | 200 |
| 100M/40M | 462 | 370 | 210 | 580 | 310 | 680 | 1,500 | 500 | 200 |

GSN VPN FTTB (多機型)(108.4.1)(路由型)

| FTTB速率 | 月租費 | | | | | | 裝置費 | | |
|----------|---------------|-----------|----------------|------------|--------------|-----------------|--------------|---------------|-----|
| | 每月應繳 電路月租費 | 8折 優惠價 | GSN VPN 寬頻費 | 每月應繳 費用 | VPNv6 寬頻費 | VPNv6 每月應繳費用 | 接線費 (不綁約) | 接線費 (綁約2年) | 設定費 |
| 16M/3M | 307 | 246 | 1,900 | 2,146 | 2,000 | 2,246 | 1,500 | 500 | 200 |
| 35M/6M | 383 | 306 | 2,000 | 2,306 | 2,100 | 2,406 | 1,500 | 500 | 200 |
| 60M/20M | 407 | 326 | 3,000 | 3,326 | 3,100 | 3,426 | 1,500 | 500 | 200 |
| 100M/40M | 462 | 370 | 4,000 | 4,370 | 4,100 | 4,470 | 1,500 | 500 | 200 |

(圖片資料來源：GSN 網站i)

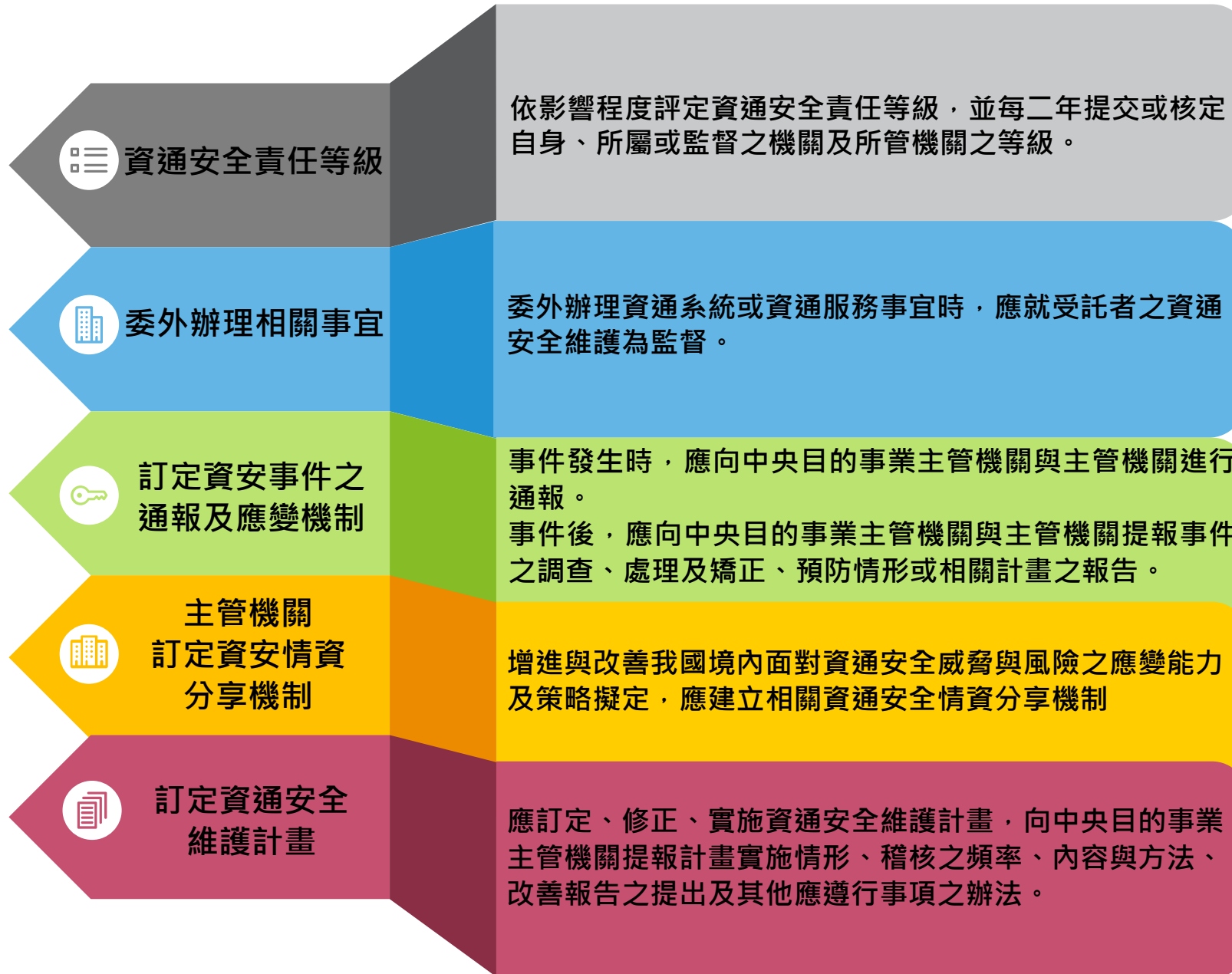
機房管理實務(案例分享)

意見交流



附錄

資通安全管理法細則暨子法重點概覽



資通安全責任等級分級辦法(以「A級機關」為例)

資通安全責任等級

A級

B級

C級

D級

E級

各機關業務之資訊外洩或核心資通系統之運作受影響或停頓，產生**全國性影響**者。包括下列事項：

1. 國家機密
2. 全國性民眾或公務員個人資料檔案之持有或處理
3. 外交、國防、國土安全事項
4. 公務機關涉及全國性之能源、水資源、通訊傳播、交通、銀行與金融緊急救援事項
5. 關鍵基礎設施提供者，經中央目的事業主管機關考量致生災害性之影響
6. 全國性民眾服務之資通系統維運
7. 全國性跨公務機關共用資通系統之維運
8. 公立醫學中心

資通安全責任等級分級辦法(以「公務機關」為例)

A 級公務機關應辦事項

| 制度面向 | 辦理項目 | 辦理項目細項 | 辦理內容 |
|--------------------------|------------------------|-------------------|---|
| 管理面 | 資通系統分級及防護基準 | | 初次受核定或等級變更後之一年內依完成資通系統分級，並完成控制措施；其後應每年至少檢視一次資通系統分級妥適性。 |
| | 資訊安全管理系統之導入及通過公正第三方之驗證 | | 初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001資訊安全管理系統國家標準、ISO 27001資訊安全管理系統、其他具有同等或以上效果之系統或標準、或其他公務機關自行發展並經主管機關認可之標準並於三年內完成公正第三方驗證。 |
| | 資通安全專責人員 | | 初次受核定或等級變更後之一年內，配置四人，須以專職人員配置。 |
| | 內部資通安全稽核 | | 每年辦理二次。 |
| | 業務持續運作演練 | | 全部核心資通系統每年辦理一次。 |
| | 資安治理成熟度評估 | | 每年辦理一次。 |
| 技術面 | 安全性檢測 | 網站安全弱點檢測 | 全部核心資通系統每年辦理二次。 |
| | | 系統滲透測試 | 全部核心資通系統每年辦理一次。 |
| | 資通安全健診 | 網路架構檢視 | 每年辦理一次。 |
| | | 網路惡意活動檢視 | |
| | | 使用者端電腦惡意活動檢視 | |
| | | 伺服器主機惡意活動檢視 | |
| | | 目錄伺服器設定及防火牆連線設定檢視 | |
| | 資通安全威脅偵測管理機制 | | 初次受核定或等級變更後之一年內，完成監控機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。 |
| | 政府組態基準 | | 公務機關經初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。 |
| | 資通安全防護 | 防毒軟體 | 初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。 |
| 網路防火牆 | | | |
| 具有郵件伺服器者，應備電子郵件過濾機制 | | | |
| 入侵偵測及防禦機制 | | | |
| 具有對外服務之核心資通系統者，應備應用程式防火牆 | | | |
| | 進階持續性威脅攻擊防禦措施 | | |
| 認知與訓練 | 資通安全教育訓練 | 資通安全及資訊人員 | 每年至少四名人員各接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。 |
| | | 一般使用者與主管 | 每人每年接受三小時以上之一般資通安全教育訓練。 |
| | 資通安全國際專業證照及職能訓練證書 | 資通安全專業證照 | 初次受核定或等級變更後之一年內，資通安全專職人員總計應持有四張以上，並持續維持證照與證書之有效性。 |
| | | 資通安全職能評量證書 | |