NARLabs 國家實驗研究院

國家高速網路與計算中心

TWCC多層次資安防護架構設計分享

報告人：李柏毅

平臺維運組

NARLabs
承諾．熱情．創新

大綱

- TWCC計畫與設施營運目標
- TWCC資安防護架構說明
- 資料傳輸安全
- 網路安全
- 資訊安全維運中心
- DDoS清洗中心
- APT偵測防護
- 國際資安標準
- 108年資安防護強化項目

TWCC計畫目標

孕育國家級AI及大數據平台

培育AI 系統與工具之軟體廠商

高品質及有效率的營運AI雲端基礎設施

促成(引導)產業及政府利用AI 來提升其營運績效(產業AI化及AI產業化)

集結各領域AI專業的團隊與社群

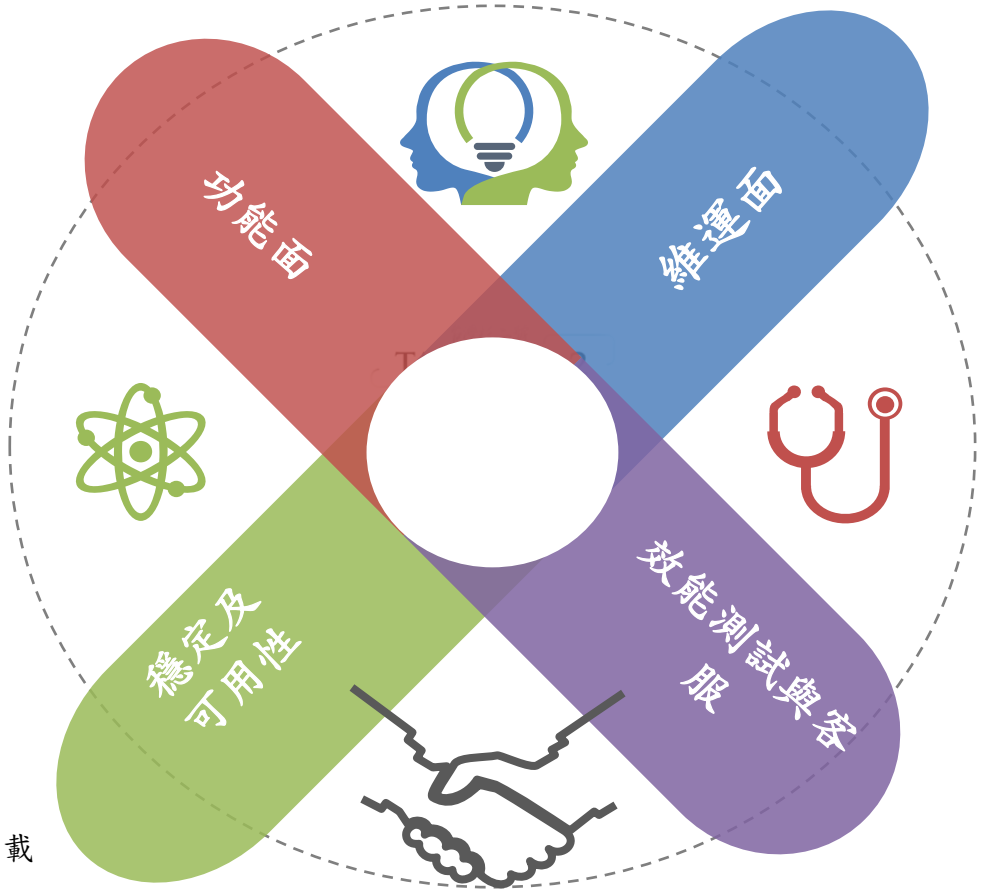
重要領域的示範(如生醫,災防,IOT)

匯聚各領域之數據集與應用

設施營運執行目標

1. 基礎的雲端平台服務
   a. 提供用戶可自行設定儲存、網路與防火牆的虛擬主機服務
2. 大型叢集的容器服務
   a. 由K8S 提供自動化擴充與負載平衡
   b. 由Singularity 提供HPC 容器使用介面
   c. 提供多項 NGC 之AI Images(如 Tensorflow, Caffe等)
3. 友善的使用者
   a. 採用業界使用經驗與流程
   b. 擷取Alpha 及 Best 測試回饋

1. 具高可用性的架構
   a. 長期使用不用停機
   b. 超過99%以上的整體系統可用度
2. 採用穩定性測試的方法程序
   a. 模擬最常用的使用情境
   b. 長時間的負載測試
   c. 持續7天以上的低中負載及1天的壓力負載
3. **整合式雲端安全防護服務**
   a. **偵測網路威脅，確保使用者資料及平臺對外服務不受網路攻擊影響**



1. 高效率的持續交付維運程序
   a. 自動原始碼的擷取及建立
   b. 自動單元及功能測試
   c. 自動化部署
   d. 滾動式軟體升級, 客戶不受升級影響
   e. 當升級部署有問題時能自動回復
2. 主動式整體系統監控
   a. 監控系統的整體可用性
   b. 監控整體系統資源使用狀況及效能
   c. 當系統有潛在問題能主動告警

1. 充分的效能基準測試
   a. 不同雲端服務平台及Container 平台之比較
   b. 提供差異化的服務
   c. 識別出潛在的效能或擴充增進的方式
   d. 遵循與參與國際之HPC 與 AI 之效能基準測試活動
2. 客戶服務
   a. 建立客服組織與流程, 確保客戶問題能迅速反應
   b. 不斷回饋客戶使用的滿意程度,確保客戶能順暢地使用我們的系統

資安防護設計概念

1.可用性

提昇系統服務之可考度，讓需要使用資訊服務的使用者能夠隨時存取服務。

2.完整性

加強資料的保存與驗證，避免資料受到未經授權的新增、刪除或修改。

3.機密性

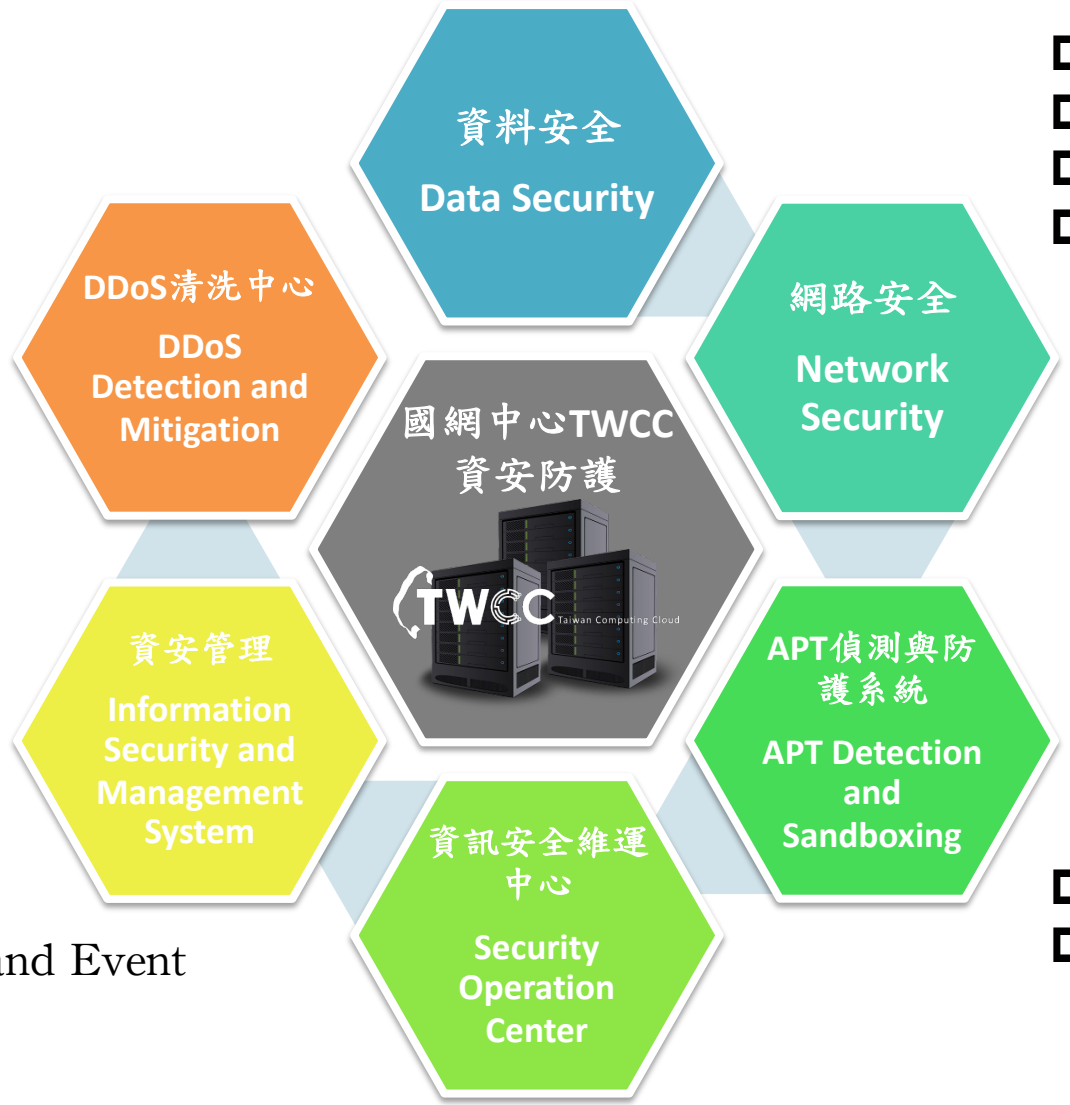
提昇資料保護，在傳輸或保存時，都可以有效避免資料遭到未經授權之存取。

TWCC資安防護藍圖

- Flow Analyzer
- DDoS Threat Detection
- DDoS Threat Mitigation

- ISO/IEC 27001
- BS10012
- CSA STAR Level 2
- ISO/IEC 27017
- ISO/IEC 27018

- SIEM(Security Information and Event Management)
- Security Operation Center

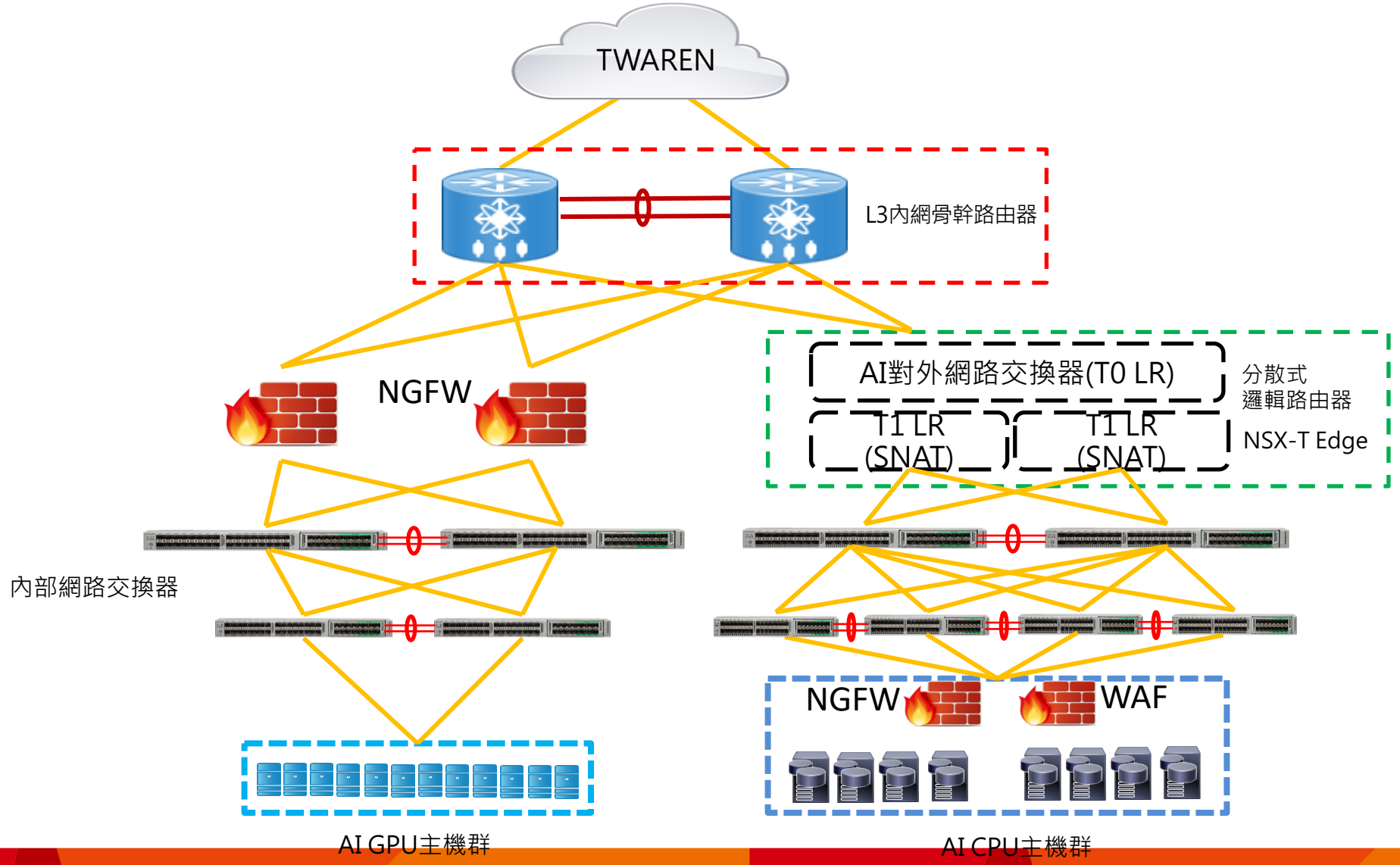


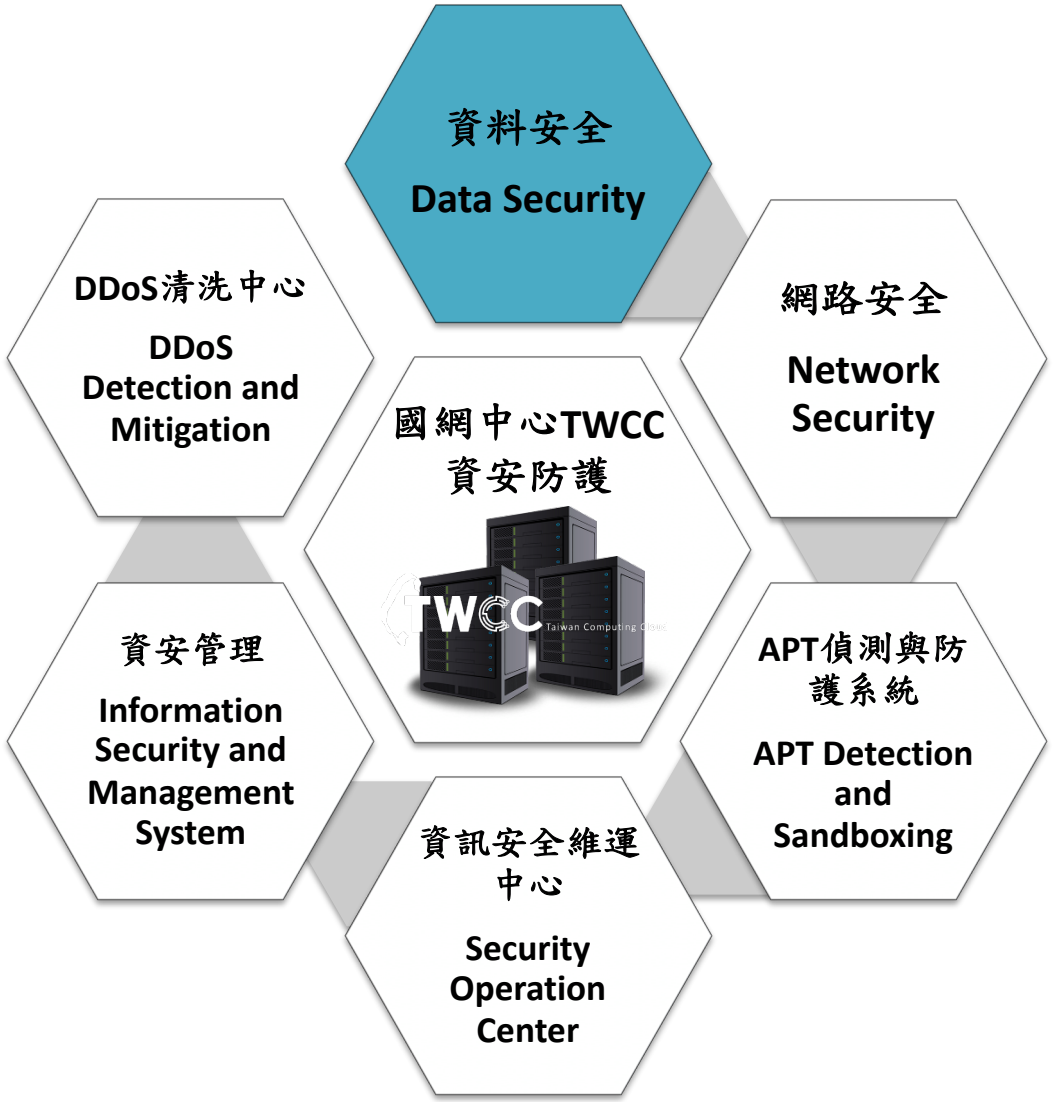
- Data in rest
- Data in Transaction
- Micro Segmentation
- Distributed Storage System

- Network Firewall
- Web Application Firewall
- Intrusion Detection/Prevention System

- Automated Sandboxing
- APT Threat Detection and Alerting

TWCC網路與資安防護架構示意圖

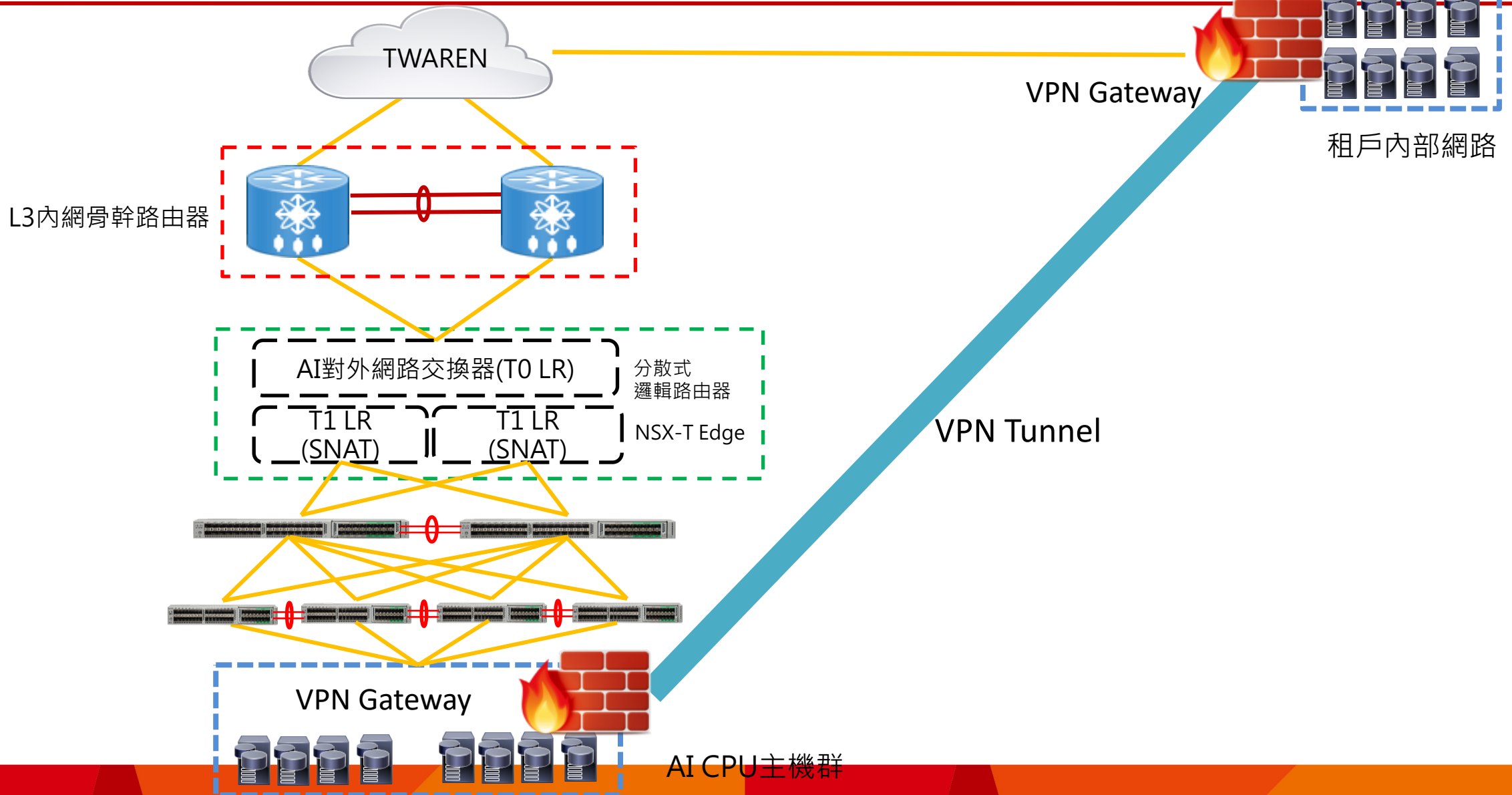



資料安全
Data Security
DDoS清洗中心
DDoS Detection and Mitigation
網路安全
Network Security
國網中心TWCC資安防護
TWCC
Taiwan Computing Cloud
資安管理
Information Security and Management System
APT偵測與防護系統
APT Detection and Sandboxing
資訊安全維運中心
Security Operation Center

資料傳輸安全

- 建立虛擬私人網路(Virtual Private Network)
  - 在不受信任的網路環境中，透過通道協定(Tunneling Protocol)，建立加密的傳輸機制，確保資料傳輸的機敏性，避免資料被竊聽而讓未經授權的人員存取。
  - TWCC之Openstack VM服務提供Palo Alto虛擬防火牆讓租戶付費使用，而Palo Alto虛擬防火牆就提供建立Site-to-site VPN的功能，讓使用者可以將承租的VM與單位內部的主機串接成虛擬內部網路。

VPN通道建立示意圖


TWAREN
VPN Gateway
租戶內部網路
L3內網骨幹路由器
AI對外網路交換器(T0 LR)
分散式
邏輯路由器
T1 LR
(SNAT)
T1 LR
(SNAT)
NSX-T Edge
VPN Tunnel
VPN Gateway
AI CPU主機群

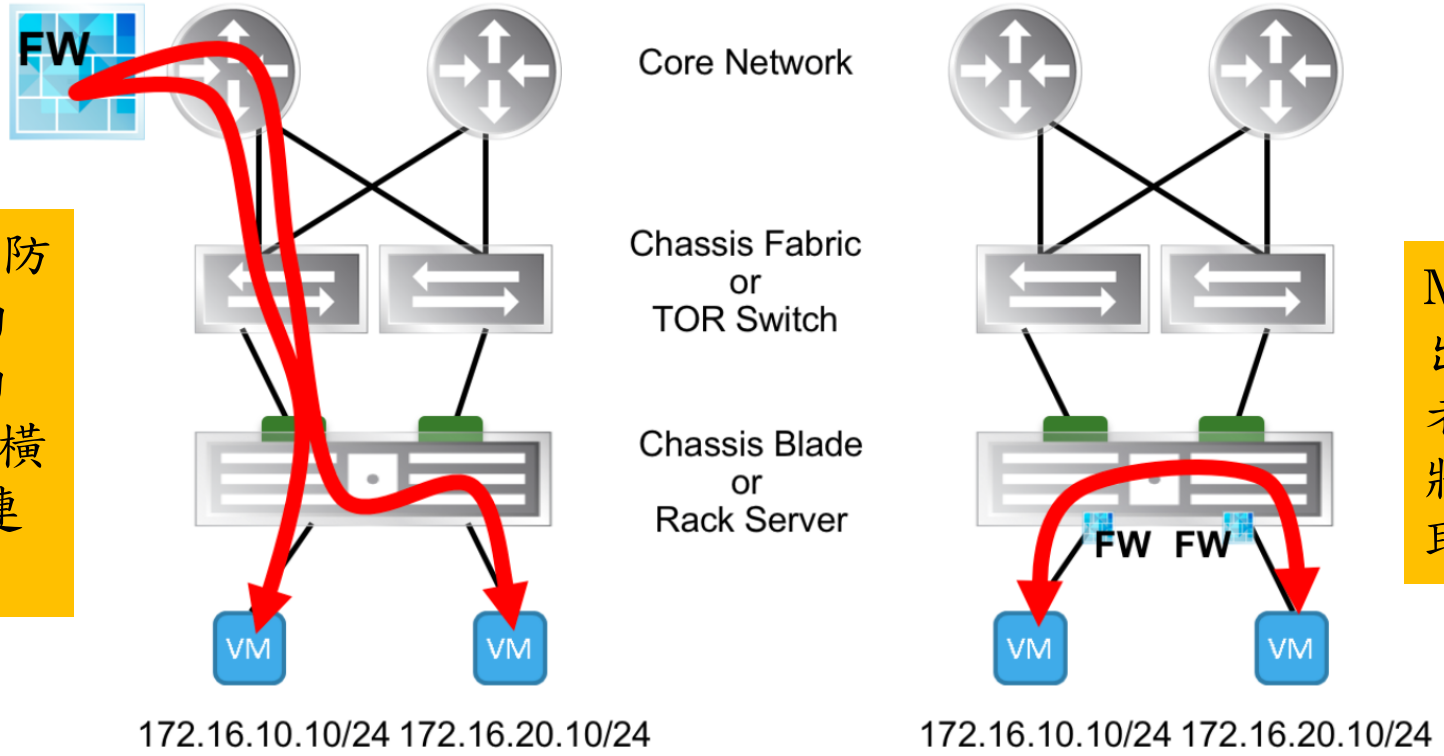
資料傳輸安全

- 預設使用加密通訊協定
  - 預設使用加密傳輸通訊協定，如22/TCP，進行資料傳輸
  - TWCC上之Container服務預設要求使用者使用SSH加密傳輸協定登入管理。
  - TWCC上之OpenStack VM服務亦以SSH或是RDP(Remote Desktop Protocol)等加密通訊協定作為預設對外服務連接埠。
- 預先交換金鑰
  - 虛擬主機服務可讓使用者使用預先設定之金鑰組，避免遭到帳號密碼暴力破解攻擊，提昇系統安全性

虛擬主機隔離

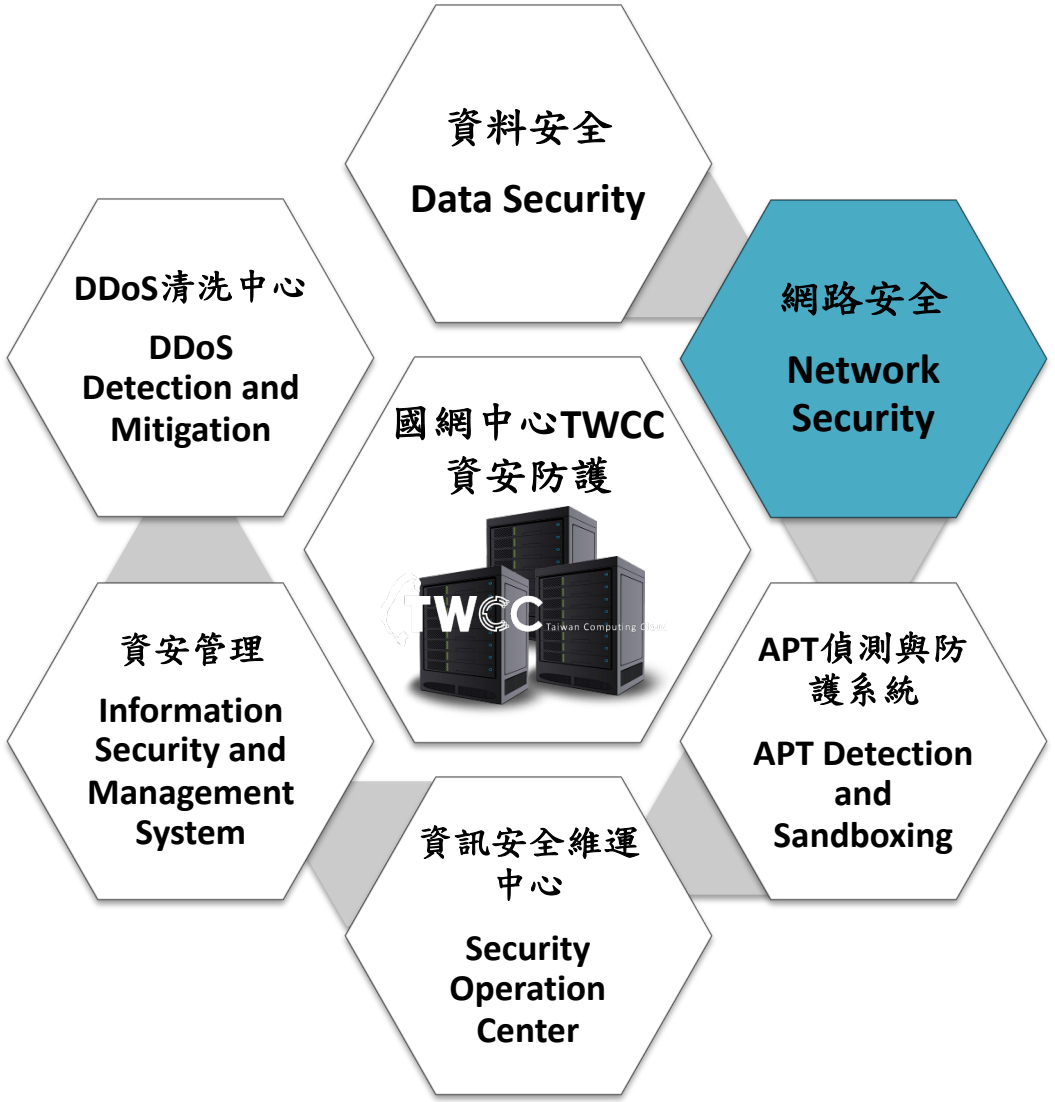
- 落實虛擬主機網路區隔
  - 使用Micro Segmentation實現虛擬主機邏輯區隔，讓各租戶間的系統資訊以及資料不被未經授權的使用者或是系統管理員存取。

使用Routing Mode的防火牆控制全部主機的存取規則，包含縱向存取(出Internet)以及橫向存取(虛擬主機間連線)。



Micro Segmentation的出現讓虛擬主機使用者可以自行定義防火牆存取規則，強化存取控制。

圖片來源: http://www.beyondcli.com

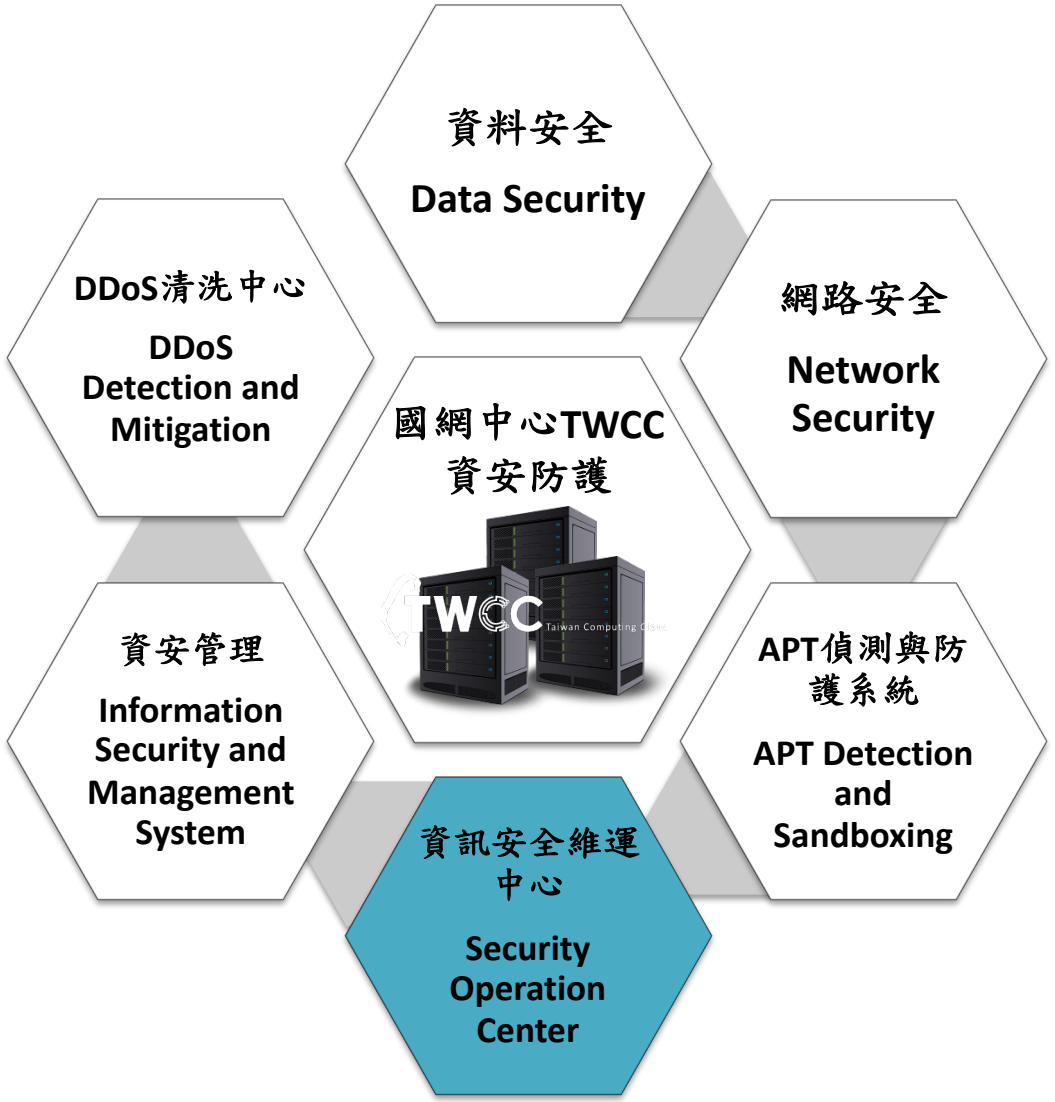

資料安全
Data Security
DDoS清洗中心
DDoS Detection and Mitigation
網路安全
Network Security
國網中心TWCC資安防護
TWCC
Taiwan Computing Cloud
資安管理
Information Security and Management System
APT偵測與防護系統
APT Detection and Sandboxing
資訊安全維運中心
Security Operation Center

網路安全

- 網路防火牆(Network-based Firewall)
  - 佈署位置：國網中心臺中分部TWCC GPU運算主機群出口，採HA架構
  - 說明：佈署於TWCC GPU運算主機群之網路閘道口，提供網路區隔、網路流量紀錄、存取控制、虛擬私人網路(VPN)和網路位址轉換(Network Address Transfer, NAT)等功能。
- 主機防火牆(Host-based Firewall)
  - 佈署位置：國網中心臺中分部TWCC CPU運算主機群
  - 說明：佈署於TWCC CPU運算主機群OpenStack上之虛擬主機，提供存取控制以及系統邏輯區隔功能，讓租戶可以自行定義網路安全規則。

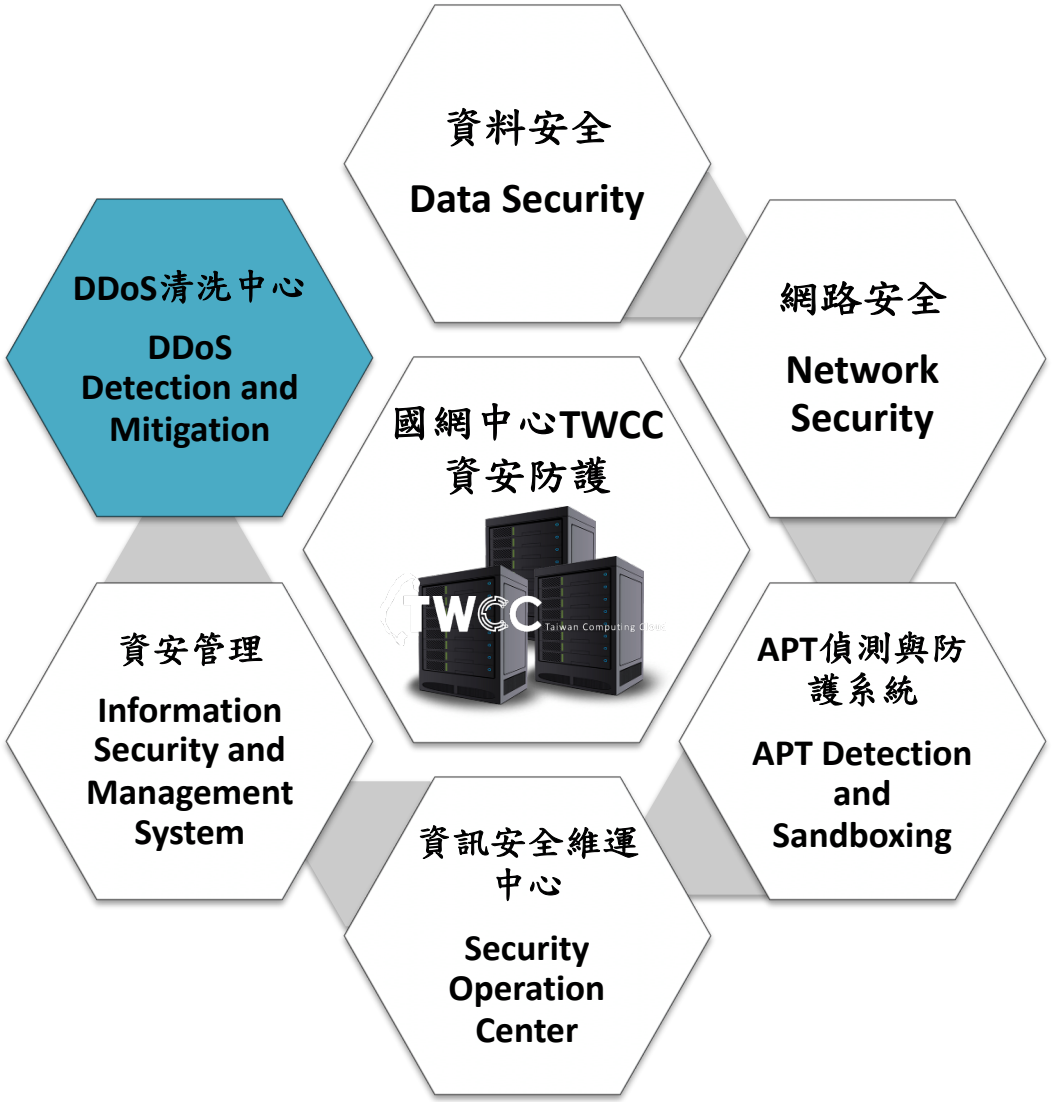
網路安全

- 入侵偵測防禦系統
  - 佈署位置：國網中心臺中分部TWCC GPU運算主機群出口，採HA架構
  - 說明：佈署於TWCC GPU運算主機群之網路閘道口，提供網路威脅偵測功能，監控進出網路流量，可偵測惡意程式、間諜軟體、殭屍網路…等網路威脅並進行阻擋以及攻擊日誌保存。
  - TWCC上常見的攻擊態樣包含帳號密碼暴力破解攻擊(Brute Force Attack)，DNS服務漏洞利用…等。


資料安全
Data Security
DDoS清洗中心
DDoS Detection and Mitigation
網路安全
Network Security
國網中心TWCC資安防護
TWCC
Taiwan Computing Cloud
資安管理
Information Security and Management System
APT偵測與防護系統
APT Detection and Sandboxing
資訊安全維運中心
Security Operation Center

資訊安全維運中心

- 安全資訊與事件管理平臺(SIEM)
  - 設備佈署位置：國網中心臺中分部
  - 維運點：國網中心臺南分部
  - 說明：收集網路防火牆、重要主機與設備系統日誌，進行關聯性分析與威脅判斷。一旦發現高風險事件則會發出告警，並由SOC維運人員進行事件追蹤與應變處理。


資料安全
Data Security
DDoS清洗中心
DDoS Detection and Mitigation
網路安全
Network Security
國網中心TWCC資安防護
TWCC
Taiwan Computing Cloud
資安管理
Information Security and Management System
APT偵測與防護系統
APT Detection and Sandboxing
資訊安全維運中心
Security Operation Center

DDoS攻擊介紹

- 阻斷式服務攻擊(Denial of Service, DoS)是透過攻擊服務漏洞或是資源消耗的方式，影響網路服務對外的可用性，甚至最終阻斷網路服務提供。

- 分散式阻斷服務攻擊(Distributed Denial Of Service, DDoS)則是透過許多不同的攻擊來源，對服務主機發動DoS攻擊，進而達到阻斷網路服務提供。

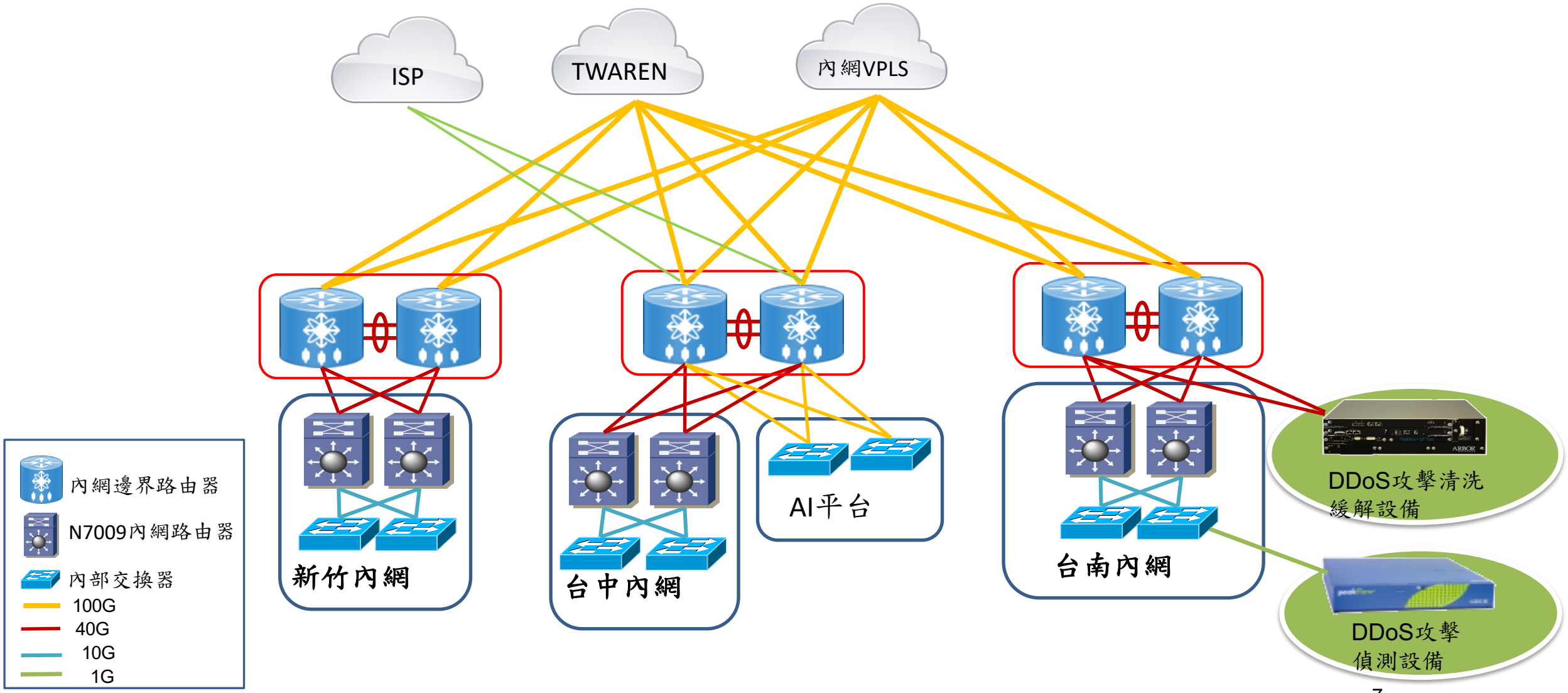
DoS/DDoS攻擊種類

- 資源消耗, 如UDP Flood, DNS Amplification等
  - 消耗網路頻寬:短時間內發送大量封包，造成網路擁塞，進而引醒網路服務提供品質，甚至讓需要使用服務的人無法存取。
  - 佔用系統資源:短時間內發送大量連線請求，占用網頁伺服器之系統資源，癱瘓伺服器之服務。
- 系統漏洞, 針對Apache伺服器的Exploit攻擊
  - 攻擊特定系統漏洞，可遠端不斷重啟系統或造成系統當機，進而癱瘓系統服務，達到攻擊目的。

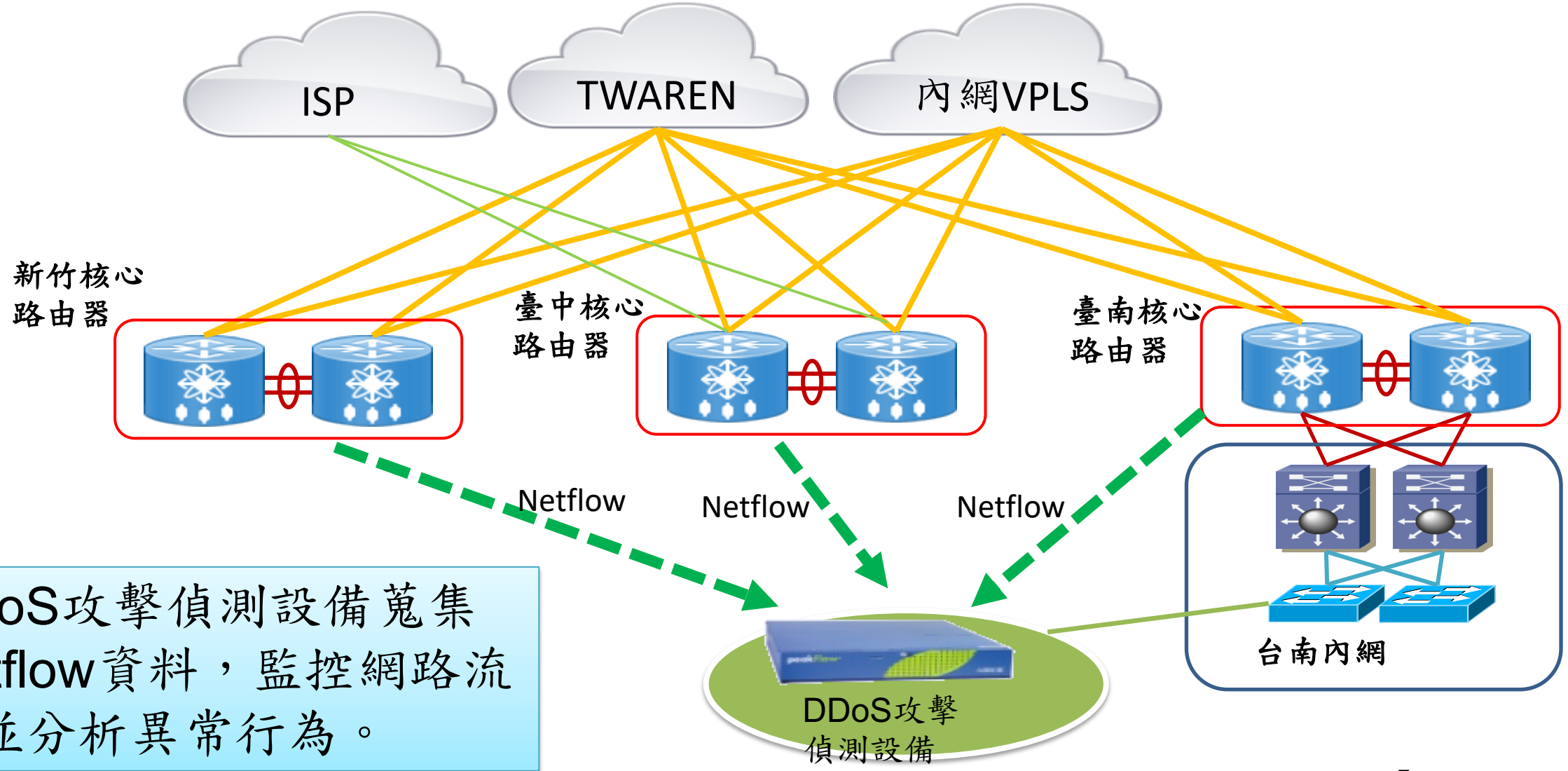
DDoS防護設備說明

- DDoS攻擊偵測
  - 佈署位置：國網中心臺南分部
  - 說明：收集維運點之NetFlow進行DDoS攻擊偵測，當DDoS攻擊發生時，可與區網核心路由器溝通，引導DDoS攻擊流量至DDoS緩解設備進行流量清洗。
- DDoS攻擊緩解
  - 佈署位置：國網中心臺南分部
  - 設備效能：規劃須達15Gbps以上
  - 說明：針對異常流量以及DDoS攻擊進行過濾以及攻擊緩解，以確保網路服務之可用性以及連線品質。

DDoS清洗中心架構圖



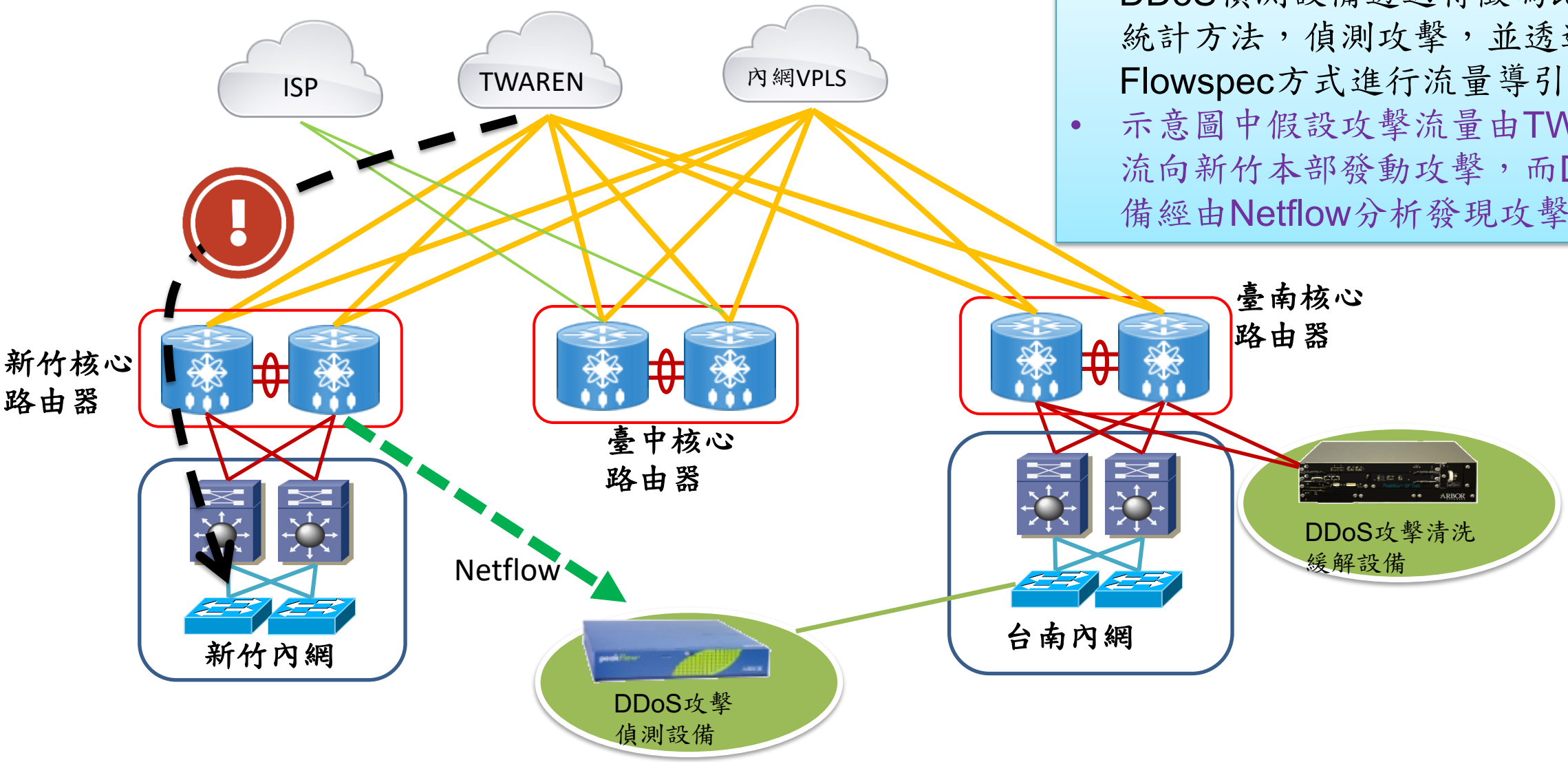
DDoS清洗中心運作示意圖



DDoS攻擊偵測設備蒐集Netflow資料，監控網路流量並分析異常行為。

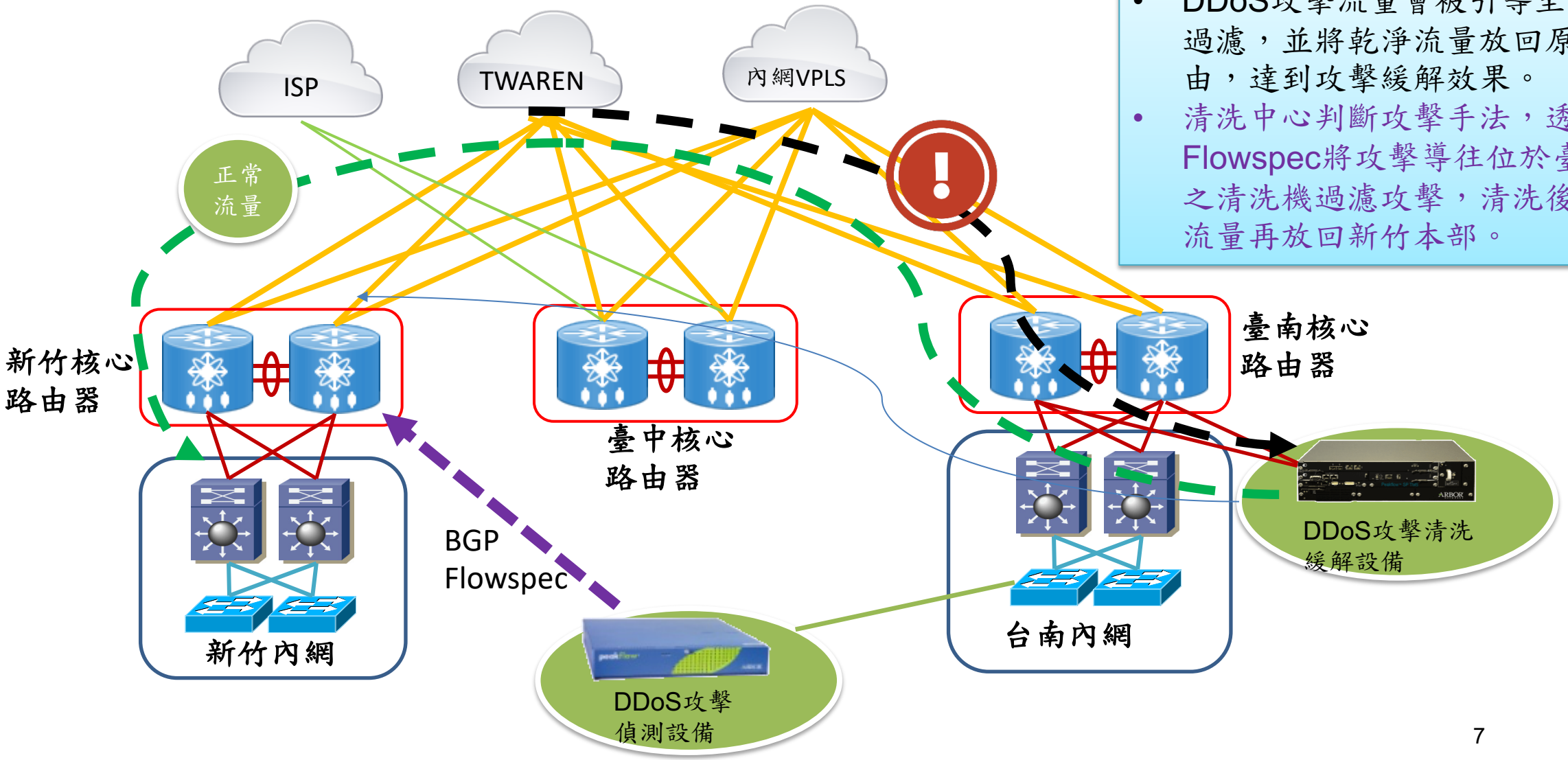
DDoS清洗中心運作示意圖

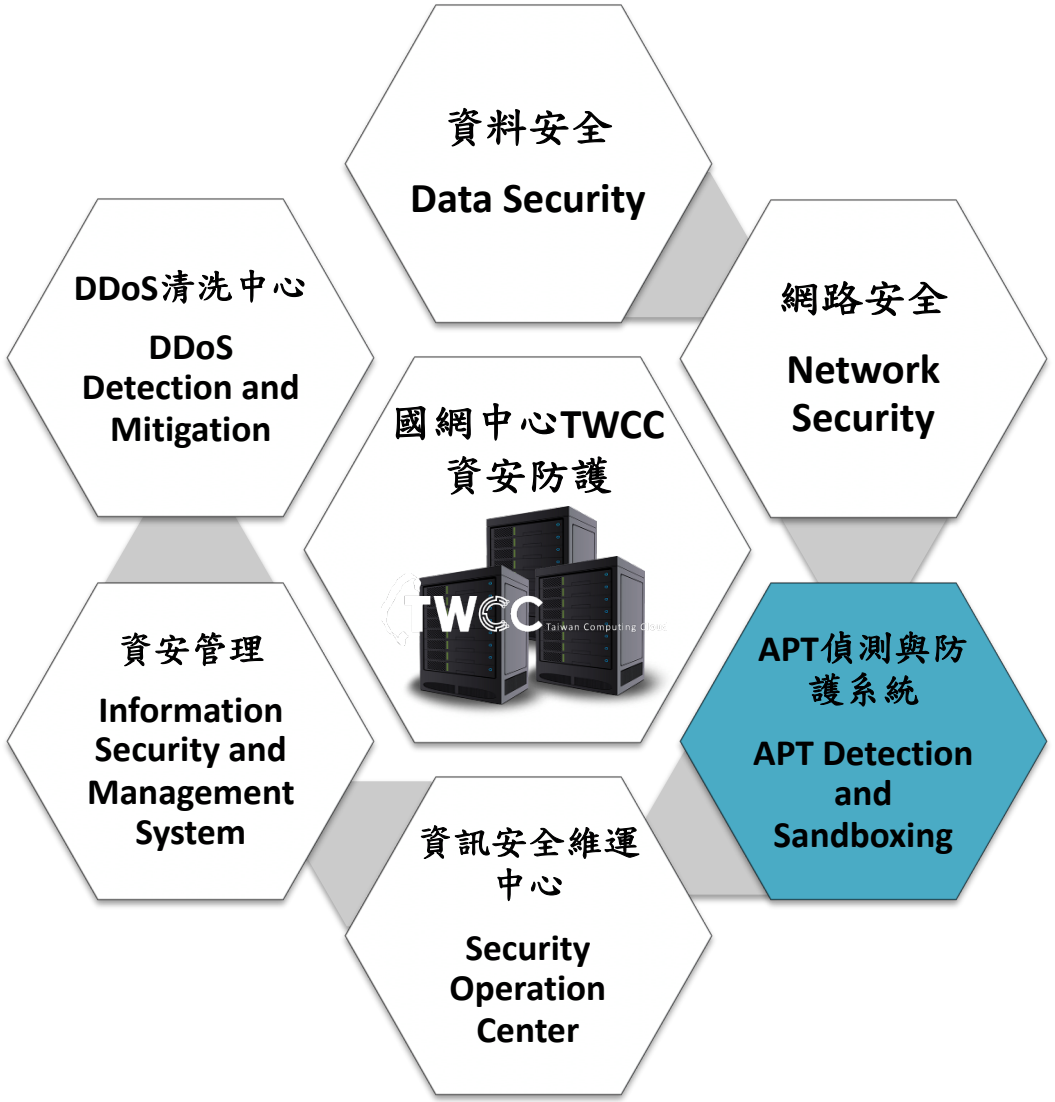
- DDoS偵測設備透過特徵碼比對以及統計方法，偵測攻擊，並透過BGP Flowspec方式進行流量導引
- 示意圖中假設攻擊流量由TWAREN流向新竹本部發動攻擊，而DDoS設備經由Netflow分析發現攻擊。



DDoS清洗中心運作示意圖

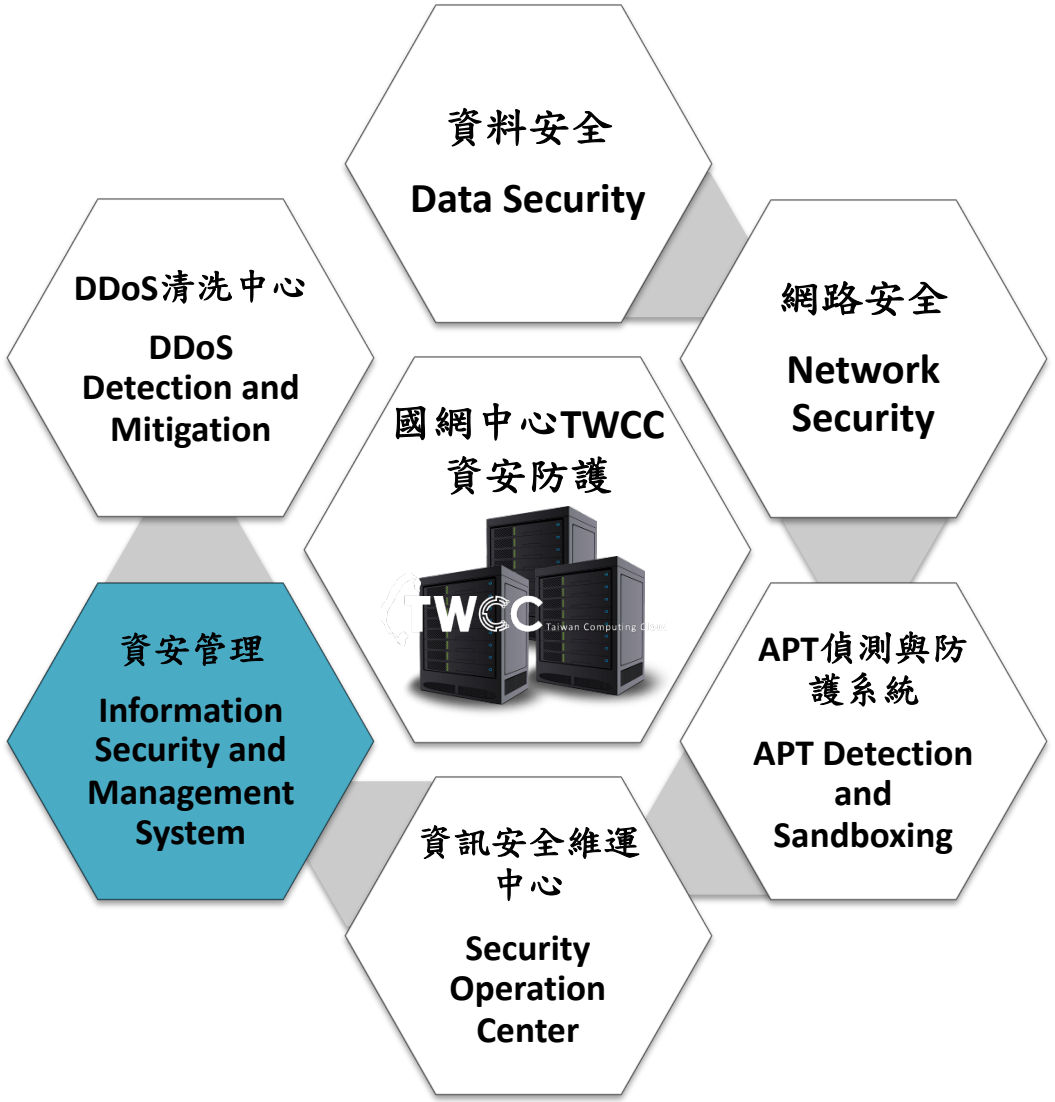
- DDoS攻擊流量會被引導至清洗機過濾，並將乾淨流量放回原本的路由，達到攻擊緩解效果。
- 清洗中心判斷攻擊手法，透過BGP Flowspec將攻擊導往位於臺南分部之清洗機過濾攻擊，清洗後的乾淨流量再放回新竹本部。




資料安全
Data Security
DDoS清洗中心
DDoS Detection and Mitigation
網路安全
Network Security
國網中心TWCC資安防護
TWCC
Taiwan Computing Cloud
資安管理
Information Security and Management System
APT偵測與防護系統
APT Detection and Sandboxing
資訊安全維運中心
Security Operation Center

APT防護系統

- 透過網路行為與惡意程式偵測機制，偵測可能的APT活動並發出告警
- 可監測網頁行為或是電子郵件傳輸內容
- 透過動態沙箱機制，檢測檔案安全性
- 可支援多種作業系統檔案，包含Windows檔案格式, PDF, Office檔案, Java, html, 或是Android APK等不同檔案格式。
- 預計於2019年Q2完成TWCC出口部署，採監聽模式進行APT攻擊偵測。


資料安全
Data Security
DDoS清洗中心
DDoS Detection and Mitigation
網路安全
Network Security
國網中心TWCC資安防護
TWCC
Taiwan Computing Cloud
資安管理
Information Security and Management System
APT偵測與防護系統
APT Detection and Sandboxing
資訊安全維運中心
Security Operation Center

國際資安標準驗證

- 國際資安標準提供可驗證的資訊安全管理作業模式，針對不同的資訊服務進行作業流程及控制措施制定，供資訊服務提供商作為參考。
- 中心除定期進行ISO/IEC 27001:2013資訊安全管理系統驗證外，近年來為強化雲端服務提供以及個人資料保護，亦開始導入相關國際資安標準，以確保中心服務流程與資安防護符合國際標準規範。

導入國際資安認證機制

資訊安全管理系統

ISO/IEC 27001:2013為目前最被廣泛使用的資訊安全管理系統國際標準規範，透過11個管理領域、39個控制目標和133個控制要點，架構完整的資訊安全管理系統。

ISO/IEC ISO 27017主要目的在於提供雲端服務廠商一個雲端服務環境的建置與維運安全規範建議。

個人資料保護

雲端服務安全

ISO/IEC ISO 27018和BS 10012都是屬於個人資料保護的國際資安認證，確保服務維運商能夠妥善保管並維護使用者資料。

簡報結束

敬請指教