

TANet

青少年網路內容防護計畫



TANWP

執行單位：國立中山大學
計畫主持人：鄺獻榮 教授暨處長
協同主持人：蔡崇煒 副教授暨副處長

01 計畫特色



- ◆ 依兒童及少年福利與權益保障法第43、46條，防護學術網路內容安全。
- ◆ 107年度起受教育部委託開發防護系統維運至今，密切配合阻擋兒少不宜之網域。
- ◆ 已導入12個區網中心及轄下22個縣市教育網路中心，防護範圍涵蓋全國。
- ◆ 持續強化技術、改善報表系統呈現方式，並與相關單位建立合作關係。
- ◆ 研發AI生成黑名單功能、結合各作業系統替代NGA之防護軟體。



系統研發與維運 UI介面改善

防護技術研發與維運、維護資料庫系統、改善報表系統UI介面、建置防護系統資訊首頁。



研發AI生成黑名單 替代NGA防護軟體

開發AI生成黑名單機制識別潛在不當資訊網站，並提供替代NGA之防護軟體及操作方式。



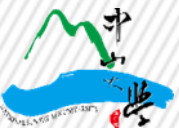
防護範圍 涵蓋全國

已導入12個區網中心及轄下22個縣市教育網路中心，防護範圍涵蓋全國。



- ◆ 本計畫自107年起開發不當資訊防護系統，於110年完成全國區網導入作業，提供全國青少年網路內容的防護機制，平均每月有數千萬次不良資訊的連線訪問，透過本系統的防護機制，已將這些潛在的威脅排除在青少年的學術網路之外。
- ◆ 自111年起持續更新設備與防護系統，並透過與第三方機構合作逐漸擴大防護範圍。
- ◆ 目前致力於結合AI應用，希望能透過使用者行為的分析發現潛在的不當網站內容，達到主動偵防的效果。

年度	瀏覽次數	阻擋次數	阻擋比率
110年度合計	370,153,246,220	400,903,711	0.11%
111年度合計	432,753,551,605	753,726,648	0.17%
112年度合計	518,831,716,474	1,057,379,266	0.20%
113年度合計	547,567,273,661	2,583,697,527	0.47%





03

TANet青少年網路內容防護計畫年度時間軸

國立中山大學受教育部委託開發 不當資訊防護系統 (TANWP)

- 防護技術研發及實測
- 防護架構規劃
- 導入高屏澎網路中心實測
- 各區設備建置及導入測試

管理系統建置並導入3個區網中心

- 導入竹苗區網、雲嘉區網、花蓮區網
- 22縣市教育網中心系統轉換教育訓練
- 建立全國數據報表系統
- 監控系統建置

區網設備更新及系統優化

- 宜蘭區網建置
- 防護資料庫重新定義及分類
- 報表系統更新優化

運用AI技術輔助防護

- 結合CDN計畫
- AI輔助生成黑名單
- 深度資料探勘
- NGA替代方案

107年



108年



109年



110年



111年



112年



113年

開發新防護技術並導入4個區網

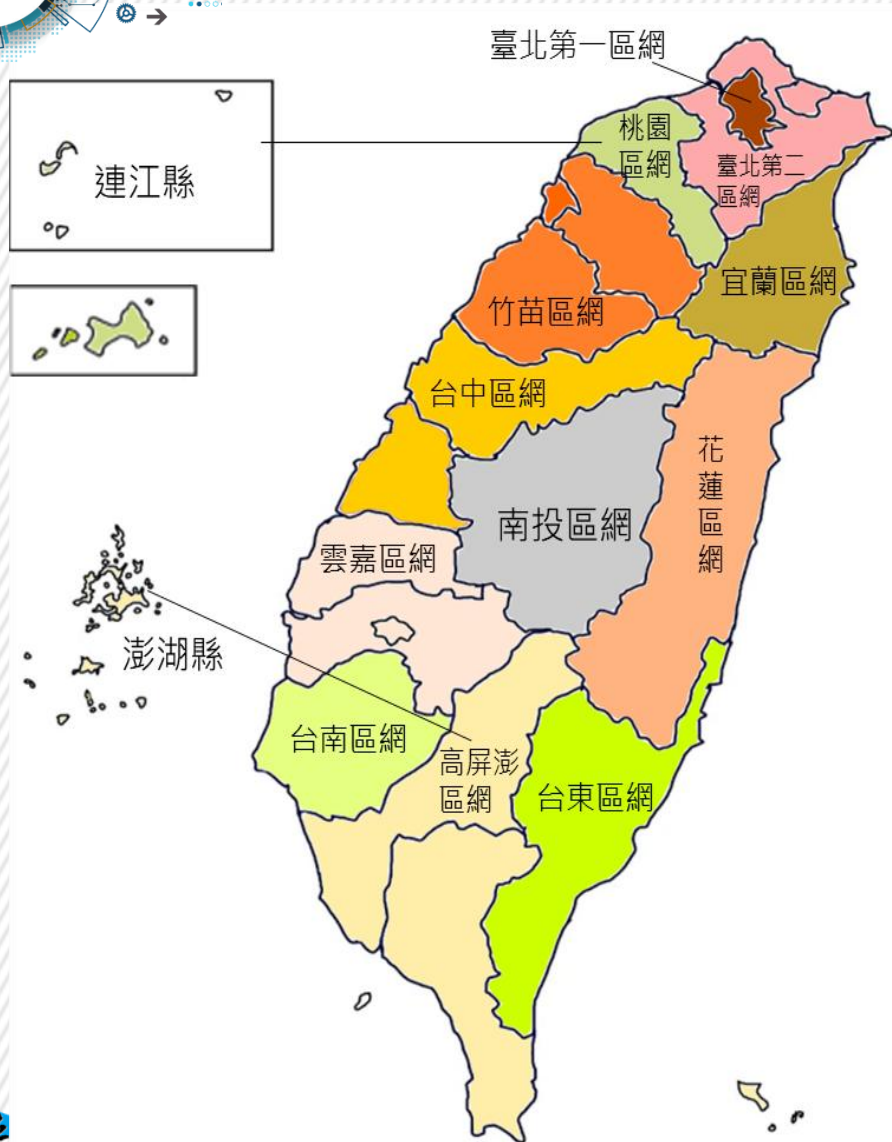
- 開發獨創三層式防護技術
- 導入臺北第一區網、臺北第二區網、桃園區網、臺南區網

22縣市教育網系統轉換並導入3個區網

- 南投區網、臺中區網、臺東區網
- 全面轉換不當資訊防護系統 (22縣市教育網系統)

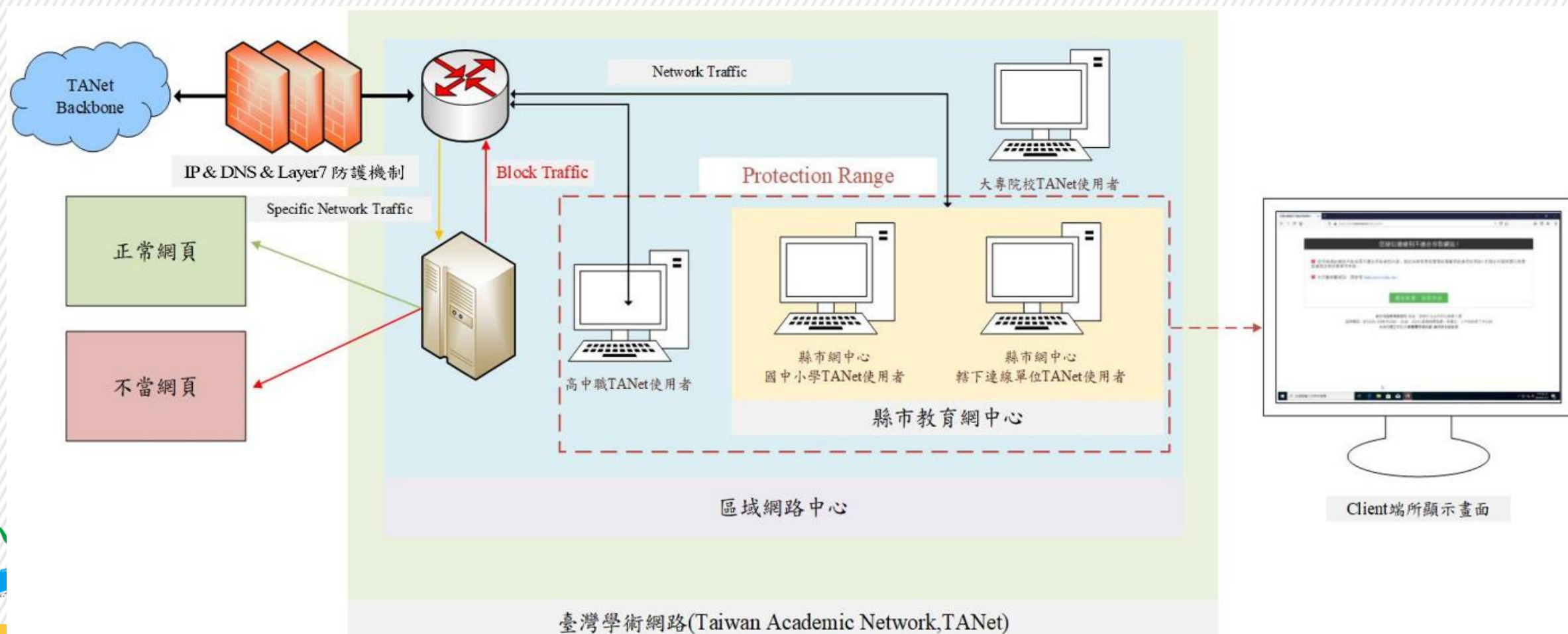
管理系統建置及協防

- 區網防護系統維運
- 技術開發與系統數位儀表板優化、AI智能黑名單
- 防護首頁開發
- 第三方機構合作



執行年度	執行項目	項目內容	執行情況	備註
107 年度	高屏澎區網	高雄市	已導入	皆已新採購防護設備建置
		屏東縣	已導入	
		澎湖縣	已導入	
108 年度	臺北第一區網	臺北市	已導入	
	臺北第二區網	新北市	已導入	
		基隆市	已導入	
	桃園區網	桃園市	已導入	
		金門縣	已導入	
		連江縣	已導入	
109 年度	臺南區網	臺南市	已導入	
		新竹縣	已導入	
		新竹市	已導入	
	竹苗區網	苗栗縣	已導入	
		雲林縣	已導入	
		嘉義縣	已導入	
	雲嘉區網	嘉義市	已導入	
		花蓮縣	已導入	
110 年度	花蓮區網	花蓮縣	已導入	
	南投區網	南投縣	已導入	
	臺中區網	臺中市	已導入	
		彰化縣	已導入	
111 年度	臺東區網	臺東縣	已導入	
111 年度	宜蘭區網	宜蘭縣	已導入	
112 年度	管理系統建置	- 防護系統首頁 - 報表系統	各項管理系統規劃與開發	
113 年度	結合 AI 技術	- AI 輔助產生黑名單 - 資料探勘 - 資料視覺化	結合其他 AI 領域技術精進防護系統	

- ◆ 防護機制：過濾防護範圍內 HTTP 或 HTTPS 網頁連線封包，透過 IP、DNS、Layer7 三重防護機制比對資料庫，若為黑名單網站則發送阻擋封包（DNS Response & HTTP Injection）讓使用者頁面重新導向特定網頁。



05

開發AI智能生成黑名單系統

◆ AI生成黑名單步驟：

1. 資料收集與預處理

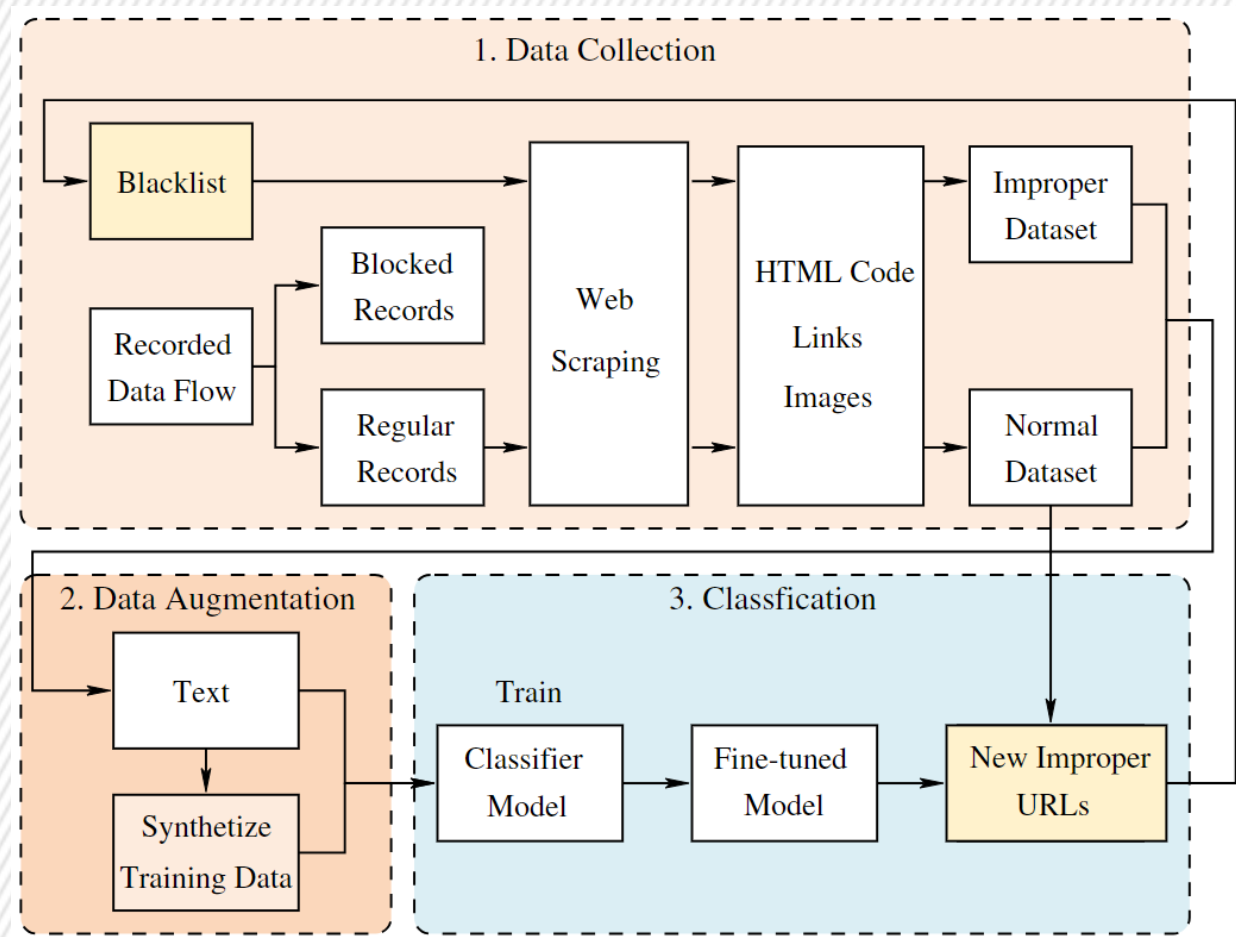
建立爬蟲系統爬取網頁，收集黑名單與使用者瀏覽紀錄之網頁資料。

2. 對不平衡資料集進行強化

3. 分類器訓練與優化

4. 將AI判斷結果交由人工審核

如果AI模型判斷將網頁分類為不當資訊時，將進一步採取人工審核。



05 替代NGA之防護機制

◆ 持續進行不同監護服務導入大量黑名單之配套功能研發建置。

系統	軟體或系統服務	大量導入黑名單功能方案
Android / ChromeOS	Google Family Link	Chrome 擴充功能
Windows / XBox	家長監護選項 (Microsoft Family Safety)	Edge 擴充功能
macOS / iOS / iPadOS	分級保護控制 (Screen Time)	捷徑和腳本程式

Google Family Link



Microsoft Family Safety



Screen Time

