

110 年雲嘉區域網路中心第 1 次管理會暨資訊安全研討會 議程表

時間：110 年 9 月 8 日(星期三) 10:00-16:00

地點：Google Meet 線上會議室

主辦單位：雲嘉區域網路中心

協辦單位：國立中正大學資訊處

與會人員：雲嘉區網中心連線單位

視訊網址：<https://meet.google.com/uis-ywto-esd>

議程：

時間	活動議題	主講人/主持人
09:40~10:00	開放線上會議室	
10:00~10:10	致歡迎詞	國立中正大學 資訊處/黃仁竑 資訊長
10:10~11:00	雲嘉區網管理委員會交流會議	國立中正大學 資訊處/黃仁竑 資訊長 連線單位/與會貴賓
11:10~12:00	教育部所屬公務機關資安稽核 經驗分享	薛雅芳 技士
12:00~13:30	午間休息	
13:30~14:30	惡意程式攻擊	敦陽科技/技術處長 楊柏翰
14:30~15:30	雲端安全	敦陽科技/技術處長 楊柏翰
15:30~15:50	Q & A	

110 年度雲嘉區域網路中心第 1 次管理會會議紀錄

雲嘉區網中心業務報告：

1. 雲嘉區域網路中心主任黃仁竑教授致詞。
2. 有關 IPv6 之支援狀況，請各連線單位配合教育部政策啟用 IPv6 之連線應用，未啟用之單位說明如下：
大專院校：
長庚科技大學(嘉義分部)：因台北本部連接中央研究院，並依 TANet 技術小組第 96 次會議決議，將線路調整回介接 TANet 網路(台北第二區網中心)，目前還未進行調整。
中國醫藥大學(北港分部)：此單位長期在台中區網參加管理會，有關 IPv6 的啟用，商請台中區網中心協助詢問執行狀況。
高中職：
協志工商：目前學校轉型中，暫停招生 3 年。
弘德工商：學校經營面臨問題。
3. 臺灣學術網路(TANet)無線漫遊服務原則自 110 年 1 月 1 日起全面改用 eduroam 為認證機制。惟升級 eduroam 的最後期限，將於本(110)年度區網中心期中或期末會議討論。
 - ✓ TANetRoaming 將俟全國各級學校無線網路認證服務皆升級至 eduroam 後，始停止服務。
 - ✓ 區網中心將協助無線漫遊中心推動 eduroam 服務，並調查轄下各大專院校、高中職無線網路升級 eduroam 意願及系統架構，於彙整後提供無線漫遊中心。
 - ✓ 無線漫遊中心會持續更新 eduroam 相關建置指引及辦理教育訓練，協助各連線單位了解 eduroam 技術及問題的解決。
 - ✓ eduroam 的 EAP 優先完成支援 MS-CHAPv2 及 GTC(無線網路控制器配合更新)。
4. 教育部轉內政部警政署刑事警察局函文，涉及詐欺案件之非法網站清單。請連線單位依據內政部警政署刑事警察局 110 年 8 月 27 日刑防字第 1100101277 號及臺灣學術網路管理規範第 11 條「為阻斷不當或不法行為存續或擴散」辦理。
5. 110 年度教育部學術與部屬機關(構)分組資通安全通報演練。
 - ✓ 演練期程：
 - 資料整備作業:自計畫頒布至 110/9/3 日止。
 - 區網中心 24 個連線單位資料填寫及密碼變更作業已於 8/31 完成。資安通報演練作業:110/09/13 至 110/09/17 日止。
 - ✓ 參與演練單位收到通知後於 1 小時內至「教育機構通報演練平臺」<https://drill.cert.tanet.edu.tw> 完成通報應變處理。

6. 連線單位 HTTPS 檢測

- ✓ 依教育部臺教資(四)字第 1100115174 號辦理
 - 區域網路中心負責檢測轄下連線單位對外網站，於 110 年 9 月 27 日前完成轄下連線單位對外網站檢測報部。
 - 檢測工具:財團法人台灣網路中心免費檢測工具網址：
<https://check.twnic.tw>。
 - 目標：檢測網站並通過 HTTPS、TLS 及 Certificate 等三項測試。
- ✓ 注意事項
 - 建議進行檢測的電腦啟用 IPV6。
 - 使用非 TANet IP 進行檢測。

7. 青少年網路內容防護計畫

- ✓ 防護系統介紹及相關統計資料說明
 - 當學術網路的使用者欲前往不當網站時，系統將進行網站的阻擋。
 - 防護縣(市)教育網路中心以及區域網路中心所屬高中職連線單位。
- ✓ 三層式的防護機制：DNS 防護、Layer7 防護、IP 防護。
- ✓ 嘉義市、嘉義縣、雲林縣教育網路中心、高中職連線學校均已上線。

各單位意見交流：

1. 嘉義縣教育網路中心：縣網中心 IPv4 有部分網段沒有 DNS 反解，有些高中職在 DNS 向上集中過程，有某些網段可能在轉移過程中有哪個環節沒有設定好，這部分再請區網協助瞭解。
2. 萬能工商：也有 IPv4 部分網段沒有反解，區網一併協助瞭解。
3. 嘉義市教育網路中心：收到涉及詐欺案件之非法網站之名單函文，其清單非常多，要在 DNS 阻擋並不容易，不當資訊系統也有跟 DNS 過濾之機制，不知是否可以在此系統直接統一阻擋。
4. 萬能工商：https 憑證是否有機會由教育部統一購置，以預防未來 Chrome 瀏覽器阻擋之情形。GSN 有提供憑證，但學術網路沒有。
5. 嘉義縣教育網路中心：有關非法網站之名單，DNS 對外查詢可以轉至教育部 163.28 主機協助做處理，對內由自行的主機做查詢服務。
6. 中正大學：有關教育部所屬公務機關資安稽核的技術問題，連線單位如有需求，中正可以協助指導。
7. 華南高商：有關高中職資安分級，嘉義地區的學校大致都核定在 D 級的部分，目前教務系統是比較大的問題，這個部分還未達到向上集中的要件，國教署行程預計在今年底或明年初關注教務系統的部分，另提醒高中職不要再自行架設 Email，儘量申請教育雲帳號。

110年度雲嘉區域網路中心

第一次管理委員會

110年9月8日

會議大綱

- ◎ IPv6應用推動狀況
- ◎ eduroam無線網路漫遊服務
- ◎ 涉及詐欺案件之非法網站
- ◎ 資通安全通報演練
- ◎ TANet連線單位HTTPS檢測
- ◎ 青少年網路內容防護計畫
- ◎ 各單意見交流
- ◎ 教育部所屬公務機關資安稽核經驗分享



連線單位IPv6服務狀況

- ◎ 區網偵測IPv6服務異常單位：
- ◎ 大專院校
 - 大同技術學院
 - 長庚科技大學
 - 中國醫藥大學(北港校區)(台中區網協調執行狀況)
- ◎ 高中職
 - 協同中學
 - 新港藝術高中
 - 協志工商(學校轉型中)
 - 弘德工商(學校經營面臨問題)



eduroam無線網路漫遊服務

- ◎ 臺灣學術網路(TANet)無線漫遊服務原則自110年1月1日起全面改用eduroam為認證機制。
- ◎ 高中職以下學校導入eduroam已納入前瞻計畫項目，請各縣市網路中心持續協助導入。
- ◎ eduroam的EAP優先完成支援MS-CHAPv2及GTC(無線網路控制器配合更新)。
- ◎ TANet無線網路漫遊中心：**升級eduroam驗證機制意願調查表**。



涉及詐欺案件之非法網站

- ◎ 教育部轉內政部警政署刑事警察局函文，涉及詐欺案件之非法網站清單。
 - 臺教資(四)字第1100105361號
 - 臺教資(四)字第1100107557號
 - 臺教資(四)字第1100113621號
 - 臺教資(四)字第1100117166號
- ◎ 依據內政部警政署刑事警察局110年8月27日刑防字第1100101277號及臺灣學術網路管理規範第11條「為阻斷不當或不法行為存續或擴散」辦理。



110年度教育部學術與部屬機關(構) 分組資通安全通報演練

- 目的
 - ✓ 檢驗單位聯絡人資料正確性(完成)
 - ✓ 測試連線單位通報及處理能力，區網審核機制完整性
- 區網中心及連線學校參與演練
- 演練期程
 - ✓ 資料整備作業:自計畫頒布至110/9/3日止
 - 區網中心24個連線單位資料填寫及密碼變更作業已於8/31完成
 - ✓ 資安通報演練作業:110/09/13至110/09/17日止
- 參與演練單位收到通知後於1小時內至「**教育機構通報演練平臺**」<https://drill.cert.tanet.edu.tw>完成通報應變處理



連線單位HTTPS檢測

- ◎ 依教育部臺教資(四)字第1100115174號辦理
 - 區域網路中心負責檢測轄下連線單位對外網站
 - 於110年9月27日前完成轄下連線單位對外網站檢測報部
 - 檢測工具:財團法人台灣網路中心免費檢測工具網址
<https://check.twnic.tw>
 - 目標 :檢測網站並通過HTTPS、TLS及Certificate等三項測試
- ◎ 注意事項
 - 建議進行檢測的電腦啟用IPV6
 - 使用非TANet IP進行檢測



通過HTTPS、TLS及Certificate等三項測



首頁 新聞 方法論 典範 統計 關於

現代化網路協定檢測

測試你的網站 Test your website

測試說明

先進IP協定位址？網域名稱DNSSEC認證？安全連線？網路安全選項？

[about the test](#)

你的網址

開始測試

測試你的郵件主機 Test your email

測試說明

先進IP協定位址？網域名稱DNSSEC認證？防止網路釣魚？網路安全選項？

你的 email 地址

開始測試

測試你的網路連線 Test your ip address

測試說明

先進IP協定位址？網域名稱DNSSEC認證？

[about the test](#)

開始測試

HTTPS

HTTPS(HyperText Transfer Protocol Secure),被說明為HTTP over TLS、HTTP over SSL或HTTP Secure，是透過網路進行安全通訊的傳輸協定，HTTPS經由HTTP進行通訊，進一步利用SSL/TLS來加密傳輸封包

HTTP

✓ HTTPS 狀態

✓ HTTPS 重定向

✓ HSTS

TLS

✓ TLS版本

✓ 加密演算法(Cipher suite)

✓ SECURE RENEGOTIATION

Certificate

✓ trust chain of certificate

✓ public key of certificete

✓ signature of certificate

✓ domain name on certificate

青少年網路內容防護計畫

- 防護系統介紹
 - 當學術網路的使用者欲前往不當網站時，系統將進行網站的阻擋
 - 防護縣(市)教育網路中心以及區域網路中心所屬高中職連線單位
- 三層式的防護機制
 - DNS防護
 - Layer7防護
 - IP防護
- 現況
 - 嘉義市、嘉義縣、雲林縣教育網路中心、高中職連線學校均已上線

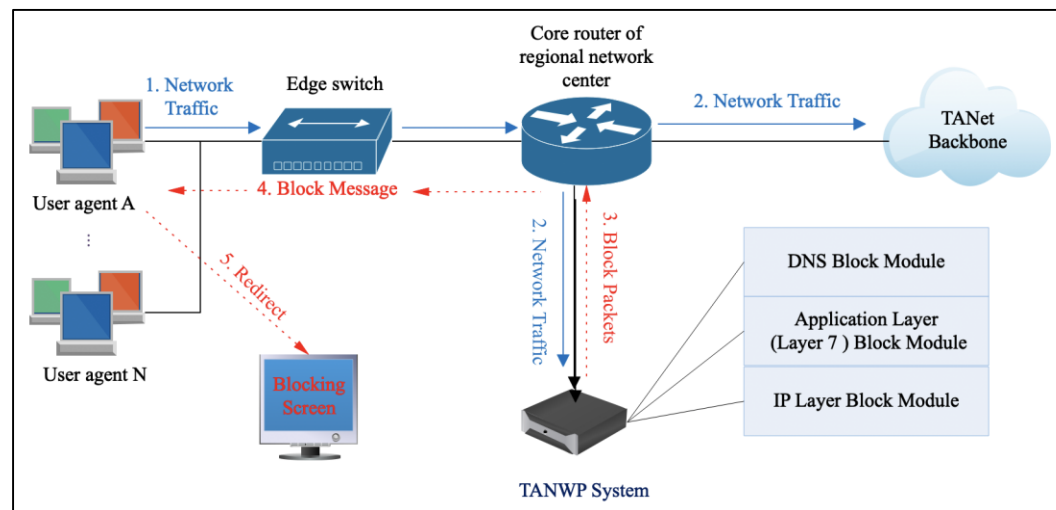
您疑似連線到不適合存取網站！

1 您所檢視的網頁可能含有不適合存取資訊內容，因此依照教育部管理政策暫時拒絕您的存取! 如有任何疑問請向教育部資訊及科技教育司申訴。

2 本計劃相關資訊，請參考 twb.moe.edu.tw。

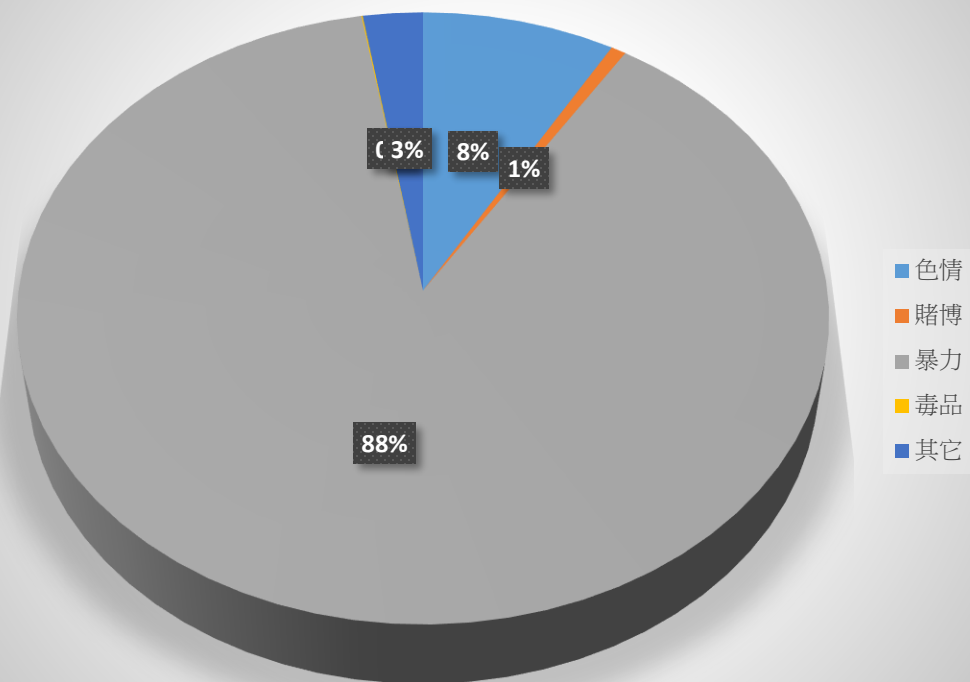
網址誤擋 · 我要建議

歡迎蒞臨教育部網站 地址：10051 台北市中山南路 5 號
諮詢電話：(07)525-2000 #2500、2518、2519 | 客服時間為週一至週五，上午9:00至下午5:00
諮詢信箱：tanwp@mail.nsysu.edu.tw
系統由國立中山大學圖書與資訊處-資訊安全組維護

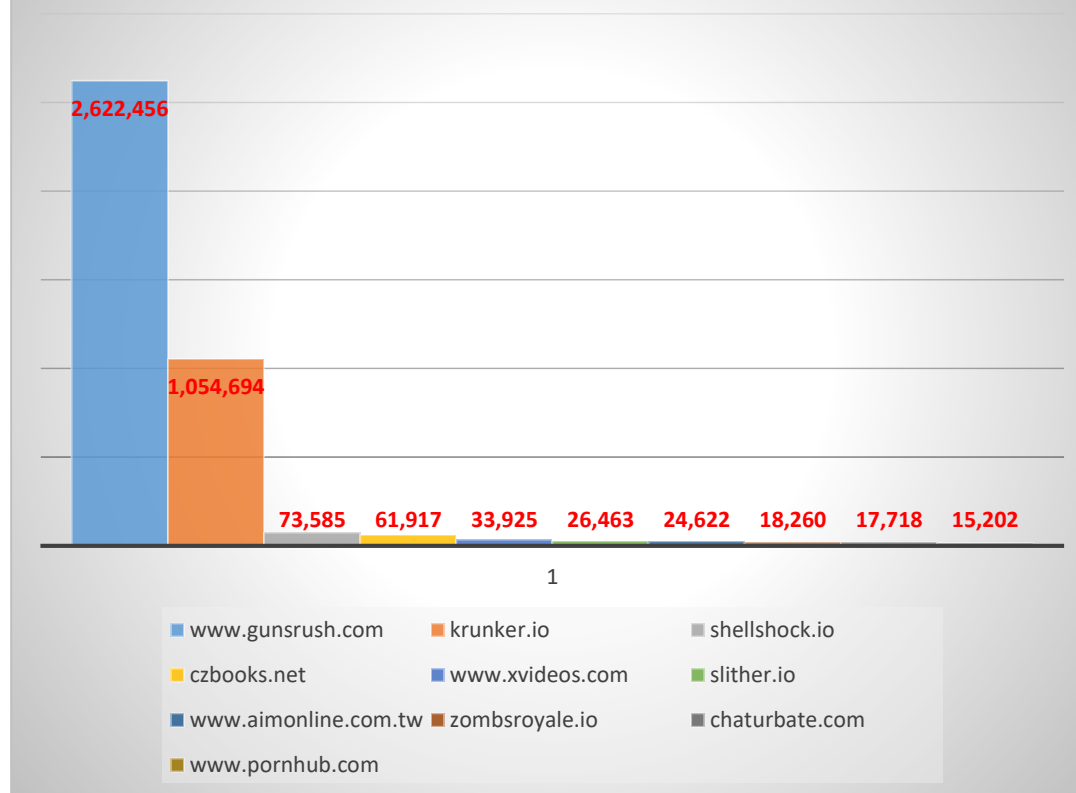


相關統計資料

阻擋類別



阻擋網域前十名



各單意見交流

- ◎ 縣市教育網路中心現況報告
 - 雲林縣教育網路中心
 - 嘉義縣教育網路中心
 - 嘉義市教育網路中心
- ◎ 其他單位報告
- ◎ 臨時動議



國立中正大學資訊處

教育部所屬公務機關資安稽核經驗分享

薛雅芳 技士