**100年第二次北區區網管理委員會**

**會議記錄**

日期: 100/10/04

時間: 14：20～17：30

地點: 計資中心106會議室

**目錄**

[壹、 北區區網會議報告 3](#_Toc309562184)

[講者: 李光偉](#_Toc309562185)

[I. 臺大區網中心特優 3](#_Toc309562186)

[II. 連線現況說明 3](#_Toc309562187)

[III. 相關管理網頁 4](#_Toc309562188)

[IV. 服務 6](#_Toc309562189)

[貳、 北區區網網管會議 6](#_Toc309562190)

[講者: 李美雯](#_Toc309562191)

[I. 區網學校與ISP介接 7](#_Toc309562192)

[II. 100年區網中心資安防護 7](#_Toc309562193)

[III. 網站資安防護 7](#_Toc309562194)

[IV. 「社交工程」危機意識宣導訓練 7](#_Toc309562195)

[V. 北區學術資訊安全維運中心 8](#_Toc309562196)

[VI. 資安Case Study 8](#_Toc309562197)

1. 北區區網會議報告

講者: 李光偉

Tel:(02)33665008

 E-mail:edward@ntu.edu.tw

1. 臺大區網中心特優
* 99年區網中心年終績效評估獲選為特優，謝謝大家的支持，100年年終考核又到了請大家多支持。
* http://speed.hinet.net/ 為中華電信提供有上行下行速率
* http://www.ascc.sinica.edu.tw/netsrv/speed/index.php 為中研院提供，建議選800M以上的檔案越大越準確。
1. 連線現況說明
2. 目前連線單位為53個學校單位
<http://tprc.tanet.edu.tw/center03.php>
3. 各連線學校流量
<http://tprc.tanet.edu.tw/mrtg/>
4. 目前區網連線學校都在新世代骨幹網路路由器下，連線速率從100 Mbps 提昇至1Gbps 需重提計畫書，並確認是GiBIC介面而不是Ethernet RJ45 UTP介面，因為到目前為止某些ISP會以他們layer 2 Switch的UTP port可以到1Gbps來提供200Mbps以上的頻寬。
5. 連線學校及單位IP網段網頁如下:

[**http://tprc.tanet.edu.tw/data/ip\_new\_ver.php**](http://tprc.tanet.edu.tw/data/ip_new_ver.php)

1. 臺大區網中心服務窗口

黃怡菁 yichuang@ntu.edu.tw

電話：02-33665009

1. 相關管理網頁

1. 連線學校通過審核後提昇速率的原則：

1. 連接區網中心路由器 FastEhernet port連線速率最低為10 Mbps最高100M bps。bps是 bits per second縮寫
2. 連接區網中心路由器GigaEhernet port連線速率最低為100 Mbps最高為 1 Gbps。
3. 區網違規管理系統及處理方式說明

<http://tprc.tanet.edu.tw/disobey>

可利用台大區網中心所發帳號自行至上列網址先填報處理情形再恢復IP的使用，帳號有問題請洽黃怡菁小姐(33665009)。



1. 區網違規管理系統表列 (只能看不能取消限制)

<http://tprc.tanet.edu.tw/disobey/disobey.php>

歡迎告知各校師生可以自行查詢。

1. 目前臺大區域網路後台管理系統網址如下 https://tprc.tanet.edu.tw/data\_sys/login.php



* 各校網管人員如有更換請至臺大區域網路後台管理系統修改資料，如忘記密碼可與黃怡菁小姐連絡。



1. 服務

1.區網違規查詢及自行解除IP鎖定系統

2.網頁弱點掃描及阻擋色情網頁

3.應用課程：每年暑假舉辦研討會

4.101年管理委員會名單

1. 北區區網網管會議

講者: 李美雯

部門: 臺灣大學計資中心

Email: **mli@ntu.edu.tw**

TEL: 3366-5010

1. 區網學校與ISP介接
* 中華電信 Hinet – 1G bps
* 台灣固網 TFN – 1G bps
* 和信電訊 KGT – 1G bps
1. 100年區網中心資安防護
* 資安技術教育訓練與宣導活動
* ISMS資安顧問到府輔導
* 一年多次網站弱點掃描
* 一年兩次社交工程演練
* 其他服務
	+ 「7x24全天候網站掛馬警告系統」服務
	+ 網站程式碼弱點掃瞄
1. 網站資安防護
* 網站弱點掃描
	+ 掃描網站程式弱點，並提供修復建議報告
	+ 請自行上網申請掃描<http://mozart.cc.ntu.edu.tw/>
* 網站源碼檢測
	+ 找出網站程式碼中的安全問題，並提供修補建議
	+ email申請 yichuang@ntu.edu.tw
* 網站安全監控與檢測
	+ 計中提供了7x24全天候網站安全監控與檢測服務
	+ email申請 yichuang@ntu.edu.tw
1. 「社交工程」危機意識宣導訓練
* 各機關人員每年至少須接受
	+ 「 1 小時」社交工程防制宣導講習（含 E-Learning 課程）
* 宣導課程應分「兩階段」辦理：
	+ 第一階段(於演練作業辦理前)：
		- 對機關所有人員，全面性實施教育訓練
	+ 第二階段(於演練作業完成後)：
		- 對開啟惡意郵件或點閱惡意郵件連結或附件之「應重點宣導人員」再次進行宣導，以強化其警覺性
1. 北區學術資訊安全維運中心
* 教育部委託於100年7月成立7×24全年無休的北區學術資訊安全維運中心(A-SOC)
* 提供北區學術網路資安事件之偵測、通報與追蹤
* 彙整台北區網中心(台大)、台北區網中心(政大)及桃園區網中心等維運點之資安訊息
* 配合教育學術資安資訊分享機制(A-ISAC)
* 惡意程式檢查步驟
	+ 查找系統可疑之Process
		- 可使用微軟 Process Explorer
		- 確認Process是否正常
			* <http://www.liutilities.com/products/wintaskspro/processlibrary/>
	+ 系統啟動區查找惡意程式
		- 可使用微軟 Autoruns for Windows
	+ 未來將提供上述資訊給網管
* 連線學校配合事項
	+ 確實處理資安事件單
	+ 若有任何誤判懷疑與證據，請據實回報以修正觸發規則
	+ 網段更改或網管人員/資安人員名單有變動請上網修改並通知北區A-SOC
1. 資安Case Study
* Advanced Persistent Threat(APT)
	+ 針對特定組織或平台所作的複雜且多方位的網路攻擊
	+ 進階持續性滲透攻擊
	+ 攻擊結合人的介入，而不只是自動化程式
	+ 出於經濟或長期收益之動機
* 知名APT攻擊
	+ 極光（Aurora）APT攻擊Google和其他科技公司
	+ Stuxnet蠕蟲攻擊
	+ HBGary與駭客組織(Anonymous)交手
* 評估控制APT的可能性
	+ 未來APT將會一直與我們同在
	+ 繼續部署攔截對策
		- 入侵偵測，弱點掃描，防毒軟體和系統更新…
	+ 即時的監控網路流量和電腦上的活動
		- 儘快偵測到攻擊來源，並遏制它所造成的影響
		- 隔離被入侵的設備，關閉伺服器和收集資料以作鑑識分析之用