

108年學年度第一次 竹苗區網管理委員會

國立交通大學 資訊技術服務中心

2018/03/28

教育體系因應資通安全管理法之規劃說明

- 教育部說明投影片可至TANet網站下載：

<https://noc.tanet.edu.tw/index.php/download/seminar-1080121>

The screenshot shows the TANet 100G Network Operation Center website. The header includes the site name "臺灣學術網路 - 網路維運中心 TANet" and "Taiwan Academic Network - Network Operate Center". The navigation bar has links for Home, Announcements, Traffic, Sites, Downloads, and Tools. A sidebar on the left lists the same categories. The main content area shows a breadcrumb trail: Home > Downloads > Seminar Information > TANet 100G Network Operation Center. A dropdown menu is open under "研討資訊" (Seminar Information), showing "TANet 100G 網路維運技術研討會(1080121)" and "TANet 100G 網路維運技術研討會(1070129)". Below this, a list of seminars is displayed, including "TANet 100G 網路維運技術研討會邀請函(1080121)" and "1.靈活、安全和自動化的未來數位網路". The seminar "4.教育體系因應資通安全管理法之規劃說明" is highlighted with a red box, and its corresponding PDF file "4.教育體系因應資通安全管理法之規劃說明.pdf" is also highlighted with a red box. The URL in the browser address bar is "https://noc.tanet.edu.tw/index.php/download/seminar-1080121".

資安法規

- 總統107年6月6日公布資通安全管理法。
- 行政院107年11月21日發布相關子法：
 - 資通安全管理法施行細則
 - 資通安全責任等級分級辦法
 - 資通安全事件通報及應變辦法
 - 特定非公務機關資通安全維護計畫實施情形稽核辦法
 - 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法
- 行政院107年12月05日函定自108年1月1日施行。

責任等級分級辦法

- A級：本部、國立大學附設醫院（醫學中心）及常設試務機構。
- B級：本部所屬機關、國家教育研究院、國家圖書館、**公立大專校院**、國立大學附設醫院（區域醫院或地區醫院）、財團法人高等教育評鑑中心基金會。
- C級：本部其他所屬機構、國家運動訓練中心、及有維運自行或委外開發核心資通系統「**公立高級中等以下學校**」或特定非公務機關。

教育體系各單位因應措施

- 教育部後續會規劃各單位應辦事項執行狀況調查，辦理審查事宜。
- 因公私立學校應有一致性規範，教育體系各任務編組(區域網路中心、縣市教育網路中心)及私立學校，資科司依「資通安全分級作業辦法」修訂「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」一併規範。

各級單位應辦事項-管理面

辦理事項	辦理內容	A	B	C
資通系統分級及防護基準	完成資通系統分級，並完成防護基準；每年至少檢視一次妥適性	1年內		2年內
ISMS之導入及通過公正第三方之驗證	2年內全部核心資通系統導入資訊安全管理系統。	3年內完成第三方驗證；並持續維持期驗證有效性。		O*
業務持續運作演練	全部核心資通系統	每年1次	每2年1次	
辦理內部資通安全稽核		每年2次	每年1次	每2年1次
資通安全專職(責)人員 (1年內)		4人	2人	1人*
資安治理成熟度評估 (公務機關)		每年1次		X

管理面應辦事項C級單位因應措施

- ISMS 導入

- 短期：資科司後續將與國教署協調規劃輔導團隊，輔導C級學校導入教版管理規範。
- 長期：高級中等以下學校全部核心系統向上集中為共通系統，將責任等級降至D級。

- 專職(責)人員

- 短期：本部同意高級中等以下學校得以專責人員配置，兼任資訊行政教師減授教學節數。
- 長期：國教署配合修正「高級中等學校組織設置及員額編制標準」，資安人力法制化。

各級單位應辦事項-技術面

辦理項目	辦理內容	A	B	C
安全性檢測 全部核心資通系統*	網站安全弱點檢測	每年2次	每年1次	每2年1次
	系統滲透測試	每年1次	每2年1次	
資通安全健診*	網路架構檢視、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設定檢視	每年1次	每2年1次	
資通安全威脅偵測管理機制*	完成威脅偵測機制建置，並持續維運	1年內		X
	依行政院指定方式提交監控管理資料	O	O	X
資通安全防護 (啟用，並持續使用及適時進行軟、硬體之必要更新或升級)	防毒軟體、網路防火牆、具有郵件伺服器者，應備電子郵件過濾機制	1年內		
	IDS/IPS、具有對外服務之核心資通系統者，應備應用程式防火牆 (WAF)	1年內		X
	APT攻擊防禦	1年內	X	
政府組態基準 (GCB)	依主管機關公告之項目，完成GCB導入作業，並持續維運 (公務機關)	1年內		X

技術面應辦事項配套措施

應辦單位	辦理項目	因應措施
A、B、C級	網站安全弱點檢測	由成功大學網站防護團隊協助辦理。
	ABC級系統滲透測試	資科司將規劃教育體系技術團隊協助辦理。
	資通安全健診	請北、南區學術資訊安全維運中心協助辦理相關教育訓練課程。
A、B級	資通安全威脅偵測管理機制	臺灣學術網路連線單位可結合臺灣學術網路資安監控系統(南、北SOC, Mini-SOC)進行威脅偵測機制。

New-E3課程平台

- 網址：<https://e3new.nctu.edu.tw>
- 將用來存放教育訓練講義及影片。



The login interface features a purple background with the NCTU logo and the text '國立交通大學 數位教學平台'. It includes input fields for '帳號' (Account) and '密碼' (Password), a yellow '登入' (Login) button, and language options 'TW' and 'EN'. At the bottom, there are links for '校內使用者忘記密碼' and '校外使用者忘記密碼'.

國立交通大學
數位教學平台

帳號

密碼

登入

TW EN

[校內使用者忘記密碼](#) [校外使用者忘記密碼](#)



The screenshot shows the platform's main page with a purple header containing a menu icon, a logo, and a user profile icon. The main content area is titled '竹苗區網教育訓練' and lists training materials under the heading '107年教育訓練'. The list includes folders for '全方位資訊安全防護-理論與實務@賴弘捷老師', '手機網路安全防護@劉得民老師', '雲端安全管理@賴弘捷老師', and '資訊安全實務@劉得民老師', each containing PDF documents.

竹苗區網教育訓練

107年教育訓練

- ▼ 全方位資訊安全防護-理論與實務@賴弘捷老師
 - 學員版全方位資訊安全防護-理論與實務.pdf
- ▼ 手機網路安全防護@劉得民老師
 - 2018-交通大學-資訊安全-網路封包分析_sLFnPA6.pdf
 - 2018-使用手機與網路的自身安全防護.pdf
 - 2018-網路手機的資訊安全案例分享.pdf
- ▼ 雲端安全管理@賴弘捷老師
 - 交大雲端安全管理.pdf
- ▼ 資訊安全實務@劉得民老師
 - 2018-交通大學-資訊安全-網路封包分析.pdf
- ▼ DNS概念與DNS服務主機實作(上)@謝祿適老師

學術網路單位所屬電子郵件帳戶密碼外洩

- TACERT通報學術網路部分單位所屬電子郵件帳戶疑似帳號及密碼外洩情資，情資內容共計有 96,784 筆電子郵件帳戶。
- TACERT將陸續派發電子郵件通知該電子郵件使用者進行密碼變更作業。
- 建議措施：
 - 1. 進行電子郵件安全宣導，降低電子郵件帳戶密碼外洩可能性。
 - 2. 進行電子郵件主機系統更新、特權帳號清查及檢查是否有異常行為帳戶。
 - 3. 對電子郵件主機系統未使用空帳號進行清查與刪除，若久未使用之帳號進行密碼變更作業。

近期重複開單事件- DNS嘗試解析惡意domain

- 近期重複開單之事件中有部分為DNS伺服器嘗試解析已知的惡意domain，可能為內部使用者透過單位DNS伺服器嘗試解析惡意domain所致，可遵循以下步驟查詢嘗試解析惡意domain之使用者：
 - 確認DNS伺服器僅允許單位內使用者進行遞迴查詢。
 - 於DNS伺服器上針對事件告知的惡意domain作封鎖
 - 於DNS伺服器上建立log機制以查出嘗試解析惡意domain之IP
 - 對使用該IP之主機進一步檢查以排除問題

近期重複開單事件- DNS嘗試解析惡意domain

- Bind9 阻擋特定domain解析設定方式：
 - 修改named.conf加入想要阻擋的domain
ex：zone “test.com” { type master; file “block.db”; };
 - 新增block.db的zonefile，加入“* IN A 127.0.0.1”之正解：

```
$TTL 24h
@ SOA @ ns2.hcrc.edu.tw. 2019032500 1d 12h 1w 3h
    ; Serial, Refresh, Retry, Expire, Neg. cache TTL

; Silence a BIND warning
@      IN      NS      ns2.hcrc.edu.tw.
@      IN      A       127.0.0.1
*      IN      A       127.0.0.1
```


近期重複開單事件- DNS嘗試解析惡意domain

- Bind9 query log設定方式：
 - 於named.conf中的logging段加入設定：

```
logging {  
    category queries { query-log;};  
    channel query-log {  
        file "/var/log/query.log" versions 10 size 1000m;  
        severity info;  
        print-time yes;  
        print-severity yes;  
        print-category yes;  
    };  
};
```

近期重複開單事件- DNS嘗試解析惡意domain

- 設定完成後須重啟服務：service named restart
- 使用dig指令測試是否生效：

```
[c:\~]$ dig iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwa.com @163.28.64.240
```

```
;; ANSWER SECTION:  
iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwa.com. 86400 IN A 127.0.0.1
```

- 使用grep過濾query log：

```
root@ns2[/etc/namedb]#cat /var/named/var/log/query.log | grep iuqer | tail -n 1  
25-Mar-2019 16:43:05.203 queries: info: client 140.113.200.52#49182: query: iuqerfsodp9ifjaposdfjhgosurijfaewrwergrwa.com IN A +E (163.28.64.240)
```

DDoS清洗宣導

- 區網中心收到DDoS供即通知會第一時間轉知受攻擊單位。
- 受攻擊單位可依據被攻擊IP主機之服務狀況評估是否需申請清洗服務。
- 如需清洗服務請與區網中心聯繫，由區網中心協助填寫申請。
- 完成清洗後系統會自動生成通報事件單，連線單位老師須登入**資安通報應變平台**完成填寫通報應變

- 申請清洗服務**不會**產生任何費用！

清洗IP*	
DNS IP	
單位名稱*	交大區網中心 ▼
通訊協定*	TCP ▼
服務說明*	例如:WEB FTP
通訊埠*	例如:80
申請理由	
	送出 (本系統僅適用於TANET部份地區)

Q & A

