

台北區網網管會議

臺灣大學計資中心
游子興

davisyou@ntu.edu.tw
3366-5008

台北區網中心服務窗口

* 服務窗口

* 游子興(Router/電路)

* davisyou@ntu.edu.tw

* 02-33666008

* 游忠憲(資安)

* chyue@ntu.edu.tw

* 02-33665013

* 郭幸香(行政)

* hsingkuo@ntu.edu.tw

* 02-33665009

* 李美雯

* mli@ntu.edu.tw

* 02-33665010

台北區網現況與服務說明



- * 共計52間連線學校
- * 區網中心連線設備兩台：
 - * 區網主幹 Router: Cisco 6509
 - * 區網 Switch: Cisco 2960

台北區網連線架構與頻寬統計

北區區網連線架構圖

Taipei Regional Network Architecture



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

* 使用介面統計:

- * TenGiga:
 - * 2 ports
- * Giga:
 - * 55 ports
- * FastEthernet:
 - * 41 Ports

台北區網101學年度重要事項

101年9月

區網網頁備份主機建置

101年10月

區網網頁改版

101年11月

MRTG 連線圖修正

102年2月：

與台大頻寬升級為 10Gb

102年3月

增設中研院備援線路1Gb

102年4月

區網實體線路重新整線

102年5月

完成 ISMS稽核

102年7月

101年度區網教育訓練

102年8月

HINET頻寬升級3Gb

101年

九月

十月

十一月

十二月

102年

一月

二月

三月

四月

五月

六月

七月

八月

台北區網營運服務目標

* 網路服務可用性

- * 提升區網中心路由器介接之實體線路的可用性，避免眾多連線學校線路交錯導致拉扯而中斷，於102年4月完成區網路由器實體線路重整
- * 中研院提供 Google/YouTube 之 Cache 服務，為提升網路應用服務之可用性，於102年3月增設與中研院之備援線路1G

* 網路連線順暢性

- * 102年4月區網中心與臺大連線由2Gbps升級為10Gbps
- * 102年8月區網中心與HINET連線由2Gbps升級3Gbps

台北區網營運服務目標

* 強化技術能力

- * 為提升網管人員技術能力，今年暑假期間舉辦**10**場教育訓練，課程內容包含先進網路技術、網路管理、及資訊安全(含智財權與個資保護)等相關議題。

* 通過教育版資訊安全管理制度(ISMS)認證

- * 為建立完善之資訊安全管理制度，降低組織內的重要資產與資訊之風險，台北區網中心於**97**年開始導入教育版ISMS制度
- * **98**年至**102**年每年皆通過教育版ISMS 第三方認證

台北區網網頁相關服務

* 區網網站

- * <http://tprc.tanet.edu.tw/index.php>

* 網路流量統計

- * <http://tprc.tanet.edu.tw/mrtg>

- * <http://mrtg.tanet.edu.tw/>

* 台大區網成員使用IP網段

- * <http://tprc.tanet.edu.tw/a5.php>

* 後台管理系統

- * https://tprc.tanet.edu.tw/data_sys/login.php

- * 各校異動，**請至後台管理系統更新**

- * 網管/資安負責老師

- * 使用網段

台北區網網頁相關服務(Cont.)



基本資料

區/縣(市)教育網路中心	台北區網中心	網址	http://tprc.tanet.edu.tw	
	地址	臺北市羅斯福路四段一號		
單位主管姓名	孫雅麗	E-Mail	sunny@ntu.edu.tw	
	電話	02-33665001	傳真	02-23637204
網路管理 負責人姓名	游子興	E-Mail	davisyou@ntu.edu.tw	
	電話	02-33665008	傳真	02-23637204

提供服務項目：

關於台北區網

- » [中心簡介](#)
- » [組織與人力](#)
- » [網路架構](#)
- » [連線單位資訊](#)
- » [連線單位IP查詢系統](#)
- » [連線單位頻寬資料](#)
- » [連線統計資料 MRTG](#)
- » [TANet IPv6 網絡查詢](#)
- » [TANET](#)
- » [TANet相關管理原則](#)

因應個資法，將連線單位資訊移至會員專區查詢

台北區網網頁相關服務(Cont.)

database manage interface - Windows Internet Explorer

https://tpc.tanet.edu.tw/data_sys/base.php 憑證錯誤 database manage interface

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

網路(P) 安全性(S) 工具(O) ?

區網資料庫管理目錄 首頁

違規系統: <https://tpc.tanet.edu.tw/disobey/>

投票系統: <http://tpc.tanet.edu.tw/vote>

首頁管理系統: <http://tpc.tanet.edu.tw/manage>

連線單位相關資料處理

- 連線單位/聯絡人
 - 新增連線單位與聯絡人資料
 - 修改連線單位或聯絡人資料
 - 連線單位聯絡人查詢
- IP
 - 新增IP範圍至連線單位或首次設定gateway/router
 - 刪除連線單位部分IP範圍
 - 修改router/修改gateway
 - 連線單位現有IP查詢
 - 單位伺服器連線IP
- 頻寬(bandwidth)
 - 修改連線單位頻寬
 - 查詢連線單位頻寬
- ISP
 - ISP測試平台IP列表查詢
 - ISP測試平台IP列表修改
- 北區區網維修
 - 北區區網維修記錄

搜尋學校/單位關鍵字: 搜尋

或搜尋聯絡人關鍵字: 搜尋

學校/單位	聯絡人	電話	手機	傳真	EMail
臺北醫學大學	林恩德	02-27361661轉2611	0970405792	02-27339049	netgroup@tmu.edu.tw
國立臺北護理健康大學	舒方	02-28227101轉2227		02-28212149	tracy@ntunhs.edu.tw
臺北市立教育大學	呂世場	02-23113040轉8514		02-23817242	ghost@tmue.edu.tw
亞東技術學院	陳東栢	02-77380145轉1821	0922-981135	02-77388828	fi015@mail.oit.edu.tw
政治作戰學校	張鴻正	02-28963237	0922-346559	02-28930423	mybubumy@hotmail.com
致理技術學院	鄭博成	(02)2257-6167轉1483,1242		02-22591114	bccheng@mail.chihlee.edu.tw
真理大學	溫雅得	02-26212121轉1615	0919958566	02-26232373	wen@email.au.edu.tw
臺北藝術大學	許煒成	02-28961000轉2232	0921-615281	02-28967690	chw@tnua.edu.tw
國防醫學院	蔡親中	02-87923311轉18260		02-87923181	nvg@ndmctsg.edu.tw
康寧專校	張宗銓	02-26321181轉373		02-26337354	raymond@knjc.edu.tw
華夏技術學院	王士傳	02-89415109轉101	0920-892992	02-29415730	chwan@cc.hwh.edu.tw
實踐大學	黃麗華	02-25381111轉1821,1823	0912581651	02-25337014	lihwa@mail.usc.edu.tw
銘傳大學	吳寶林	02-28824564轉2559		02-28831082	qiwu@mail.mcu.edu.tw
德霖技術學院	高玉馨	02-22733567轉537		02-22749468	hebe@mail.dlit.edu.tw
德明財經科技大學	黃洪源	02-26585801轉2510	0933-916611	02-26582507	xiayu@takming.edu.tw
黎明技術學院	賴志明	02-22975275		02-22975275	mrlai@mail.lit.edu.tw

台北區網網頁相關服務(Cont.)

歡迎光臨臺大區域網路後台管理系統

連線單位帳戶
登入

帳號:

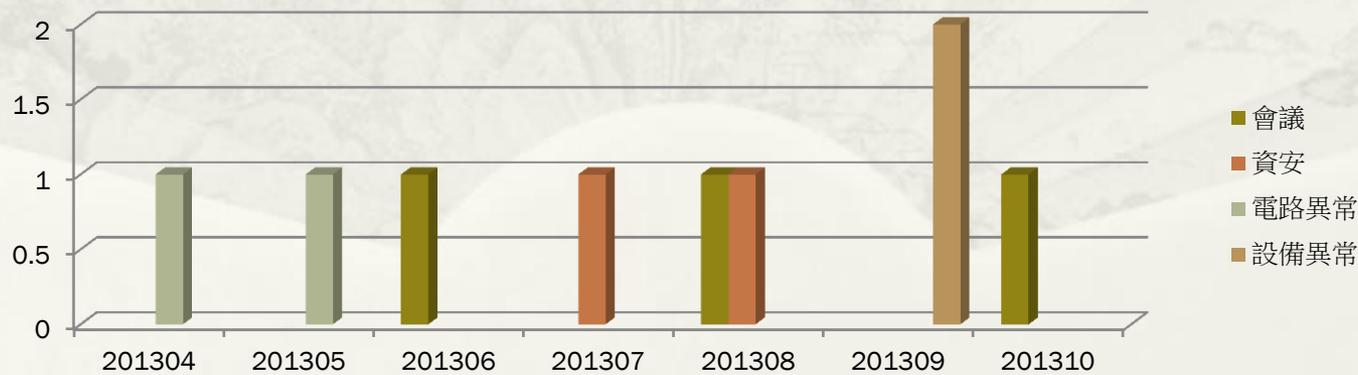
密碼:

[建立新帳戶](#)

為加強資料庫安全，連線密碼已使用 Hash Key 加密。

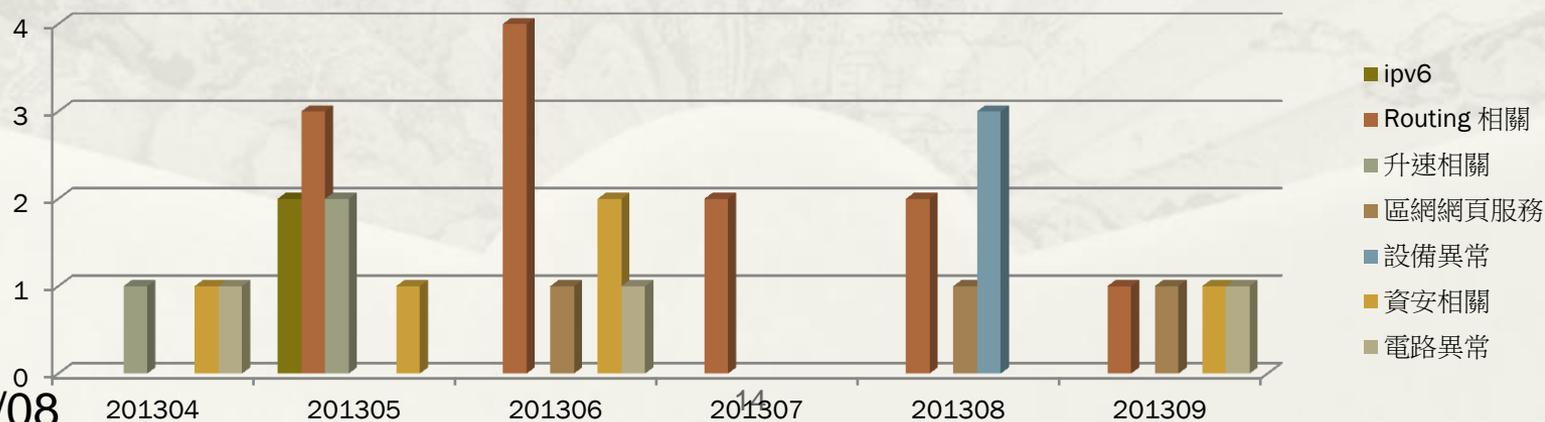
2013/04~2013/09 公告服務紀錄

月份	會議	資安	電路異常	設備異常	總計
201304			1		1
201305			1		1
201306	1				1
201307		1			1
201308	1	1			2
201309				2	2
201310	1				1
總計	3	2	2	2	9



2013/04~2013/09 咨詢服務紀錄

月份	ipv6	Routing相關	升速相關	網頁服務	設備異常	資安相關	電路異常	總計
201304			1			1	1	3
201305	2	3	2			1		8
201306		4		1		2	1	8
201307		2						2
201308		2		1	3			6
201309		1		1		1	1	4
總計	2	12	3	3	3	5	3	31



諮詢服務範例1

- * 2013/5/15 上午多所高中來電反應無法連線某些網站
- * 經查詢路由發現經過教育部之封包皆無法正常回來
- * 調查後發現新北市教育網使用BGP放出上述學校之網段，導致路由由台大區網送出，卻由政大區網經新北市教育網回來。
- * 詢問後原因在於教育部規劃新北市高中職未來電路將統一接回新北市教育網，不小心提前啟用該Router之設定，造成約二十多所高中職受影響。
- * 緊急移除設定後於 5/16 下午恢復正常

諮詢服務範例1 - 國外之 Traceroute 服務

* <http://centralops.net/co/Traceroute.aspx>

140.131.122.100 Traceroute results - Windows Internet Explorer

http://centralops.net/co/Traceroute.aspx

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

Traceroute Trace the path from this server to another

from **centralops.net** (Dallas, Texas, USA)

to

ip version auto require ipv6 require ipv4

don't resolve IP addresses

user: anonymous [140.112.3.82]
balance: 49 units
[log in](#) | [account info](#)

Central Ops.net

諮詢服務範例1 - 國外之 Traceroute 服務 (正常情況)

Tracing route to **140.131.122.100** [**140.131.122.100**]...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	0	0	0	208.101.16.73	208.101.16.73-static.reverse.softlayer.com
2	0	0	0	66.228.118.153	ae11.dar01.sr01.dal01.networklayer.com
3	0	0	0	173.192.18.254	ae14.bbr02.eq01.dal03.networklayer.com
4	0	0	0	173.192.18.208	ae7.bbr01.eq01.dal03.networklayer.com
5	33	33	33	173.192.18.141	ae0.bbr01.cs01.lax01.networklayer.com
6	30	30	30	173.192.18.167	ae7.bbr02.cs01.lax01.networklayer.com
7	38	88	39	173.192.18.150	ae0.bbr02.eq01.sjc02.networklayer.com
8	41	41	41	173.192.18.243	ae1.bbr01.eq01.pal01.networklayer.com
9	41	41	41	198.32.176.160	public-peering-twgate.net
10	178	164	178	175.41.60.5	5-60-41-175.twgate-ip.twgate.net
11	167	190	167	175.41.61.169	169-61-41-175.twgate-ip.twgate.net
12	165	165	165	175.41.61.46	46-61-41-175.twgate-ip.twgate.net
13	165	165	165	203.72.43.9	internet-moe-n-tanet.edu.tw
14	188	188	182	192.83.196.112	bb-ntu-twaren.tanet.edu.tw
15	170	171	171	192.192.7.182	
16	*	*	*		

-> 教育部
-> 台大區網

諮詢服務範例1 - 國外之 Traceroute 服務 (異常情況)

Tracing route to 140.131.122.100 [140.131.122.100]...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	1	1	1	70.84.211.97	61.d3.5446.static.theplanet.com
2	1	0	0	70.87.254.1	po101.dsr01.dllstx5.networklayer.com
3	0	0	1	70.85.127.105	po51.dsr01.dllstx3.networklayer.com
4	5	0	0	173.192.18.224	ae16.bbr01.eq01.dal03.networklayer.com
5	34	34	34	173.192.18.141	ae0.bbr01.cs01.lax01.networklayer.com
6	34	34	34	173.192.18.167	ae7.bbr02.cs01.lax01.networklayer.com
7	89	41	41	173.192.18.150	ae0.bbr02.eq01.sjc02.networklayer.com
8	39	40	40	173.192.18.243	ae1.bbr01.eq01.pal01.networklayer.com
9	42	42	59	198.32.176.160	public-peering-twgate.net
10	39	40	40	175.41.60.9	9-60-41-175.twgate-ip.twgate.net
11	168	168	167	175.41.60.13	13-60-41-175.twgate-ip.twgate.net
12	175	175	175	175.41.61.46	46-61-41-175.twgate-ip.twgate.net
13	184	184	184	203.72.43.9	internet-moe-n-tanet.edu.tw
14	169	168	169	192.83.196.119	bb-nccu-twaren.tanet.edu.tw
15	189	188	189	192.83.196.76	

- > 教育部
- > 政大區網
- > 新北市教育網

諮詢服務範例2

- * 2013/9/23 台北市教育網來電反映無法連到 www.amazon.co.jp
- * 懷疑因為此網站IP是54.240.252.0 而被阻擋

```
C:\Windows\System32>ping www.amazon.co.jp
```

```
Ping www.amazon.co.jp [54.240.252.0] <使用 32 位元組的資料>:
```

諮詢服務範例2

- ACL 阻擋

- * 發現連線學校界面上有如下 ACL:
 - * deny ip any 0.0.0.0 255.255.255.0
 - * 阻擋目的 IP: X.X.X.0 (0 結尾 ip)
 - * deny ip any 0.0.0.255 255.255.255.0
 - * 阻擋目的 IP: X.X.X.255 (255 結尾 ip)
- * IP 位址 X.X.X.0 或 X.X.X.255 結尾是否合法?

諮詢服務範例2

- ACL 阻擋

- * 將私有IP: 192.168.0.0/255.255.0.0
(192.168.0.0/16) 直接當成一個 ClassB
 - * 網路位址: :192.168.0.0
 - * 廣播位址: 192.168.255.255
 - * 因此下列位址可以被分配給主機
 - * 192.168.1.0、192.168.2.0 ...
 - * 192.168.1.255、192.168.2.255 ...
- * 將上述 ACL 刪除後，連線
www.amazon.co.jp 恢復正常

教育部資通安全通報演練計畫

畫

* 目的：

- * 檢驗「教育機構資安通報平台」所登錄單位資安聯絡人資料之正確性。
- * 檢驗各區縣網通報反應及處理能力與審核機制是否完善。
- * 測試學術機構分組資安聯絡人聯絡管道是否暢通。
- * 測試各單位於發現資安事件時，是否可正確、快速執行通報作業。
- * 測試通報網站、電子郵件、電話等各種通訊聯絡管道暢通與存活率。

教育部資通安全通報演練計畫

畫

* 演練時程：

- * 演練資料整備作業：自102年09月30日起至102年10月13日止
- * 資安通報演練作業：
 - * **第一梯次演練：102年10月14日至102年10月18日止。**
 - * **第二梯次演練：102年10月21日至102年10月25日止。**

教育部資通安全通報演練計畫

畫

* 整備項目：

* 教育機構資安通報平台帳號資料確認



* 教育機

資料確認

教育部資通安全通報演練計

畫

* 注意事項：

- * 本年度因進行OID帳號分割，各聯絡人需以各自帳號登入進行聯絡人資料確認及密碼更新作業。
- * 密碼更新於單位收到演練公文開始至演練結束期間，至少前二位連絡人需進行密碼變更，方算完成作業。
- * 建議使用高強度密碼，以大、小寫英文、數字、符號至少擇其二種組合成6碼以上之密碼。

教育部資通安全通報演練計

畫

* 演練方式：

- * 本次演練將以「**告知通報**」形式進行，教育部將於資安通報演練作業期間以**郵件**及**簡訊**傳送「資安事件通報單」。演練模擬事件通知簡訊及郵件上皆加註「**告知通報演練**」字樣，另事件單編號皆以「**DRILL**」開頭進行編碼。
- * 系統將以教育部模擬之**10**種情境樣本以亂數方式於演練期間分別發送至所有學術單位，執行演練單位於收到**mail**及簡訊通知後，應於**1小時**內至教育機構資安通報演練平台完成事件通報流程，並依事件等級於處理時限內完成事件應變處理並結案。
演練平台網址：<https://drill.cert.tanet.edu.tw>

教育部資通安全通報演練計畫

畫

* 範例說明：

發佈編號	NTUSOC-INT-201302-XXXX	發佈時間	2013-02-XX 12:57:49
事件類型	系統被入侵	發現時間	2013-02-XX 15:23:00
事件主旨	教育部資安事件通告—00 國民小學[XXX.XXX.XXX.XXX]主機疑似中毒警訊通知		
事件描述	本中心研判來源主機疑似感染病毒，並對目標主機進行可疑連線。請針對該來源 IP 執行程式內容與系統安全狀態檢測，並恢復系統正常運作狀態，來降低受駭範圍。入侵偵測系統偵測到使用者主機 (XXX.XXX.XXX.XXX) 可能感染電腦病毒，嘗試傳送惡意封包攻擊目標 IP (多個目標 IP)。		
手法研判	無		
處理建議	更新防毒軟體的病毒碼或安裝相關修正檔，或關閉不使用的應用軟體與通信埠以及定期執行弱點掃描程式。利用資安網站所提供的自動檢查及移除程式來檢查電腦所感染到的蠕蟲病毒。建議用戶收到未經授權的來源 IP 存取，可在防火牆上阻擋外部 IP 來存取主機。請用戶留意主機有無異常動作。(如：新增帳號、開啟不明 Port、或執行不明程式) 若目標 IP 用戶皆無上述問題，則請用戶多注意來源 IP 將可能發動攻擊。時常查閱網路上著名資安網站所公佈相關訊息。		
參考資料	無		

教育部資通安全通報演練計畫

畫

* 範例說明(cont.) :

各機關因受外在因素所產生資通安全事件時通報事項：

以下表單各欄位若為紅色◎標示，則為必填欄位。
欄位中不得輸入特殊符號，例如：「;」、「"」、「'」、「\$」、「&」、「%」、「!」、「^」、「*」、「<」、「>」、「_」、「|」、「-」。

1. 通報型態： 告知通報

2. 事件發生時間：

◎IP 位置 (IP address) : 此欄位填入被通報之 IP
範例: 120.114.2

◎網際網路位置 (web-url) :
範例: <https://www.xxx.edu.tw/cba.index>

教育部資通安全通報演練計畫

畫

* 範例說明(cont.) :

◎作業系統(名稱/版本):	<input type="text"/>	此欄位填入該主機作業系統 若尚無法得知可寫“待確認”
		範例 1: Centos Linux 5
		範例 2: Windows XP SP2
◎受駭應用軟體(名稱/版本):	<input type="text"/>	範例: <u>sendmail</u> server, 此為不確定版本的範例
◎已裝置之安全防護軟體:	<input type="text"/>	
防毒軟體(名稱/版本):	<input type="text"/>	範例: Avira 10.0.0.561

教育部資通安全通報演練計畫

畫

* 範例說明(cont.) :

其它 (名稱/版本):

4. 資通安全事件：基本資料 選擇此事件單之類別

事件分類 :

- INT (入侵攻擊) :
 - 系統被入侵(資訊設備遭惡意使用者入侵) ↓
 - 對外攻擊(對外部主機進行攻擊行為) ↓
 - 針對性攻擊(針對特定個人的資訊洩漏與身分盜取) ↓
 - 散播惡意程式(主機對外進行惡意程式散播) ↓

教育部資通安全通報演練計畫

畫

* 範例說明(cont.) :

◎破壞程度：↵	(文字勿超過 200 中文字，標點符號請用全形)↵	
造成的破壞程度形容↵ 若尚未確定可寫“待確認”↵		
◎事件說明：↵	可直接複製事件主旨↵ EX：“主機疑似中毒”↵	中文字，標點符號請用全形)↵

教育部資通安全通報演練計畫

畫

* 範例說明(cont.) :

5. 資通安全事件：影響等級及說明

1. 事件等級：取底下三個欄位中最高等級當成最後之事件等級
2. 第 3、4 級事件係屬於重大資安事件，教育部各長官需親自督導進度
3. 若有 3、4 級事件，請立刻電話告知您所屬的主管機關
4. 如果您無法確定如何填寫時，請電話連絡您所屬的主管機關請求協助
5. 等級 0 之資安事件教育部另有規範，請至少填入等級 1

◎資安事件判斷：

若無特別事件皆為一級事件

(1) 機密性衝擊



1 級-非核心業務資料遭洩漏

教育部資通安全通報演練計畫

畫

* 範例說明(cont.) :

◎可能影響範圍及損失評估 (文字勿超過 200 字，標點符號請用全形)

若尚無法評估可寫“待評估”

教育部資通安全通報演練計

畫

* 範例說明(cont.) :

7. 是否同時進行通報流程與應變流程?

是 ↓

(請繼續完成 II.應變流程之作業)↵

否 ↓

(會先完成 I.通報流程 並結束，後續時間請儘快完成 II.應變流程)↵

應變流程↵

1. 緊急應變措施↵

已中斷網路連線，待處理完成後再上線 ↓

已停止伺服器之服務，待處理完成後再上線 ↓

教育部資通安全通報演練計畫

畫

* 評分標準：

各區（縣）網路中心評分標準說明

給分標準	1	0
評分項目		
密碼更新率	達80%	未達80%
通報完成率	所轄連線單位於24小時內完成通報的比率達80%	所轄連線單位於24小時內完成通報的比率未達80%
審核及時率	所轄連線單位事件單審核作業於時限內完成率達70%以上但未達80%	所轄連線單位事件單審核作業於時限內完成率未達70%

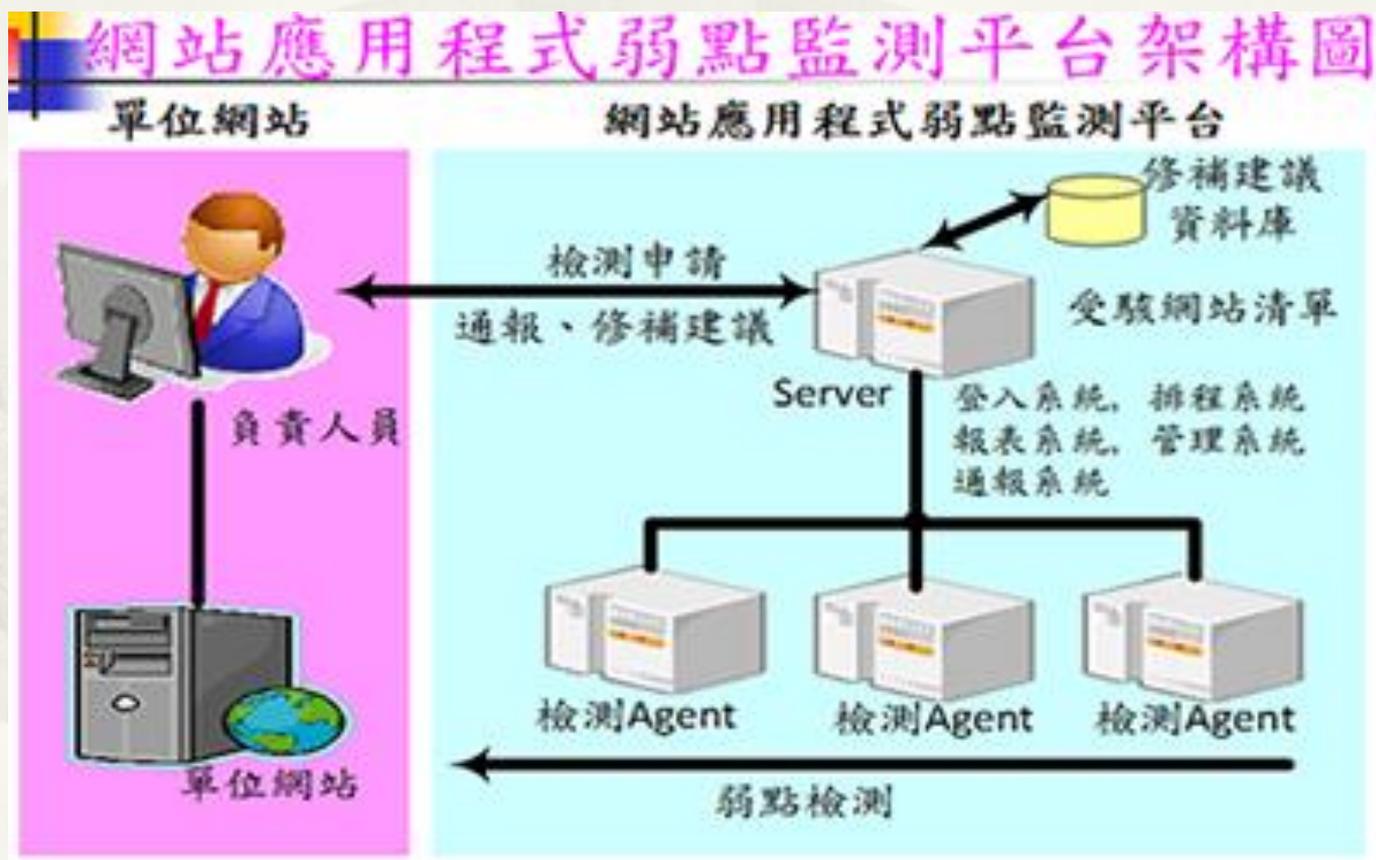
教育部資通安全通報演練計畫

畫

* 評分標準(cont.) :

各機構及學校評分標準說明			
給分標準	2	1	0
評分項目			
通報及時率	4小時內完成	24小時內完成	24小時內未完成
應變及時率	時限內完成	(時限+4小時)內完成	未於(時限+4小時)內完成
資料正確率	2位以上資安聯絡人所有欄位資料填寫完整	填寫2位以上資安聯絡人，但僅一位資安聯絡人所有欄位資料填寫完整	1.未填寫資安聯絡人 2.資安聯絡人資料資料均不完整

弱點監測平台架構圖



弱點監測平台特色

目前位置：網站排程

- 前次設定排程時間：2010/11/9 下午 05:25:19
- 排程間隔時間：0 小時
- 同時線上可排程數：10
- 目前線上排程數：0 (包含等待中、執行中、輕負運送中)
- 剩餘可排程數：10
- 剩餘可排程數：10

網站排程

檢測網址

檢測類別

- XSS檢測 [不使用POST檢測]
- SQL Injection檢測 [不使用POST檢測]
- 惡意檔案執行檢測
- 不適當配置處理檢測
- 目錄索引檢測
- 備份檔案檢測

排程選擇：

檢測服務時間

- 檢測時段
- 日間 (06:00~18:00)
- 夜間 (18:00~06:00)

▶ 從首頁登入設定-開啟

設定已中斷排程

檢測網址

排程選擇：

檢測服務時間

- 檢測時段
- 日間 (06:00~18:00)
- 夜間 (18:00~06:00)

取消排程

檢測網址

可取消大於2天後的排程

相關連結

- [網站排程](#)
- [網站維護](#)
- [網站結果](#)
- [修補建議查詢](#)
- [列印檢測同意書](#)

最新消息
關於系統
下載專區
問 & 答
網站維護
網站排程
網站結果
修補建議查詢
列印檢測同意書

重建阿 您好
[退出][修改]

網頁弱點掃描應用程式弱點監測平台-成大資通安全研究中心營運組 - Google 瀏覽器

www.tw.ac.edu.tw/bscc/azp

<<Pre 2010 年 11 月 Next>>

日	一	二	三	四	五	六
	1 過期 過期	2 過期 過期	3 過期 過期	4 過期 過期	5 過期 過期	6 過期 過期
7 過期 過期	8 過期 過期	9 過期 過期	10 過期 過期	11 過期 過期	12 過期 過期	13 過期 過期
14 過期 過期	15 日間 夜間	16 日間 夜間	17 日間 夜間	18 日間 夜間	19 日間 夜間	20 日間 夜間
21 日間 夜間	22 日間 夜間	23 日間 夜間	24 日間 夜間	25 日間 夜間	26 日間 夜間	27 日間 夜間
28 日間 夜間	29 日間 夜間	30 日間 夜間				

*檢測時段說明：
1 日間：當日早上06:00~當日18:00
2 夜間：當日下午18:00~隔日06:00

防洩漏個資掃描平台簡介

- * 協助教育單位評估可能洩漏個資的風險
- * 針對網站開放性區域
- * 提供個資洩漏風險分析報告

防洩漏個資掃描平台特色

檢測關鍵字

系統資訊
1. 關鍵字區分自訂與系統預設，使用者可自定關鍵字加強檢測結果。

自訂

自訂	建立時間	功能
自訂		
系統預設		
清單	2011-07-23	—
身份證字號	2011-05-16	—
行動電話	2011-05-16	—
關鍵字	2011-05-06	—

第一頁 | 上一頁 | 1 | 下一頁 | 最後一頁 | 1/1

防洩漏個資掃描平台特色

(cont.)

結果功能：

忽略功能：

忽略功能說明：

- 套用：隱藏該網站之前設定為忽略的結果資料。
- 還原：還原套用忽略後，所隱藏的結果資料。
- 刪除：刪除該網站之前設定為忽略的所有結果資料，需重新設定忽略結果資料。

總檢測個資比例圖

類別	百分比
無個資	85.3%
含個資	14.7%

風險比例圖

風險等級	百分比
高風險	~3%
中風險	~3%
低風險	96.1%

) 疑似洩漏個人資料清單										
來源	連結	身份證	信用卡	室內電話	手機號碼	地址	關鍵字	email	風險	功能
google		0	0	0	0	40	0	0	高	<input type="button" value="忽略"/>
google		0	0	100	0	40	0	0	高	<input type="button" value="忽略"/>
spider		0	0	0	0	40	0	0	高	<input type="button" value="忽略"/>



問題與討論
