臺灣學術網路 電腦危機處理中心

資安通報平台簡介
及
通報應變說明

講師：張明達

TAIWAN ACADEMIC NETWORK COMPUTER EMERGENCY RESPONSE TEAM

臺灣學術網路
電腦危機處理中心
TACERT

Tel: 07-5250211 Fax: 07-5250212
VoIP代表號：98400000
service@cert.tanet.edu.tw
804高雄市鼓山區蓮海路70號

cert.tanet.edu.tw
TACERT

課程大綱

- TACERT中心簡介
- 教育機構資安通報流程簡介
- 事件單種類及通報簡介
- 學術網路資安事件統計
- 平台功能介紹
- Q & A

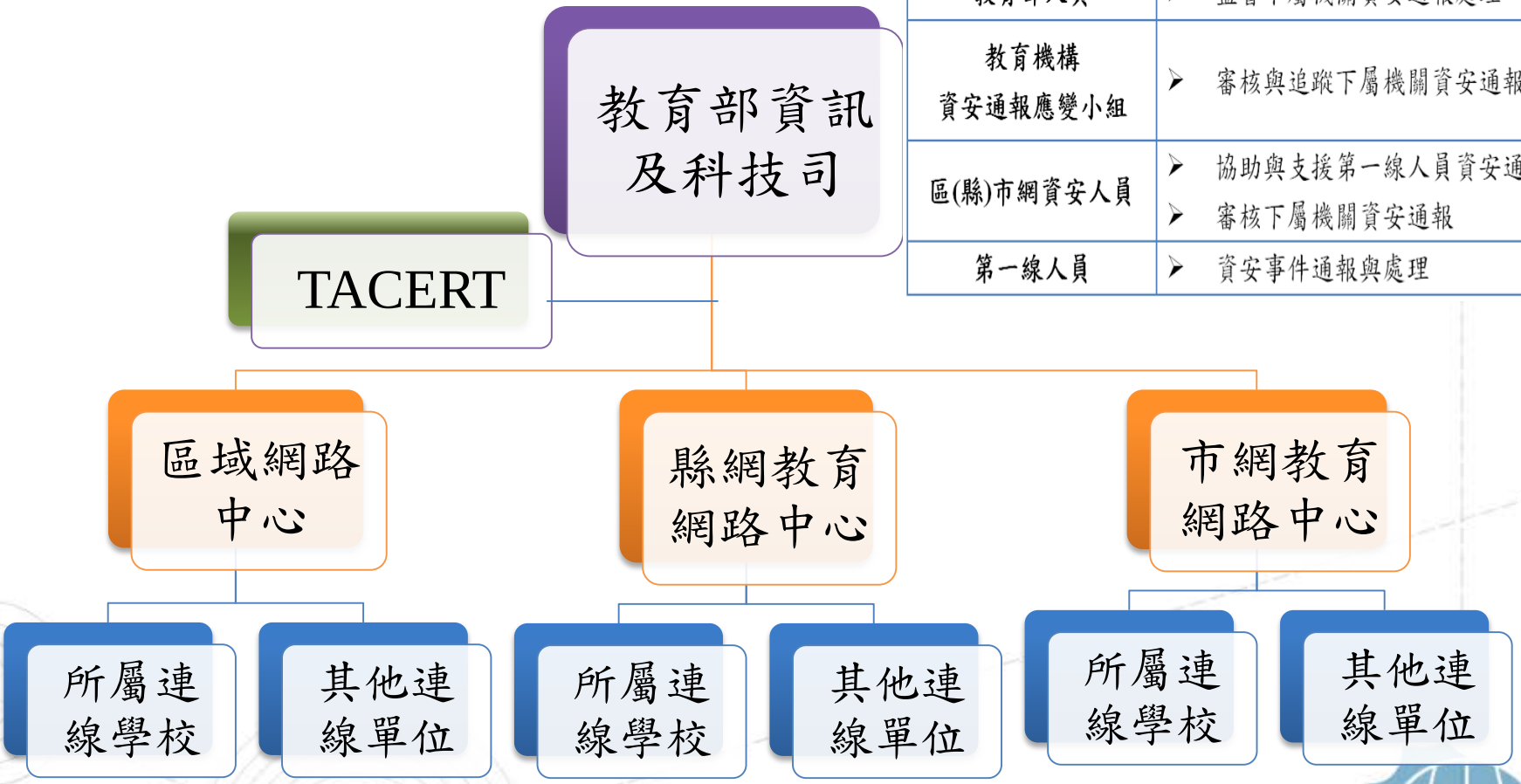
TACERT中心簡介

臺灣學術網路危機處理中心(TACERT)成立緣起

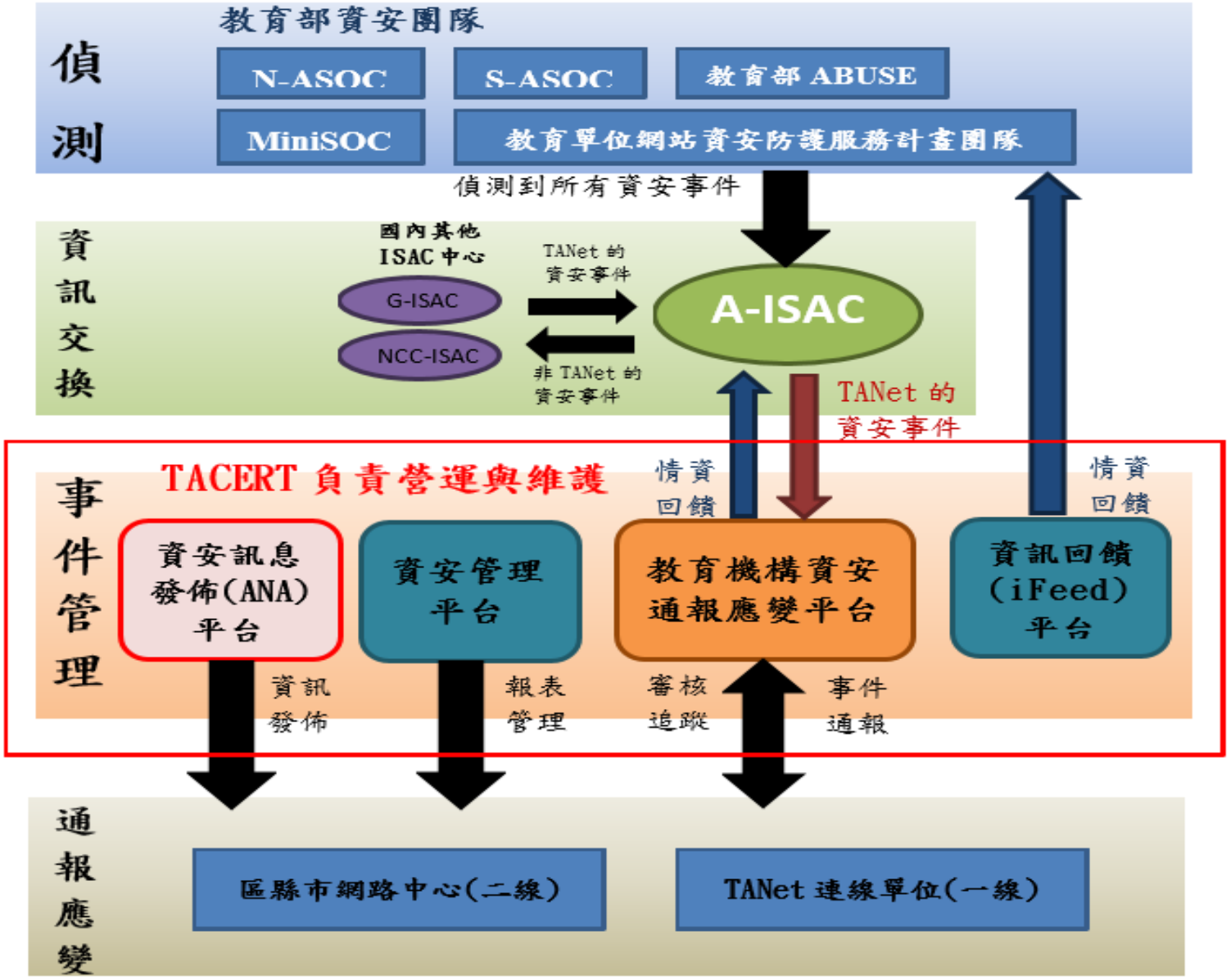
- 學術網路近年來成為臺灣網路攻擊的主要目標之一
- 面對層出不窮、日新月異的網路攻擊事件，需要有一個共同平台進行資安事件通報及應變
- 故教育部資訊及科技教育司(原教育部電算中心)成立***臺灣學術網路危機處理中心***(Taiwan Academic Network Computer Emergency Response Team)，簡稱**TACERT**，並委由國立中山大學營運。
- 臺灣學術網路危機處理中心將致力於強化學術網路資通安全的防護力，形成臺灣網路資安防護網重要的一環。

TACERT組織架構

使用角色	工作事項
教育部人員	➢ 監督下屬機關資安通報處理
教育機構 資安通報應變小組	➢ 審核與追蹤下屬機關資安通報
區(縣)市網資安人員	➢ 協助與支援第一線人員資安通報 ➢ 審核下屬機關資安通報
第一線人員	➢ 資安事件通報與處理



教育機構資安通報機制運作



TACERT具體營運目標

- 一、教育機構通報應變平台維運
- 二、資安預警情資管理
- 三、資安通報演練
- 四、資安事件諮詢與技術支援
- 五、資安防護教育訓練
- 六、國內資安組織合作
- 七、提升資訊安全研究能量
- 八、資安事件分析

資安事件階段處理目標

事前預防

- 資安預警情資
- 提供資安訊息、資安新知
- 辦理資安防護教育訓練

事發控制

- 自動化的通報應變平台
- 完整的資安通報流程機制
- 即時資安諮詢服務

事終檢討

- 資安事件分析報告
- 資安事件處理教材
- 加強安全性與防護設定

教育機構資安通報流程簡介

通報應變規劃重點

1.為使通報應變流程更有效掌握，通報應變平台之流程 畫分為**通報流程**與**應變流程**。

2.第一線人員由於處理時間的限制，可先進行通報流程，待完成處理後再進行應變流程。

3.請各單位盡可能通報與應變同時進行。

4.所有通報應變流程之通報，都必須審核過後才是(教育部規範)正式結束通報流程。

如此規劃著眼於不同層級之資安人員可充分掌握所發生之資安事件，並能依輕重等級啟動不同對應之處理機制。

依資安等級區分

1、2級資安事件

- 事件處理時間通報於**24小時**內完成，應變於**72小時**內完成(通報+應變)
- 電子郵件通知寄發
  - 事件單成立後1個小時
  - 事件單成立後每隔12個小時
  - 事件單成立後72小時後每隔12個小時寄發逾時通知

3、4級資安事件

- 針對政府或國家等級之攻擊行為或其他重大資訊安全事件。
- 事件處理時間為**36小時**內完成
- 需和上級管理單位報備且建立連絡並指定相關人員待命追蹤處理狀況
- 電子郵件通知寄發
  - 事件單成立後1個小時
  - 事件單成立後每隔12個小時
  - 事件單成立後36小時後每隔12個小時寄發逾時通知

事件單處理流程

事件發生

- 產生通知：
  -新進告知通報通知
  (簡訊+MAIL)

通報處理

- 處理時效：
  -通報**24小時**
  -應變**72小時**
- 產生通知：
  -通報應變相關通知
  -待審核通知
  (MAIL)

事件審核

- 審校時效：
  於通報完成後**8小時**內
- 產生通知：
  -審核相關通知
  (MAIL)

事件結案

- TACERT覆核完畢後事件結案進入歷史工單
- 產生通知：
  -結案通知
  (MAIL)

事件單種類及通報簡介

告知通報事件單(INT&DEF)

教育機構資安通報平台

事件類型:入侵事件警訊

工單編號:AISAC-166

發單單位-事件類別-年度月份-流水編號

原發布編號	ICST-INT-201010-0023	原發布時間	2010-10-0801:51:30
事件類型	對外攻擊	原發現時間	2010-10-08
事件主旨	140.　.218.　資訊設備對外攻擊警訊通知		
事件描述	技術服務中心發現 貴單位註冊 IP 140.　.218.　於 2010/10/07 16:54 ~ 16:55 左右對外進行攻擊行為。 該電腦嘗試透過 TCP Port 135與445攻擊微軟MS08-067相關弱點。 為避免不必要之資安風險，請針對該系統進行詳細檢查並加強相關防範措施。		
手法研判	MS08-067		
建議措施	回復措施： 1.檢查該系統上是否有不明程式正大量對外建立網路連線(可能但不限於TCP Port 135與445)，若有則停止該程式並刪除系統上該不明程式檔案。 2.由於所得資訊有限，無法提供較明確之回復措施，請依該系統平台參考相關檢查暨回復措施。 3.對於此次攻擊行為，技術服務中心無法經由外部確認是否已完成相關回復措施。 相關建議： 1.檢查防火牆記錄，查看內部是否有對外大量不同目的 IP 之異常連線，特別注意但不限於 TCP Port 135與445。 2.檢查個別系統上是否有異常連線、異常執行中程序、異常服務及異常開機自動執行程式等。 3.注意個別系統之安全修補，若僅移除惡意程式而不修補，再次受相同或類似攻擊的機率極高。修補程式須持續更新，自動安裝更新程式機制可參考微軟保護電腦三步驟。 4.系統上所有帳號需設定強健的密碼，非必要使用的帳號請將其刪除。 5.安裝防毒軟體並更新至最新病毒碼。 6.檢驗防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠。 7.若無防火牆可考慮安裝防火牆或於 Windows 平台使用 Windows XP/2003 內建之 Internet Firewall/Windows Firewall或 Windows 2000 之 TCP/IP 篩選。Linux 平台可考慮使用 iptables 等內建防火牆。		
參考資料	微軟資訊安全錦囊 http://www.microsoft.com/taiwan/security/protect/ 微軟內建防火牆: http://www.microsoft.com/taiwan/security/protect/firewall.asp http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx http://www.microsoft.com/windowsxp/using/networking/learnmore/icf.mspx 微軟相關弱點 http://www.microsoft.com/technet/security/current.aspx(英文-更新較快) http://www.microsoft.com/taiwan/security/bulletins/default.asp(中文-更新較慢) http://www.microsoft.com/taiwan/technet/security/bulletin/ms08-067.mspx http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx		
此事件需要進行通報，請 貴單位資安聯絡人登入資安通報應變平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

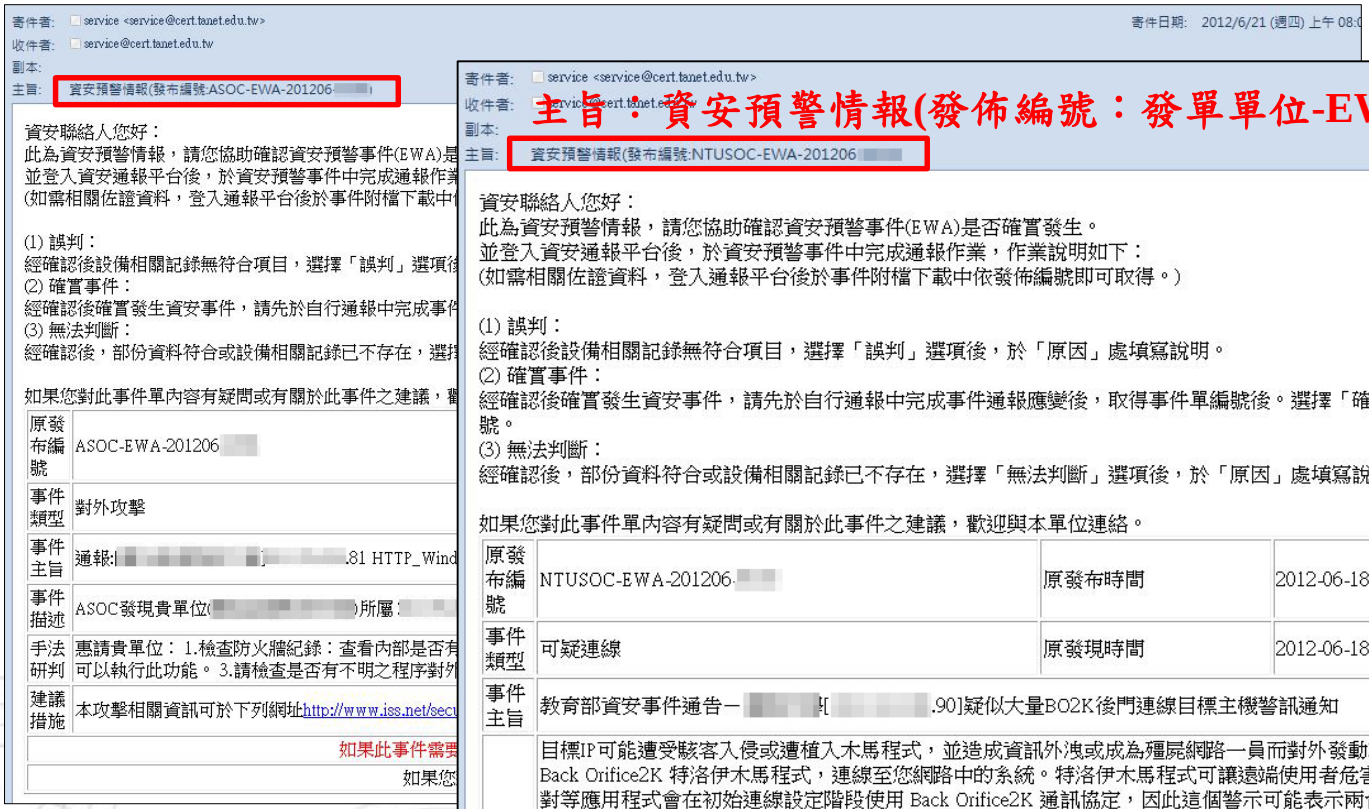
◎標示為必填欄位

通報流程：
填寫受害主機設備的基本資訊、事件分類、等級判斷與損害程度的資訊

應變流程：
填寫單位緊急應變措施、解決辦法與解決時間。

預警情報事件單(EWA)

*資安預警情報只派發MAIL通知，不派發簡訊通知



寄件者: service <service@cert.tanet.edu.tw>
收件者: service@cert.tanet.edu.tw
副本:
主旨: 資安預警情報(發布編號:ASOC-EWA-201206[redacted])
寄件日期: 2012/6/21 (週四) 上午 08:0

資安聯絡人您好：
此為資安預警情報，請您協助確認資安預警事件(EWA)是
並登入資安通報平台後，於資安預警事件中完成通報作業
(如需相關佐證資料，登入通報平台後於事件附檔下載中

(1) 誤判：
經確認後設備相關記錄無符合項目，選擇「誤判」選項後
(2) 確實事件：
經確認後確實發生資安事件，請先於自行通報中完成事件
(3) 無法判斷：
經確認後，部份資料符合或設備相關記錄已不存在，選擇

如果您對此事件單內容有疑問或有關於此事件之建議，

原發布編號	ASOC-EWA-201206[redacted]
事件類型	對外攻擊
事件主旨	通報:[redacted].81 HTTP_Wind
事件描述	ASOC發現貴單位([redacted])所屬[redacted]
手法研判	惠請貴單位： 1.檢查防火牆紀錄：查看內部是否有可以執行此功能。 3.請檢查是否有不明之程序對外
建議措施	本攻擊相關資訊可於下列網址http://www.iss.net/secu

如果此事件需要
如果您

寄件者: service <service@cert.tanet.edu.tw>
收件者: [redacted]
副本:
主旨: 資安預警情報(發布編號:NTUSOC-EWA-201206[redacted])
寄件日期: 2012/6/18 (週一) 上午 0

主旨：資安預警情報(發佈編號：發單單位-EWA-年度月份-EWA編號

資安聯絡人您好：
此為資安預警情報，請您協助確認資安預警事件(EWA)是否確實發生。
並登入資安通報平台後，於資安預警事件中完成通報作業，作業說明如下：
(如需相關佐證資料，登入通報平台後於事件附檔下載中依發佈編號即可取得。)

(1) 誤判：
經確認後設備相關記錄無符合項目，選擇「誤判」選項後，於「原因」處填寫說明。
(2) 確實事件：
經確認後確實發生資安事件，請先於自行通報中完成事件通報應變後，取得事件單編號後。選擇「確實事件」選項後，於右側填入自行通報事件單編號。
(3) 無法判斷：
經確認後，部份資料符合或設備相關記錄已不存在，選擇「無法判斷」選項後，於「原因」處填寫說明。

如果您對此事件單內容有疑問或有關於此事件之建議，歡迎與本單位連絡。

原發布編號	NTUSOC-EWA-201206[redacted]	原發布時間	2012-06-18 07:33:09
事件類型	可疑連線	原發現時間	2012-06-18 07:19:00
事件主旨	教育部資安事件通告－[redacted].90]疑似大量BO2K後門連線目標主機警訊通知		
事件描述	目標IP可能遭受駭客入侵或遭植入木馬程式，並造成資訊外洩或成為殭屍網路一員而對外發動攻擊。 這個警示表示，有遠端使用者正嘗試使用 Back Orifice2K 特洛伊木馬程式，連線至您網路中的系統。特洛伊木馬程式可讓遠端使用者危害被安裝特洛伊木馬伺服器的系統。 此外，一些對等應用程式會在初始連線設定階段使用 Back Orifice2K 通訊協定，因此這個警示可能表示兩台電腦間的對等通訊。 入侵偵測防禦系統偵測到大量來源IP，啟用包含木馬後門特徵之封包，對目標IP（[redacted].90）目標 PORT （2015）進行連線。 感染 Back Orifice 特洛伊木馬，會讓遠端攻擊者取得對系統未經授權的存取。這類型的攻擊可能導致系統關機、記錄鍵盤輸入，以及允許無用的檢視/關閉程序。Back Orifice2K 特洛伊木馬可能也會允許遠端使用者，藉由重新設定系統及重新導向流量，來危害您的網路。 此外，請調查舉證報告中的封包記錄，以判斷目標主機是否正在執行對等應用程式。 ●影響的平台： 套裝軟體 Microsoft Windows 2000 Microsoft Windows NT Microsoft Windows 98 Microsoft Windows 95 Microsoft Windows Me		
手法研判	建議解決方案: - 若目標IP該連線行為已得到授權，則請忽略此訊息。 - 若目標IP該連線為異常行為，可先利用掃毒軟體進行全系統掃描，並利用ACL暫時阻擋該可疑IP。同時建議管理者進行以下檢查： a.請查看目標IP有無異常動作(如：新增帳號、開啟不明Port、執行不明程式)。 b.確認防毒軟體的病毒碼已更新為最新版本、系統已安裝相關修正檔，或關閉不使用的應用軟體與相關通訊埠。 部署防毒掃描程式來掃描您的系統是否具有此種病毒。請使用可移除受感染檔案的掃描程式。 視您的安全性政策而定，您可能想要求使用者從網路中的電腦上解除安裝對等應用程式。		

資安預警情報

- 資安預警情報(EWA)為教育部各資安計畫團隊或是其他情資來源單位，偵測到**疑似網路攻擊行為**時所發送的預警通知。
- **由一線單位進行檢查、處理及填報作業，區縣市網路中心進行追蹤作業**
- 連線單位收到資安預警通知時，請檢查該主機是否有異常網路活動跡象，並進行處理狀態回覆：
  - 確實事件：先於通報平台採**『自行通報』**取得事件單編號
  - **誤報：請詳填原因 (以利發單單位調校規則)**
  - 無法判斷：證據不足
- 處理時效：一星期內

資安預警情報回報方式

EWA事件單

事件編號	ASOC-EWA-201206
單位名稱	
填表時間	2012-06-21 08:02:46
發佈時間	2012-06-21 02:09:50
發生時間	2012-06-21 01:28:49
受害IP	.135
受害網址	
事件等級	low
事件分類	
主旨	通報 .135 Stacheldraht_Agent
說明	ASOC發現貴單位)所屬 .135 疑似對外進行 Stacheldraht_Agent 攻擊
手法研判	Stacheldraht 是基於 Tribe FloodNet (TFN) 工具的「分散式拒絕服務」(DDoS) 攻擊工具，係以 Tribe FloodNet (TFN) 工具為基礎。它結合了 Trin00 (AKA trinoo) 的功能與 TFN 的功能，並針對這些功能
應變措施	惠請貴單位： 1.確認內部主機是否有不明程式或網路路由問題造成此攻擊行為。 2.利用工具程式(如:TCPview、procexp)於來源主機觀
參考資訊	本攻擊相關資訊可於下列網址 http://www.iss.net/security_center/reference/vuln/Stacheldraht_Agent.htm內查詢

EWA事件單狀態

○ 誤判		
◉ 確實事件	事件單編號	
○ 無法判斷		
原因		

送出

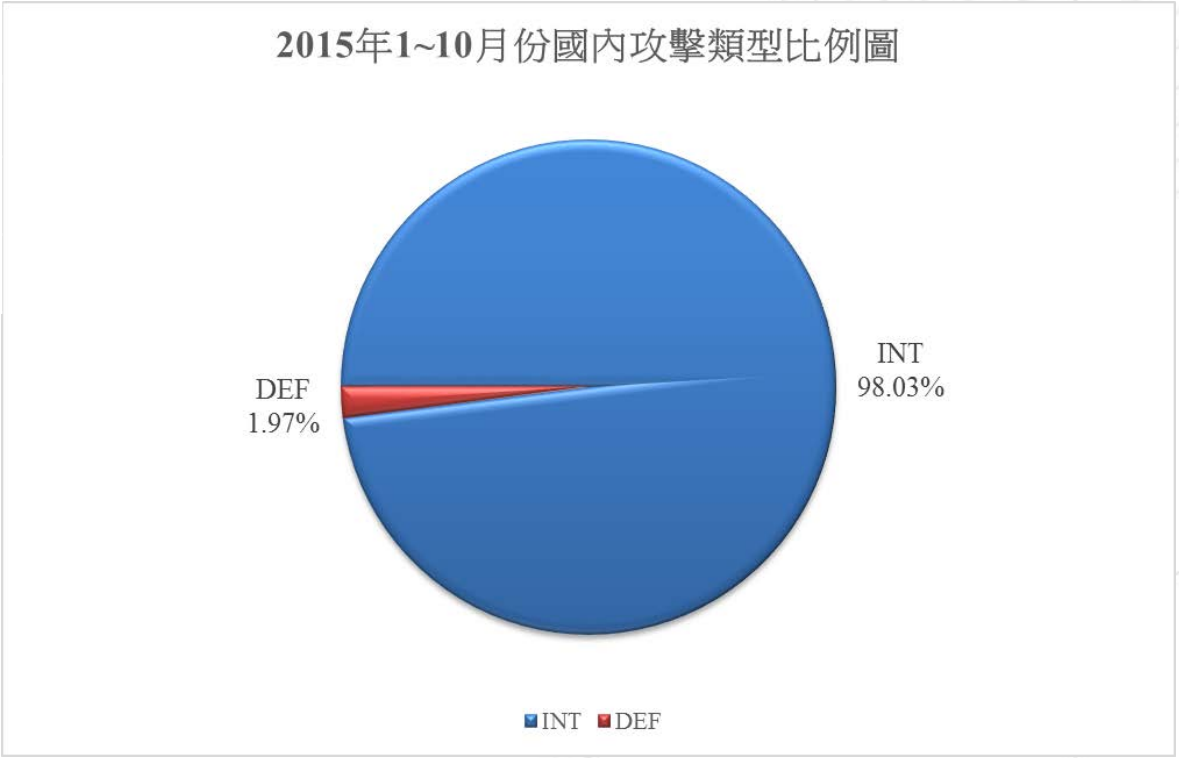
完整資安預警(EWA)事件單訊息

回報資安預警(EWA)事件單的處理狀況

學術網路資安事件統計

學術網路資安事件類型比例

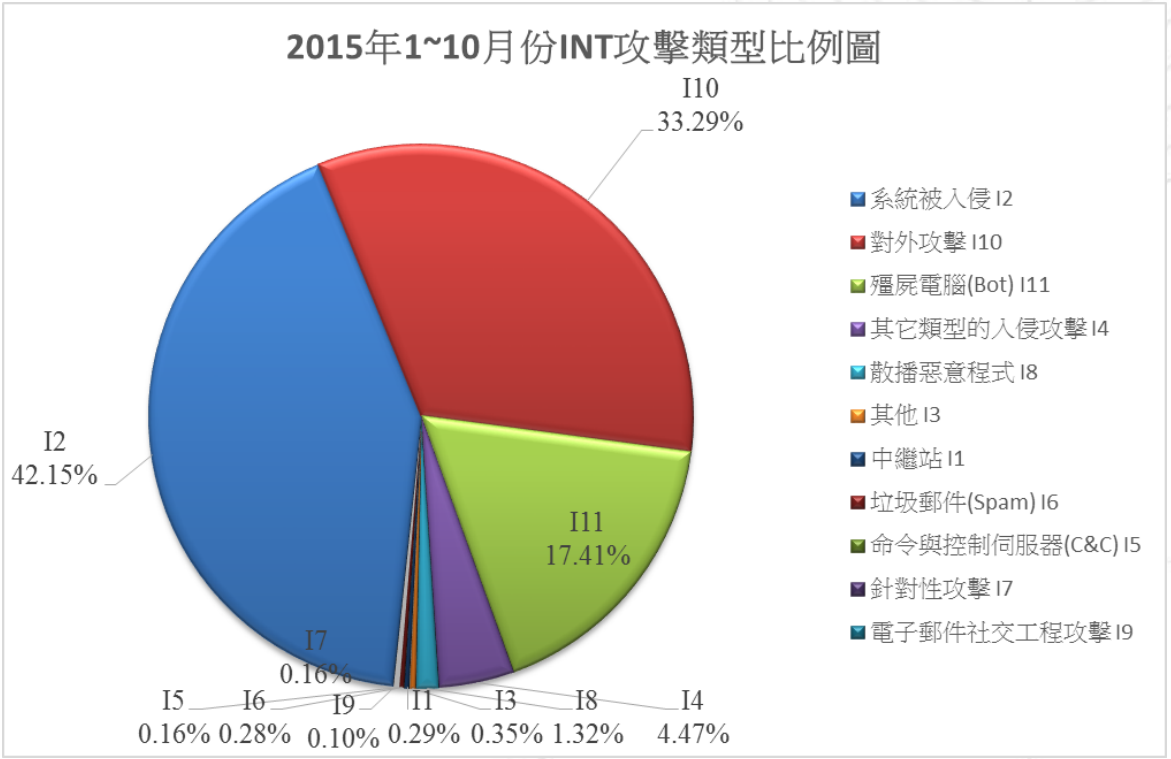
事件類別	數量
INT	17,839
DEF	359
總計	18,198



- 統計時間：104年1月至104年10月
- 資料來源：教育機構資安通報平台

學術網路資安事件INT子類型比例

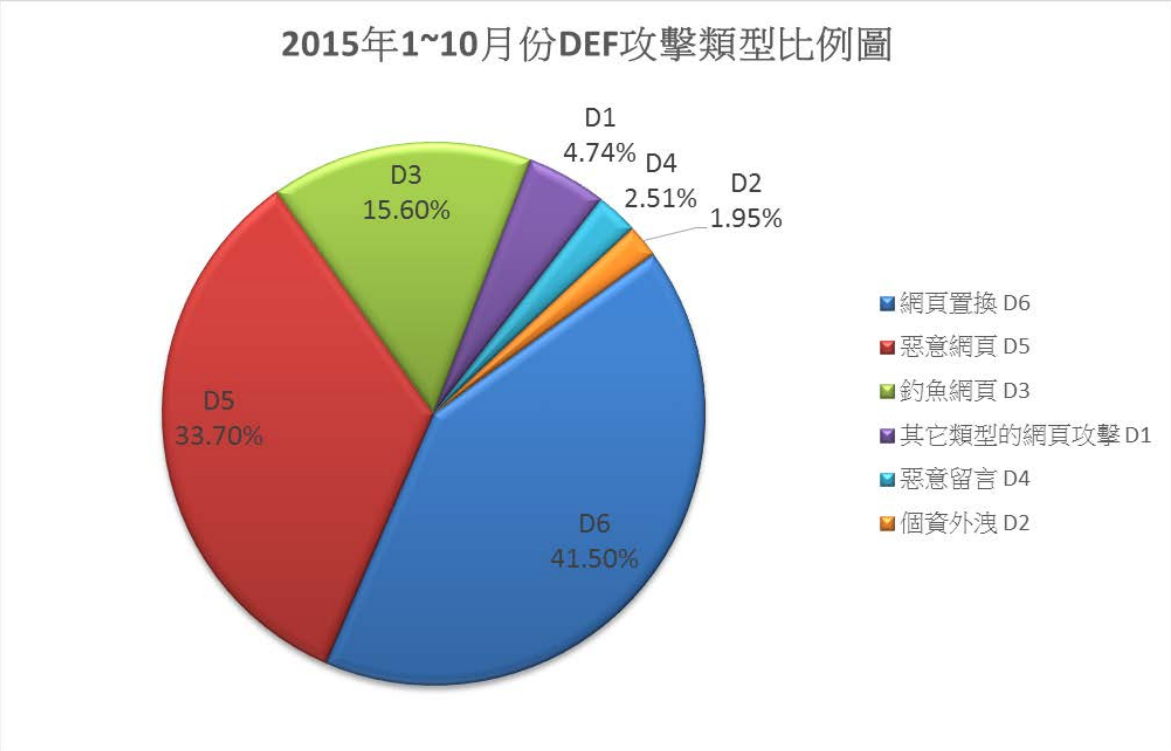
事件子類別	數量
系統被入侵	7,520
對外攻擊	5,939
殭屍電腦(BOT)	3,106
其它類型的入侵攻擊	798
散播惡意程式	236
其他	63
中繼站	52
垃圾郵件(SPAM)	50
命令與控制伺服器(C&C)	29
針對性攻擊	28
電子郵件社交工程攻擊	18
總計	**17,839**



- 統計時間：104年1月至104年10月
- 資料來源：教育機構資安通報平台

學術網路資安事件DEF子類型比例

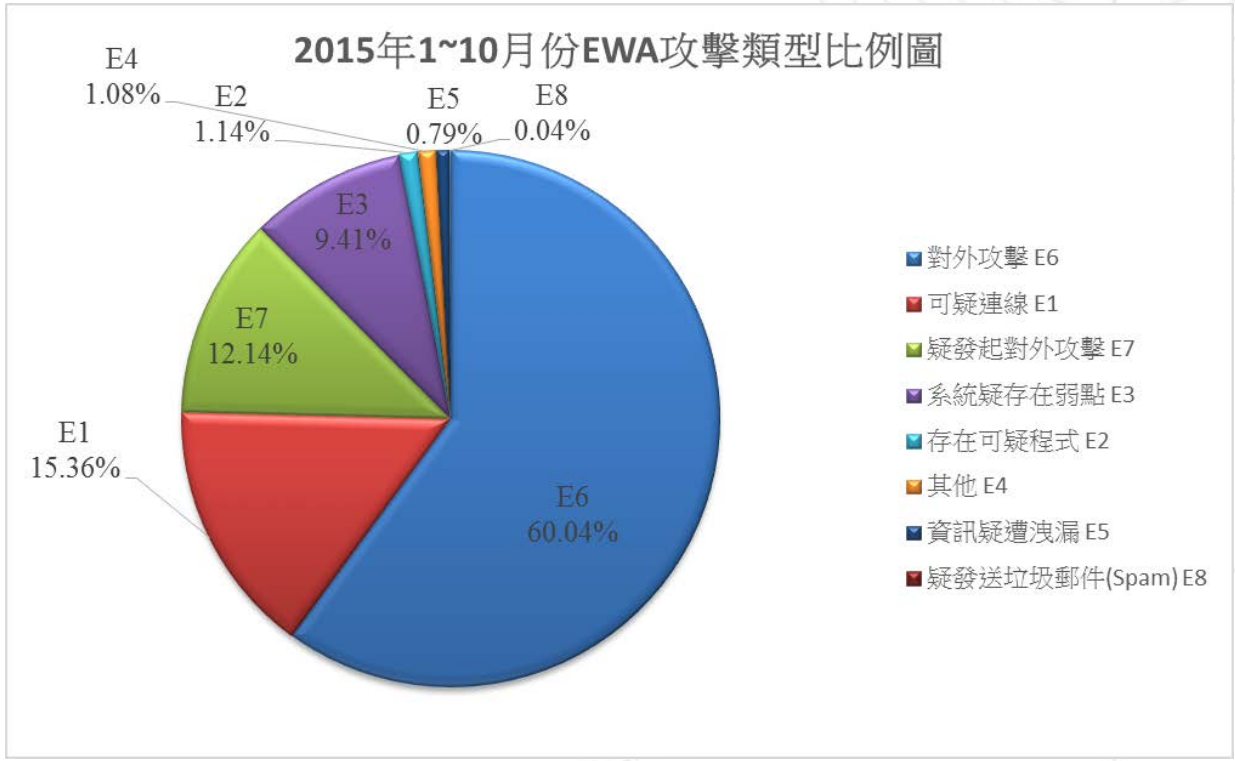
事件子類別	數量
網頁置換	149
惡意網頁	121
釣魚網頁	56
其它類型的網頁攻擊	17
惡意留言	9
個資外洩	7
總計	359



- 統計時間：104年1月至104年10月
- 資料來源：教育機構資安通報平台

學術網路資安預警事件EWA子類型比例

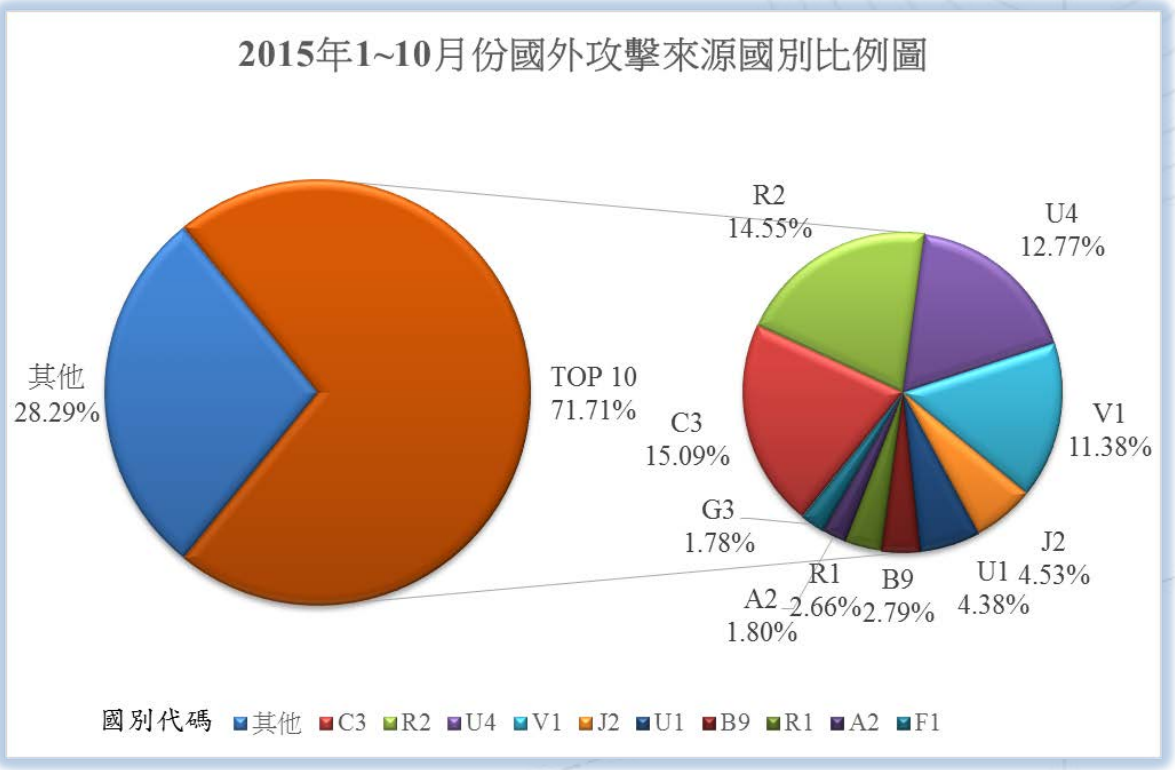
事件子類別	數量
對外攻擊	4,708
可疑連線	1,204
疑發起對外攻擊	952
系統疑存在弱點	738
存在可疑程式	89
其他	85
資訊疑遭洩漏	62
疑發送垃圾郵件(SPAM)	3
總計	**7,841**



- 統計時間：104年1月至104年10月
- 資料來源：教育機構資安通報平台

國外惡意威脅來源國別比例

國家	攻擊IP數量
China(C3)	806
Russian Federation(R2)	777
United States(U4)	682
Venezuela(V1)	608
Japan(J2)	242
Ukraine(U1)	234
Bulgaria(B9)	149
Romania(R1)	142
Argentina(A2)	96
France(F1)	95
其他	1,511
總計	**5,342(91)**



- 統計時間：104年1月至104年10月
- 資料來源：教育機構資安通報平台

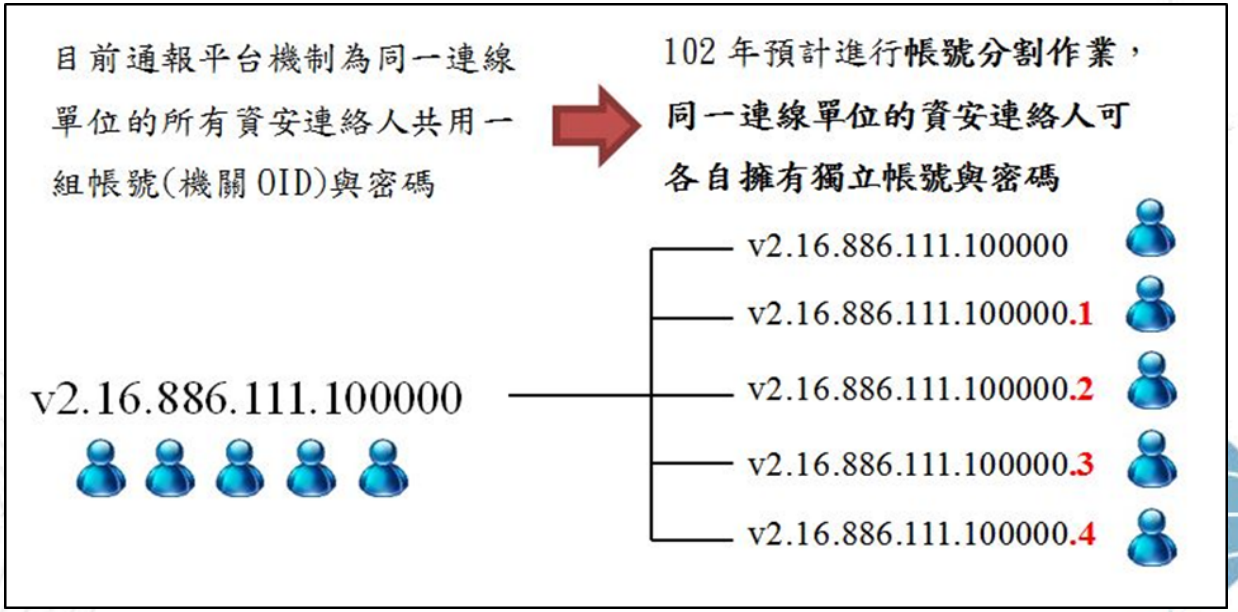
平台功能介紹

教育機構資安通報平台

- 教育機構資安通報平台網址：info.cert.tanet.edu.tw

會員登入

- 使用OID及密碼登入
- 一個單位最多有五位連絡人
- 每個連絡人OID及密碼可不同



機關OID查詢

- 可至研考會網站(網址為「http://oid.nat.gov.tw/」)，點選「組織與團體物件識別碼(OID)查詢」進行查詢
- 來電(信)至本中心查詢

密碼查詢

- 密碼查詢機制將核對「單位OID」、「連絡人姓名」、「連絡人郵件」、「連絡人手機」及「驗證碼」，且**以上資訊需和教育機構資安通報平台內連絡人資料符合**
- 以「**重設8碼亂數密碼**」，並以簡訊及電子郵件通知該連絡人

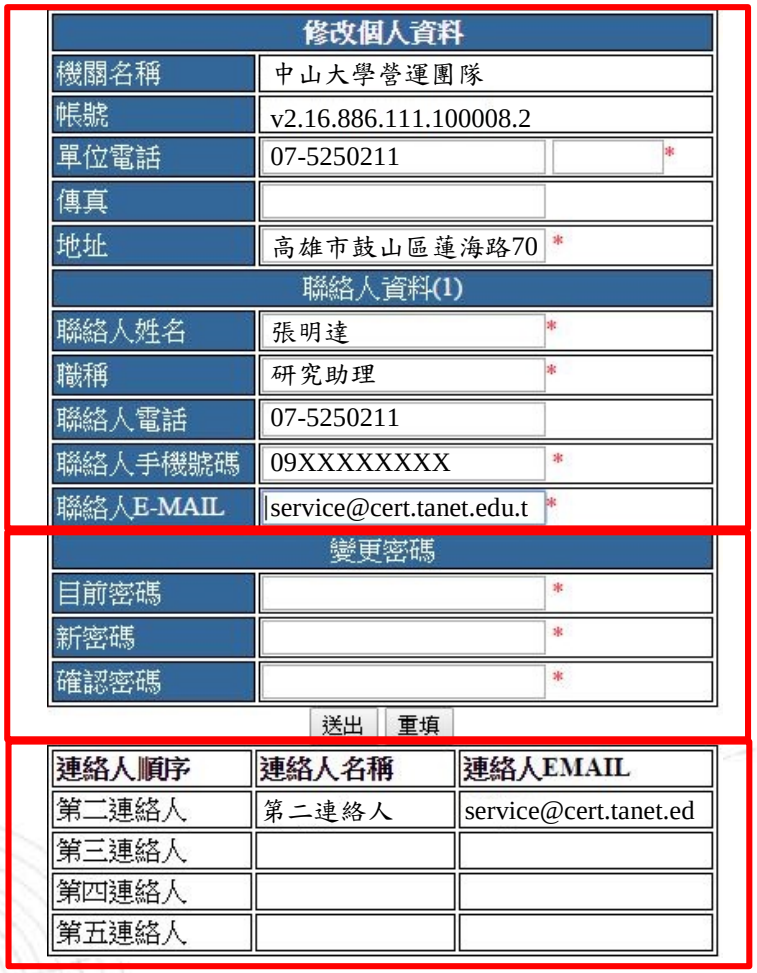
登入畫面


單位資訊
二級單位資訊
三級單位資訊
教育機構資安通報平台
Ministry of education information & communication security contingency platform
聯絡資訊
機關名稱:【測試用】高雄市立資安國民小學
使用者:Robin
主管機關:nsqc網路中心
聯絡電話:07-7654321#
E-Mail:service@cert.tanet.edu.tw
教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail:service@cert.tanet.edu.tw
回首頁
修改個人資料
登出
個人資料區
事件單編號
發佈時間
距通報時間(小時)
流程
Page 1/1
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳 號 管 理
事件附檔下載
資安預警事件
事件單處理區
台灣學術網路危機處理中心(TACERT)

資安通報平台功能簡介

- 個人資料區各功能說明：
  - 首頁：顯示未處理完成事件
  - 修改個人資料：修改個人連絡資料
- 事件單處理區各功能說明：
  - 通報/應變：未完成通報應變事件單表列於此，以利處理
  - 自行通報：如發現資安事件或EWA事件單確認屬實，可利用此攻能完成通報應變。
  - 事件單處理狀態：未結案前之事件單狀態查詢
  - 歷史通報：已結案事件單表列於此
  - 帳號管理：管理第三~五連絡人帳號開啟關閉
  - **事件附檔下載：事件單佐證表列於此，依發佈編號查詢下載。**
  - 資安預警事件：預警事件單表列於此
- 網址：https://info.cert.tanet.edu.tw
  - 操作手冊：http://cert.tanet.edu.tw/pdf/doc6.doc

修改個人資料



修改個人資料	
機關名稱	中山大學營運團隊
帳號	v2.16.886.111.100008.2
單位電話	07-5250211 *
傳真	
地址	高雄市鼓山區蓮海路70 *
聯絡人資料(1)	
聯絡人姓名	張明達 *
職稱	研究助理 *
聯絡人電話	07-5250211
聯絡人手機號碼	09XXXXXXXX *
聯絡人E-MAIL	service@cert.tanet.edu.t *
變更密碼	
目前密碼	*
新密碼	*
確認密碼	*

送出 重填

連絡人順序	連絡人名稱	連絡人EMAIL
第二連絡人	第二連絡人	service@cert.tanet.ed
第三連絡人		
第四連絡人		
第五連絡人		

個人基本資料區

密碼變更區

單位其他連絡人資料區

帳號管理功能(1)


回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳 號 管 理
事件附檔下載
資安預警事件
帳號名稱
帳號狀態
帳號管理
第三資安連絡人
已開啟
關閉此帳號
送出
第四資安連絡人
已開啟
關閉此帳號
送出
第五資安連絡人
已開啟
關閉此帳號
送出
台灣學術網路危機處理中心(TACERT)

帳號管理功能(2)


回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳 號 管 理
事件附檔下載
資安預警事件
帳號名稱
帳號狀態
帳號管理
第三資安連絡人
已開啟
關閉此帳號
送出
第四資安連絡人
已開啟
關閉此帳號
送出
第五資安連絡人
已開啟
關閉此帳號
送出

帳號管理功能(3)


回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳 號 管 理
事件附檔下載
資安預警事件
帳號名稱
帳號狀態
帳號管理
第三資安連絡人
已關閉
開啟此帳號
送出
第四資安連絡人
已開啟
關閉此帳號
送出
第五資安連絡人
已開啟
關閉此帳號
送出
台灣學術網路危機處理中心(TACERT)

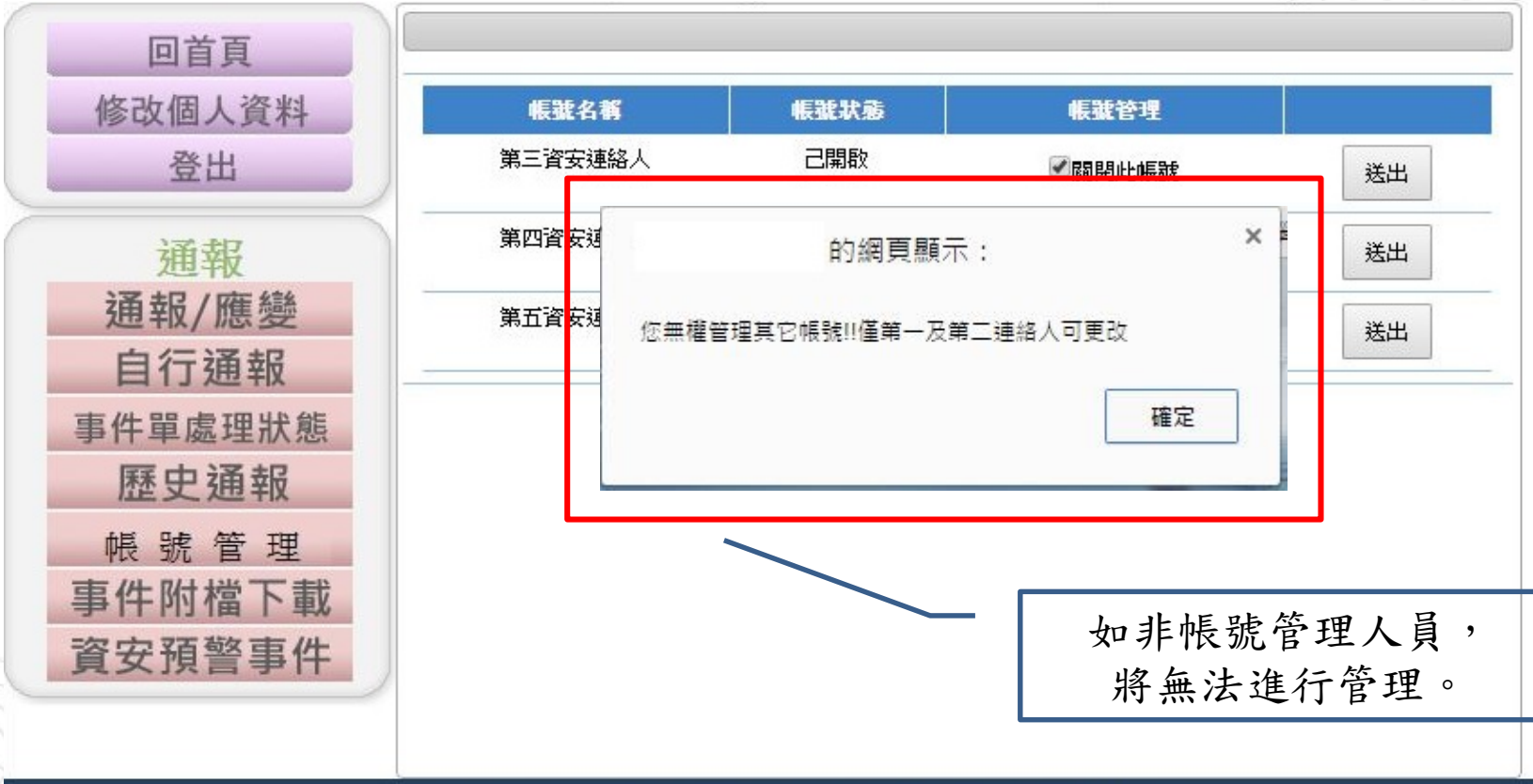
帳號管理功能(4)


回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳 號 管 理
事件附檔下載
資安預警事件
帳號名稱
帳號狀態
帳號管理
第三資安連絡人
已關閉
開啟此帳號
送出
第四資安連絡人
已關閉
開啟此帳號
送出
第五資安連絡人
已關閉
開啟此帳號
送出
台灣學術網路危機處理中心(TACERT)

帳號管理功能(5)


回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳 號 管 理
事件附檔下載
資安預警事件
帳號名稱
帳號狀態
帳號管理
第三資安連絡人
已開啟
關閉此帳號
送出
第四資安連絡人
已關閉
開啟此帳號
送出
第五資安連絡人
已關閉
開啟此帳號
送出
第三連絡人帳號
2.16.886.111 .2
第三連絡人密碼
ek4aQdSs
開啟帳號後，
告知該連絡人帳號及密碼
台灣學術網路危機處理中心(TACERT)

帳號管理功能(6)


回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
帳號管理
事件附檔下載
資安預警事件
帳號名稱
帳號狀態
帳號管理
第三資安連絡人
已開啟
關閉此帳號
送出
第四資安連
送出
第五資安連
送出
的網頁顯示：
您無權管理其它帳號!!僅第一及第二連絡人可更改
確定
如非帳號管理人員，
將無法進行管理。

事件附檔下載

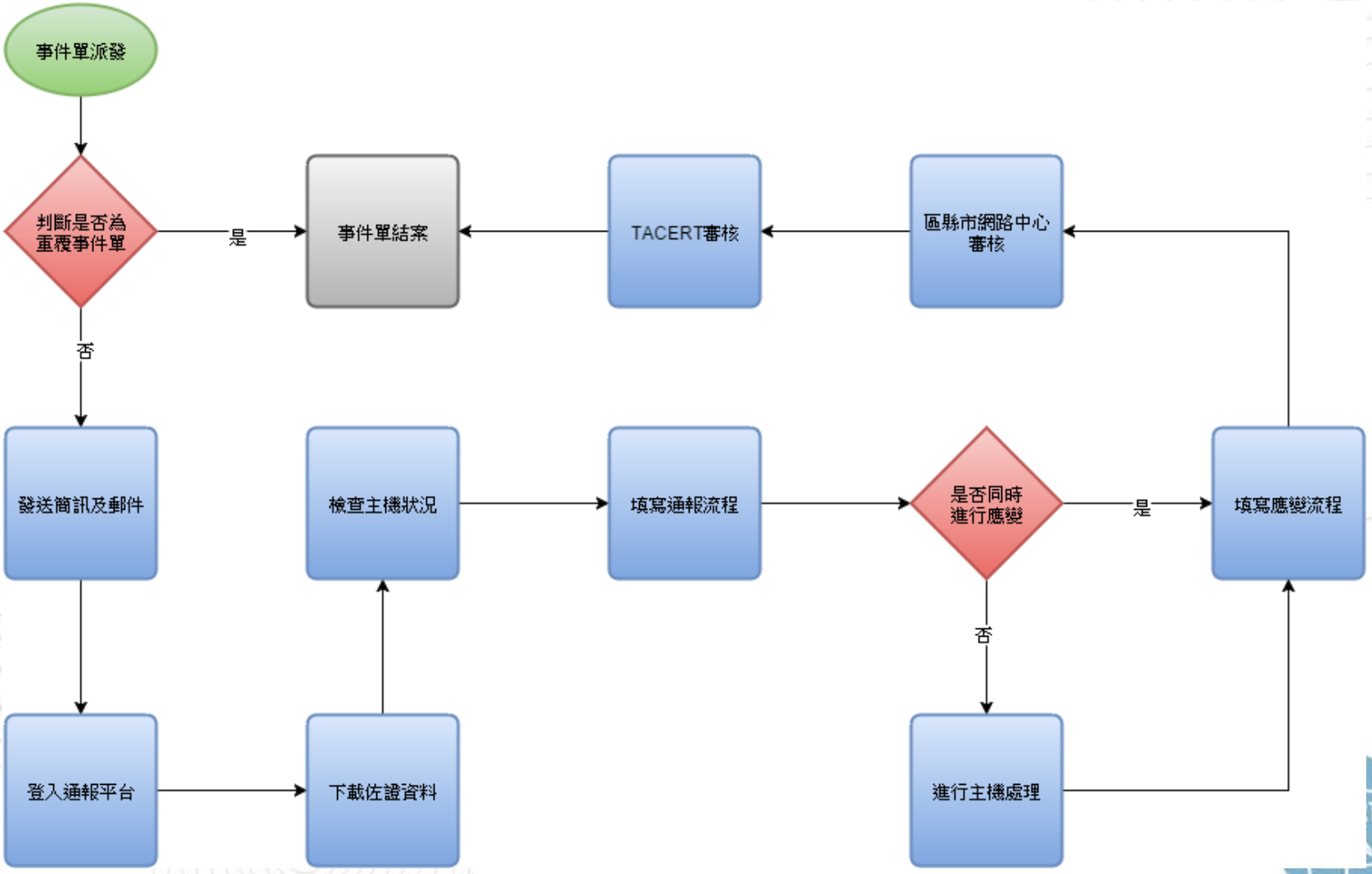
- 舉發單位所提供的**佐證資料**可至「**事件附檔下載**」中下載
- 依事件單、EWA發佈編號或事件單編號搜尋

資安預警事件


教育機構資安通報平台
Ministry of education information & communication security contingency platform
聯絡資訊
機關名稱
使用者:
主管機關
聯絡電話
E-Mail:
教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail:service@cert.tanet.edu.tw
回首頁
修改個人資料
登出
通報
通報/應變
自行通報
事件單處理狀態
歷史通報
事件附檔下載
資安預警事件
事件單編號
發佈時間
距通報時間(小時)
流程
Page 1/1
尚有111張EWA預警單未處理，請按此查閱相關資訊
於首頁顯示
未處理預警單數量
查閱相關資訊
連結資安預警事件
台灣學術網路危機處理中心(TACERT)


機構資安通報平台
聯絡資訊
主管機關:
聯絡電話:
E-Mail:
教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail:service@cert.tanet.edu.tw
事件編號:
狀態:
所有
查詢
第一頁
上一頁
下一頁
最終頁
EWA編號
單位名稱
事件等級
事件分類
狀態
NTUSOC-EWA-201209
low
對外攻擊
未處理
可疑連線
ASOC-EWA-201209-
台灣學術網路危機處理中心(TACERT)

事件單處理流程


事件單派發
判斷是否為重覆事件單
是
事件單結案
TACERT審核
區縣市網路中心審核
否
發送簡訊及郵件
檢查主機狀況
填寫通報流程
是否同時進行應變
是
填寫應變流程
否
登入通報平台
下載佐證資料
進行主機處理


Q
&
A
dreamstime.com