臺灣學術網路 電腦危機處理中心

資安通報平臺及資安事件處理流程簡介

TACERT工作團隊
李柏毅

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

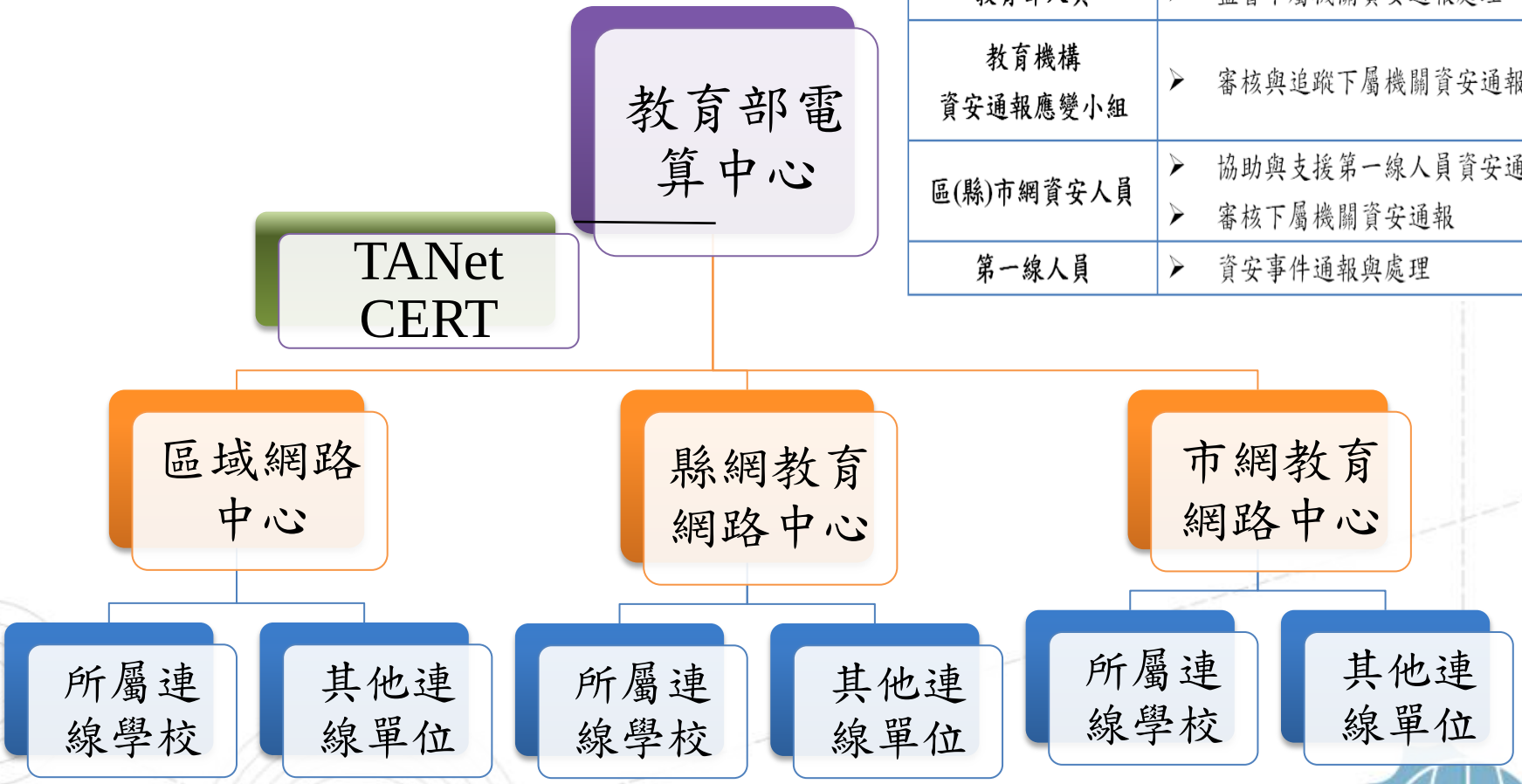
cert.tanet.edu.tw
TACERT

台灣學術網路危機處理中心(TACERT)成立緣起

- 台灣學術網路近年來成為台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
- 故教育部電算中心成立***台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。
- 台灣學術網路危機處理中心日後將致力於強化學術網路資通安全的防護力，形成台灣網路資安防護網重要的一環。

TACERT運作方式

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



TACERT具體營運目標

- 一、資安事件的通報應變
- 二、教育機構資安通報平台的系統維護與開發
- 三、資安事件處理支援
- 四、資安訊息公告
- 五、資安防護教育訓練
- 六、資安通報演練作業
- 七、提升資訊安全研究能量

資安通報應變平台的營運與資安演練

- 提供自動化且完整的通報應變系統，藉以提昇資安事件通報效率，有效把握資安事件的處理進度，將損害降到最低並迅速恢復系統網路的正常運作
- 教育機構資安通報平台由崑山團隊進行開發，現由中山團隊進行維運。
- 定期進行資安通報演練，使台灣學術網路的各連線單位熟悉整個通報流程

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

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:國立中山大學
使用者[redacted]
主管機關:高屏區域網路中心
聯絡電話:07-525-2000
E-Mail[redacted]
教育機構資安通報應變小組
聯絡電話:07-525-0211
E-Mail[redacted]
個人資料區
工單處理區
回首頁
修改個人資料
登出
通報
自行通報
事件單處理狀態
歷史通報
新進告知通報
無通報資料
應變待處理
無通報資料

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。

通報應變流程說明

- 依來源區分
  - 告知通報
  - 自行通報
- 依處理方式區分
  - 通報應變同時處理
  - 通報應變分開處理
- 依資安等級區分
  - 1、2級資安事件(輕微資安事件)
  - 3、4級資安事件(嚴重資安事件)

依資安等級區分

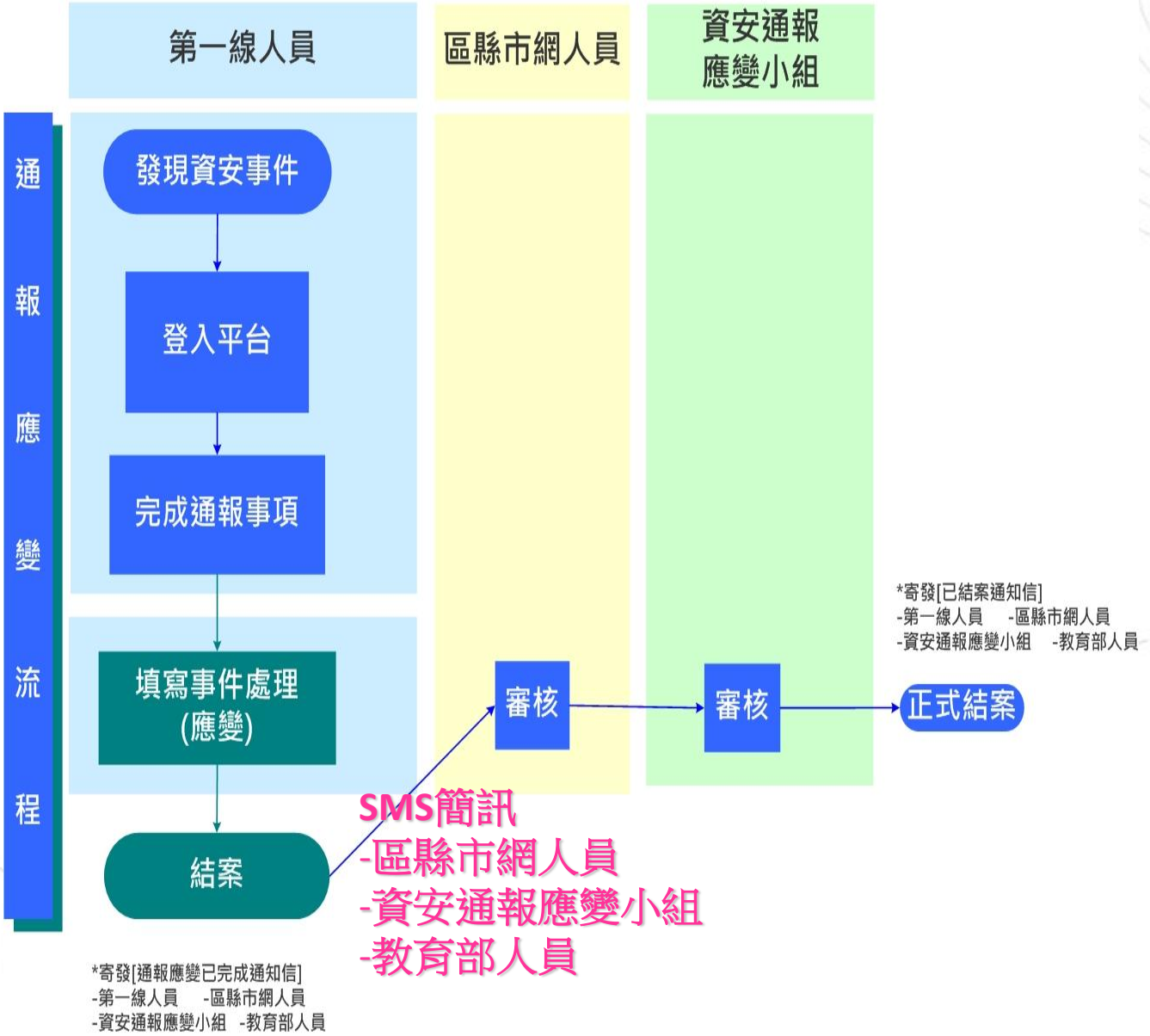
1、2級資安事件

- 事件處理時間為72小時內完成
- 電子郵件通知寄發
  - 事件單成立後1個小時
  - 事件單里立後每隔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

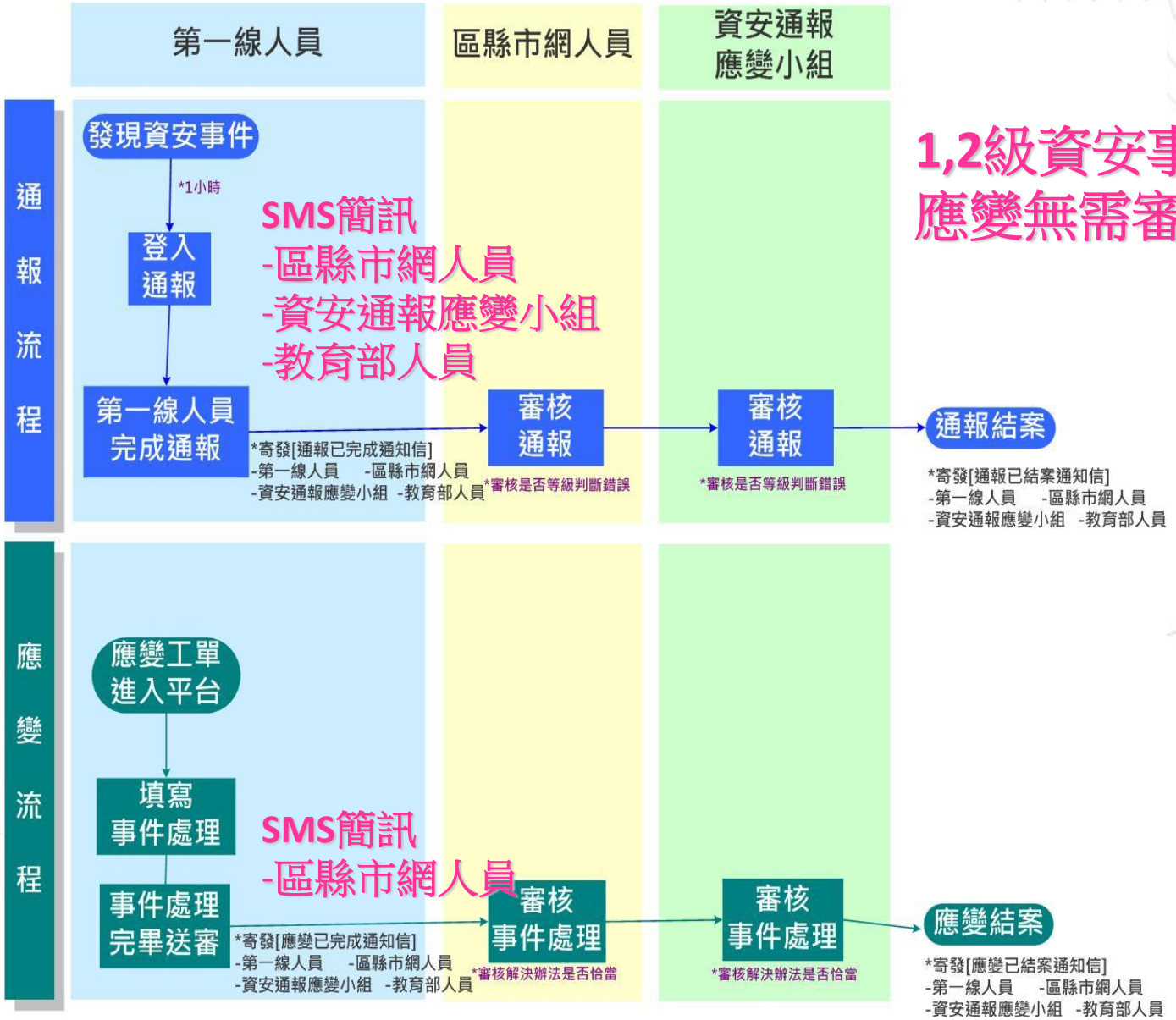
3、4級資安事件

- 事件處理時間為36小時內完成
- 如為自行通報，需和上級管理單位報備且建立連絡網。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
  - 事件單里立後每隔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

通報應變同時處理流程


第一線人員
區縣市網人員
資安通報
應變小組
通報應變流程
發現資安事件
登入平台
完成通報事項
填寫事件處理
(應變)
結案
審核
審核
正式結案
*寄發[已結案通知信]
-第一線人員 -區縣市網人員
-資安通報應變小組 -教育部人員
SMS簡訊
-區縣市網人員
-資安通報應變小組
-教育部人員
*寄發[通報應變已完成通知信]
-第一線人員 -區縣市網人員
-資安通報應變小組 -教育部人員

通報應變分開處理流程


第一線人員
區縣市網人員
資安通報
應變小組
通報流程
發現資安事件
*1小時
登入通報
第一線人員完成通報
SMS簡訊
-區縣市網人員
-資安通報應變小組
-教育部人員
*寄發[通報已完成通知信]
-第一線人員 -區縣市網人員
-資安通報應變小組 -教育部人員
審核通報
*審核是否等級判斷錯誤
審核通報
*審核是否等級判斷錯誤
通報結案
*寄發[通報已結案通知信]
-第一線人員 -區縣市網人員
-資安通報應變小組 -教育部人員
1,2級資安事件
應變無需審核
應變流程
應變工單進入平台
填寫事件處理
事件處理完畢送審
SMS簡訊
-區縣市網人員
*寄發[應變已完成通知信]
-第一線人員 -區縣市網人員
-資安通報應變小組 -教育部人員
審核事件處理
*審核解決辦法是否恰當
審核事件處理
*審核解決辦法是否恰當
應變結案
*寄發[應變已結案通知信]
-第一線人員 -區縣市網人員
-資安通報應變小組 -教育部人員

事件工單

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

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。			

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，但是證據不充分時所發送的預警通知。
- 連線單位收到資安預警通知時，請檢查該主機是否有異常的網路活動跡象，並進行處理狀態回覆：
  - 確實資安事件，請上通報平台自行通報。
  - 誤報，請提供原因。
  - 證據不足，無法判斷。

EWA管理平台

https://120.114.62.80/EWAManager/login.htm

公告 登入

OID：

密碼：

登入

自動化縣市網監控、資安分享平台與miniSOC建置專案計畫
聯絡電話：06-2051573

EWA管理平台

登出 教育部

一共23筆/每頁10筆/共3頁 下載PDF報表 下載Excel報表

AISAC編號	發佈編號	單位名稱	發送時間	確認情形
AISAC-EWA-0272	ASOC-EWA-20110319-8122	[redacted]	2011-03-19 03:43:18	無法判斷
AISAC-EWA-0265	ASOC-EWA-20110316-8110	[redacted]	2011-03-16 16:07:44	無法判斷
AISAC-EWA-0262	ASOC-EWA-20110316-8107	[redacted]	2011-03-16 15:57:47	無法判斷
AISAC-EWA-0261	ASOC-EWA-20110316-8106	[redacted]	2011-03-16 15:57:46	無法判斷
AISAC-EWA-0260	ASOC-EWA-20110316-8105	[redacted]	2011-03-16 15:57:45	無法判斷
AISAC-EWA-0259	ASOC-EWA-20110316-8104	[redacted]	2011-03-16 15:57:44	無法判斷
AISAC-EWA-0256	ASOC-EWA-20110316-8095	[redacted]	2011-03-16 11:27:46	無法判斷
AISAC-EWA-0243	ASOC-EWA-20110310-8067	[redacted]	2011-03-10 12:04:04	無法判斷
AISAC-EWA-0242	ASOC-EWA-20110309-8059	[redacted]	2011-03-09 12:14:04	誤報事件
AISAC-EWA-0241	ASOC-EWA-20110309-8058	[redacted]	2011-03-09 11:44:05	誤報事件

第一頁 下一頁 最後頁

資安事件處理支援

- 根據資安通報系統傳遞之資訊，啟動相關之反應與處理系統
- 追蹤台灣學術網路資安事件的處理狀況
- 透過設置資安諮詢專線、專屬電子郵件、留言版…等方式，提供資安相關的技術支援，協助第一線的資訊人員進行即時處理

專線電話：07-5250211
傳真專線：07-5250212

資安防護教育訓練

- 每年度至少舉辦全國巡迴4場次的資安議題研討會，推廣資訊安全觀念，扎根資訊安全教育，以提升台灣學術網路的使用單位基本的資安防護教育

- 將針對縣市區網的資安人力進行較進階的資安技術防護訓練，以加強縣市區網人員的資安能力

TACERT網站

- TANet CERT網址：http://cert.tanet.edu.tw

最新消息
-提供最新國內外資安新聞

近期活動
-提供資安相關研討會訊息

資安統計數據

TACERT網站功能

- 即時訊息
  提供最新訊息及活動資訊

- 安全通報
  提供相關安全性更新資訊

- 網路資源
  提供資安相關程式、參考網站及資安文件

預期成效

- **事前：確實的通報演練和即時的資安預警**
  - 讓台灣學術網路的連線單位能夠隨時掌握最新的資安公告及弱點威脅動態
  - 確實演練，讓資安人員及主管熟悉資安事件應變
- **事發：快速的資安事件通報機制**
  - 使用通報應變平台
  - 即時掌握台灣學術網路的資安事件，並有效追蹤事件發生的原因、處理進度、損害預估…等
  - 視需求進行技術支援
  - 在最短時間內對資安事件做出應變措施
  - 降低資安事件發生帶來的損害和風險，並防止災害繼續擴大。

預期成效

- **事終：完善的知識管理以及資訊分享**
  - 藉由A-ISAC平台有效預測網路威脅，做出準確的威脅預警，並即時進行安全公告
  - 與其他單位進行資訊交流，充實平台資源
  - 對資安防護和資安技術研發皆有相當大的助益
- **有效提昇台灣學術網路的使用安全**
  - 透過在資安事件的事前、事發、及事終的完整配套措施
  - 提昇台灣學術網路的整體資訊安全防護能力
  - 提供給台灣更安全的網路使用環境

相關網址

- TANet CERT網址：http://cert.tanet.edu.tw
- 教育機構資安通報平台網址：https://info.cert.tanet.edu.tw
- EWA管理平台：https://120.114.62.80/EWAManager/login.htm

連絡方式

- 電話：07-5250211
- 傳真：07-5250212
- MAIL：service@cert.tanet.edu.tw
- 留言版：http://cert.tanet.edu.tw/prog/saverpt.php

謝謝