



教育機構資安通報平台

電算中心呂芳發
2010年9月14日



教育機構資安通報平台

☐ <https://info.cert.tanet.edu.tw/>

教育機構資安通報平台 - Windows Internet Explorer

https://info.cert.tanet.edu.tw/

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

我的最愛 取得更多附加元件 其他 教育 7609 M160 isp ncu ncucc nflow e學苑 kimo tyrc Google pkts

教育機構資安通報平台

教育機構資安通報平台
ministry of education information & communication security contingency platform

會員登入

機關OID
登入密碼

請填入驗證碼 **登入**

[忘記密碼](#)

公告 **帳密更新Q&A** **資安事件單(資安工單)錯誤回報 Q&A**

有鑑於通報平台正式上線後，發生部分資安事件單(資安工單)錯誤事項。為使資安事件通報應變更加有效率，通報平台歸納與規劃數個【資安事件錯誤回報單】提供各單位進行錯誤回報。本Q&A已正式通過教育部審核，請各單位協助處理。後續也將定期更新此【資安事件單錯誤回報Q&A】。

(1)底下依照不同錯誤加以說明並提供回報格式，請各單位協同處理。
(2)為加速處理，來信請寄samtn125@gmail.com，boyi@staff.nsysu.edu.tw。
(3)信件將統一由下列服務單位加以正式回覆：

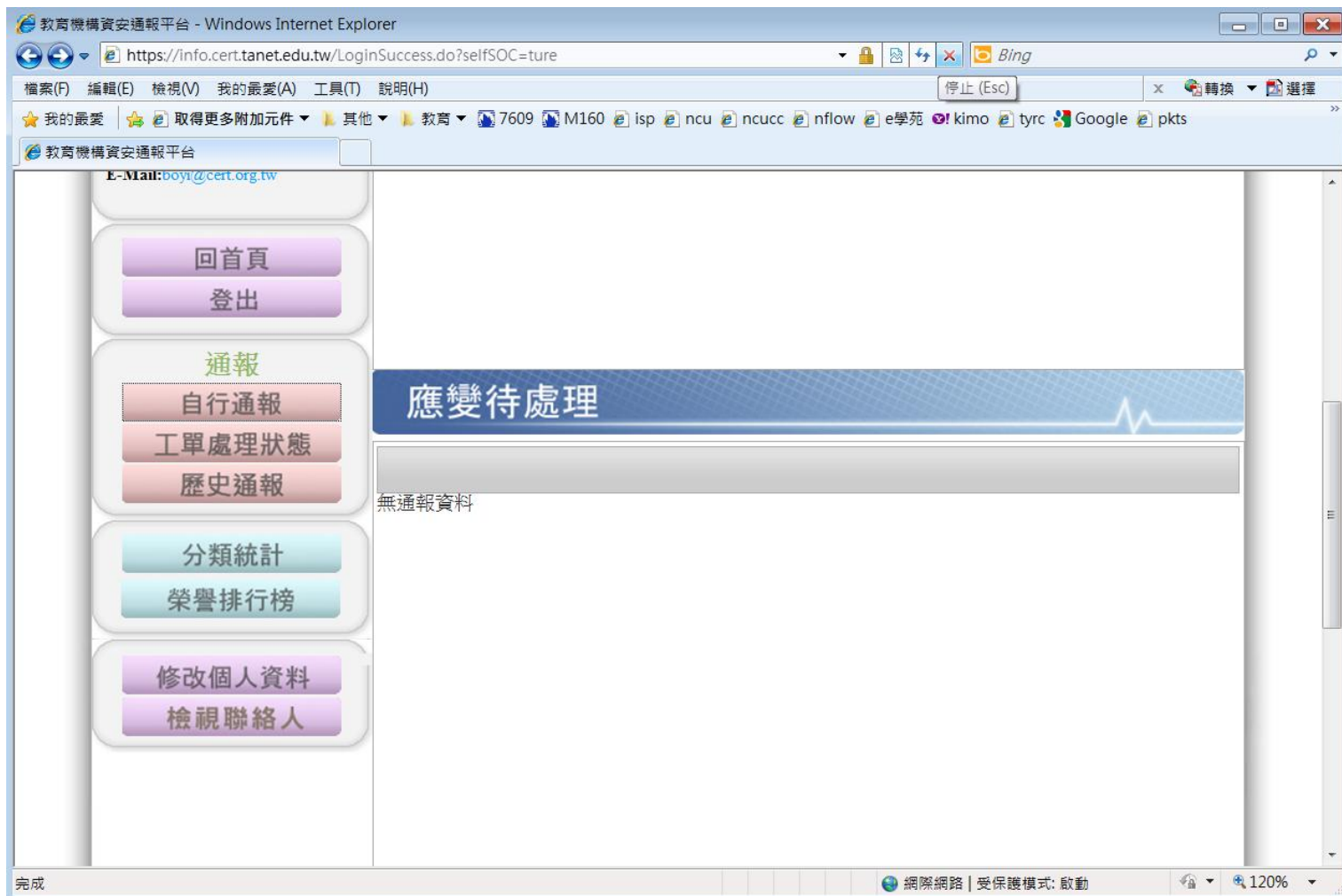
臺灣學術網路危機處理中心(TANet Cert)
服務電話：(07)525-0211
E-mail：service@cert.tanet.edu.tw
網址：http://cert.tanet.edu.tw/

1. 資安事件單重複
可能發生原因：
(1)單位有多個資安聯絡人，在不同時間針對相同資安事件重複進行通報，產生單一事件多筆事件單。

完成 網際網路 | 受保護模式: 啟動 120%



教育機構資安通報平台

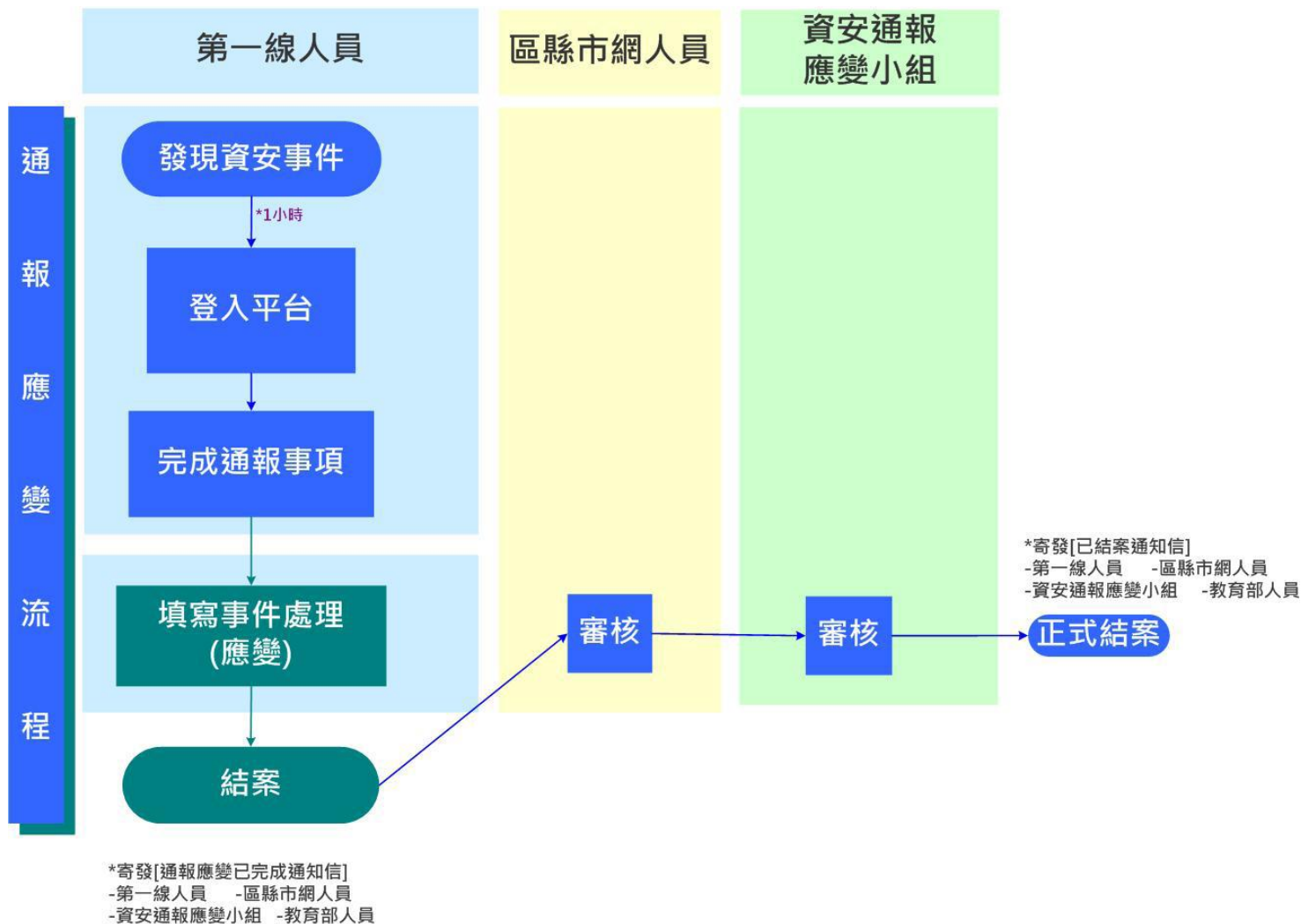




通報期限

- ☐ 發生資安事件時，請盡速登入教育機構資安通報平台進行通報流程。
- ☐ 事件等級3.4級，需於36小時內登入教育機構資安通報平台完成所有通報應變流程。
- ☐ 事件等級1.2級，需於72小時內登入教育機構資安通報平台完成所有通報應變流程。

通報流程





通報流程

❑ I. 通報流程

一，發生資通安全之機關（機構）聯絡資料：

❑ 機關（機構）名稱：國立中央大學

◎通報人：呂芳發 ◎電話：03-422-7151 ◎傳真：03-425-2561

◎E-mail: tanet_ncu@cc.ncu.edu.tw

❑ 主管機關 機關名稱：桃園區域網路中心 資安人員：呂芳發

電話：03-422-7151 傳真：03-425-2561 E-mail: tanet_ncu@cc.ncu.edu.tw

❑ 教育機構資安通報應變小組 聯絡電話：07-525-0211

傳真：07-525-0212 E-mail: boyi@cert.org.tw



通報流程

☐ 二、各機關因受外在因素所產生資通安全事件時通報事項：

☐ ☒ 為必填

欄位不得輸入特殊符號(如：「;」、「"」、「'」、「\$」、「&」、「%」、「!」、「^」、「*」、「<」、「>」、「_」、「|」、「-」)

☐ 1 〉通報型態:主動通報(各單位自行發現資安事件)

☐ 2 〉事件發生時間

☐ 3 〉設備資料：IP位置 (IP address),網際網路位置 (web-url),作業系統 (名稱/版本),設備廠牌機型 ,已裝置之安全防護軟體(防毒軟體 ,防火牆)



通報流程

□4 〉資通安全事件：基本資料

◎事件分類：

INT（非法入侵）：

主機被入侵(主機遭駭客入侵)

主機對外攻擊(主機對外進行攻擊行為)

主機發現木馬(主機遭駭客置入木馬)

主機針對性攻擊(範例:電子郵件帳號遭駭客竊取，大量發Email)

主機發現惡意程式(範例:主機遭駭客置入僵尸程式)

DEF（網頁攻擊）：

惡意網頁(網頁遭駭客置換或放置不當內容)

惡意留言(網頁遭駭客放上惡意留言)

網頁置換(網頁遭駭客換)

釣魚網站(主機遭駭客置入釣魚網站)

其它類型的網頁攻擊

其它

◎破壞程度：(文字勿超過200中文字，標點符號請用全形)

◎事件說明：(文字勿超過200中文字，標點符號請用全形)



通報流程

□5 > 資通安全事件：影響等級及說明

◎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

◎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

◎若有3、4級事件，請立刻電話告知您所屬的主管機關

◎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

◎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：

1. 機密性衝擊 -

無（0級）

1級-非核心業務資料遭洩漏

2級-非屬密集或敏感之核心業務資料遭洩漏

3級-密集或敏感公務遭洩漏

4級-國家機密資料遭洩漏



通報流程

2. 完整性衝擊 -

無（0級）

1級-非核心業務系統或資料遭竄改

2級-核心業務系統或資料遭輕微竄改

3級-核心業務系統或資料遭嚴重竄改

4級-國家重要資訊基礎建設系統或資料遭竄改

3. 可用性衝擊

無（0級）

1級-非核心業務運作遭影響或短暫停頓

2級-核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作

3級-核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作

4級-國家重要資訊基礎建設運作影響或系統停頓，無法於可容忍中斷時間內回復正常運作

◎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）



通報流程

□6 > ◎是否需要支援?



是

你的上層機關資安人員為: 呂芳發

聯絡電話:03-422-7151

E-mail:tanet_ncu@cc.ncu.edu.tw

期望支援方式: “電話告知 “ “Email告知 “



否:通報單位自行解決

□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

□ II. 應變流程

◎ II.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
- 直接處理完成，解決辦法詳見【解決辦法】
- 其它

◎ II.2 【解決辦法】(文字勿超過200中文字，標點符號請用全形)

◎ 解決時間：



TANet Cert

□ 臺灣學術網路危機處理中心(TANet Cert)進行服務

服務電話：(07)525-0211

E-mail：service@cert.tanet.edu.tw

網址：<http://cert.tanet.edu.tw/>



Computer Center, National Central University.



Thank You!