資安事件通報處理與通報平台操作

新北市政府教育局
教育研究及資訊發展科

- 資安事件探討
- 政府資安相關威脅
- 學術網路資安事件
- 校園資安業務說明
- 資安通報平台操作
- 資安通報演練說明

資安事件探討

銓敘部證實 59萬筆文官個資遭外洩

分享 分享 留言 列印 存新聞 A- A+

2019-06-24 23:45 聯合報 記者鄭煥／即時報導 讚 1,570 分享

銓敘部證實，22日接獲外部情資，知悉國外網站揭露疑似銓敘部掌理的個人資料達59萬筆。 圖／擷自Google Maps

銓敘部掌管的文官個資驚傳遭外洩，銓敘部今晚在官網證實，22日接獲外部情資，知悉國外網站揭露疑似銓敘部掌理的個人資料達59萬筆，已依照「資通安全管理法」向行政院國家資通安全會報技術服務中心，進行資安事件通報。

此次文官個資外洩影響範圍，自2005年起至2012年6月30日間，中央及地方機關公務人員送審人員歷史資料，實際影響人數為24萬3376筆，欄位包含身分證字號、姓名、服務機關、職務編號、職稱。

銓敘部指出，除向行政院資安中心通報，疑似外洩資料的資訊系統，早已在2015年3月下線，為求審慎，銓敘部即刻對此案現行運作的相關資通系統進行弱點檢測及重新檢視防護措施。

針對此事件，銓敘部表示，已協請行政院資通安全處，協助進行根因調查及全機關全面性資通安全檢測，未來將確實檢討改進，並依「資通安全管理法」及「個人資料保護法」，持續精進各項資通安全及個資保護相關作為。

行政院、個資、資安

資料來源:聯合報電子新聞網站

資料外洩、網路釣魚、自動化威脅 2019年資安3大風險

能力雜誌 | 46 人追蹤 追蹤

2019年4月3日 下午 12:59

留言

手持裝置普及、社群平台興起、GDPR的實施，使駭客入侵的管道、勒索手法更變化多端，企業與消費者想避免成為「受駭者」，須針對2019年的資安3大風險做好妥善的防範。

【文 / 趨勢科技】

趨勢科技發表《2019資安年度預測報告》，針對網路安全威脅與網路犯罪攻擊趨勢，提出3大重點警示：憑證資料外洩遭盜用詐騙事件將不斷增加、網路釣魚攻擊手段將取代漏洞攻擊套件成為主要攻擊手法，以及工控系統的安全性持續受到威脅。

趨勢科技台灣區暨香港區總經理洪偉淦表示：「回顧2018年全球資安政策推動，可觀察到各組織及企業對於資料安全的重視；重大資訊安全事件的發生亦凸顯連網裝置普及所面臨的資安問題。預期在2019年企業和組織將導入更多連網設備，而連網速度也將大幅提昇，資訊安全面臨更廣泛與多元的挑戰，不僅企業對於資訊安全團隊的需求更提高，多層式智能防護的資安政策也會在企業經營中扮演關鍵的角色，企業領導人對於網路安全的重視及培養經營團隊資安意識，更是建構自身企業網路安全防護架構的重要基石。」

資料來源:擷取能力雜誌新聞

世界經濟論壇發布2018年全球風險報告

鉅亨網 | 795 人追蹤 追蹤

留言

鉅亨網新聞中心 2018年1月23日 上午 10:15

經濟參考報今 (23) 日報導，世界經濟論壇 1 月 17 日發布《2018 年全球風險報告》稱，2018 年經濟增長勢頭強勁，全球風險也進一步加劇，其中環境風險居首位，但經濟的強勁發展為應對全球風險帶來了機遇。

報告指出，參加調查的 59% 的受訪者認為，2018 年風險會增加，只有 7% 的人認為會下降。地緣政治狀況惡化是導致產生上述悲觀預測的部分原因，93% 的受訪者認為主要大國間的政治或經濟對抗將變得更為激烈，近 80% 的受訪者預計大國間爆發戰爭的可能性增加。

與 2017 年相同，環境問題又一次成為全球專家們最大的擔憂，在發生機率和潛在危害兩個排序中，與環境相關的五項因素在總計 30 類風險的排名中都十分靠前，其中，極端天氣更被視為最大風險。

可能性最高的十大風險分別是：極端天氣事件、自然災害、網路攻擊、數據詐騙或數據盜竊、氣候變化減緩與應對措施失敗、大規模非自願移民、人為環境災害、恐怖襲擊、非法貿易、主要經濟體資產泡沫。

資料來源:YAHOO電子新聞網站

- 資安威脅趨勢


SWIFT
BANGLADESH BANK
WannaCry
bitcoin
網路與經濟罪犯影響電子商務與金融運作


BLACK ENERGY
Stuxnet
關鍵資訊基礎設施資安風險倍增


BARRACUDA
RSA
SECURITY
CLOUDFLARE
DigiNotar
資安(訊)供應商持續遭駭破壞供應鏈安全

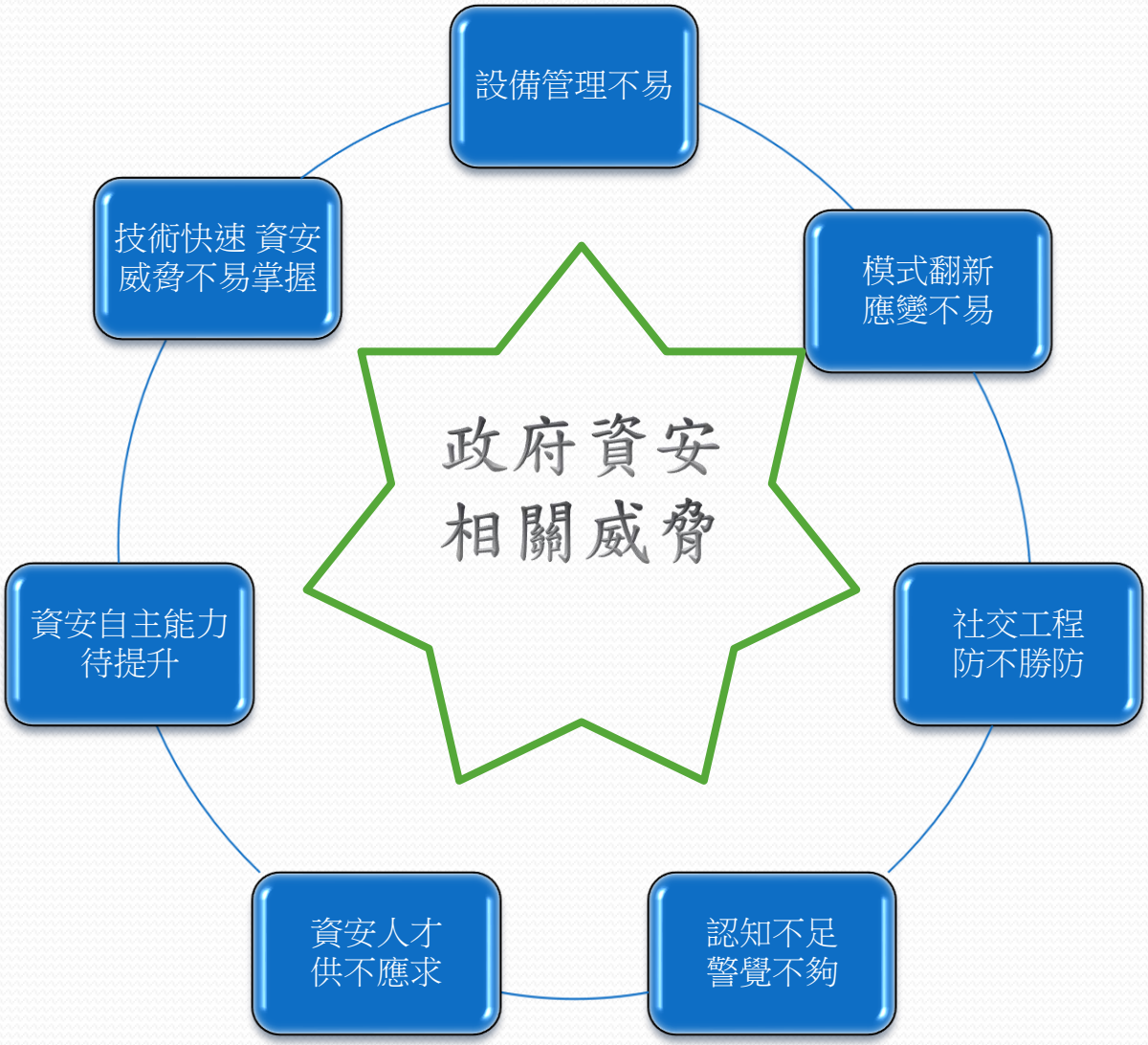

MIRAI
INTERNET of THINGS
物聯網設備資安弱點威脅升高


NORTHROP GRUMMAN
YAHOO!
進階持續威脅攻擊竊取機密資料

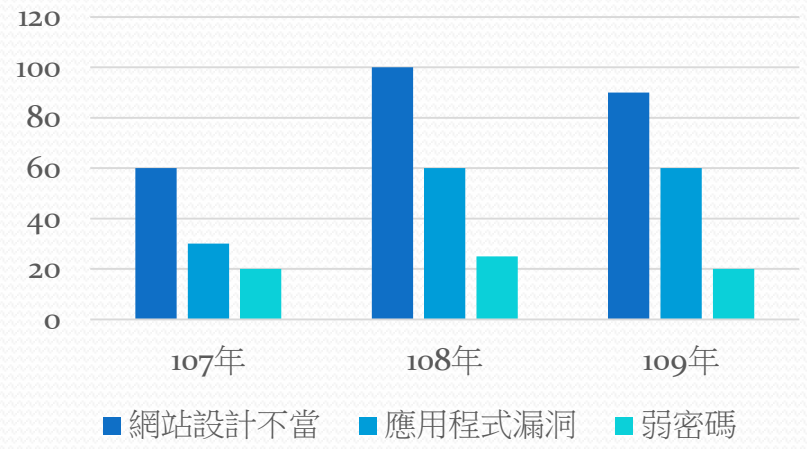
網路攝影機容易有資安漏洞

參考網址:https://www.youtube.com/watch?v=FjPckliTqBo

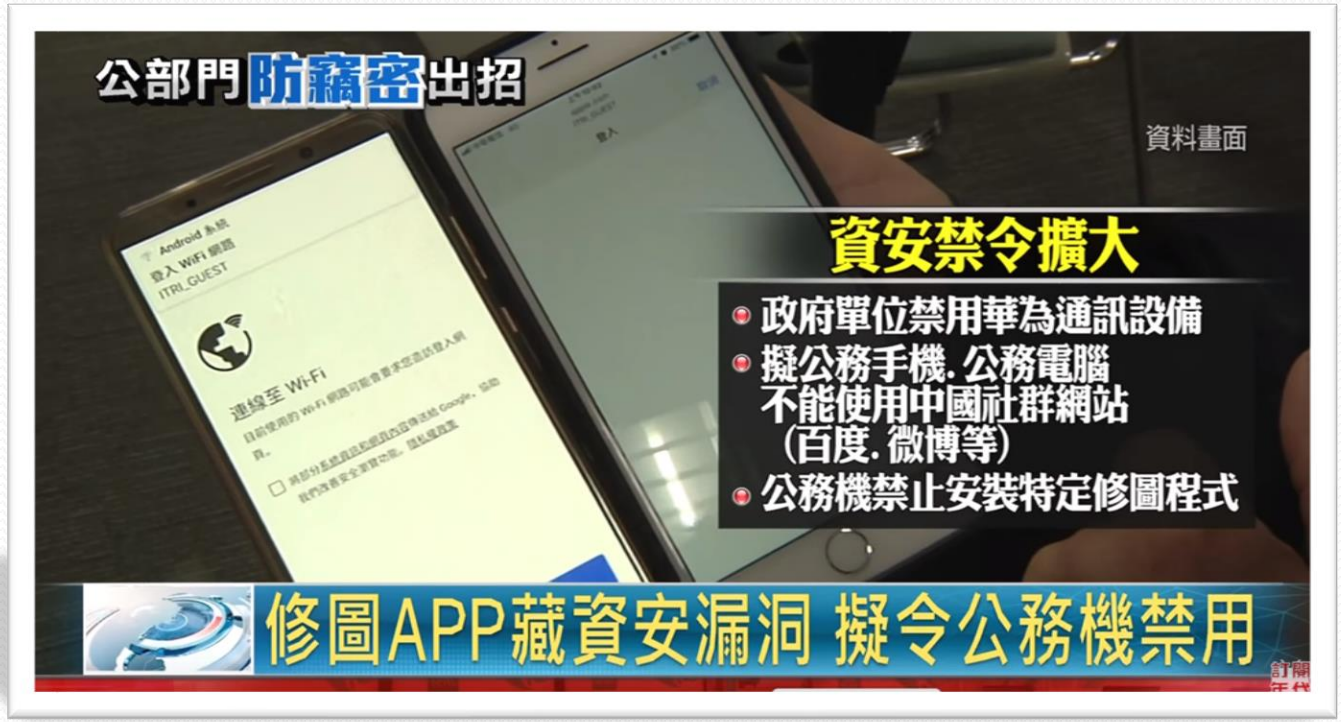
政府資安相關威脅


政府資安
相關威脅
設備管理不易
模式翻新
應變不易
社交工程
防不勝防
認知不足
警覺不夠
資安人才
供不應求
資安自主能力
待提升
技術快速 資安
威脅不易掌握

- 政府資安事件發生原因
- 109年政府資安事件通報，以網頁攻擊事件類型為主，其中前3大事件發生原因依序為網站設計不當、應用程式漏洞及弱密碼



不當APP軟體常有資安漏洞



參考網址:https://www.youtube.com/watch?v=2eLus-1A42k

學術網路資安事件

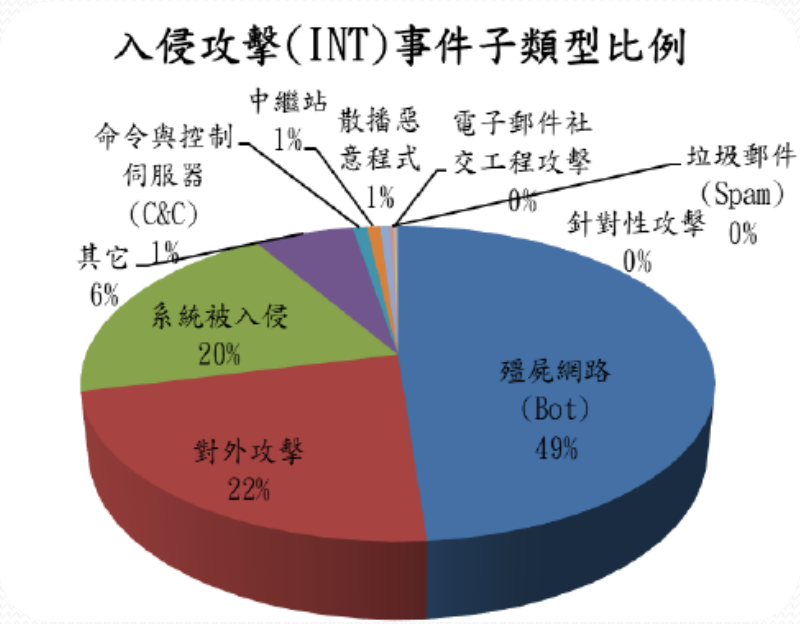
- 學術網路資安事件類型比例

事件類型	數量
入侵攻擊(INT)	15,836
網頁攻擊(DEF)	178
資安預警(EWA)	10,114
總計	26,128

- 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

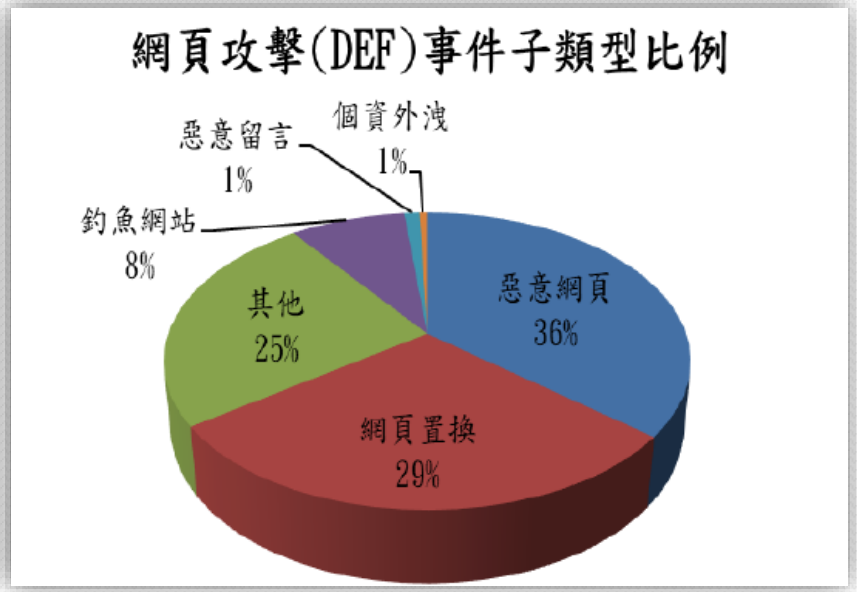
事件類型	子類別	數量
入侵攻擊(INT)	殭屍網路(Bot)	7,726
	對外攻擊	3,559
	系統被入侵	3,153
	其它	962
	命令與控制伺服器(C&C)	136
	中繼站	128
	散播惡意程式	101
	垃圾郵件(Spam)	34
	電子郵件社交工程攻擊	19
	針對性攻擊	18
總計		15,836



- 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

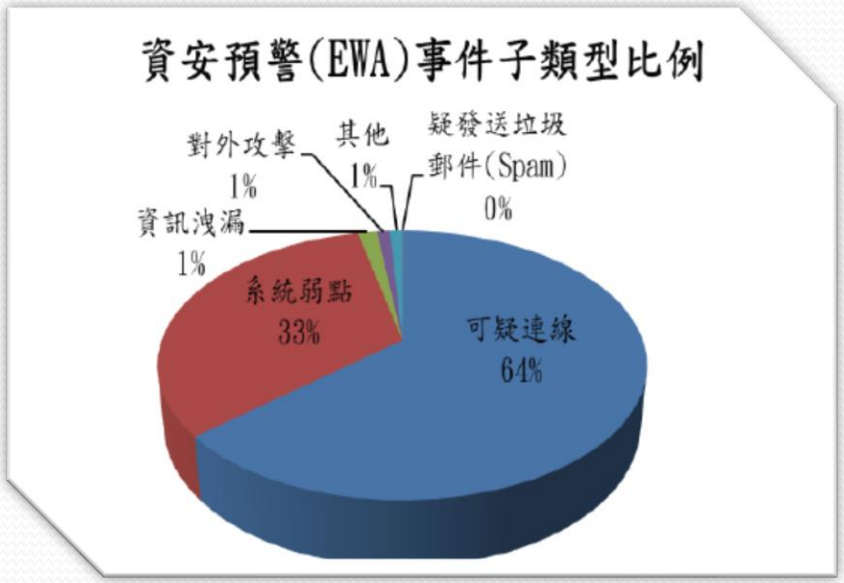
事件類型	子類別	數量
網頁攻擊（DEF）	惡意網頁	64
	網頁置換	52
	其他	44
	釣魚網站	15
	惡意留言	2
	個資外洩	1
總計		178



- 資料來源:教育機構資安通報平台

- 資安預警EWA事件類型比例

事件類型	子類別	數量
資安預警(EWA)	可疑連線	6,441
	系統弱點	3,319
	資訊洩漏	152
	對外攻擊	102
	其他	97
	疑發送垃圾郵件(Spam)	3
總計		10,114



- 資料來源:教育機構資安通報平台

網站介紹

- 台灣學術網路危機處理中心
  - https://cert.tanet.edu.tw/prog/index.php

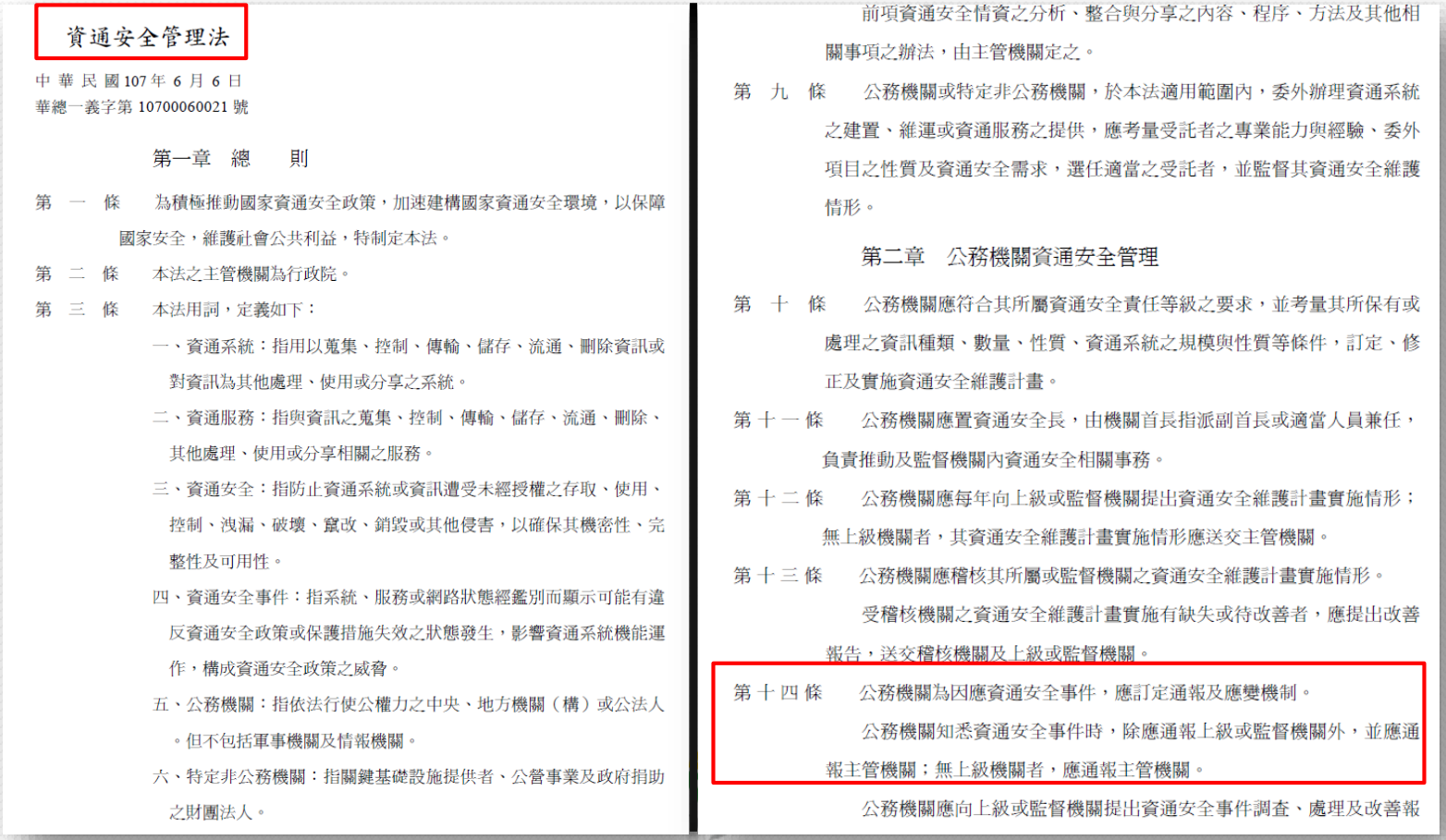
校園資安業務說明

校園資安相關業務依據

- 資通安全管理法
- 資通安全管理法施行細則
- 資通安全事件通報及應變辦法
- 教育機構資安通報應變手冊
- 教育體系資通安全暨個人資料管理規範
- 資通安全維護計畫實施情形參考表
- 個人資料保護法

資通安全管理法

- 依據：



資通安全管理法

中 華 民 國 107 年 6 月 6 日
華總一義字第 10700060021 號

第一章　總　　則

第　一　條　　為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。

第　二　條　　本法之主管機關為行政院。

第　三　條　　本法用詞，定義如下：

一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

四、資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

五、公務機關：指依法行使公權力之中央、地方機關（構）或公法人。但不包括軍事機關及情報機關。

六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。

第　九　條　　公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

第二章　公務機關資通安全管理

第　十　條　　公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。

第十一條　　公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。

第十二條　　公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。

第十三條　　公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。

受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。

第十四條　　公務機關為因應資通安全事件，應訂定通報及應變機制。

公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。

公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報

資安法之立法目的與規範對象

立法目的

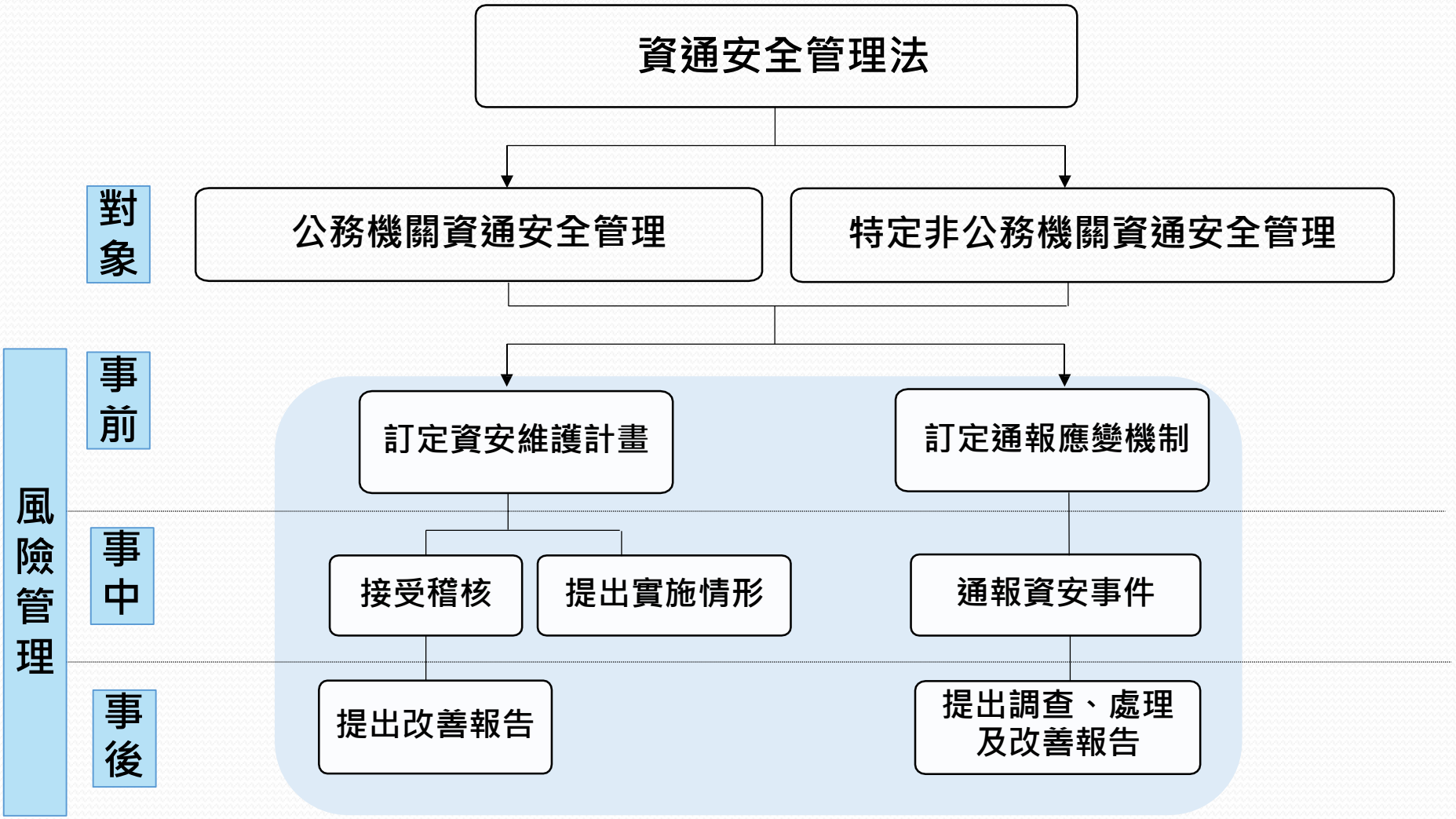
為**積極推動國家資通安全政策**，**加速建構國家資通安全環境**，以保障國家安全，維護社會公共利益。

規範對象

以對人民生活、經濟活動及公眾或國家安全有重大影響者為納管對象。

- 公務機關
  - 中央與地方機關(構)
  - 公法人
- 特定非公務機關
  - 關鍵基礎設施提供者
  - 公營事業
  - 政府捐助之財團法人

資通安全管理法管理架構



資安管理法子法架構

- 機關資安責任等級分級提報

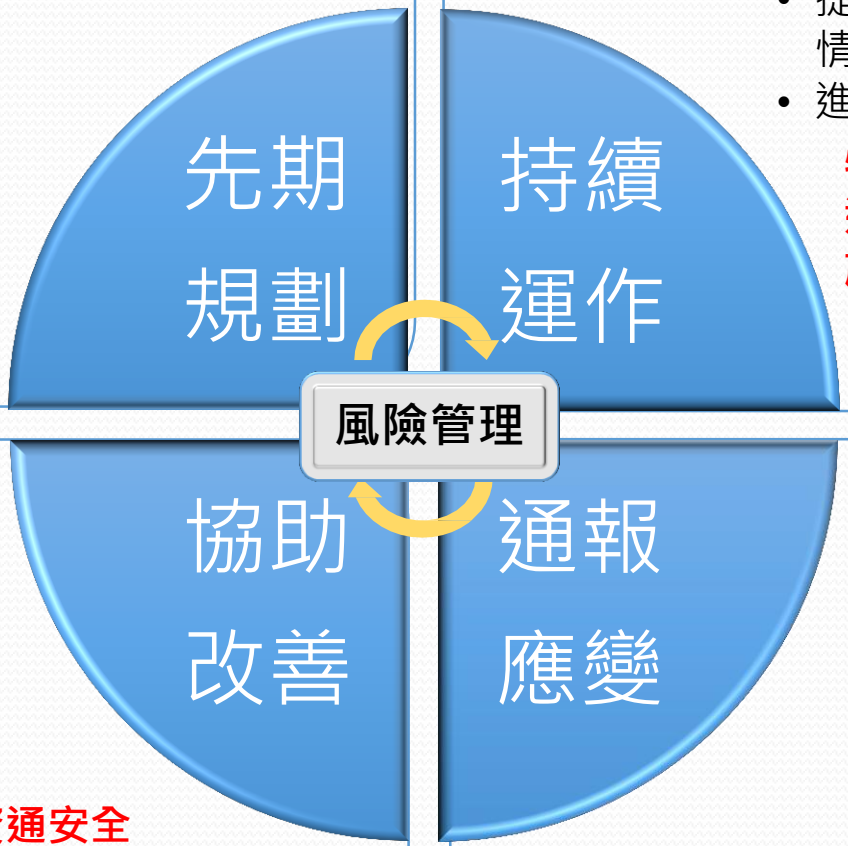
  資通安全責任等級分級辦法

- 訂定資安維護計劃

  資通安全管理法施行細則

- 提出資安維護計劃實施情形
- 進行稽核

  特定非公務機關資通安全維護計畫實施情形稽核辦法



- 提出稽核改善報告
- 情資分享

  資通安全情資分享辦法

- 人員獎懲

  公務機關所屬人員資通安全事項獎懲辦法

- 訂定資安事件通報應變機制
- 通報資安事件
- 提出事件調查改善報告

  資通安全事件通報及應變辦法

各責任等級應辦事項(管理面)

責任等級		資通系統分級及防護基準	資訊安全管理系統之導入及通過公正第三方之驗證	資通安全專責人員	內部資通安全稽核	業務持續運作演練	資安治理成熟度評估
A	公務機關	1年內完成	• 2年內導入CNS 27001資訊安全管理系統國家標準 • 3年內完成公正第三方驗證	4人	2次/年	1次/年	1次/年
	特定非公務機關	1年內完成	• 2年內導入CNS 27001資訊安全管理系統國家標準 • 3年內完成公正第三方驗證	4人	2次/年	1次/年	--
B	公務機關	1年內完成	• 2年內導入CNS 27001資訊安全管理系統國家標準 • 3年內完成公正第三方驗證	2人	1次/年	1次/2年	1次/年
	特定非公務機關	1年內完成	• 2年內導入CNS 27001資訊安全管理系統國家標準 • 3年內完成公正第三方驗證	2人	1次/年	1次/2年	--
C	公務機關	• 1年內完成資通系統分級 • 2年內完成防護基準	• 2年內導入CNS 27001資訊安全管理系統國家標準	1人	1次/2年	1次/2年	--
	特定非公務機關	• 1年內完成資通系統分級 • 2年內完成防護基準	• 2年內導入CNS 27001資訊安全管理系統國家標準	1人	1次/2年	1次/2年	--

各責任等級應辦事項(技術面)

責任等級		安全性檢測		資通安全健診	資通安全監控管理機制	政府組態基準	資通安全防護					
		網站安全弱點檢測	系統滲透測試				防毒軟體	防火牆	郵件過濾	入侵偵測及防禦機制	應用程式防火牆	進階持續性威脅攻擊防禦措施
A	公務機關	2次/年	1次/年	1次/年	√	√	√	√	√	√	√	√
	特定非公務機關	2次/年	1次/年	1次/年	√	--	√	√	√	√	√	√
B	公務機關	1次/年	1次/2年	1次/2年	√	√	√	√	√	√	√	--
	特定非公務機關	1次/年	1次/2年	1次/2年	√	--	√	√	√	√	√	--
C	公務機關	1次/2年	1次/2年	1次/2年	--	--	√	√	√	--	--	--
	特定非公務機關	1次/2年	1次/2年	1次/2年	--	--	√	√	√	--	--	--
D		--	--	--	--	--	√	√	√	--	--	--

各責任等級應辦事項(認知與訓練面)

責任等級		資通安全教育訓練		資通安全專業證照及職能訓練證書	
		資通安全及資訊人員	一般使用者與主管	資通安全專業證照	資通安全職能訓練證書
A	公務機關	12小時/年(4名)	3小時/年(每人)	4張	4張
	特定非公務機關	12小時/年(4名)	3小時/年(每人)	4張	--
B	公務機關	12小時/年(2名)	3小時/年(每人)	2張	2張
	特定非公務機關	12小時/年(2名)	3小時/年(每人)	2張	--
C	公務機關	12小時/年(1名)	3小時/年(每人)	1張	1張
	特定非公務機關	12小時/年(1名)	3小時/年(每人)	1張	--
D		--	3小時/年(每人)	--	--

資安通報平台操作

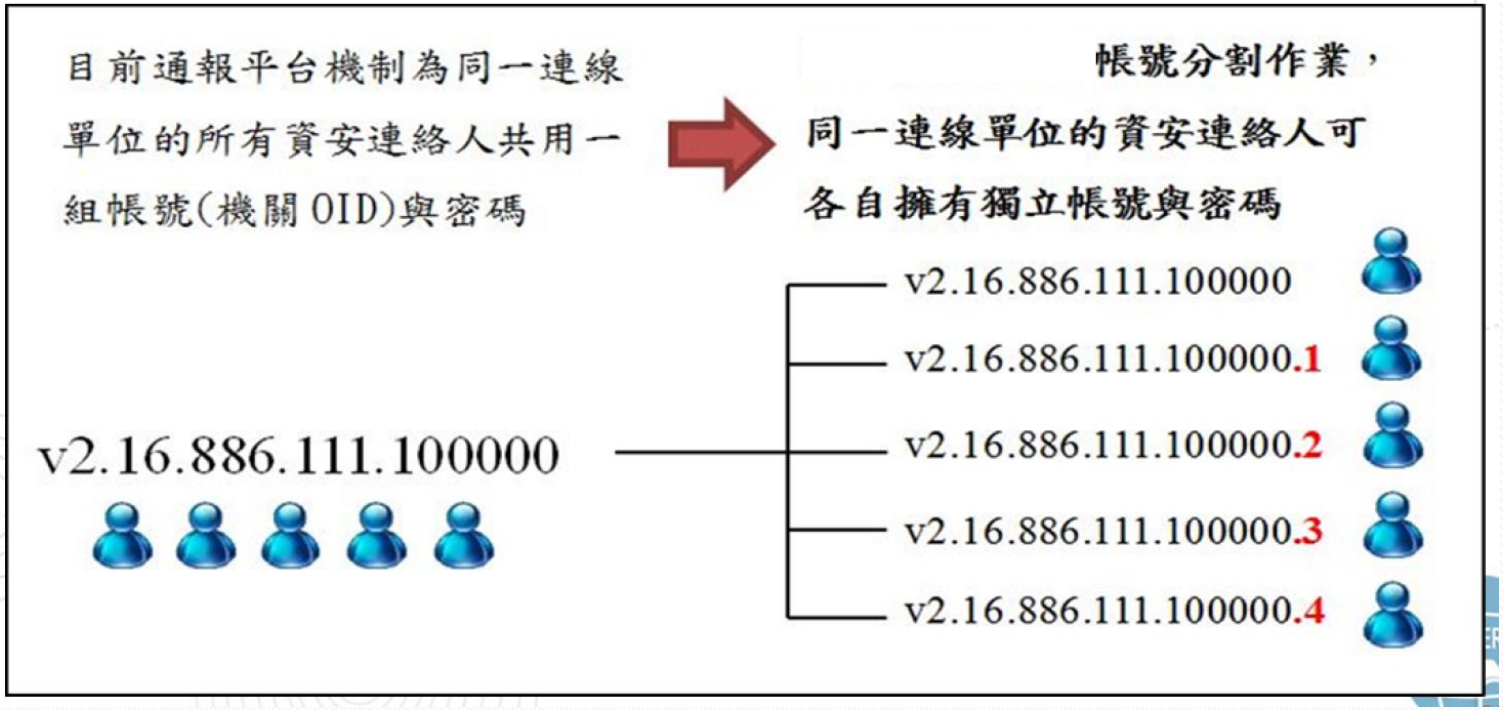
教育機構資安通報平台

教育機構資安通報平台網址:
https://info.cert.tanet.edu.tw/prog/index.php

- 會員登入
  - 使用OID帳號登入
  - 一個學校至少**兩位聯絡人**
  - 每個聯絡人OID密碼可不同

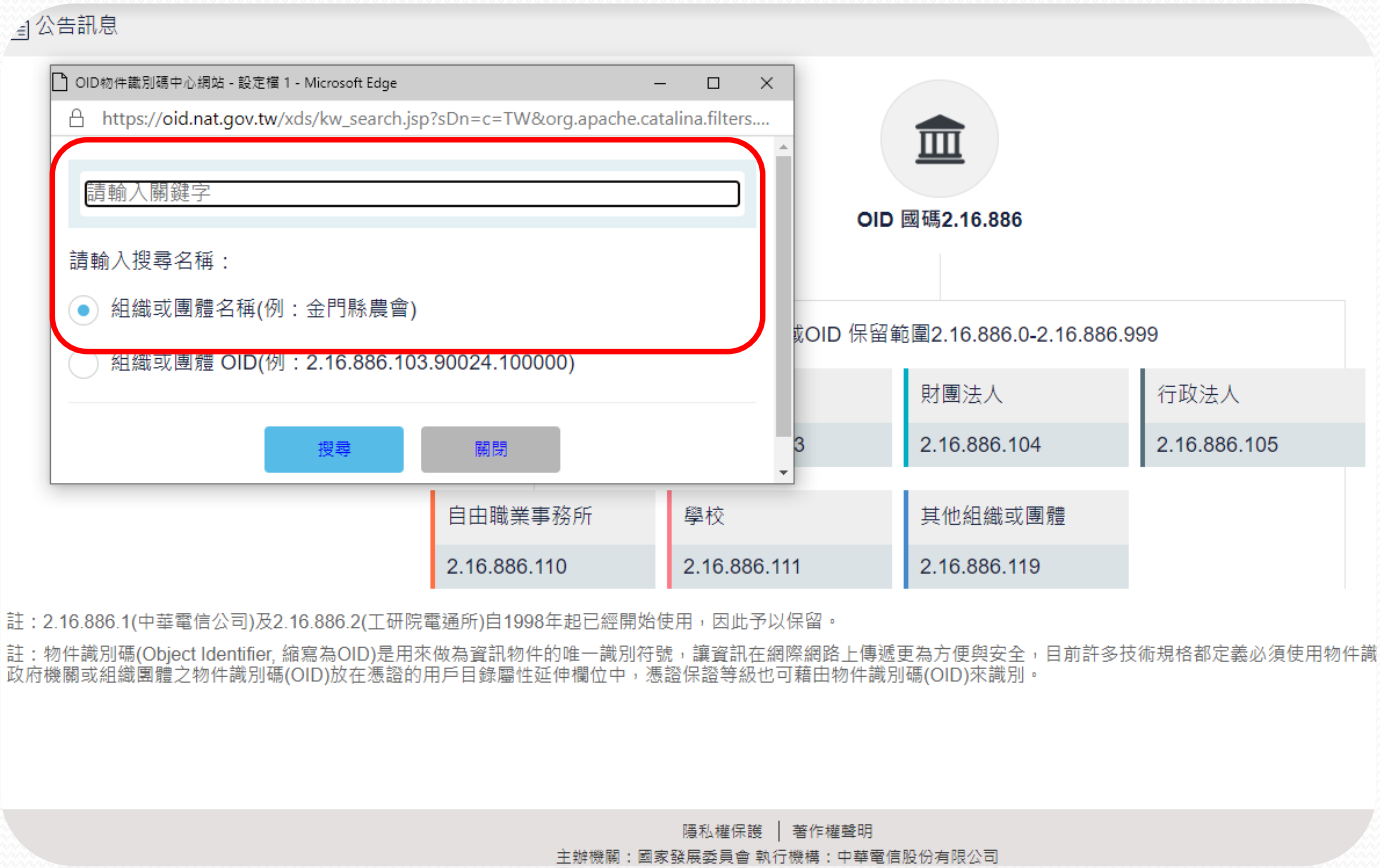
- 忘記密碼
  - 點選密碼查詢
  - 詢問前校內資安通報承辦人
  - 聯絡TACERT(臺灣學術網路危機處理中心)
    服務電話：(07)525-0211

- 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



- 忘記單位(學校)OID
  - 可至**國家發展委員會**網站(https://oid.nat.gov.tw/OIDWeb/)，點選「**組織及團體物件識別碼(OID)查詢**」進行查詢
  - 可來電(信)至教育機構資安通報平台詢問

- 搜尋學校關鍵字建議輸入學校全名
  - 例如:新北市立**國民中學



密碼查詢

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

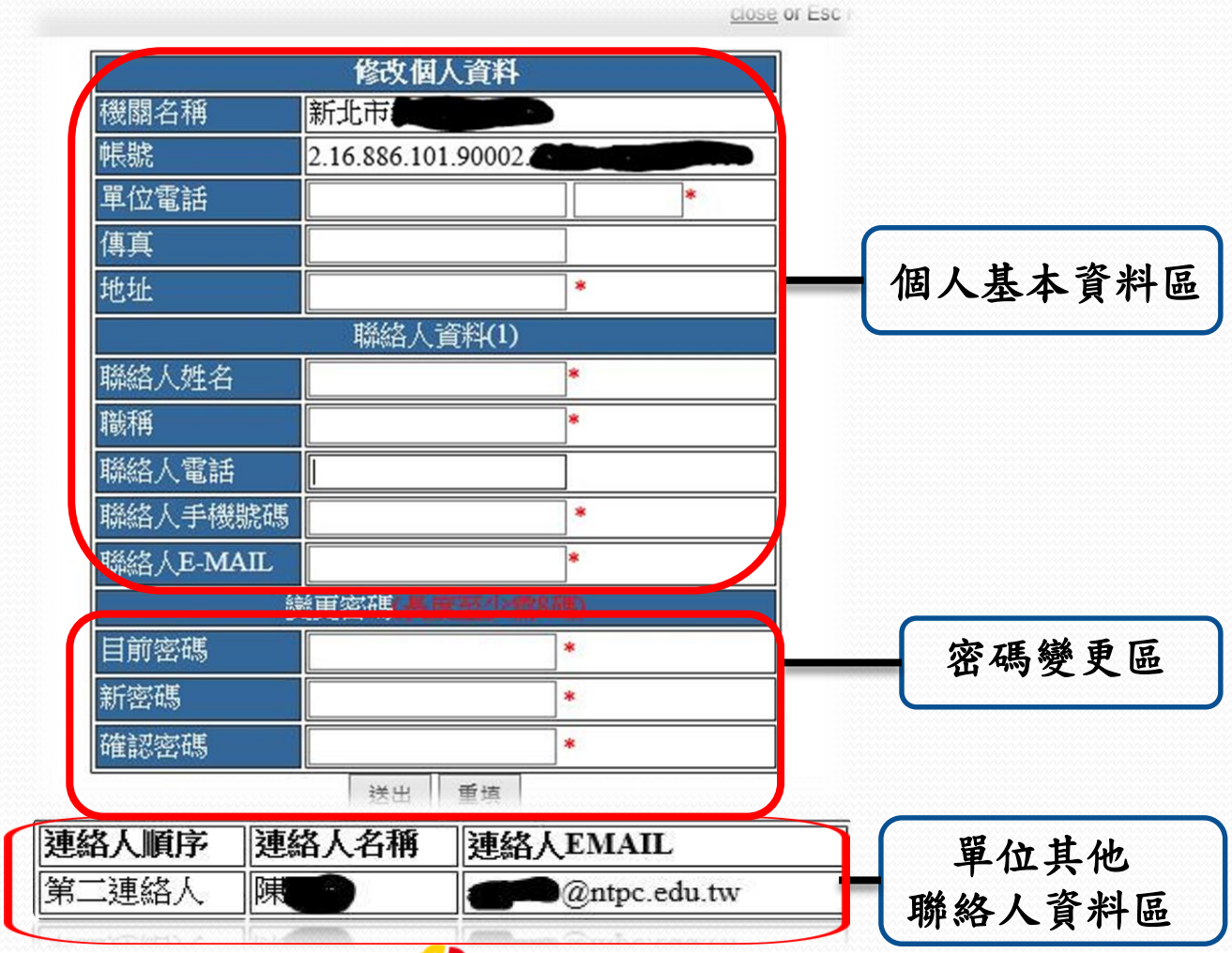
登入畫面


單位資訊
主管單位資訊
教育機構單位資訊
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:新北市[redacted]
使用者:[redacted]
主管機關:新北市教育網路中心
聯絡電話:02-8072-3456[redacted]
E-Mail:[redacted]
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
個人資料區
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
事件統計
演練資訊
事件單處理區
事件單編號
發佈時間
距通報時間(小時)
流程
Page 1/1
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：修改個人聯絡資料
- 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，可利用此功能完成通報應變
  - 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：管理聯絡人帳號開啟關閉
  - 事件附檔下載：事件單佐證表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/prog/index.php

修改個人資料


修改個人資料
機關名稱
新北市
帳號
2.16.886.101.90002.
單位電話
傳真
地址
聯絡人資料(1)
聯絡人姓名
職稱
聯絡人電話
聯絡人手機號碼
聯絡人E-MAIL
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
@ntpc.edu.tw
個人基本資料區
密碼變更區
單位其他
聯絡人資料區

帳號管理功能


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
事件統計
演練資訊
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
帳號管理說明文件下載

連線單位資安聯絡人異動

- 確保資安事件能夠即時通知與處理，資安聯絡人發生異動時，務必確保資安事件的處理業務能妥善完成交接
  - 資安聯絡人員至少需有二位，以建立代理人制度
  - 將主要負責人員填寫於第一、二聯絡人
  - 教育機構資安通報平台的帳號密碼進行交接
  - 登入教育機構資安通報平台於「修改個人資料」進行聯絡人資訊更新

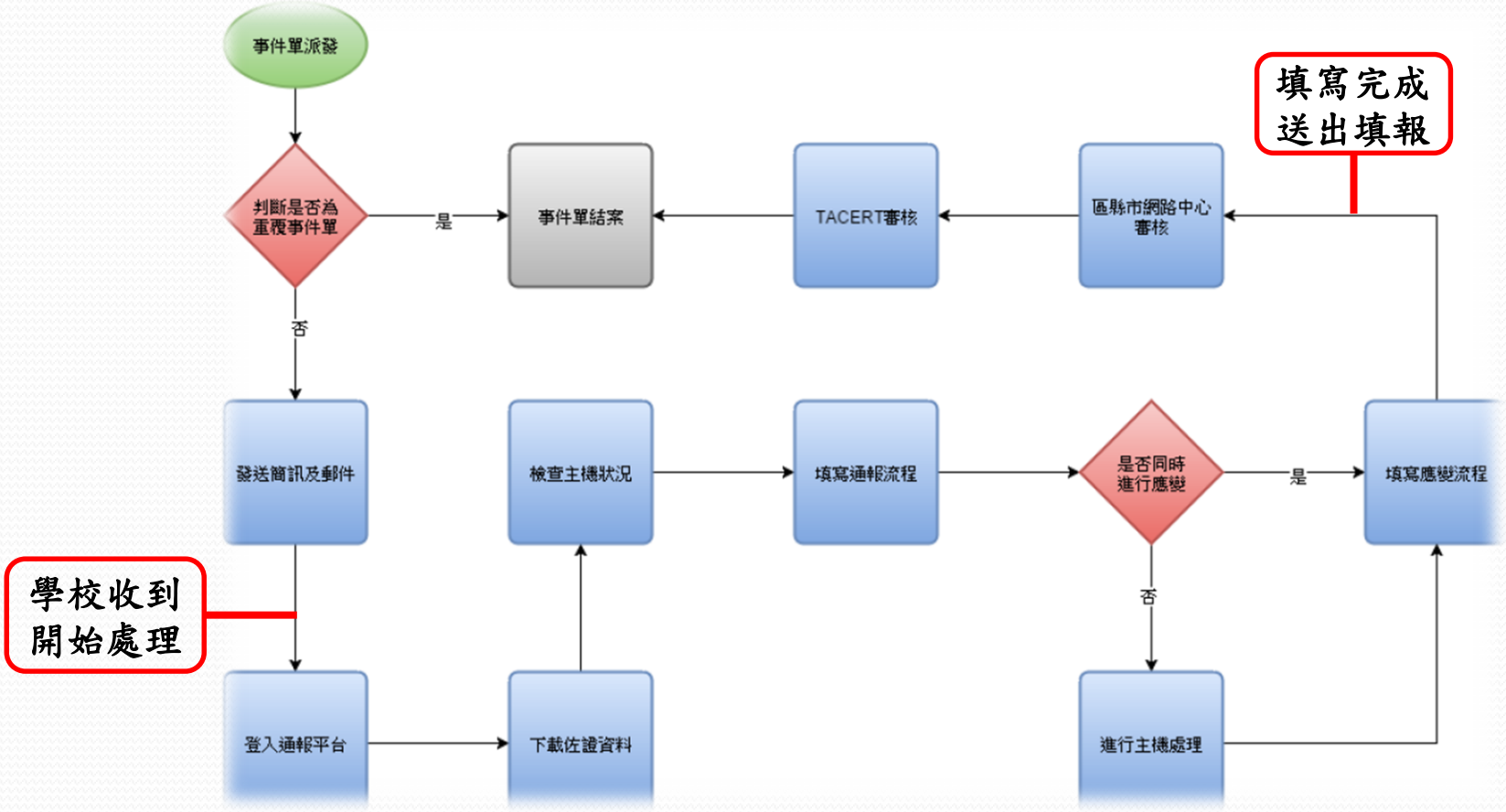
事件附檔下載

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

資安預警事件附檔下載

- 為方便資安預警事件處理，資安預警事件之佐證資料整合於資安預警事件介面中，可依EWA發佈編號搜尋

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
填寫完成送出填報
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
學校收到開始處理
否
登入通報平台
下載佐證資料
進行主機處理

通報應變規劃重點

- 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
- 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
- 請學校盡可能通報與應變同時進行
- 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

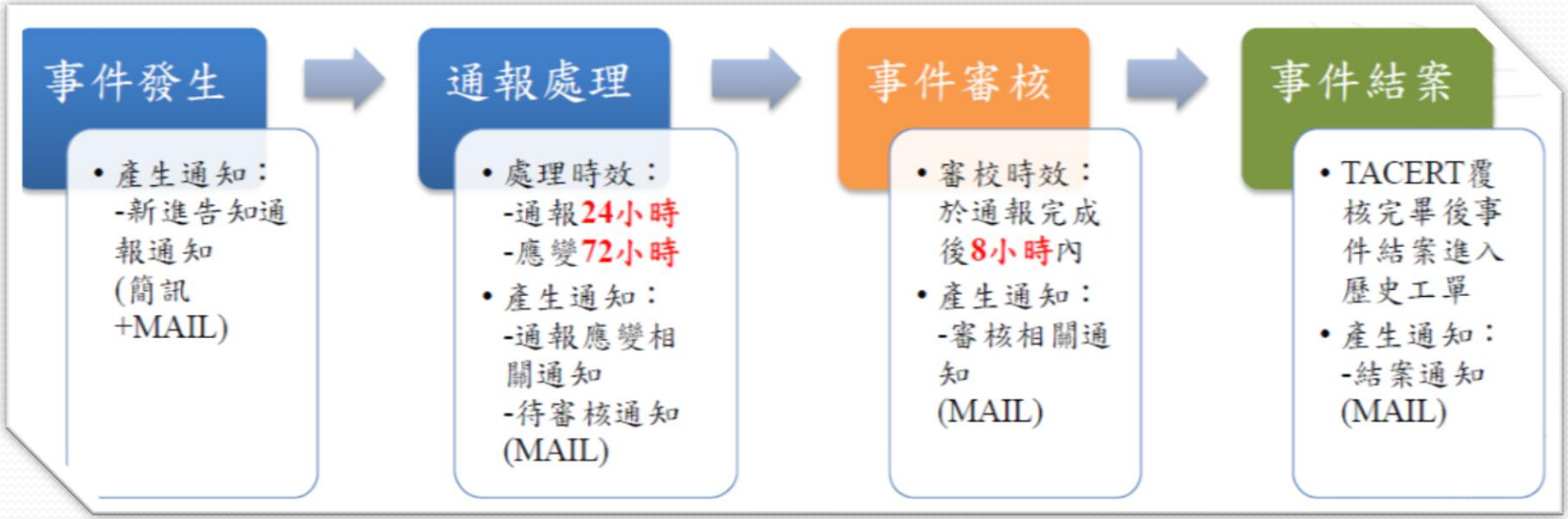
依資安等級區分

- 第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個小時通知
    - 事件單成立後72小時後每隔12個小時寄發逾時通知

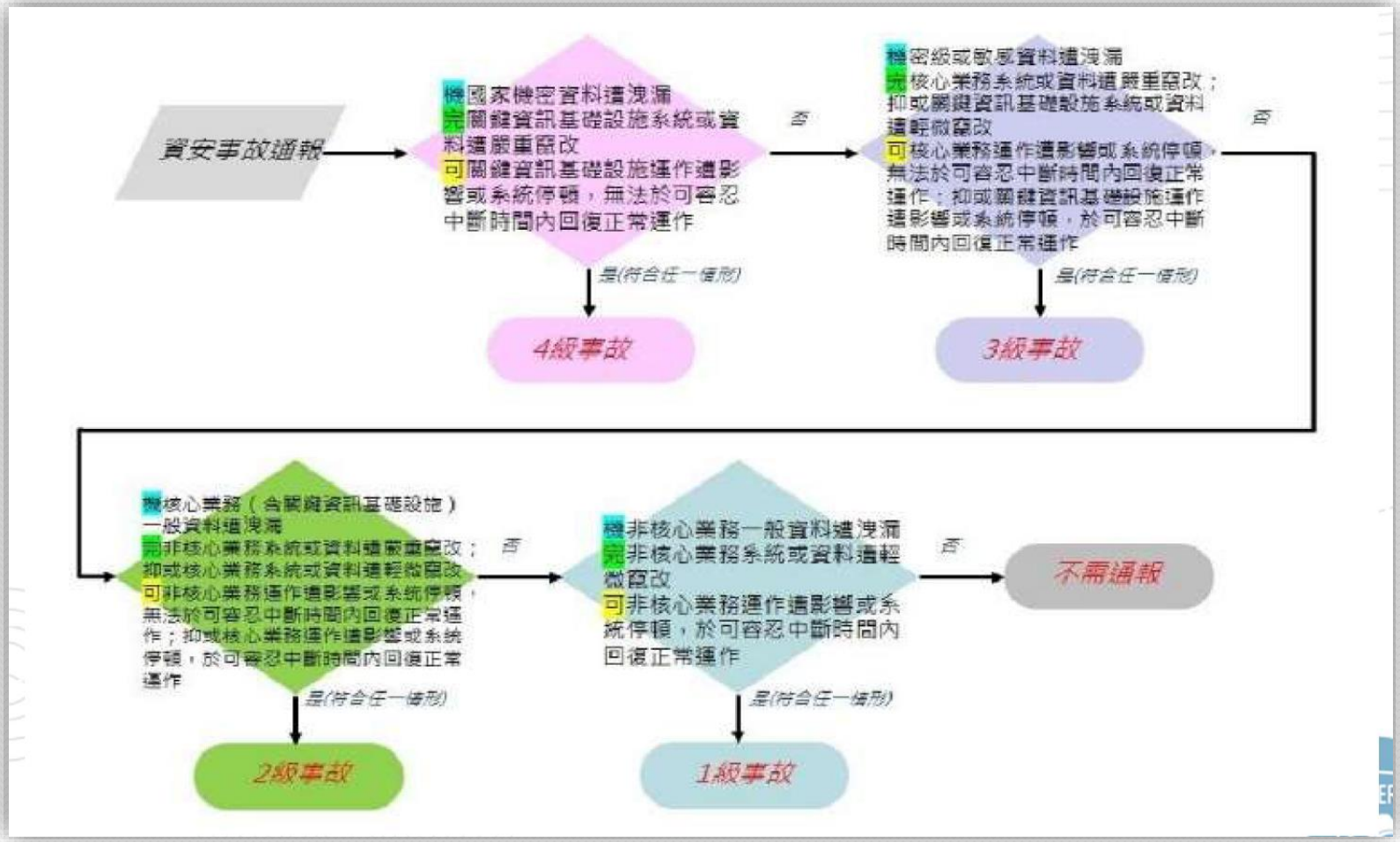
依資安等級區分

- 第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聯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個小時通知
    - 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)

事件等級評估流程


資安事故通報
機國家機密資料遭洩漏
完關鍵資訊基礎設施系統或資料遭嚴重竄改
可關鍵資訊基礎設施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
否
是(符合任一情形)
4級事故
機密級或敏感資料遭洩漏
完核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改
可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；抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作
否
是(符合任一情形)
3級事故
機核心業務（含關鍵資訊基礎設施）一般資料遭洩漏
完非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改
可非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；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作
否
是(符合任一情形)
2級事故
機非核心業務一般資料遭洩漏
完非核心業務系統或資料遭輕微竄改
可非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作
否
不需通報
是(符合任一情形)
1級事故

資通安全事件通報及應變辦法

第13條

特定非公務機關知悉資通安全事件後，應依下列規定時間完成損害控制或復原作業，並依中央目的事業主管機關指定之方式辦理通知事宜：

二、第三級或第四級資通安全事件，於知悉該事件後三十六小時內。

特定非公務機關依前項規定完成損害控制或復原作業後，應持續進行事件之調查及處理，並於一個月內依中央目的事業主管機關指定之方式，送交調查、處理及改善報告。

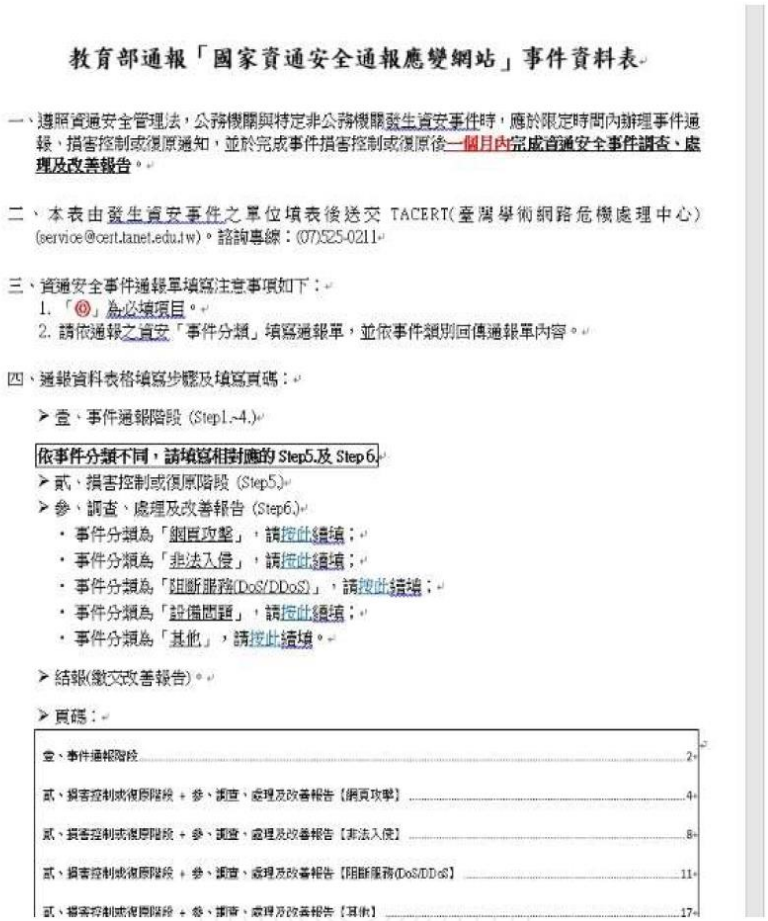
通報資安平台後之工作事項

- [填寫]資安事件改善報告(初稿)
- [填寫]教育部通報「國家資通安全通報應變網站」事件資料表

改善報告建議格式

依據資通安全管理法施行細則第8條:「本法第十四條第三項及第十八條第三項所定資通安全事件調查、處理及改善報告，應包括下列事項：

一、事件發生或知悉其發生、完成損害控制或復原作業之時間。
二、事件影響之範圍及損害評估。
三、損害控制及復原作業之歷程。
四、事件調查及處理作業之歷程。
五、事件根因分析。
六、為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。
七、前款措施之預定完成時程及成效追蹤機制。」，故事件調查處理改善報告，應包含上述旨揭內容。



教育部通報「國家資通安全通報應變網站」事件資料表

一、遵照資通安全管理法，公務機關與特定非公務機關發生資安事件時，應於限定時間內辦理事件通報，損害控制或復原通知，並於完成事件損害控制或復原後一個月內完成資通安全事件調查、處理及改善報告。

二、本表由發生資安事件之單位填表後送交 TACERT(臺灣學術網路危機處理中心)(service@cert.tanet.edu.tw)。諮詢專線：(07)525-0211

三、資通安全事件通報單填寫注意事項如下：
1.「◎」為必填項目。
2. 請依通報之資安「事件分類」填寫通報單，並依事件類別回傳通報單內容。

四、通報資料表格填寫步驟及填寫頁碼：

➢ 壹、事件通報階段 (Step1.~4.)

依事件分類不同，請填寫相對應的 Step5.及 Step6.

➢ 貳、損害控制或復原階段 (Step5.)
➢ 參、調查、處理及改善報告 (Step6.)
- 事件分類為「網頁攻擊」，請按此續填；
- 事件分類為「非法入侵」，請按此續填；
- 事件分類為「阻斷服務(DoS/DDoS)」，請按此續填；
- 事件分類為「設備問題」，請按此續填；
- 事件分類為「其他」，請按此續填。

➢ 結報(繳交改善報告)。

➢ 頁碼：

壹、事件通報階段 2
貳、損害控制或復原階段 + 參、調查、處理及改善報告【網頁攻擊】 4
貳、損害控制或復原階段 + 參、調查、處理及改善報告【非法入侵】 8
貳、損害控制或復原階段 + 參、調查、處理及改善報告【阻斷服務(DoS/DDoS)】 11
貳、損害控制或復原階段 + 參、調查、處理及改善報告【其他】 17

壹、事件通報階段

【壹、事件通報】通報階段	
◎ 填報時間：____年____月____日____時____分 填表人姓名： 填表人連絡電話： 填表人 Email： 填表人手機：	
Step1. 事件相關基本資料	
一、發生資通安全之機關聯絡資料	
◎ 機關(機構)名稱	【此欄由教育部填寫】
◎ 審核機關名稱	【此欄由教育部填寫】
◎ 通報人	【此欄由教育部填寫】
◎ 電話	【此欄由教育部填寫】
◎ E-mail	【此欄由教育部填寫】
◎ 是否代其他單位通報	■ 是，該單位名稱：國立○○大學 □ 否
◎ 資安事件調查廠商	Ex.中華資安國際
Step2. 詳述事件發生過程	
二、事件發生過程：	
◎ 事件發現時間:	____年____月____日____時____分
◎ 事件分類與異常狀況 (事件分類為單選項；異常狀況為複選項)	□網頁攻擊 □網頁置換 □惡意留言 □惡意網頁 □釣魚網頁 □網頁木馬 □網站個資外洩 □非法入侵 □系統遭入侵 □植入惡意程式 □異常連線 □發送垃圾郵件 □資料外洩 □阻斷服務(DoS/DDoS) □服務中斷 □效能降低 □設備問題 □設備故障/毀損 □電力異常 □網路服務中斷 □設備遺失 □其他：_____
◎ 事件說明及影響範圍	【請說明事件發生經過，如機關如何發現此事件、處理情形等】

貳、損害控制或復原階段 + 參、調查、處理及改善報告【其他】

Step5.及 Step 6.填寫說明：請依據「網頁攻擊」或「非法入侵」或「阻斷服務(DoS/DDoS」或「設備問題」或「其他」之類別，選填表格。

【貳、損害控制或復原】【其他】(應變處置階段)

Step5.請填寫機關緊急應變措施

五、完成損害控制或復原

◎ 保留受害期間之相關設備紀錄資料《複選》(最少選填一項，如未保留相關紀錄，請於「其他保留資料或資料處置說明」欄位說明

□ 已保存遭入侵主機事件檢視器《單選》

〈□1個月 □16個月 □6個月以上 □其他____〉

□ 已保存防火牆紀錄 〈單選〉

〈 □1個月 □16個月 □6個月以上 □其他____〉

□ 已保存未授權存在之惡意網頁/留言/檔案/程式樣本，共____個

□ 其他保留資料或資料處置說明【如未保存資料亦請說明】

◎ 事件分析與影響評估《複選》最少選填一項，如無對應分析評估結果，請於「影響評估說明補充」欄位說明 經分析已保存之紀錄，是否發現下列異常情形：

□ 異常連線行為【請列出異常IP與異常連線原因，如：存取後台管理頁面】

□ 異常帳號使用【請列出帳號並說明帳號權限，與判別準則，如：非上班時間帳號異常登入/登出】

□ 發現資料外洩情況【如：異常打包資料 請說明外洩資料類型/欄位與筆數，如：個人資料/機密性資料/非機敏性資料】

□ 影響評估補充說明【請填寫補充說明】

◎ 封鎖、根除及復原《複選》最少選填一項，如無對應處理方式，請於「應變措施補充說明」欄位說明

□ 移除未授權存在之惡意網頁/留言/檔案/程式，共____筆(必填)

□ 停用/刪除異常帳號(必填)【請說明停用/刪除之帳號，如無須移除，請填寫「無」】

□ 暫時中斷受害主機網路連線行為至主機無安全性疑慮

□ 重新建置作業系統與作業環境，完成日期_____

□ 惡意程式樣本送交防毒軟體廠商，共____個

□ 應變措施補充說明【請填寫補充說明】

◎ 應變處置綜整說明【請說明損害控制或復原之執行狀況】：

是否已完成損害控制或復原

□否，尚未完成損害控制或復原

□是，已完成損害控制

□是，已完成損害控制並復原

完成損害控制或復原時間：____年____月____日____時____分

【參、調查、處理及改善報告】【其他】(結報階段)

Step6. 資安事件結案作業【其他】

六、事件調查與處理：

◎ 受害資訊設備數量：電腦總計____臺；伺服器總計____臺；其他設備____總計____臺；

◎ IP位址(IP Address)(無；可免填)

外部IP：

內部IP：

◎ 網際網路位址（Web-URL）(無；可免填)：

◎ 作業系統名稱、版本：

□Windows系列 □Linux系列 □其他作業平台版本：

◎ 受害系統是否通過資安管理認證(ISMS)：□是 □否

◎ 資安監控中心(SOC)：□無 □機關自行建置

□委外建置，該廠商名稱：

◎ 受害主機是否納入SOC監控範圍：□是 □否

◎ 機關是否裝置資安防護設備：□是 □否(不須填寫資安防護類型)

學校端應變流程與工作事項

- 處理與修正事件問題
- 申請並執行弱點掃描與滲透測試作業
- 招開資安會議
- 擬定公告內容與配套措施
- 事件處理簡報
- 根因分析, 調整改善報告
- 繳交改善報告

告知通報事件單(INT&DEF)

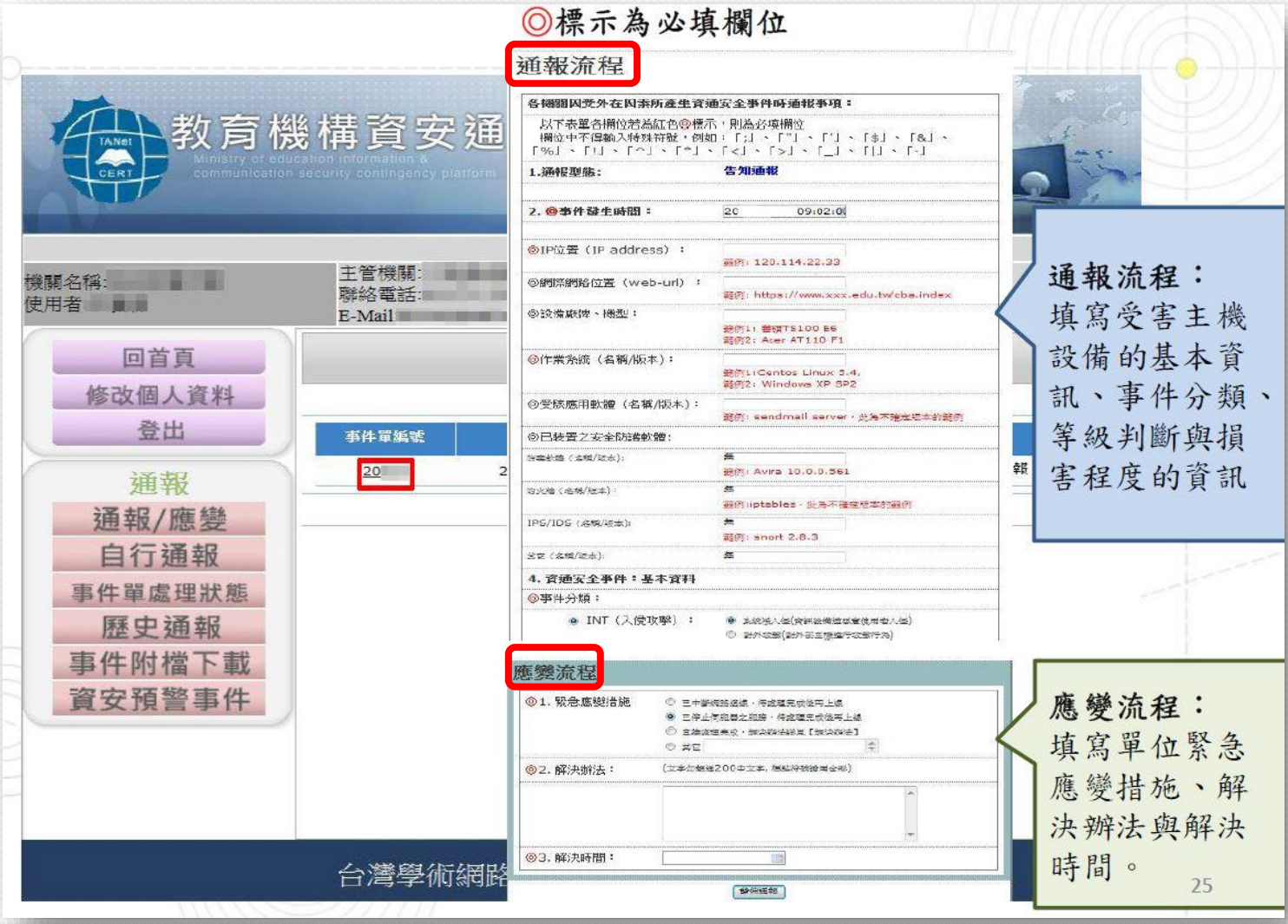
教育機構資安通報平台

事件類型:入侵事件警訊

工單編號:AISAC-166

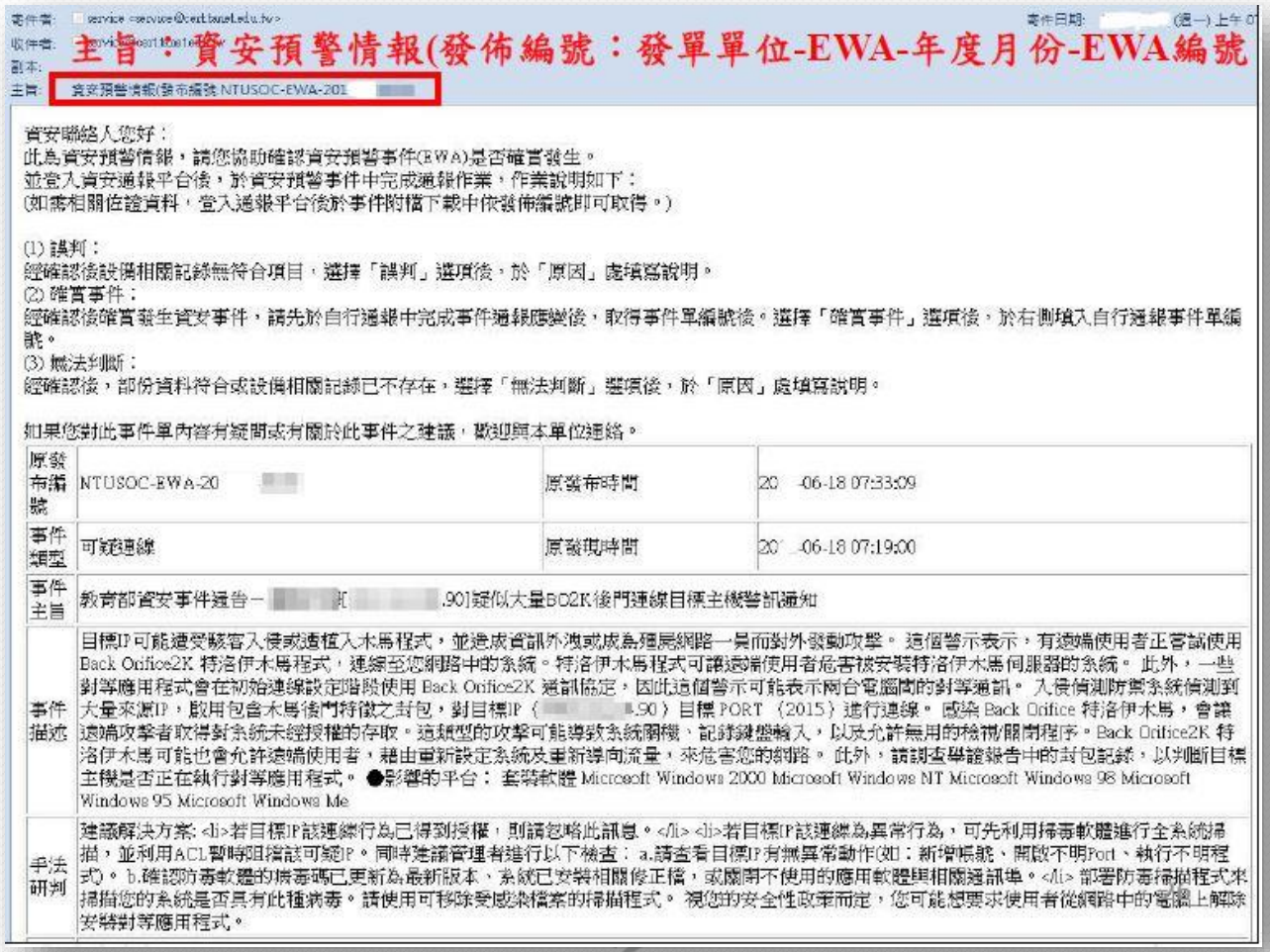
發單單位-事件類別-年度月份-流水編號

原發布編號	ICST-INT-	原發布時間	-10-0801:51:30
事件類型	對外攻擊	原發現時間	
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 201 '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
教育機構資安通
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
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
應變流程：
填寫單位緊急應變措施、解決辦法與解決時間。
25

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**



主旨：資安預警情報(發佈編號：發單單位-EWA-年度月份-EWA編號

主旨: 資安預警情報(發布編號 NTUSOC-EWA-201

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-20	原發布時間	20 -06-18 07:33:09
事件類型	可疑連線	原發現時間	20 -06-18 07:19:00
事件主旨	教育部資安事件通告－ 到 .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（ .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
- 由學校單位進行檢查、處理及填報作業，教育局進行追蹤作業
- 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，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


教育機構資安通
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
EWA編號
EWA事件單
EWA事件單狀態
誤判
確實事件
無法判斷
事件單編號
原因
送出
台灣學術網路
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

資安通報平台威脅情報說明

當收到資安情資後，經適當且有效的系統調查後，並未發現有直接或 間接證據可證明系統遭受到資安事件之威脅即可選擇 **TII(威脅情報)**。

建議您在進行系統調查時進行下列步驟：

(1)檢查系統或網路相關 LOG 資訊，查看是否有異常之處。

(2)利用如 TCPVIEW 工具軟體或 netstat 指令來查看系統是否有開啟可疑之服務或是否有可疑之來源連線。

(3)查看防火牆之連線記錄，確認是否有可疑之連線。

(4)如果有設置入侵偵測軟體（IDS），進行查看是否有惡意的連線行為。


4. 資通安全事件：基本資料
事件分類：
TII（威脅情報）：
經確認為威脅情報(說明)
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)
中繼站(主機成駭客之中繼站，接收惡意程式連線)
電子郵件社交工程攻擊(帳號遭盜用對外發動社交工程攻擊)
垃圾郵件(Spam)(資訊設備從事Spam Mail散播行為)
命令與控制伺服器(C&C)(主機疑似為駭客之Botnet C&C Server)
殭屍電腦(Bot)(資訊設備疑似成為駭客所控制之Botnet成員)
其它類型的入侵攻擊
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(網頁遭駭客置換)
釣魚網頁(主機遭駭客置入釣魚網頁)
個資外洩(主機遭個資外洩)
其它類型的網頁攻擊

資安通報演練說明

教育部資安通報演練計畫

- 檢驗「教育機構資安通報平台」所登錄學校**資安聯絡人資料之正確性**
- 檢驗教網中心通報反應及處理能力機制是否完善
- 測試學術機關(構)分組資安聯絡人聯絡管道是否暢通
- 測試學校於發現資安事件時，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

資安演練期程

- 演練資料整備作業:
  - 即日起至**110年9月3日止**，110年8月30日執行清查作業
  - 確認教育機構資安通報平台資安聯絡人資料更新
  - 演練學校請於演練資料整備期間內至「教育機構資安通報平台」登錄資料，學校依序至少應填列2名資安聯絡人，並檢查資安聯絡人資料是否正確並完成密碼更新

資安演練期程

- 資安通報演練作業:
  - 110年9月6日至110年9月10日
  - 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「資安演練事件通知單」；為避免與真實事件產生混淆，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演練單位，學校收到mail及簡訊通知後，於**1小時**內至教育機構資安通報演練平台完成事件通報及應變處理

教育機構通報演練平台網站

- 演練平台網址：https://drill.cert.tanet.edu.tw

演練模擬事件類型

演練模擬資安事件情境

模擬狀況編號	攻擊類型(事件類型)	攻擊子類型(事件子類型)	攻擊事件說明
1	DEF	勒索病毒	單位內主機被植入勒索病毒，系統資料遭到加密
2	DEF	密碼漏洞	單位內 IoT 設備未更改預設帳號密碼
3	DEF	個資外洩	單位人員誤將個人資料置於公開網路上，導致外部人員可下載相關資訊
4	DEF	惡意留言	發現單位電腦系統被植入惡意程式，並對外進行 APT 攻擊
5	DEF	網頁漏洞	單位內網站具有跨網站腳本攻擊(Cross-site scripting，簡稱 XSS)的漏洞，可能造成瀏覽者的危害
6	INT	對外攻擊	單位內電腦被入侵，並被利用來進行遠端桌面(RDP)暴力攻擊
7	INT	挖礦主機	發現單位電腦系統被入侵，並進行挖礦惡意行為
8	INT	BOT	單位電腦被入侵，而成為BOTNET所控制的Bot主機
9	INT	SPAM	單位網站被置入詐騙網頁，誘導使用者至釣魚網站
10	INT	對外攻擊	單位內電腦感染特洛伊木馬病毒而對外攻擊

・演練子類型會依前一年較常發生之類型進行更新，以演練計畫核定內容為主

資安通報聯絡人資訊

- 填報或行政諮詢:教育局吳先生，(02)8072-3456#518
- 技術或網路查詢:資安駐點工程師王先生，(02)8072-3456#534
- 技術問題或忘記密碼:臺灣學術網路危機處理中心郭先生，(07)525-0211

Q&A

謝謝

如有任何問題，歡迎與我們聯絡