教育部對臺灣大學

資安稽核與資安攻防演練作業

線上說明會

112年11月

電子公文

校級公文 112/10/17
1120095998

檔　　號：
保存年限：

教育部 函

地址：100217 臺北市中正區中山南路5號
承辦人：楊儒昇
電話：(02)7712-9119
電子信箱：ru.sheng0327@mail.moe.gov.tw

受文者：國立臺灣大學

發文日期：中華民國112年10月16日
發文字號：臺教資通字第1122704034號
速別：普通件
密等及解密條件或保密期限：
附件：教育部112年度對所屬公務單位之國立大專院校資安攻防演練計畫書

主旨：檢送「教育部112年度對所屬公務單位之國立大專院校資安攻防演練計畫書」1份，請查照。

說明：

一、請於資安攻防演練前推派主要及次要演練窗口至「教育體系資安攻防演練平台」(以下簡稱演練平台，網址：https://codc.moc.edu.tw/）註冊。

二、窗口註冊完成後請至攻防演練平台下載盤點清單並填寫，並於112年11月10日（週五）晚上24時前至演練平台上傳盤點清單。

三、若對資安攻防演練平台或計畫書內容有問題，請洽「教育體系資安檢測技術服務中心」，聯絡人資訊如下：

(一) 何小姐(03)571-2121#52885。
(二) 陳小姐(03)571-2121#31268。
(三) 呂小姐(03)571-2121#52891。
(四) 廖先生(03)571-2121#52861。

國立臺灣大學 公文系統驗證

電子公文

校級公文 112/08/23
1120077523

檔　　號：
保存年限：

教育部 函

地址：100217 臺北市中正區中山南路5號
承辦人：楊儒昇
電話：(02)7712-9199
電子信箱：ru.sheng0327@mail.moe.gov.tw

受文者：國立臺灣大學

發文日期：中華民國112年8月23日
發文字號：臺教資通字第1122703304C號
速別：普通件
密等及解密條件或保密期限：
附件：受稽機關稽核通知事項、受稽機關現況調查表、資通安全實地稽核項目檢核表(適用公務機關)

主旨：有關112年本部對國立臺灣大學資通安全稽核，受稽機關配合事項，請查照。

說明：

一、依本部111年4月18日臺教資(四)字第1112701315號函送資通安全稽核計畫(諒達)辦理。

二、貴機關業經選定為受稽機關，相關配合辦理事項如下：

(一) 稽核範圍:受稽機關資通安全維護計畫所包括之全機關及核心資通系統之各項資安管理政策、程序等。

(二) 作業時程:

1、技術檢測: 112年12月18日至19日。
2、實地稽核: 113年1月10日。

(三) 稽核團隊: 名單將另行通知。

(四) 實地稽核啟始會議計15分鐘，由貴機關進行資安推動情形簡報。

國立臺灣大學 公文系統驗證

大綱

1. 演練概述
2. 演練架構與內容說明
3. 網頁遭受攻擊處理方式
4. 教育部資通安全稽核
5. 資通安全弱點通報系統簡介
6. 問題討論

演練概述

概述

為了解教育體系**國立大專院校**之**對外資通系統網站**實際受攻擊時其**通報應變**與**內外部防護**實施情形，將仿造惡意人士於外部網路以（黑箱測試）發掘單位潛在弱點，本演練為教育體系量身規劃資安攻防演練專案，以增進教育體系資安防護能量。

目的

- 教育部為落實資通安全管理法、資通安全事件通報及應變辦法之規定，規劃每年所屬公務機關之**國立大專院校**選定為受演練對象，由教育體系資安檢測技術服務中心（TACCST）協助辦理資安攻防演練。
  - 強化所屬國立大專院校資安防護工作之完整性及有效性
  - 增進發生資安事件時之緊急應變、系統復原及協調管控等能力
  - 檢討防護改善降低資安風險

教育體系資安檢測技術服務中心
Taiwan Academic Network Center for Cyber Security Technology

演練架構及內容說明

實施對象與範圍

實施對象

全國立大專院校（共47間）

作業時程

- 演練作業：112年11月27日（一）至112年12月29日（五）之工作日，共5週
- 複測作業：113年1月8日（一）至113年1月26日（五）之工作日，共3週

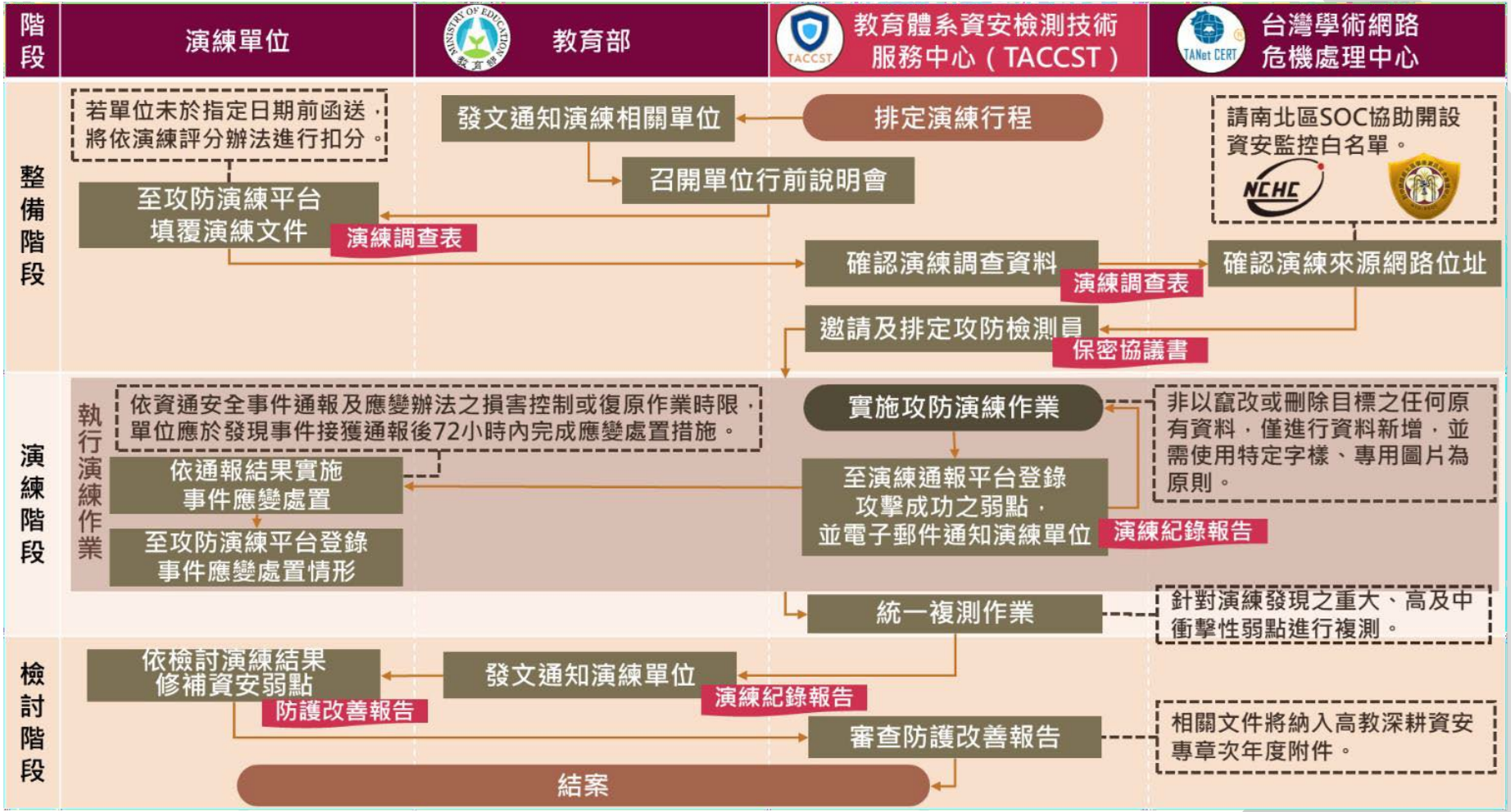
範圍標的

- 使用演練單位之**單位名義**、**DN**或**IP**，並可**透過外部Internet連線**之**服務型網頁**。
- 本年度計分實施範圍以行政、教學網站為主，不含括教學研究網站（如實驗室），所有發現皆實施演練通報。

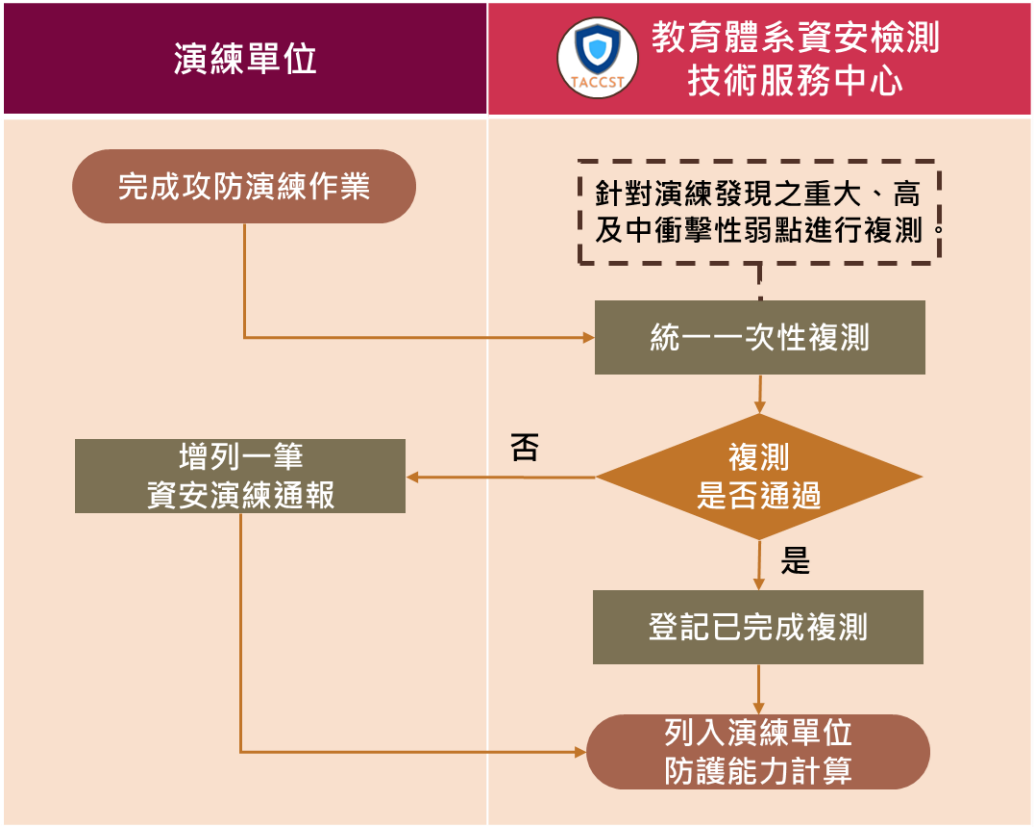
弱點演練項目

- 因應近期資安威脅，以納入最新版本之開放式網頁應用安全計畫（Open Worldwide Application Security Project, OWASP）類別之網站應用（Web Application）前10大項目為原則之資安弱點進行測試，實際演練機關資安防護與應變處理能力。
- 演練過程中為避免影響網站系統維運及人員社交爭議，不採用DoS、DDoS及社交攻擊等手法。

整體流程


階段
演練單位
教育部
教育體系資安檢測技術服務中心（TACCST）
台灣學術網路危機處理中心
整備階段
若單位未於指定日期前函送，將依演練評分辦法進行扣分。
發文通知演練相關單位
排定演練行程
請南北區SOC協助開設資安監控白名單。
召開單位行前說明會
至攻防演練平台填覆演練文件
演練調查表
確認演練調查資料
演練調查表
確認演練來源網路位址
邀請及排定攻防檢測員
保密協議書
演練階段
執行演練作業
依資通安全事件通報及應變辦法之損害控制或復原作業時限，單位應於發現事件接獲通報後72小時內完成應變處置措施。
實施攻防演練作業
非以竄改或刪除目標之任何原有資料，僅進行資料新增，並需使用特定字樣、專用圖片為原則。
依通報結果實施事件應變處置
至演練通報平台登錄攻擊成功之弱點，並電子郵件通知演練單位
演練紀錄報告
至攻防演練平台登錄事件應變處置情形
統一複測作業
針對演練發現之重大、高及中衝擊性弱點進行複測。
檢討階段
依檢討演練結果修補資安弱點
發文通知演練單位
演練紀錄報告
防護改善報告
審查防護改善報告
相關文件將納入高教深耕資安專章次年度附件。
結案

複測流程


演練單位
教育體系資安檢測
技術服務中心
TACCST
完成攻防演練作業
針對演練發現之重大、高
及中衝擊性弱點進行複測
統一一次性複測
否
增列一筆
資安演練通報
複測
是否通過
是
登記已完成複測
列入演練單位
防護能力計算

提繳資料

提繳資料

- 每單位由一名窗口註冊「教育體系資安攻防演練平台」，以提繳調查清冊及回覆應變處理情形（計中負責）。
  - 攻防演練平台預定於112年10月4日（三）開放註冊，相關註冊與使用方式將由教育部後續函文之攻防演練實施計畫中說明。
  - 清冊提繳至112年11月13日（一）晚上24點止，並採最後一次繳交時間計算。
- 調查清冊填寫範例：

項次	對外網路位址IP	名稱	防護分級	業務單位	網頁位址（URL/服務埠）	備註
範例	123.123.123.123; 123.123.123.125-126; 123.123.123.128;	國立檢測大學招生系統	中	學務處	https://www.test.edu.tw	置於國立演練大學之備援機

通報及應變作業

通報方式

- 每單位至多可於攻防演練平台登記2名通報接收窗口（計中負責）。
- 檢測中心將以**電子郵件**為主，**簡訊**為輔方式通知演練單位窗口。
  - 如因單位填覆資訊填寫錯誤造成演練期間警訊發送錯誤，將以檢測中心第一次發出警訊時間做為分數計算標準，造成通報時間落差由單位承擔。

應變處理作業

- 單位需於接獲通報起72小時內（日曆天）至攻防演練平台回覆應變處理情形（計中負責）。

注意事項– 基本防護作業

演練實施前

- 請演練單位自行查檢項目：
  - 重新檢視防火牆相關設定是否合宜
  - 檢視測試網站與帳號等已確實關閉或移除
  - 確認內部使用網站未暴露於網際網路

演練實施中

- 演練過程不會刻意針對網站進行破壞性測試，惟為避免發生非預期狀況，導致系統發生當機或資料毀損等情事，演練單位於演練期間應做**系統備援**與**定期（建議每日）備份重要資料**等防護措施。

- 演練單位可利用防火牆、入侵防禦系統及防毒軟體等偵測工具，**檢視網路、系統有無異常狀況**，並維持網站日常連線狀態及日常防護作業，勿刻意阻撓資安攻防演練。

演練單位重點時程

期程	作業事項	演練單位窗口注意事項
112年9月20/25/27日	了解作業內容	參與說明會、了解演練作業內容。
112年10月4日（三）	開放平台註冊	演練單位窗口註冊教育體系資安攻防演練平台、提繳清冊。
112年11月13日（一） 晚上24:00	提繳清冊截止	繳交系統清冊至攻防演練平台。
112年11月27日（一）至 112年12月29日（五）	演練作業	留意電子郵件或簡訊之事件通報資訊，並於接獲通報後72小時內填覆處理情形。
113年1月8日（一）至 113年1月26日（五）	複測作業	留意電子郵件或簡訊之事件通報資訊。

各單位準備工作

各單位事前準備事項

- 一台備用主機或VM主機。
- 準備靜態網頁。
  - 可參考中英文網站製作平台
- 將靜態網頁放在備用主機或VM主機

目前本校各單位網站管理方式可分為以下幾種：

- **網站伺服器自行管理**
  - ✓ 放置於單位內的主機
  - ✓ 放置於委外廠商公司內的主機
  - ✓ 放置於雲端（AWS）
- **網站伺服器於計中VM租賃區**
- **網站伺服器於計中Homapge主機**

網站伺服器自行管理

- 單位準備一台備用主機，放置靜態網頁。
- 接獲通報時，原主機網路斷線或關機，備用主機改為原IP。

計中VM租賃區

- 如單位網站在計中VM租賃區。
- 單位事先準備靜態網頁，建議放在計中Homepage網頁空間。
- 接獲通報時，通知計中VM管理人員，指向各單位之Homepage靜態網頁。

Homepage網頁

- 如單位網站在計中Homepage網頁。
- 請準備靜態頁面。
- 接獲通報時，重新上傳靜態頁面至Homepage 。

網頁遭受攻擊處理方式

處理流程

資安事件

通知

計中

通知

各單位
資安窗口

通知

72小時內

網頁
負責人

修補網頁漏洞

置換靜態網頁

各單位
資安窗口

一小時內

填寫「資通安全事件報告單」
並將電子檔寄回計中。
（scyteam@ntu.edu.tw）

表單下載連結：

教育部資通安全稽核

教育部技術檢測-實施對象與範圍

- **實施對象**

  國立臺灣大學

- **作業時程**

  技術檢測：112年12月18日（一）至112年12月19日（二），共2天

- **檢測項目**

  物聯網設備安全檢測

  使用者電腦安全檢測

物聯網設備安全檢測

- **針對智慧裝置如：**

  網路攝影機、門禁設備、網路印表機、無線網路基地台、路由器、環控系統、或其他物聯網設備 ，透過網路或臨機操作方式執行檢他物聯網設備 ，透過網路或臨機操作方式執行檢測。

使用者電腦安全檢測

- 使用NMAP網路工具，掃描臺灣大學140.112.X.X網段的使用者電腦。
- 依據掃描結果抽樣可能存在風險的 5 台高風險使用者電腦，進行人工及自動化工具的深度檢測。
- 盤點的目的，抽檢到的單位要協同帶領教育部人員實地查看。

教育體系資安檢測技術服務中心

文件名稱	使用者電腦安全檢測清單	機密等級	密
文件編號	TACCST-B-02-09-07	版次	V1.1

※提醒檢測當天請維持使用者電腦開機

使用者電腦安全檢測清單						
IP 網段						
編號	網路位址 IP	處室	職稱	姓名	所在地點	作業系統
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
總臺數			台			

※請自行增刪欄位。

教育部實地稽核-實施對象與範圍

- **實施對象**

  國立臺灣大學

- **作業時程**

  實地稽核：113年1月10日（三），共1天

- **查核項目**

  臺灣大學擁有核心系統之單位（計資中心、教務處、學務處）

  資通系統盤點清單（計資中心預計11月底完成全校系統盤點檢核）

政府組態基準
資通安全弱點通報
系統簡介

資安責任等級

- 臺大資安責任等級B
  - 資安法應辦事項要求 B級機關 需導入 GCB 和 VANS

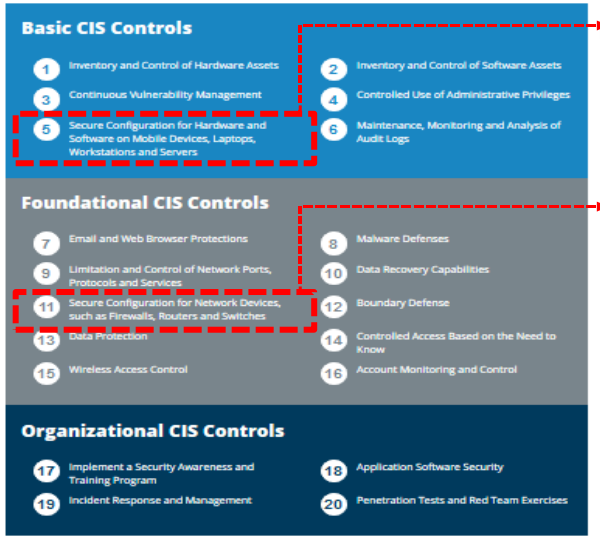
政府組態基準GCB簡述（一）

- 政府組態基準（Government Configuration Baseline，以下簡稱GCB）目的在於規範資通訊終端設備（如：個人電腦、伺服器主機及網通設備）的一致性安全設定（如：密碼長度、更新期限等），以降低成為駭客入侵管道，進而引發資安事件之疑慮。

1. 發展一致的安全組態設定
2. 提升政府機關資通訊終端設備使用安全性

政府組態基準GCB簡述（二）

- 美國網路安全協會於2019年公布CIS Controls（V7.1）文件中，在Basic Controls與Foundational Controls項目皆強調安全設定（Secure Configuration）之重要性。



5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

相關資安弱點：

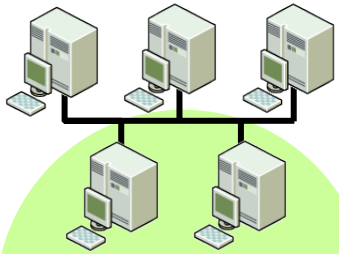
- 不當的預設組態設定
- 預設帳號與弱密碼
- 預設啟用非必要服務

政府組態基準GCB簡述（三）

情境：使用者不小心將含有惡意程式的隨身碟插入公務電腦中

禁止可攜式媒體的Autoruns與自動播放功能

強制作業系統進行安全性更新以保持最新狀態

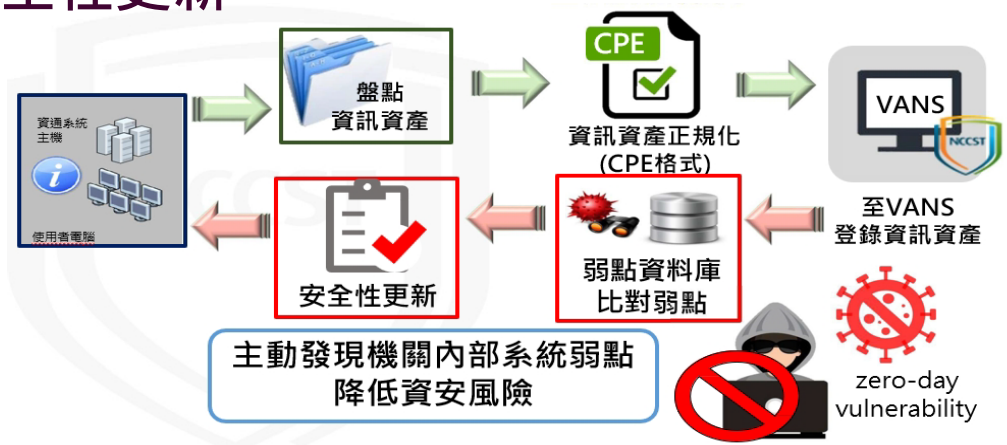


設定禁止電腦回應多點傳送與廣播類型的封包

降低遭受惡意程式感染之機率

資通安全弱點通報VANS（一）

- 政府機關資安弱點通報機制（Vulnerability Alert and Notification System, VANS）結合資訊資產管理與弱點管理，將資訊資產清冊與弱點資料庫比對，以掌握所使用資訊資產是否存在已公開揭露之弱點資訊，並依風險情形完成安全性更新。



資通安全弱點通報VANS（二）

- 資訊資產涵蓋範圍

各責任等級應辦事項（技術面）

責任等級		安全性檢測		資通安全監控管理機制 ASOC	政府組態基準 GCB	資通安全弱點通報機制 VANS	資通安全防護					
		網站安全弱點檢測	系統滲透測試				防毒軟體	網路防火牆	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	○	○	○	○	○	○	○	○	○
B	公務機關	1次/年	1次/2年	○	○	○	○	○	○	○	○	
C	公務機關	1次/2年	1次/2年			○	○	○	○			

本校現況：目前導入GCB與VANS單位「計資中心、教務處、學務處」。

未來規劃：經資產盤點擁有「核心資通系統」之單位先行導入GCB與VANS並逐步推動至全校

資通安全委員會-應辦事項清單

工作	優先順序	開始日期	到期日
全校一級單位-資安窗口指派	高	2023年5月22日	2023年5月31日
全校一二級單位主管與校聘人員資通安全教育訓練時數-每人3小時	高	2023年6月1日	2023年9月1日
舉辦全校資通系統與IOT設備盤點說明會	高	2023年7月1日	2023年7月31日
全校資通系統與IOT設備盤點	高	2023年7月1日	2023年8月30日
全校一二級單位網頁統一BCP測試演練作業	高	2023年9月1日	2023年11月30日
全校GCB+VANS軟體推廣安裝	一般	2023年12月1日	2024年12月31日

問題與討論

線上簽到表

相關連結：

- Homepage介紹

  https://www.cc.ntu.edu.tw/chinese/services/serv_i01.asp

- 中英文網站製作平台（網頁遭置換緊急應變措施）

  https://webpageprod.ntu.edu.tw/emergencyprocedure.htm?

- 計中靜態網頁範例

  https://homepage.ntu.edu.tw/~webpage/emergy/Default.html

- 計中靜態網頁範例

  https://www.youtube.com/watch?v=CtZvgktmaCw

⚠ 靜態網頁中一定要有聯絡資訊 ⚠