



教育部



NAR Labs 財團法人國家實驗研究院
國家高速網路與計算中心
National Center for High-performance Computing



資訊安全宣導列車「惡意程式攻擊」課程

為培養臺灣學術網路 (TANet) 之學校資安人員資安的觀念及區縣網資安人員處理資安事件能力，讓資安人員者能夠熟悉與掌握曾經發生過的資安事件，經由實務體驗課程得以認知資訊安全相關危害及如何防範，以減少相似類型的資安事件再次發生機會，期望透過資安列車宣導，建立資安危機意識，達到強化資安意識。

壹、辦理單位

主辦單位：教育部

承辦單位：財團法人國家實驗研究院國家高速網路與計算中心

協辦單位：國立臺灣大學計算機及資訊網路中心

貳、課程介紹

「惡意程式攻擊」課程將探討學術網路常見的惡意程式態樣，透過實際探討常見的惡意程式種類及特性，針對感染的原因進行分析且了解程式感染流程，並搭配實作方式體驗惡意程式攻擊手法，讓學員理解惡意程式的概念與技術，最後藉由資安事件的案例進行防範機制探討。

參、課程日期

110 年 8 月 26 日(四) 上午 9:30 至下午 4:30

肆、參加資格及名額數

- 一、北區/縣市網路中心：臺北區域網路中心(1)、臺北區域網路中心(2)、新北市教育網路中心、臺北市教育網路中心等四中心；各中心 2 名資安人員。
- 二、北區/縣市網路中心邀請各轄下學校 20 名資安人員(各校 1 名)。
- 三、名額有限，採優先報名順序參加，額滿為止。

伍、課程方式

【實體課程】名額：25 人 / 臺灣大學計算機及資訊網路中心 電腦教室 206 室

【視訊課程】名額：65 人 / 系統：Cisco Webex Meetings

陸、報名方式

- 一、報名網址：<https://forms.gle/UuGqWHrr6gzQg8s9A>
- 二、報名至 8 月 23 日(一)中午 13:00 截止；若場次額滿將提前結束。
- 三、依報名單位和姓名實際全程參與課程，將提供課程時數共 6 小時，請於報名表單擇一勾選「公務人員時數 / 教師研習時數 / 課程證書」
- 四、協辦單位於 8 月 24 日(二)mail 課程提醒事宜和視訊課程連線代碼，至報名聯繫信箱。



資訊安全宣導列車「惡意程式攻擊」課程

柒、課程議程

時間	課程內容	
09:10~09:30	課程一	現場報到 / 視訊連線
09:30~10:50		惡意程式簡介
11:00~12:00		術網路常見之惡意程式態樣
13:10~13:20	課程二	課程準備 / 視訊連線
13:20~14:50		惡意程式攻擊手法分析實作
14:50~16:10		案例討論:惡意程式防範探討
16:10~16:30		Q & A / 賦歸

【說明】課程一、二全程參加者；將提供課程時數 6 小時。

捌、課程師資

財團法人國家實驗研究院國家高速網路與計算中心 / 資訊安全科技組 講師群

玖、注意事項

一、實體課程

- 1、考量疫情期間「實體課程」請配合全程配戴罩、進入教室需量測體溫，並保持室內 1.5 公尺社交距離，座位以間隔坐為原則。
- 2、「實體課程」僅提供午餐並規劃用餐區，請配合工作人員指示，並自備環保餐具、杯等；教室外備有飲水機，請自取。
- 3、臺大校園目前尚有管制，入校須持訪客證，才可進入；訪客證將於報名截止後，mail 提供 (配合學校政策作業，若已解封則無提供)。建議由距離臺大計中較近之校門「語文中心門或辛亥門」進入。詳細管制資訊，請參閱臺大網頁 (https://ga.ntu.edu.tw/main_ch/docDetail/55/55/28445/1100513)。

二、線上課程：限報名視訊課程學員參加

- 1、課程中請學員全程關閉麥克風。
- 2、登入名稱請設定報名之「單位/姓名」；待核准參加課程。
- 3、課程中如有任何疑問，可至提供之線上平台提問；將由講師群協助處理，或於課程結束前進行 Q&A 討論。

三、課程講義電子檔，徵詢講師同意後提供；若涉及版權或機敏資料於課程後則不對外公開。

四、主辦單位保有最終修改、變更、活動解釋及取消本活動之權利，若有相關異動將另行通知。

五、聯繫窗口 E-mail：asoc_support@narlabs.org.tw

