臺灣學術網路各連線單位

因應第三方機關進行資安調查作業參考指引

一、緣起及目的

近來臺灣公私各部門屢遭駭客攻擊，部分單位淪為駭客利用而不自知，故現今資安防護不再僅賴各連線單位審慎因應，更需各相關單位密切合作。各單位若能透過資訊安全調查合作，必能防範潛在資安威脅，進而提升國家資通安全防護水準。為因應各第三方單位(如檢調機關)進入校園進行資安事件調查需求，並使臺灣學術網路所轄各連線單位協助第三方機關進行資安事件調查作業有所依據。教育部規劃「臺灣學術網路各連線單位因應第三方機關進行資安調查作業參考指引」(以下稱本指引)，以有效確保各連線單位之權利與明確協助第三方機關進入校園調查之作業。

二、適用對象

臺灣學術網路轄下各連線單位。

三、 適用範圍及限制

(一)適用範圍

當各連線單位收到第三方機關校園資安事件調查需求公文時，依該連線單位相關作業依據(如 XX 大學處理檢警調單位進入校園執行採證等公務作業流程)辦理，若無相關依據時得參考本指引進行協助資安調查處理（指引圖如附錄)，並可向教育部申請諮詢服務或相關技術支援。

(二)適用限制

本指引所提之資安調查，僅限於第三方機關進入校園，進行非涉及法律規範資安取證作業，不適用於檢調單位依相關法令提出調查時之需求。

四、作業內容及程序

各相關單位依據本指引進行資安處理時之作業內容如下：

(一)教育部

教育部接獲第三方機關公文通知時，在初步確認該事件影響範圍及其危害程度後，指派相關資安團隊提供各連線單位協助與諮詢服務。

(二)第三方機關

1. 當第三方機關有進入校園進行資安事件調查之需求時，請第三方機關敘明依據後正式函文給各連線單位。

2. 當各連線單位告知第三方機關需教育部協助時，請第三方機關正式發文至教育部，以利指派相關資安團隊協助各連線單位。

3. 第三方機關與資安團隊召開「行前會議」時，配合事宜:

   (1) 為使會議有效進行順利，請第三方機關至資安團隊所在地進行相關討論。

   (2) 第三方機關需提供案情說明之文件與佐證資料(含電子檔)給資安團隊參考，以利資安團隊向各連線單位進行說明。

   (3) 第三方機關需說明案情嚴重性、有無危及國安、危害等級、影響範圍與案情調查之必要性，以利資安團隊協助各連線單位進行損害控制。

   (4) 為增進資安事件處理效率，請第三方機關說明調查當日之蒐證指引、使用之蒐證設備、工具與指令等。

4. 第三方機關至各連線單位進行資安調查作業時，配合事宜:

   (1) 第三方機關需有資安團隊、各連線單位資訊相關人員陪同始得進入校園。

   (2) 第三方機關當日所調查取證之資料(含電子檔)應提供一份給資安團隊存查。

(3) 第三方機關需自行準備進行取證之相關設備器材。

(4) 第三方機關之取證人員應提供相關證件作身分認證，並且需配合各連線單位之要求簽署保密協約。

(5) 第三方機關需於調查取證作業完成後，應提供資安調查書面報告(含電子檔)給教育部、資安團隊與各連線單位存查。

(三)資安團隊

1. 資安團隊可視案件需求，評估是否與第三方機關召開「行前會議」。
2. 資安團隊協助各連線單位進行資安調查諮詢，事先準備工作：

   (1) 瞭解受查設備之系統資訊與規格。

   (2) 整理相關單位之承辦人員聯絡方式。

   (3) 取得各連線單位所提供之可調查日期。

   (4) 協調召開「行前會議」之時間。

   (5) 詢問各連線單位與其所屬區或縣（市）網路中心參與「行前會議」之意願。

3. 資安團隊與第三方機關召開「行前會議」後，應通知各連線單位及其所屬之區或縣（市）網路中心調查日期。
4. 資安團隊於調查當日現場可提供各連線單位諮詢服務，不進行取證相關作業。

(四)區或縣（市）網路中心

1. 本指引所述之區或縣（市）網路中心係各連線單位所介接之 2 線單位，一般國中小及市立高中職為縣（市）網路中心，各大學及國立高中職以上為區網路中心。

2. 當區或縣（市）網路中心接獲轄下各連線單位之請求協助通知時，得視需要派員參與調查作業。

3. 當調查完畢後，區或縣（市）網路中心應對各連線單位進行後續資安關懷，以增進各連線單位資安防禦能量。

(五)各連線單位

1. 當各連線單位接獲第三方機關之公文通知時，可向教育部申請提供協助或自行處理第三方機關調查事宜。

2. 當各連線單位資安調查需教育部提供協助時，請配合以下事宜：

   (1) 請各連線單位提供受查設備之相關資訊與可前往調查日期給予資安團隊參考。

   (2) 各連線單位可得視需要派員前往參與第三方機關與資安團隊召開之「行前會議」。

   (3) 調查當日所取證之資料如為機敏資訊，各連線單位需準備保密協約文件，請提供第三方機關之取證人員填寫。

附錄

臺灣學術網路各連線單位
因應第三方機關進行資安調查作業參考指引圖