TWCERT/CC 資安 Q & A

1.0 版

107 年 11 月 7 日

聲 明

本文件之交通燈號協議 (Traffic Light Protocol, TLP)為白色燈號 (TLP: WHITE)，無揭露限制，為可對外公開之內容。當資訊具有最小或沒有可預見之誤用風險時，資料可以被標註為白色燈號，透過公開發布之規則即可讓此份文件對外發布。接收方取得此份資料時，透過一般發布資訊之流程，亦可對外公開此資訊。

(一) 基本認知

什麼是資訊安全？

資訊安全是運用一整套適當的控制措施，確保資訊資產受到妥善的保護，避免因人為疏失、蓄意或天然災害等因素，導致遭竊、不當使用、洩漏、竄改或破壞。

資訊安全的基本內容包含機密性、完整性與可用性：

1. 機密性 (Confidentiality)：資料不得被未經授權之個人、實體或程序所取得或揭露的特性。
2. 完整性(Integrity)：對資產之精確與完整安全保證的特性。

(i) 可歸責性 (Accountability)：確保實體之行為可唯一追溯到該實體的特性。

(ii) 鑑別性 (Authenticity)：確保一主體或資源之識別就是其所聲明者的特性。鑑別性適用於如使用者、程序、系統與資訊等實體。

(iii) 不可否認性 (Non-repudiation)：對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。

3. 可用性(Availability)：已授權實體在需要時可存取與使用之特性。

(二) 什麼是資安事件?

資安事件係指任何可能威脅系統或其資訊安全之活動。駭侵事件係指系統或其資訊安全已確實受損，相關案例包括由電腦網絡取得資訊、網頁遭置換，或是線上服務的可靠性遭到降級。

(三) 什麼是網路攻擊?

網路攻擊是透過網路空間，故意操控、破壞、降級或摧毀電腦、網路或儲存其中的資訊之行為，並嚴重影響國家安全、穩定及經濟繁榮。

(四) 什麼是電腦病毒？

答：1986 年，可令個人電腦的正常運作受到影響的有害程式首次被人發現，被稱之為電腦病毒。為何這些有害程式被稱為電腦病毒？因為電腦病毒與生物病毒(例如：H5N1)有很多相似之處：

1. 兩者均需要貯存在一個主體內。就電腦病毒而言，主體通常指受感染的檔案 / 磁碟。
2. 兩者均可自行衍生，由一個主體感染另一個主體。最後，兩類病毒均會對主體造成損害。

電腦病毒造成的破壞主要是造成干擾 (例如： 影響滑鼠 / 鍵盤)、刪除硬碟機的檔案、影響硬碟機的格式，以及破壞基本輸入輸出系統的數據；1995 年起出現的「巨集病毒」，則是透過電腦用戶之間的文件交換，迅速擴散藏於文件中的病毒。儘管如此，只要我們採取適當的防護措施，電腦受病毒感染的機會還是可以避免或減輕。

(五) 十項基本資安要訣

1. 使用防毒軟體

防毒軟體的功能，在於保護您的電腦避免被已知的電腦病毒感染，導致電腦遭駭或資料損毀。然而道高一尺魔高一丈，隨著電腦病毒日新月異，防毒軟體也因此需要時時更新。請檢視您的防毒軟體公司網站，看看是否有病毒樣本介紹，並下載更新程式。

2. 成為負責任的網路公民

凡使用網際網路服務者，都是網路公民。一如生活中的一般公民，網路公民也有其責任：維護資訊安全，遵守網路禮節，並尊重相關法令。

3. 不要開啟來路不明的電子郵件

刪除來路不明的電子郵件。小心檢視電子郵件的附加檔案，尤其是.exe 檔—即便您知道是誰寄送檔案給您。有些檔案會散播電腦病毒，有些則會永久損毀檔案並傷害電腦和網站。請不要轉寄您不全然確定附加檔案安全的電子郵件。

4. 定期備份電腦檔案

您家中所有的電腦均應另行以光碟或 USB 儲存備份。

5. 定期下載並安裝防毒軟體更新程式

作業系統和應用程式軟體常有安全漏洞，故須定期檢視防毒軟體廠商網站，下載並安裝防毒軟體更新程式，以及時修補安全漏洞。

6. 定期檢視電腦安全

全面性電腦安全檢查最少應一年執行兩次。

7. 不使用電腦時請斷線

網際網路是收發訊息的雙向管道。若不使用網際網路時，建議您登出帳號或是關閉數據機，避免他人盜用您的帳號或入侵您的電腦。

8. 使用難猜的密碼，並妥善保存

請不要將密碼寫在小紙條後，貼在您的電腦上。不要設定太好猜的密碼；建議混合字母、數字和符號。請不要設定與您姓名相關的密碼;定期更換密碼的同時，也請不要把您的密碼給別人！

9. 電腦要設置防火牆

請務必安裝防火牆—這並不難。防火牆可協助阻擋駭客入侵您或您家人的電腦，竊取包括電話號碼與信用卡號碼在內的個人資訊。

10. 不要和陌生人共享電腦存取途徑，並請了解檔案分享的風險

您的電腦作業系統可能允許其他在同一網路(包括網際網路)的電腦存取您硬碟裡的檔案以「共享」。這種共享行為可以用來散播電腦病毒或是讓他人有機會偷窺您電腦的檔案。請檢視您的作業系統及其他應用程式，學習如何停止共享檔案。千萬不要跟陌生人共享您的電腦存取途徑！

若對於此份文件或是本中心有任何疑問或建議，歡迎您不吝指教，並可以下列任一方式連絡本中心。

- 官方網站 ： https://www.twcert.org.tw/
- 連絡電話 ： 02-23776418 (台北辦公室)
  03-4115579 (桃園辦公室)
- 一般連絡 ： twcert@cert.org.tw
- 漏洞通報 ： cve@cert.org.tw
- 事件通報 ： http://surl.twcert.org.tw/mvPLG