資安法規面面觀

◎ 劉建良

壹、前言

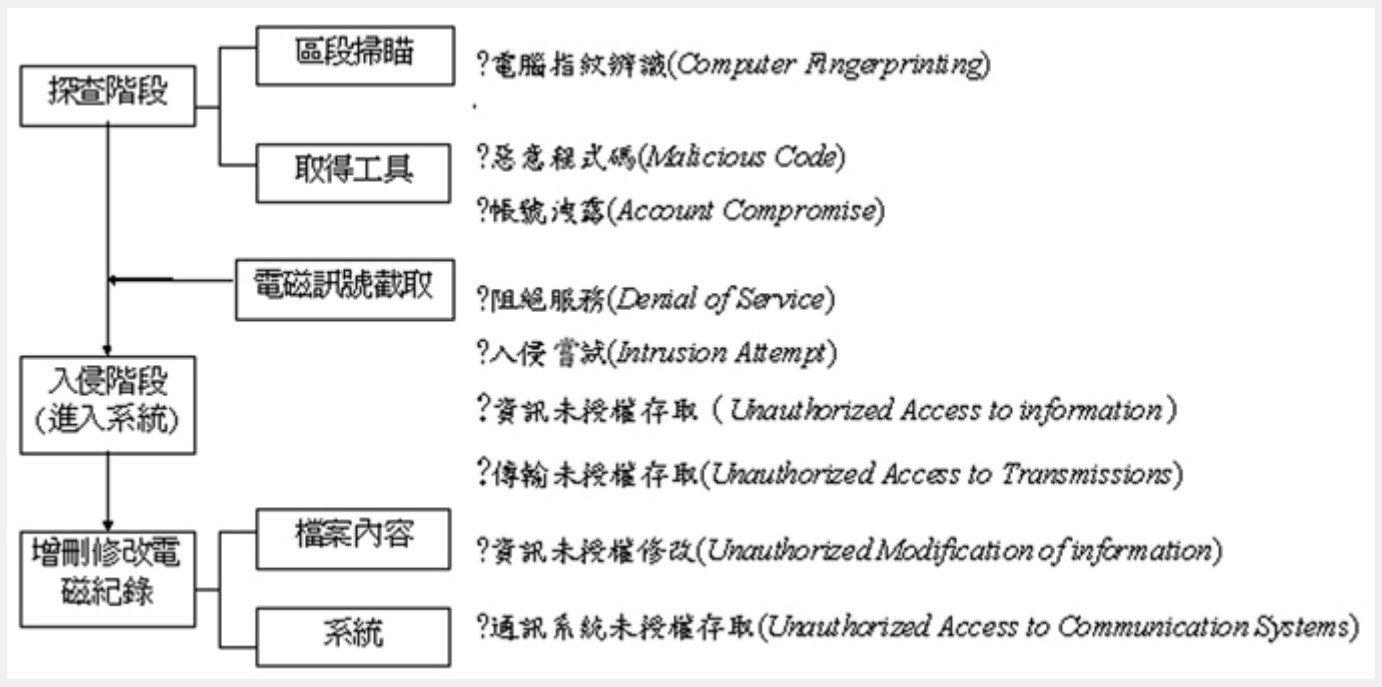
爲掌握全球資安法制的發展情形，特別探究歐盟與美國資通安全相關防護公約與典章，包含歐盟對會員國所提出之「電腦與網路濫用法制建議手冊」、全球第一部針對網路行爲規範而制訂的「網路犯罪公約」，及美國「聯邦資通安全管理法」，以了解資訊安全維護工作可能涉及的法制議題。同時依照國際法制發展趨勢，檢視我國目前資通安全法制的發展狀況。

貳、歐盟資安法制建議手冊

爲協助各會員國之電腦災害應變小組於運作過程中符合資安相關的法制依據，並遵循歐盟諸多的法制規範，歐盟於 2002 年提出「電腦與網路濫用法制建議手冊」(Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries，以下簡稱「建議手冊」)供會員國參考，以期建立符合歐盟法制之要求。

該建議手冊開宗明義地指出，災害應變的第一步，在對事件建立一致性的描述與定義，以避免定義不清導致認知上的錯誤。此定義應包括技術與法律上的定義；前者可以電腦技術指令等細節性加以描述，但法律上的定義則必須儘量抽象化，以涵蓋最大多數人的認知，並保留後續發展之彈性空間。

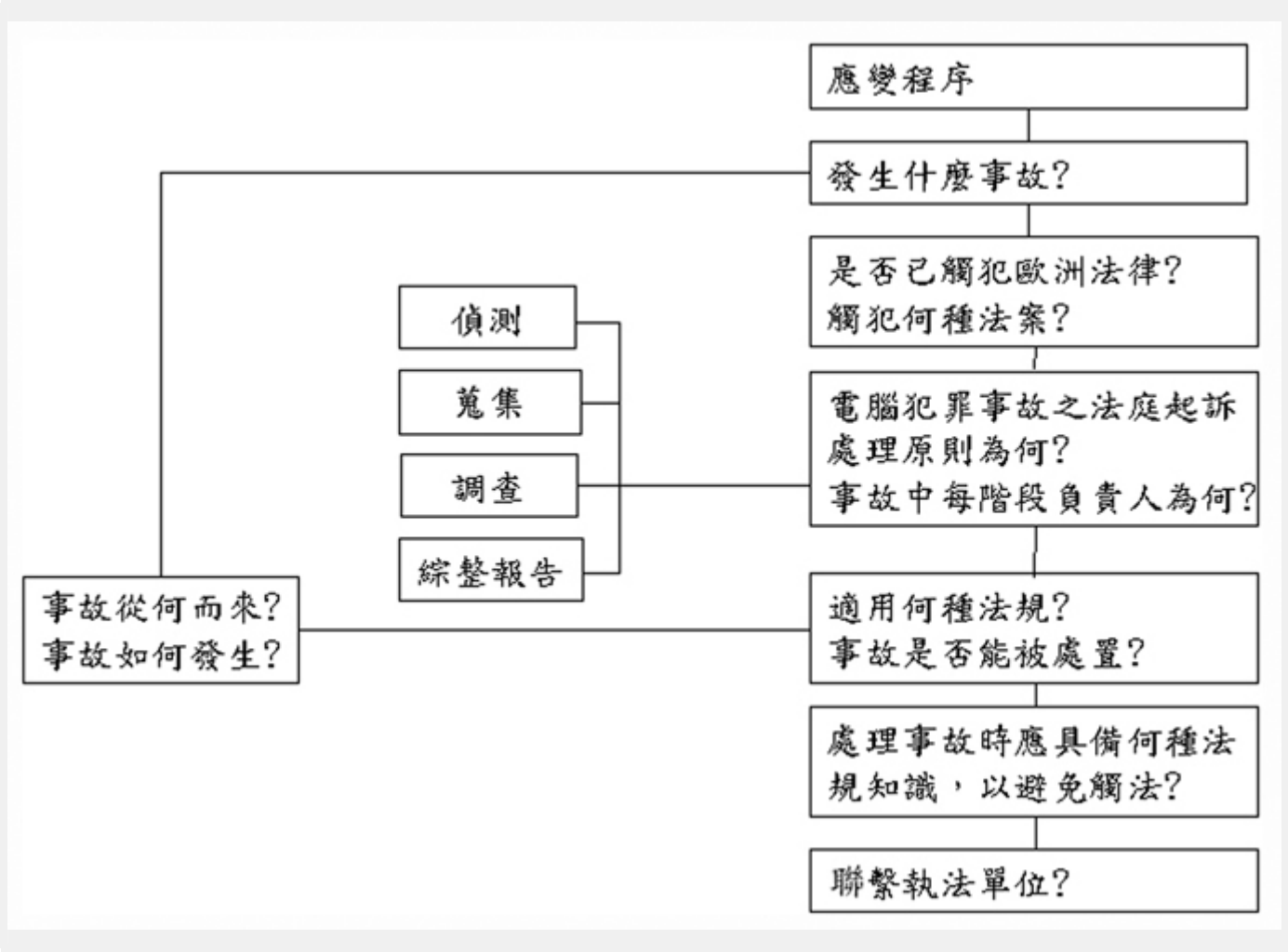
依據電腦入侵與資安事件之手法，該建議手冊定義之行爲包括：電腦指紋辨識、惡意程式碼、帳號洩露、阻絕服務、入侵嘗試、資訊未授權存取、傳輸未授權存取、資訊未授權修改及通訊系統未授權存取等。若以駭客入侵三階段行爲（探查、入侵及增刪修改電磁紀錄）論之，其相關行爲分類如圖 1 所示。



資料來源：行政院研考會「我國資安法制環境整備度研究」

圖 1 歐盟資安法制建議手冊「行爲分類」

建議手冊除定義災害應變與駭客入侵行爲模式外，並提供資安檢視流程圖(如圖 2)協助會員國偵防與鑑識資安事件，且提供網路犯罪公約之內涵，建議會員國可對照此內容訂定刑法、民法、通訊保障及監察法或行政法上的管理措施。



資料來源：Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries, 2002

圖 2 「電腦與網路濫用法制建議手冊」資安檢視流程圖

參、網路犯罪公約

網路犯罪公約是全球第一部針對網路行爲規範之國際條約，2001 年 11 月 23 日由歐洲理事會 26 個會員國與 4 個非會員國(美國、加拿大、日本及南非)於布達佩斯正式簽署通過，並於 2004 年 7 月 1 日正式生效；至 2008 年 2 月 1 日共計 43 個國家簽署，同意據以修改相關之國內法規。公約的三個主旨包括：一、提供簽約國實質法律修正的方向與依據；二、提供執法機構調查與處理犯罪行爲之程序規定與依據；三、建立快速有效的國際合作關係。

網路犯罪公約內涵所稱之犯罪，並不侷限於狹義刑法犯罪之概念，乃是定義於網路世界中所包含之網路通訊竊聽、機密資料竊取、垃圾郵件散布、個人識別資料冒用等廣義之犯罪行爲。我國雖非簽署國，但爲避免我國法制成爲犯罪者的避風港，仍應積極參照該公約修定之相關法律規範，以期達成資安法治與國際接軌。

肆、美國聯邦資訊安全管理法

美國爲有效管理及監督政府內部資訊效能與風險，布希總統於 2002 年 12 月簽署「電子化政府法案」，並通過聯邦資訊安全管理法（FISMA）後，美國政府便開始建立聯邦層級機構的資安機制。

在聯邦資訊安全管理法的要求下，每個聯邦機構必須建立一個以風險評估爲基礎的資訊安全維護計畫，計畫內容須涉及風險評估與外包商管理二項重要工作之執行，而風險評估內容必須包含技術風險、管理風險及法律風險等層面之評估；外包商管理則須訂定明確之外包商管理程序與方法。

國家標準與技術局負責制定統一性的標準與指引，並對聯邦政府機關所處理與保管的資訊進行分類，標示其資訊安全等級，同時提供資訊與資訊系統相關之安全指引。目前美國國家標準與技術局制定的資通安全準則（NIST SP 800）系列文件已廣泛應用於聯邦政府所有的資訊系統。預算管理局負責相關規範之推廣與督導，並經由年度稽核檢討作業，逐步檢視機關完成資訊與資訊系統分類、安全基準的評估、安全機制之建置及資訊系統之認證授權等工作。

伍、我國法制檢視

我國政府爲建立安全與可信賴的網路環境，確保電子化政府與電子商務之行爲模式能蓬勃發展，於是全面檢視現行法治環境，藉由新增或修訂法規之方式，健全我國網路發展環境。法務部乃著手研議網路犯罪條例，在現有之刑法中新增第 36 章電腦犯罪條文，並於民國 92 年頒布刑法修正案；同時陸續頒布電子簽章法與政府資訊公開法、修訂電腦處理個人資料保護法、研議新增濫發商業電子郵件管理條例等相關法案之推動。

綜整我國資通安全相關之法律規範，可劃分爲網路犯罪、身分認證、通訊保障、資料保護、資訊公開與機密維護，及資安治理 6 類；其所涉及之法律規範則包含刑法、電子簽章法、電信法、通訊保障及監察法等 20 項，詳如表 1。

類別	法律及規範
網路犯罪	刑法第36章妨害電腦使用罪
身分認證	電子簽章法 電子簽章法施行細則 憑證實務作業基準應載明事項準則 外國憑證機構許可辦法
通訊保障	電信法 通訊保障及監察法 通訊保障及監察法施行細則
資料保護	電腦處理個人資料保護法 電腦處理個人資料保護法施行細則 執行電腦處理個人資料保護事項協調連繫辦法 濫發商業電子郵件管理條例草案
資訊公開與機密維護	國家機密保護法 國家機密保護法施行細則 檔案法 檔案法施行細則 機密檔案管理辦法 檔案電子儲存管理實施辦法 政府資訊公開法
資安治理	行政院及所屬各機關資訊安全管理要點 行政院及所屬各機關資訊安全管理規範

表 1 我國資通安全相關之法律與規範 資料來源：作者自行整理

陸、結語

行政院國家資通安全會報自民國 90 年執行「建立我國通資訊基礎建設安全機制計畫」，積極推動政府機關落實執行資通安全相關工作，主要政策包含政府機關資訊安全長責任制度、資通安全責任等級分級作業，及機密資訊保護等，對強化政府機關之資通安全能力產生一定的影響。然而，我國尚未發展一套資通安全專屬之法典，未能以資安防護之立場訂定單一全國規範，政府機關於編列預算時亦不易有統合性之資安發展與建設等相關預算，值得深思。

此外，我國雖非 G8 之會員國，卻順利於民國 92 年 10 月以「TAIWAN」名義加入 G8 國際網路犯罪聯防組織「24/7 Computer Crime Network」，成爲第 35 個會員，協助會員間建立 24 小時打擊犯罪網，增加在執法調查層面的國際互助。此工作對於因未具備廣泛邦交國而導致跨國性之網路犯罪偵辦困難的我國而言，實屬一大突破。

參考文獻

1. •歐盟電腦與網路濫用法制建議手冊(Handbook of Legislative Procedures of Computer and Network Misuse in EU Countries)
2. Convention on Cybercrime, Budapest, 23.XI.2001
3. Sec. 1.6(a), Sec 1.6(b) of Executive Order No. 12958(1995).
4. Sec. 1.6(d) of Executive Order No. 12958(1995).
5. •See, e.g., Fred H. Cate, Another Notice Isn't Answer, USA Today, Feb. 27, 2005, at 14A; see also Editorial, Have You Been Stolen?, Wash. Post, June 30, 2005, at A22.
6. •GAO, Information Security—Emerging Cybersecurity Issues Threaten Federal Information System, p.29. GAO-05-231, 2005/05/13
7. •John Moteff, Computer Security : A Summary of Selected Federal Laws, Executive orders, and Presidential Directives, CRS Report for Congress, p.2. 2004/4/16.
8. 參照 FISMA SEC.301
9. 參見 The National Strategy to Secure Cyberspace, Pp.24-25, 2003/02
10. • •GAO, Critical Infrastructure Protection—Improving Information Sharing with Infrastructure Sectors, GAO-04-780, p. 7. 2004/07/09
11. •GAO, Critical Infrastructure Protection—Establishing Effective Information Sharing with Infrastructure Sectors, GAO-04-699T, p17. 2004/4/21
12. 行政院科技顧問組 97 年 3 月「2008 資通安全政策白皮書」
13. 行政院研考會 97 年 3 月「我國資安法制環境整備度研究」
14. •行政院研考會 95 年 9 月「資安事件通報應變作業規範(草案)」

（作者任職於國家資通安全會報技術服務中心）